aws

Guía del usuario

Amazon Relational Database Service



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Relational Database Service: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon RDS? 1
Ventajas de Amazon RDS 1
Comparación de responsabilidades 2
Modelo de responsabilidad compartida de Amazon RDS 4
Instancias de base de datos 4
Ejemplo de arquitectura de aplicaciones con Amazon RDS 5
Motores de base de datos 7
Clases de instancia de base de datos 8
Almacenamiento de instancias de base de datos 9
Instancias de base de datos en Amazon Virtual Private Cloud (Amazon VPC) 10
Regiones de AWS y zonas de disponibilidad 10
Zonas de disponibilidad 11
Implementaciones Multi-AZ 11
Control de acceso con grupos de seguridad 13
Supervisión de Amazon RDS 14
Interfaces de usuario para Amazon RDS 16
AWS Management Console 16
La interfaz de línea de comandos 17
API de Amazon RDS 17
Cómo se le cobra Amazon RDS 17
capa gratuita de AWS en Amazon RDS 17
Siguientes pasos 18
Introducción 19
Temas específicos de los motores de bases de datos 19
Instancias de base de datos 20
Clases de instancia de base de datos 23
Tipos de clase de instancia de base de datos 23
Motores de bases de datos compatibles 33
Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS 103
Cambio de clase de instancia de base de datos 109
Configuración del procesador para RDS para Oracle 109
Especificaciones de hardware 134
Almacenamiento de instancias de base de datos 182

Tipos de almacenamiento ... 182
Almacenamiento de IOPS aprovisionadas ... 184
Almacenamiento de uso general ... 189
Comparación de tipos de almacenamiento SSD ... 193
Almacenamiento magnético (heredado, no recomendado) ... 198
Volumen de registro específico (DLV) ... 198
Monitoreo del desempeño de almacenamiento ... 200
Factores que afectan al rendimiento del almacenamiento ... 201
Regiones, zonas de disponibilidad y zonas locales ... 204
AWSRegiones de ... 205
Zonas de disponibilidad ... 210
Zonas locales ... 211
Funciones admitidas de Amazon RDS por región y motor ... 213
Convenciones de tabla ... 214
Referencia rápida de características ... 214
Implementaciones azul/verde ... 217
Copias de seguridad automatizadas entre regiones ... 218
Réplicas de lectura entre regiones ... 220
Secuencias de actividades de la base de datos ... 223
Modo de pila doble ... 231
Exportación de instantáneas a S3 ... 254
Autenticación de bases de datos de IAM ... 269
Autenticación de Kerberos ... 275
Clústeres de base de datos Multi-AZ ... 289
Información de rendimiento ... 299
RDS personalizado ... 300
Amazon RDS Proxy ... 314
Integración de Secrets Manager ... 333
Integraciones sin ETL ... 334
Características nativas del motor ... 340
Facturación de instancias de base de datos para Amazon RDS ... 341
Instancias de base de datos bajo demanda ... 343
Instancias de base de datos reservadas ... 345
Configuración ... 360
Cómo crear una Cuenta de AWS ... 360
Creación de un usuario con acceso administrativo ... 361

Conceder acceso programático ... 362
Determinar las necesidades ... 364
Proporcionar acceso a la instancia de base de datos ... 367
Introducción ... 370
Creación y conexión a una instancia de base de datos de MariaDB ... 371
Requisitos previos ... 372
Crear una instancia de EC2 ... 373
Creación de una instancia de base de datos de MariaDB ... 379
(Opcional) Crear una VPC, una instancia EC2 y una instancia MariaDB mediante AWS CloudFormation ... 385
Conectarse a una instancia de base de datos MariaDB ... 387
Eliminación de la instancia de EC2 y la instancia de base de datos ... 391
(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation ... 392
(Opcional) Conecte la instancia de base de datos a una función de Lambda ... 393
Creación de una instancia de base de datos de Microsoft SQL Server y conexión a ella ... 394
Requisitos previos ... 396
Crear una instancia de EC2 ... 396
Creación de una instancia de base de datos de SQL Server ... 401
(Opcional) Crear una VPC, una instancia EC2 y una instancia de SQL Server mediante AWS CloudFormation ... 407
Conexión a una instancia de base de datos de SQL Server ... 409
Examen de la instancia de base de datos de ejemplo ... 413
Eliminación de la instancia de EC2 y la instancia de base de datos ... 414
(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation ... 415
(Opcional) Conecte la instancia de base de datos a una función de Lambda ... 416
Creación de una instancia de base de datos MySQL y conexión a ella ... 417
Requisitos previos ... 418
Crear una instancia de EC2 ... 419
Creación de una instancia de base de datos de MySQL ... 425
(Opcional) Crear una VPC, una instancia EC2 y una instancia MySQL mediante AWS CloudFormation ... 431
Conectarse a una instancia de base de datos MySQL ... 433
Eliminación de la instancia de EC2 y la instancia de base de datos ... 437

(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation ... 438
(Opcional) Conecte la instancia de base de datos a una función de Lambda ... 439
Creación y conexión a una instancia de base de datos de Oracle ... 440
Requisitos previos ... 441
Paso 1: crear una instancia de EC2 ... 442
Paso 2: crear una instancia de base de datos de Oracle ... 448
(Opcional) Crear una VPC, una instancia EC2 y una instancia de base de datos de Oracle mediante AWS CloudFormation ... 454
Paso 3: conectar el cliente de SQL a una instancia de base de datos de Oracle ... 456
Paso 4: eliminar la instancia de EC2 y la instancia de base de datos ... 460
(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation ... 461
(Opcional) Conecte la instancia de base de datos a una función de Lambda ... 461
Creación de una instancia de base de datos de PostgreSQL y conexión a ella ... 462
Requisitos previos ... 463
Crear una instancia de EC2 ... 464
Creación de una instancia de base de datos de PostgreSQL ... 470
(Opcional) Crear una VPC, una instancia EC2 y una instancia PostgreSQL mediante AWS CloudFormation ... 476
Conexión a la instancia de base de datos PostgreSQL ... 478
Eliminación de la instancia de EC2 y la instancia de base de datos ... 482
(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation ... 483
(Opcional) Conecte la instancia de base de datos a una función de Lambda ... 484
Tutorial: creación de un servidor web y de una instancia de base de datos de Amazon RDS ... 485
Lanzamiento de una instancia EC2 para conectarse con la instancia de base de datos ... 487
Crear una instancia de base de datos ... 493
Instalación de un servidor web ... 514
Tutorial: Creación de una función de Lambda para obtener acceso a su instancia de base de datos de Amazon RDS ... 526
Requisitos previos ... 527
Creación de una instancia de base de datos de Amazon RDS ... 527
Creación de una función de Lambda y un proxy ... 529
Crear un rol de ejecución de función ... 530
Creación del paquete de despliegue de Lambda ... 531

Actualización de la función de Lambda 534
Prueba de la función de Lambda en la consola 535
Cree una cola de Amazon SQS. 537
Creación de una asignación de orígenes de eventos para invocar la función de Lambda 537
Prueba y supervisión de la configuración 538
Limpiar los recursos de 539
Tutoriales y código de muestra 541
Tutoriales en esta guía 541
Tutoriales en otras AWS guías 542
Portal de contenido de laboratorios y talleres de AWS para Amazon RDS PostgreSQL 543
Portal de contenido de laboratorios y talleres de AWS para Amazon RDS MySQL 544
Tutoriales y código de muestra en GitHub 544
Cómo utilizar los AWS SDK 544
Prácticas recomendadas para Amazon RDS 546
Directrices operativas básicas de Amazon RDS 546
Recomendaciones de RAM de las instancias de base de datos 548
Mantenimiento de versiones actualizadas del motor de base de datos 548
Controladores de bases de datos de AWS 549
Uso de la monitorización mejorada 549
Uso de las métricas 549
Visualización de métricas de rendimiento 550
Evaluación de las métricas de rendimiento 553
Ajuste de consultas 555
Prácticas recomendadas para trabajar con MySQL 556
Tamaño de las tablas 556
Número de tablas 557
Motor de almacenamiento 558
Prácticas recomendadas para trabajar con MariaDB 559
Tamaño de las tablas 559
Número de tablas 560
Motor de almacenamiento 560
Prácticas recomendadas para trabajar con Oracle 561
Prácticas recomendadas para trabajar con PostgreSQL 561
Carga de datos en una instancia de base de datos de PostgreSQL 561
Trabajo con la característica autovacuum de PostgreSQL 562
Video de prácticas recomendadas de Amazon RDS for PostgreSQL 564

Prácticas recomendadas para trabajar con SQL Server ... 564
Video de prácticas recomendadas de Amazon RDS for SQL Server ... 565
Trabajo con los grupos de parámetros de base de datos ... 565
Automatización de la creación de instancias de base de datos ... 566
Vídeo de nuevas características ... 567
Acceso mediante programación a Amazon RDS ... 568
Console-to-Code ... 569
Configuración de una instancia de base de datos ... 570
Creación de una instancia de base de datos ... 571
Requisitos previos ... 571
Creación de una instancia de base de datos ... 579
Opciones disponibles ... 586
Creación de recursos con AWS CloudFormation ... 631
RDS y plantillas de AWS CloudFormation ... 631
Más información sobre AWS CloudFormation ... 631
Conexión a una instancia de base de datos ... 632
Busque la información de conexión: ... 632
Situaciones para el acceso a una instancia de base de datos ... 636
Conexión a instancias de base de datos con los controladores de AWS ... 637
Conexión a una instancia de base de datos que ejecuta un motor de base de datos específico ... 639
Administración de conexiones con RDS Proxy ... 639
Opciones de autenticación de bases de datos ... 639
Conexiones cifradas ... 640
Working with option groups (Trabajar con grupos de opciones) ... 641
Información general sobre grupos de opciones ... 641
Creación de un grupo de opciones ... 644
Copia de un grupo de opciones ... 646
Agregar una opción a un grupo de opciones ... 647
Descripción de opciones y configuración de opciones para un grupo de opciones ... 654
Modificación de una configuración de opciones ... 655
Quitar una opción de un grupo de opciones ... 659
Eliminación de un grupo de opciones ... 661
Grupos de parámetros ... 665
Descripción general de los grupos de parámetros ... 665
Grupos de parámetros de base de datos ... 670

Grupos de parámetros de clúster de bases de datos 688
Comparación de grupos de parámetros de la base de datos 702
Especificación de parámetros de base de datos 703
Creación de una caché de ElastiCache desde Amazon RDS 711
Información general sobre la creación de cachés de ElastiCache con ajustes de la instancia de base de datos de RDS 711
Creación de una caché de ElastiCache con ajustes de una instancia de base de datos de RDS 713
Migración automática de bases de datos de EC2 716
Descripción general 716
Requisitos previos 717
Limitaciones 719
Creación de recursos de IAM 719
Configuración de la migración de datos 727
Administración de migraciones 729
Monitorización 731
Tutorial: Creación de una instancia de base de datos de MySQL con un grupo de parámetros personalizados y un grupo de opciones nuevas 733
Requisitos previos 734
Creación de un grupo de parámetros personalizados 734
Modificación de los valores de parámetro 735
Creación de un grupo de opciones 736
Cómo agregar una opción 736
Creación de la instancia de base de datos de la base de datos 737
Administración de una instancia de base de datos 739
Parar una instancia de base de datos 740
Casos de uso 741
Motores de base de datos, clases y regiones compatibles 741
Compatibilidad para Multi-AZ 742
Funcionamiento 742
Limitaciones 744
Grupos de parámetros y opciones 744
Direcciones IP públicas 745
Parar una instancia de base de datos 745
Comienzo de una instancia de base de datos 747
Reinicio de una instancia de base de datos 749

Casos de uso para el reinicio de una instancia de base de datos ... 749
Cómo funciona el reinicio ... 750
Reinicio en multi-AZ ... 750
Consideraciones ... 751
Requisitos previos ... 752
Reinicio de una instancia de base de datos : pasos básicos ... 752
Conexión a una instancia de EC2 ... 754
Información general ... 755
Conexión a una instancia de EC2 ... 760
Visualización de los recursos de computación conectados ... 763
Conexión a una instancia de base de datos que ejecuta un motor de base de datos específico ... 764
Conexión de una función de Lambda ... 765
Descripción general ... 767
Conexión de una función de Lambda ... 778
Visualización de los recursos de computación conectados ... 780
Modificación de una instancia de base de datos ... 782
Programación de modificaciones ... 784
Opciones disponibles ... 785
Mantenimiento de una instancia de base de datos ... 834
Descripción general de las actualizaciones de mantenimiento de instancias de base de datos DB ... 834
Vista de mantenimiento pendiente ... 836
Aplicación de actualizaciones ... 839
Mantenimiento de implementaciones Multi-AZ ... 842
La ventana de mantenimiento de ... 843
Ajuste de la ventana de mantenimiento para una instancia de base de datos ... 846
Actualizaciones del sistema operativo ... 848
Actualización de la versión del motor ... 852
Actualización manual de la versión del motor ... 853
Actualización automática de la versión secundaria del motor ... 855
Cambio del nombre de una instancia de base de datos ... 861
Cambio de nombre para sustituir una instancia de base de datos existente ... 862
Trabajo con réplicas de lectura de instancias de base de datos ... 865
Descripción general ... 867
Diferencias entre motores de base de datos ... 871

Creación de una réplica de lectura ... 875
Promoción de una réplica de lectura ... 879
Monitoreo de la replicación de lectura ... 885
Réplicas de lectura entre regiones ... 888
Etiquetado de los recursos de RDS ... 903
¿Por qué usar etiquetas de RDS? ... 904
Funcionamiento de las etiquetas de RDS ... 905
Prácticas recomendadas ... 908
Copia de etiquetas a instantáneas de base de datos ... 909
Añadido y eliminación de etiquetas en Amazon RDS ... 910
Tutorial: especificar qué instancias de base de datos se deben detener mediante etiquetas ... 915
ARN en Amazon RDS ... 919
Creación de un nombre ARN ... 919
Obtención de un ARN existente ... 927
Uso de almacenamiento ... 930
Aumento de la capacidad de almacenamiento de la instancia de base de datos ... 930
Administración automática de la capacidad con el escalado automático de almacenamiento de ... 933
Actualización del sistema de archivos de almacenamiento ... 943
Modificación de la configuración de las IOPS aprovisionadas ... 945
Modificaciones en el almacenamiento con uso intensivo de E/S ... 947
Modificación de la configuración de uso general (gp3) ... 949
Uso de un volumen de registro específico (DLV) ... 951
Eliminación de una instancia de base de datos ... 959
Requisitos previos para eliminar una instancia de base de datos ... 959
Consideraciones a la hora de eliminar una instancia de base de datos ... 959
Eliminación de una instancia de base de datos ... 961
Tutorial: Administración de una instancia de base de datos de MySQL ... 965
Introducción ... 965
Requisitos previos ... 966
Adición de etiquetas a la instancia de base de datos ... 966
aumentar el almacenamiento ... 966
crea réplicas de lectura ... 967
Actualización de etiquetas ... 968
Configuración y administración de una implementación multi-AZ ... 972

Implementaciones de instancias de base de datos Multi-AZ 974
Conversión de una instancia de base de datos en una implementación multi-AZ. 976
Conmutación por error de una instancia de base de datos multi-AZ 978
Implementaciones de clústeres de base de datos Multi-AZ 985
Disponibilidad de clase de instancia para los clústeres de base de datos multi-AZ 986
Arquitectura de clúster de base de datos multi-AZ 987
Grupos de parámetros para clústeres de base de datos multi-AZ 989
RDS Proxy con clústeres de bases de datos multi-AZ 989
Retraso de réplica y clústeres de base de datos Multi-AZ 989
Instantáneas de clúster de base de datos multi-AZ 993
Creación de un clúster de base de datos Multi-AZ 994
Conexión a un clúster de base de datos Multi-AZ 1028
Conexión de un recurso de computación de AWS y un clúster de base de datos Multi-AZ . 1035
Modificación de un clúster de base de datos Multi-AZ 1063
Actualización de un clúster de base de datos multi-AZ 1087
Cambio de nombre de un clúster de base de datos Multi-AZ 1090
Reinicio de un clúster de base de datos Multi-AZ 1093
Conmutación por error de un clúster de base de datos multi-AZ 1095
Replicación lógica de PostgreSQL con clústeres de base de datos multi-AZ 1099
Trabajo con réplicas de lectura de clústeres de base de datos Multi-AZ 1104
Configuración de la replicación externa a partir de los clústeres de base de datos multi-AZ 1117
Eliminación de un clúster de base de datos Multi-AZ 1119
Limitaciones de los clústeres de base de datos multi-AZ 1122
Soporte extendido de RDS 1124
Información general del Soporte extendido de RDS 1125
Precios del Soporte extendido de RDS 1126
Prevención de cargos del Soporte extendido de RDS 1127
Versiones con el Soporte extendido de RDS 1127
Nombre de versiones con el Soporte extendido de RDS 1127
Responsabilidades con el Soporte extendido de RDS 1129
Responsabilidades de Amazon RDS 1129
Sus responsabilidades 1129
Creación de una instancia de base de datos o un clúster de base de datos multi-AZ 1130
Comportamiento del Soporte extendido de RDS 1131
Observaciones sobre el Soporte extendido de RDS 1131

Creación de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de RDS ... 1132
Visualización de la inscripción en el Soporte extendido de RDS ... 1133
Visualización de las fechas de soporte ... 1136
Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ ... 1139
Comportamiento del Soporte extendido de RDS ... 1140
Observaciones sobre el Soporte extendido de RDS ... 1140
Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de RDS ... 1141
Uso de las implementaciones azul/verde para actualizar las bases de datos ... 1144
Descripción general de las implementaciones azul/verde de Amazon RDS ... 1145
Disponibilidad en regiones y versiones ... 1146
Ventajas ... 1146
Flujo de trabajo ... 1147
Permitir el acceso ... 1151
Limitaciones y consideraciones ... 1152
Prácticas recomendadas ... 1160
Creación de una implementación azul/verde ... 1165
Preparación para una implementación azul/verde ... 1166
Especificación de cambios ... 1168
Carga diferida e inicialización de almacenamiento ... 1171
Creación de una implementación azul/verde ... 1173
Opciones disponibles ... 1176
Visualización de una implementación azul/verde ... 1182
Cambio de una implementación azul/verde ... 1186
Tiempo de espera de la conmutación ... 1187
Barreras de protección de la conmutación ... 1187
Acciones de conmutación ... 1188
Prácticas recomendadas para realizar la conmutación ... 1189
Verificación de las métricas de CloudWatch antes de la conmutación ... 1191
Monitoreo del retardo de réplica antes de la transición ... 1191
Conmutación de una implementación azul/verde ... 1192
Después de la conmutación ... 1195
Eliminación de una implementación azul/verde ... 1197
Copia de seguridad, restauración y exportación de datos ... 1201
Introducción a las copias de seguridad ... 1202

Almacenamiento de copia de seguridad 1203
Administración de las copias de seguridad automatizadas 1204
Intervalo de copia de seguridad 1204
Backup retention period (Periodo de retención de copia de seguridad) 1207
Habilitar las copias de seguridad automatizadas 1208
Retener copias de seguridad automatizadas 1211
Eliminación de las copias de seguridad automatizadas retenidas 1213
Motores de almacenamiento MySQL no compatibles 1217
Motores de almacenamiento MariaDB no compatibles 1218
Copias de seguridad automatizadas entre regiones 1220
Administración de copias de seguridad manuales 1238
Creación de una instantánea de base de datos para una instancia de base de datos single-AZ 1239
Creación de una instantánea de un clúster de base de datos Multi-AZ 1242
Eliminación de una instantánea de base de datos 1244
Restauración a una instancia de base de datos 1247
Restauración a partir de una instantánea 1248
Consideraciones 1250
Recuperación a un momento dado 1255
Restauración de un clúster de base de datos Multi-AZ a un momento indicado 1261
Restauración de una instantánea de clúster de base de datos Multi-AZ 1265
Restauración desde una instantánea de clúster de base de datos Multi-AZ a una instancia de base de datos 1268
Tutorial: restauración de una instancia de base de datos a partir de una instantánea de base de datos 1271
Copia de una instantánea de base de datos 1276
Copia de una instantánea de base de datos 1276
Limitaciones 1287
Consideraciones 1288
Compartir una instantánea de base de datos 1298
Uso compartido de una instantánea 1300
Uso compartido de instantáneas públicas 1304
Cómo compartir instantáneas cifradas 1306
Cancelación del uso compartido de instantáneas 1310
Exportación de datos de instantáneas de bases de datos a Amazon S3 1312
Información general acerca de la exportación de datos de instantáneas 1313

Configuración del acceso a un bucket de S3 ... 1314
Exportación de una instantánea de base de datos ... 1320
Disponibilidad en regiones y versiones ... 1324
Limitaciones ... 1324
Monitoreo de las exportaciones de instantáneas ... 1325
Cancelación de una exportación de instantáneas ... 1328
Mensajes de error ... 1329
Solución de problemas de errores de permisos de PostgreSQL ... 1331
Convenciones de nomenclatura de archivos ... 1331
Conversión de datos ... 1333
Uso AWS Backup ... 1343
Supervisión de métricas en una instancia de base de datos ... 1344
Plan de monitoreo ... 1344
Referencia de rendimiento ... 1345
Directrices de rendimiento ... 1345
Herramientas de monitoreo ... 1347
Herramientas de monitoreo automatizadas ... 1347
Herramientas de monitoreo manuales ... 1349
Visualización del estado de la instancia ... 1351
Visualización del estado de la instancia de base de datos de en un clúster de Aurora ... 1352
Recomendaciones para Amazon RDS ... 1360
Visualización de las recomendaciones ... 1362
Aplicación de recomendaciones ... 1370
Descarte de recomendaciones ... 1376
Modificación de recomendaciones descartadas a activas ... 1378
Referencia de recomendaciones ... 1379
Consulta de métricas en la consola de Amazon RDS ... 1410
Visualización del panel de Información de rendimiento ... 1411
Elección de la nueva vista de monitorización en la pestaña Monitorización ... 1412
Elección de la nueva vista de monitorización desde la página Información de rendimiento 1414
Creación de un panel personalizado ... 1416
Elección del panel preconfigurado ... 1419
Supervisión de RDS con CloudWatch ... 1421
Información general de Amazon RDS y Amazon CloudWatch ... 1422
Ver métricas de CloudWatch en ... 1424
Exportación de las métricas de Información sobre rendimiento a CloudWatch ... 1430

Creación de alarmas de CloudWatch ... 1436
Tutorial: Creating a CloudWatch alarm for DB cluster replica lag (Creación de una alarma de CloudWatch para el retraso de réplica de un clúster de bases de datos) ... 1437
Supervisión con Información sobre las bases de datos ... 1445
Precios ... 1445
Compatibilidad con motor, región y clase de instancia ... 1445
Activación del modo avanzado ... 1451
Activación del modo estándar ... 1455
Supervisión de consultas lentas ... 1461
Consideraciones ... 1463
Supervisión de carga de base de datos con Performance Insights ... 1465
Información general sobre Performance Insights ... 1466
Activación y desactivación de Información de rendimiento ... 1482
Performance Schema para MariaDB o MySQL ... 1488
Políticas de información sobre rendimiento ... 1493
Análisis de métricas mediante el panel de Información sobre rendimiento ... 1506
Visualización de las recomendaciones proactivas de Información de rendimiento ... 1558
Recuperación de métricas con la API de Información sobre rendimiento ... 1561
Registro de llamadas de Performance Insights mediante el uso de AWS CloudTrail ... 1587
Puntos de conexión de VPC (AWS PrivateLink) ... 1590
Análisis de rendimiento con DevOps Guru for RDS ... 1594
Beneficios de DevOps Guru para RDS ... 1594
Cómo funciona DevOps Guru for RDS ... 1596
Configuración de DevOps Guru for RDS ... 1597
Supervisión del sistema operativo con Supervisión mejorada ... 1606
Descripción general de la supervisión mejorada ... 1606
Configuración y habilitación del monitoreo mejorado ... 1608
Visualización de métricas OS en la consola de RDS ... 1614
Visualización de métricas del sistema operativo mediante CloudWatch Logs ... 1618
Referencia de métricas de RDS ... 1620
Métricas de CloudWatch para RDS ... 1620
Dimensiones de CloudWatch para RDS ... 1645
Métricas de Amazon CloudWatch para Información sobre rendimiento ... 1645
Métricas de contador para Información de rendimiento ... 1648
Estadísticas de SQL para Performance Insights ... 1685
Métricas del sistema operativo en Supervisión mejorada ... 1703

Supervisión de secuencias de actividades de la base de datos 1718
Visualización de los registros, los eventos y los flujos en la consola de Amazon RDS 1719
Supervisión de eventos de RDS 1723
Información general de los eventos para Amazon RDS 1723
Consulta de eventos de Amazon RDS 1725
Uso de notificaciones de eventos de Amazon RDS 1729
Creación de una regla que se desencadena en función de un evento Amazon RDS 1756
Categorías y mensajes de eventos de Amazon RDS 1762
Supervisión de registros de RDS 1817
Visualización y descripción de archivos de registro de base de datos 1817
Descarga de un archivo de registro de base de datos 1818
Ver un archivo de registro de base de datos 1820
Publicación en CloudWatch Logs 1822
Lectura del contenido del archivo de registro mediante REST 1825
archivos de registro de base de datos para Db2 1827
Archivos de registro de base de datos de MariaDB 1832
Archivos de registro de base de datos de Microsoft SQL Server 1848
Archivos de registro de base de datos de MySQL 1854
Archivos de registro de base de datos de Oracle 1872
Archivos de registro de base de datos de PostgreSQL 1883
Supervisión de llamadas a la API de RDS en CloudTrail 1898
Integración de CloudTrail con Amazon RDS 1898
Entradas de archivos de registro de Amazon RDS 1899
Supervisión de RDS con flujos de actividad de la base de datos 1904
Descripción general 1904
Configuración de la auditoría unificada de Oracle 1911
Configuración de la auditoría de SQL Server 1912
Inicio de una secuencia de actividades de la base de datos 1914
Modificación de una secuencia de actividades de la base de datos 1917
Obtención del estado del flujo de actividad 1920
Detención de un flujo de actividad de la base de datos 1921
Monitoreo de secuencias de actividades 1923
Ejemplos de políticas de IAM para flujos de actividad 1967
Supervisión de amenazas con GuardDuty RDS Protection 1970
Amazon RDS Custom 1972
Desafío de la personalización de la base de datos 1972

Modelo de administración y beneficios de RDS Custom 1974
Modelo de responsabilidad compartida en RDS Custom 1975
Configuraciones no compatibles y compatibilidad perimetral de RDS Custom 1977
Beneficios clave de RDS Custom 1977
Arquitectura de RDS Custom 1978
VPC 1979
Automatización y monitoreo personalizados de RDS 1980
Amazon S3 1985
AWS CloudTrail 1986
Seguridad de RDS Custom 1987
Cómo gestiona RDS Custom las tareas en su nombre de forma segura 1987
Certificados de SSL 1988
Protección del bucket de Amazon S3 frente al problema del suplente confuso 1988
Rotación de credenciales de RDS Custom para Oracle 1990
Trabajar con RDS Custom for Oracle 1995
Flujo de trabajo de RDS Custom for Oracle 1995
Arquitectura de base de datos de Amazon RDS Custom para Oracle 2001
Disponibilidad y compatibilidad de características con RDS Custom para Oracle 2003
Requisitos y limitaciones de Amazon RDS Custom para Oracle 2006
Configuración del entorno RDS Custom for Oracle 2010
Trabajar con CEV para RDS Custom for Oracle 2031
Configuración de una instancia de RDS Custom para Oracle 2064
Administración de una instancia de base de datos de RDS Custom for Oracle 2085
Administración de una implementación multi-AZ de RDS Custom para Oracle 2104
Trabajar con réplicas de RDS Custom para Oracle 2124
Copia de seguridad y restauración de una instancia de base de datos de RDS Custom for Oracle 2136
Trabajar con grupos de opciones en RDS Custom para Oracle 2147
Migración a RDS Custom para Oracle 2157
Actualización de una instancia de base de datos de RDS Custom para Oracle 2159
Solución de problemas de RDS Custom para Oracle 2173
Problemas conocidos de RDS Custom para Oracle 2198
Trabajar con RDS Custom for SQL Server 2202
Flujo de trabajo de RDS Custom for SQL Server 2202
Requisitos y limitaciones de Amazon RDS Custom for SQL Server 2205
Configuración del entorno de RDS Custom for SQL Server 2300

Bring Your Own Media con RDS Custom para SQL Server ... 2327
Uso de CEV para RDS Custom para SQL Server ... 2329
Creación y conexión a una instancia de base de datos de RDS Custom for SQL Server ... 2353
Administración de una instancia de base de datos de RDS Custom para SQL Server ... 2366
Uso de Microsoft Active Directory con RDS Custom para SQL Server ... 2382
Administración de una implementación multi-AZ de RDS Custom para SQL Server ... 2410
Copia de seguridad y restauración de una instancia de base de datos de RDS Custom for SQL Server ... 2427
Copia de una instantánea de base de datos de RDS Custom para SQL Server ... 2445
Migración de una base de datos en las instalaciones a RDS Custom for SQL Server ... 2457
Actualización de una instancia de base de datos de RDS Custom para SQL Server ... 2461
Solución de problemas de Amazon RDS Custom para SQL Server ... 2466
Amazon RDS en AWS Outposts ... 2508
Requisitos previos ... 2509
Compatibilidad para características de Amazon RDS ... 2510
Clases de instancia de base de datos compatibles ... 2518
Direcciones IP propiedad del cliente ... 2521
Uso de CoIP ... 2521
Limitaciones ... 2523
Implementaciones Multi-AZ ... 2525
Trabajo con el modelo de responsabilidad compartida ... 2525
Mejora de la disponibilidad ... 2526
Requisitos previos ... 2526
Trabajo con operaciones de la API para permisos de Amazon EC2 ... 2528
Creación de instancias de base de datos para RDS on Outposts ... 2529
Creación de réplicas de lectura para RDS en Outposts ... 2540
Consideraciones para restaurar instancias de base de datos ... 2544
Amazon RDS Proxy ... 2545
Disponibilidad en regiones y versiones ... 2546
Cuotas y limitaciones ... 2546
Limitaciones de RDS para MariaDB ... 2548
Limitaciones de RDS para SQL Server ... 2549
Limitaciones de MySQL ... 2550
Limitaciones de PostgreSQL ... 2551
Planificación del lugar de uso de RDS Proxy ... 2552
Conceptos y terminología de RDS Proxy ... 2553

Información general de los conceptos de RDS Proxy ... 2554
Grupo de conexiones ... 2556
Seguridad ... 2556
Conmutación por error ... 2558
Transacciones ... 2559
Introducción al proxy de RDS ... 2560
Configuración de una red proxy ... 2561
Configuración de credenciales de base de datos ... 2563
Configuración de políticas de IAM ... 2568
Creación de un proxy ... 2570
Visualización de un proxy ... 2580
Conexión a través de RDS Proxy ... 2582
Administración de un RDS Proxy ... 2586
Modificación de un RDS Proxy ... 2586
Agregar un usuario de base de datos ... 2593
Observaciones sobre la conexión de RDS Proxy ... 2594
Cómo evitar la fijación de RDS Proxy ... 2599
Eliminación de un RDS Proxy ... 2605
Trabajo con puntos de enlace del proxy de RDS ... 2606
Información general de los puntos de enlace de proxy ... 2607
Limitaciones para los puntos de conexión de proxy ... 2607
Puntos de conexión de proxy para clústeres de bases de datos de Multi-AZ ... 2608
Acceso a las bases de datos de RDS en todas las VPC ... 2610
Creación de un punto de enlace de proxy ... 2611
Visualización de puntos de enlace de proxy ... 2614
Modificación de un punto de enlace de proxy ... 2616
Eliminación de un punto de enlace de proxy ... 2617
Supervisión de RDS Proxy con CloudWatch ... 2619
Trabajo con eventos de RDS Proxy ... 2627
Eventos de RDS Proxy ... 2628
Solución de problemas de RDS Proxy ... 2631
Verificación de la conectividad para un proxy ... 2631
Problemas y soluciones comunes de ... 2633
Solución de problemas de RDS para MySQL ... 2635
Solución de problemas de RDS para PostgreSQL ... 2637
Uso del proxy de RDS con AWS CloudFormation ... 2642

Integraciones sin ETL ... 2644
Ventajas ... 2646
Conceptos clave ... 2646
Limitaciones ... 2647
Limitaciones generales ... 2647
Limitaciones de RDS for MySQL ... 2648
Limitaciones de Amazon Redshift ... 2649
Limitaciones de Amazon SageMaker Lakehouse ... 2649
Cuotas ... 2649
Regiones compatibles ... 2650
Introducción a las integraciones sin ETL ... 2650
Crear un grupo de parámetros de de base de datos personalizado ... 2650
Paso 2: seleccionar o crear una base de datos de origen ... 2651
Paso 3: Creación de un almacén de datos de destino en Amazon Redshift ... 2652
Siguientes pasos ... 2653
Creación de integraciones sin ETL con Amazon Redshift ... 2654
Requisitos previos ... 2654
Permisos necesarios ... 2654
Creación de integraciones sin ETL ... 2657
Cifrado de integraciones ... 2662
Pasos a seguir a continuación ... 2664
Creación de integraciones sin ETL con un Amazon SageMaker Lakehouse ... 2664
Requisitos previos ... 2664
Permisos necesarios ... 2664
Creación de integraciones sin ETL con un Amazon SageMaker Lakehouse ... 2667
Cifrado de integraciones ... 2672
Pasos a seguir a continuación ... 2674
Filtrado de datos para integraciones sin ETL ... 2675
Formato de un filtro de datos ... 2676
Lógica de filtros ... 2677
Prioridad del filtro ... 2678
Ejemplos ... 2678
Adición de filtros de datos ... 2679
Eliminación de filtros de datos ... 2682
Añadir y consultar datos ... 2682
Creación de bases de datos de destino en Amazon Redshift ... 2683

Añadir datos a la base de datos de origen ... 2683
Consulta de los datos de Amazon RDS en Amazon Redshift ... 2684
Diferencias de tipos de datos ... 2685
Visualización y supervisión de integraciones sin ETL ... 2689
Visualización de las integraciones ... 2690
Monitorización mediante tablas del sistema ... 2691
Monitoreo con EventBridge ... 2692
Modificación de integraciones sin ETL ... 2692
Eliminación de las integraciones sin ETL ... 2694
Solución de problemas de integración sin ETL ... 2695
No puedo crear una integración sin ETL ... 2696
Mi integración está atascada en un estado de `Syncing` ... 2696
Mis tablas no se replican en Amazon Redshift ... 2696
Una o más de mis tablas de Amazon Redshift requieren una resincronización ... 2697
Db2 en Amazon RDS ... 2701
Información general de Db2 ... 2702
Características de Db2 ... 2703
Versiones de Db2 ... 2706
Licencias de Db2 ... 2711
Clases de instancia de Db2 ... 2729
Roles predeterminados de Db2 ... 2732
Parámetros de Db2 ... 2732
Intercalación EBCDIC ... 2739
Zona horaria local de Db2 ... 2740
Requisitos previos para las instancias de base de datos ... 2743
Cuenta de administrador ... 2743
Consideraciones adicionales ... 2744
Múltiples bases de datos Db2 ... 2745
Conexión a la instancia de base de datos de Db2 ... 2747
Búsqueda del punto de conexión ... 2747
IBM Db2 CLP ... 2749
IBM CLPPlus ... 2754
DBeaver ... 2757
IBM Db2 Data Management Console ... 2761
Consideraciones relativas al grupo de seguridad ... 2771
Protección de las conexiones de Db2 ... 2772

Cifrado con SSL/TLS ... 2772
Uso de la autenticación de Kerberos ... 2779
Administración de la instancia de base de datos de RDS para Db2 ... 2795
Tareas del sistema ... 2797
Tareas de bases de datos ... 2810
Integración con S3 ... 2834
Creación de una política de IAM ... 2834
Creación de un rol de IAM y asociación de la política de IAM ... 2837
Agregue su rol de IAM a su instancia de base de datos ... 2839
Migración de datos a RDS para Db2 ... 2842
Migración de datos con servicios de AWS ... 2842
Migración de datos con herramientas nativas de Db2 ... 2854
Federación ... 2869
Federación homogénea ... 2869
Federación heterogénea ... 2874
Trabajo con las réplicas de Db2 ... 2879
Réplicas en espera ... 2879
Activaciones de base de datos ... 2879
Configuraciones de HADR ... 2880
Retención de registros de archivo ... 2880
Interrupciones durante la replicación de Db2 ... 2880
Requisitos y consideraciones sobre réplicas de Db2 ... 2881
Preparación para crear una réplica de Db2 ... 2883
Creación de una réplica de Db2 en espera ... 2884
Trabajo con copias de seguridad de réplicas de Db2 ... 2886
Solución de problemas de replicación de Db2 ... 2889
Opciones de instancias de base de datos de RDS para Db2 ... 2890
Registro de auditoría de Db2 ... 2891
Procedimientos almacenados externos ... 2907
Procedimientos almacenados externos basados en Java ... 2907
Problemas conocidos y limitaciones ... 2916
Limitación de autenticación ... 2916
Rutinas no restringidas ... 2916
Espacios de tablas de almacenamiento no automáticos durante la migración ... 2916
Establecimiento del parámetro db2_compatibility_vector ... 2917
Migración de bases de datos que contienen paquetes NO VÁLIDOS ... 2917

Procedimientos almacenados de RDS para Db2 ... 2919
Consideraciones sobre los procedimientos almacenados ... 2929
Concesión y revocación de privilegios ... 2930
Políticas de auditoría ... 2944
Grupos de búferes ... 2950
Administración de bases de datos ... 2956
Acceso al almacenamiento ... 2979
Espacios de tabla ... 2982
Funciones definidas por el usuario de RDS para Db2 ... 2994
rdsadmin.get_task_status ... 2994
rdsadmin.list_databases ... 2999
Solución de problemas ... 3001
Error de conexión a la base ... 3001
Error de E/S de archivos ... 3001
Errores en los procedimientos almacenados ... 3006
MariaDB en Amazon RDS ... 3017
Compatibilidad de características de MariaDB ... 3019
Versiones principales de MariaDB ... 3019
Motores de almacenamiento admitidos ... 3028
Calentamiento de caché ... 3030
Características no admitidas ... 3032
Versiones de MariaDB ... 3034
Versiones secundarias compatibles de MariaDB ... 3034
Versiones principales compatibles de MariaDB ... 3037
El entorno de vista previa de bases de datos ... 3038
MariaDB versión 11.4 en el entorno de vista previa de bases de datos ... 3042
Versiones obsoletas de MariaDB ... 3042
Conexión a una instancia de base de datos que ejecuta MariaDB ... 3043
Busque la información de conexión: ... 3044
Conexión desde el cliente de línea de comandos ... 3048
Conexión con los controladores de AWS ... 3048
Resolución de problemas ... 3050
Protección de las conexiones de MariaDB ... 3051
Seguridad de MariaDB ... 3051
Complementos de validación de contraseñas ... 3053
Cifrado con SSL/TLS ... 3054

Uso de nuevos certificados de SSL/TLS 3059
Mejora del rendimiento de las consultas con lecturas optimizadas de RDS 3064
Información general 3064
Casos de uso 3065
Prácticas recomendadas 3066
Utilización 3067
Supervisión 3067
Limitaciones 3068
Mejora del rendimiento de escritura con Escrituras optimizadas para RDS para MariaDB 3069
Descripción general 3069
Uso con una base de datos nueva 3071
Habilitación en una base de datos existente 3075
Limitaciones 3076
Actualizaciones del motor de base de datos de MariaDB 3077
Consideraciones 3078
Búsqueda de objetivos de actualización válidos 3079
Números de versión de MariaDB 3080
Números de versión de RDS 3083
Actualizaciones de la versión principal 3083
Actualización de una instancia de base de datos MariaDB 3084
Actualizaciones de versiones secundarias automáticas 3084
Actualización con tiempo de inactividad reducido 3088
Actualización de una versión del motor de instantáneas de base de datos de MariaDB 3093
Opciones de actualización para versiones de motor no compatibles 3095
Importación de datos en una instancia de base de datos de RDS para MariaDB 3097
Consideraciones sobre la importación de datos 3103
Importación de datos de una base de datos externa 3109
Importación de datos con un tiempo de inactividad reducido 3113
Importación de datos desde cualquier origen 3136
Replicación de MariaDB 3143
Réplicas de lectura de MariaDB 3144
Configuración de la replicación basada en GTID con una instancia de origen externa 3160
Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa 3164
Opciones para MariaDB 3171
Compatibilidad con el complemento de auditoría MariaDB 3171

Parámetros de MariaDB 3178
Visualización de los parámetros de MariaDB 3178
Parámetros de MySQL que no están disponibles 3180
Migración de datos desde una instantánea de base de datos de MySQL a una instancia de base de datos MariaDB 3183
Realización de la migración 3183
Incompatibilidades entre MariaDB y MySQL 3185
Referencia de MariaDB en Amazon RDS SQL 3187
mysql.rds_replica_status 3187
mysql.rds_set_external_master_gtid 3189
mysql.rds_kill_query_id 3192
Zona horaria local 3194
Problemas conocidos y limitaciones de MariaDB 3197
Límites de tamaño de archivo 3197
Palabra reservada InnoDB 3199
Puertos personalizados 3199
Performance Insights 3199
Microsoft SQL Server en Amazon RDS 3200
Tareas de administración comunes 3202
Limitaciones 3205
Compatibilidad con clases de instancia de base de datos 3208
Seguridad 3213
Programas de conformidad 3214
HIPAA 3214
Compatibilidad con SSL 3216
Compatibilidad con versiones 3216
Administración de versiones 3218
Parches y versiones del motor de base de datos 3219
Calendario de obsolescencia 3219
Compatibilidad de características 3220
Características de SQL Server 2022 3221
Características de SQL Server 2019 3221
Características de SQL Server 2017 3222
Características de SQL Server 2016 3223
Características de SQL Server 2014 3223
Fin del soporte de SQL Server 2012 en Amazon RDS 3223

Fin del soporte de SQL Server 2008 R2 en Amazon RDS 3224
Compatibilidad con CDC 3224
Características no compatibles y características con compatibilidad limitada 3225
Implementaciones Multi-AZ 3226
Uso de TDE 3227
Funciones y procedimientos almacenados 3227
Zona horaria local 3234
Zonas horarias admitidas 3235
Licencias de SQL Server en Amazon RDS 3248
Restauración de instancias de base de datos con licencia caducada 3248
Edición para desarrolladores de SQL Server 3249
Conexión a una instancia de base de datos que ejecuta SQL Server 3250
Antes de conectarse 3250
Búsqueda del punto de enlace de instancia de base de datos y el número de puerto 3251
Conexión a la instancia de base de datos con SSMS 3253
Conexión a la instancia de base de datos con SQL Workbench/J 3256
Consideraciones relativas al grupo de seguridad 3258
Solución de problemas 3259
Uso de Active Directory con RDS para SQL Server 3261
Uso de Active Directory autoadministrado con una instancia de base de datos de SQL Server 3262
Uso de AWS Managed Active Directory con RDS para SQL Server 3284
Actualización de aplicaciones para nuevos certificados SSL/TLS 3301
Determinación de si alguna aplicación se conecta a su instancia de base de datos de Microsoft SQL Server mediante SSL 3302
Determinación de si un cliente necesita una verificación de certificados para conectarse .. 3302
Actualización del almacén de confianza de su aplicación 3305
Actualizaciones del motor de base de datos de SQL Server 3306
Actualizaciones de la versión principal 3307
Consideraciones de actualización 3309
Comprobación de una actualización 3313
Actualización de una instancia de base de datos de SQL Server 3314
Actualización de instancias de base de datos obsoletas antes de finalizar el soporte técnico 3314
Importación y exportación de bases de datos de SQL Server 3316
Limitaciones y recomendaciones 3319

Configuración ... 3321
Uso de la copia de seguridad y la restauración nativas ... 3326
Compresión de archivos de copia de seguridad ... 3344
Solución de problemas ... 3345
Importación y exportación de datos de SQL Server por otros métodos ... 3349
Uso de BCP desde Linux ... 3363
Réplicas de lectura de SQL Server ... 3369
Configuración de réplicas de lectura para SQL Server ... 3369
Limitaciones de las réplicas de lectura con SQL Server ... 3370
Consideraciones relativas a opciones ... 3371
Sincronización de los usuarios y objetos de la base de datos ... 3373
Resolución de problemas ... 3375
Multi-AZ para RDS for SQL Server ... 3377
Adición de implementaciones Multi-AZ a una instancia de base de datos de SQL Server ... 3378
Eliminación de Multi-AZ de una instancia de base de datos de SQL Server ... 3379
Limitaciones, notas y recomendaciones ... 3379
Determinar la ubicación de la secundaria ... 3384
Migración a AG Always On ... 3384
Características adicionales para SQL Server ... 3386
Uso de la política de contraseñas con una instancia de base de datos de SQL Server ... 3387
Integración de Amazon S3 ... 3396
Uso de Database Mail ... 3419
Soporte del almacén de instancias para tempdb ... 3435
Uso de eventos extendidos ... 3439
Acceso a las copias de seguridad del registro de transacciones ... 3443
Opciones para SQL Server ... 3488
Descripción de las opciones disponibles para las versiones y ediciones de SQL Server ... 3490
Servidores enlazados con Oracle OLEDB ... 3493
Servidores enlazados con ODBC de Teradata ... 3506
Copia de seguridad y restauración nativas ... 3516
Cifrado de datos transparente ... 3521
SQL Server Audit ... 3535
SQL Server Analysis Services ... 3546
SQL Server Integration Services ... 3577
SQL Server Reporting Services ... 3601
Coordinador de transacciones distribuidas de Microsoft ... 3623

Tareas de administración de bases de datos frecuentes 3642
Acceso a la base de datos tempdb 3644
Analizar la carga de trabajo de la base de datos con el Asesor de Ajustes 3648
Cambio del db_owner a la cuenta rdsa de su base de datos 3653
Administración de intercalaciones y conjuntos de caracteres 3654
Agregar un usuario de base de datos 3663
Determinar un modelo de recuperación 3664
Determinación de la hora de la última conmutación por error 3665
Solucione los errores de PITR debidos a brechas en el LSN 3666
Cómo denegar o permitir la visualización de nombres de bases de datos 3667
Desactivación de inserciones rápidas 3668
Eliminación con drop de una base de datos de SQL Server 3669
Cambio del nombre de una base de datos Multi-AZ 3670
Restablecimiento de la pertenencia al rol db_owner para el usuario maestro 3670
Restauración de instancias de base de datos con licencia caducada 3671
Transición de una base de datos desde OFFLINE a ONLINE 3672
Uso de CDC 3672
Uso del Agente SQL Server 3676
Trabajo con registros de SQL Server 3683
Trabajo con archivos de seguimiento y volcado 3685
MySQL en Amazon RDS 3687
Compatibilidad con características de MySQL 3690
Versiones principales de MySQL 3690
Motores de almacenamiento admitidos 3693
Uso de memcached y otras opciones 3693
Calentamiento de caché de InnoDB 3694
Cambios de lenguaje inclusivo para MySQL versión 8.4 3695
Características no admitidas 3698
Versiones de MySQL 3700
Versiones secundarias compatibles en MySQL 3700
Versiones principales compatibles en MySQL 3704
Versiones de soporte extendido de RDS para RDS para MySQL 3705
El entorno de vista previa de bases de datos 3707
MySQL versión 8.4 en el entorno de vista previa de bases de datos 3711
MySQL versión 8.3 en el entorno de vista previa de bases de datos 3711
MySQL versión 8.2 en el entorno de vista previa de bases de datos 3712

MySQL versión 8.1 en el entorno de vista previa de base de datos 3712
Versiones de MySQL obsoleta 3712
Conexión a una instancia de base de datos que ejecuta MySQL 3713
Busque la información de conexión: 3714
Instalación de cliente de línea de comandos 3718
Conexión desde el cliente de línea de comandos 3718
Conexión desde MySQL Workbench 3719
Conexión con los controladores de AWS 3722
Resolución de problemas 3723
Protección de las conexiones de MySQL 3724
Validación de contraseñas 3727
Cifrado con SSL/TLS 3728
Uso de nuevos certificados de SSL/TLS 3732
Uso de la autenticación de Kerberos para MySQL 3738
Mejora del rendimiento de las consultas con lecturas optimizadas de RDS 3754
Descripción general 3754
Casos de uso 3755
Prácticas recomendadas 3756
Utilización 3757
Monitorización 3758
Limitaciones 3758
Mejora del rendimiento de escritura con escrituras optimizadas para RDS para MySQL 3760
Descripción general 3069
Uso con una base de datos nueva 3761
Habilitación en una base de datos existente 3766
Limitaciones 3767
Actualizaciones del motor de base de datos de MySQL 3768
Consideraciones 3770
Búsqueda de objetivos de actualización válidos 3770
Números de versión de MySQL 3771
Números de versión de RDS 3773
Actualizaciones de la versión principal 3774
Comprobación de una actualización 3781
Actualización de una instancia de base de datos MySQL 3782
Actualizaciones de versiones secundarias automáticas 3782
Actualización con tiempo de inactividad reducido 3785

Actualización de una versión del motor de instantáneas de base de datos de MySQL 3791
Opciones de actualización para versiones de motor no compatibles 3793
Importación de datos en una instancia de base de datos de RDS para MySQL 3796
Consideraciones sobre la importación de datos 3804
Restauración de una copia de seguridad en una instancia de base de datos MySQL. 3810
Importación de datos de una base de datos externa 3823
Importación de datos con un tiempo de inactividad reducido 3828
Importación de datos desde cualquier origen 3850
Replicación de MySQL 3857
Réplicas de lectura de MySQL 3858
Replicación basada en GTID 3877
Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa 3885
Configuración de la replicación de varios orígenes 3891
Configuración de clústeres activo-activo 3900
Casos de uso 3900
Limitaciones y aspectos a tener en cuenta de los clústeres activo-activo 3901
Preparación de un clúster activo-activo entre VPC 3905
Configuración de parámetros obligatorios para los clústeres activo-activo 3907
Conversión de una instancia de base de datos en un clúster activo-activo 3910
Configuración de un nuevo clúster activo-activo 3917
Adición de una instancia de base de datos en un clúster activo-activo 3924
Monitorización de clústeres activo-activo 3927
Detención de Group Replication en un clúster activo-activo 3928
Cambio de nombre de una instancia de base de datos en un clúster activo-activo 3928
Eliminación de una instancia de base de datos de un clúster activo-activo 3929
Exportación de datos de una instancia de base de datos MySQL 3931
Preparar una base de datos MySQL externa 3931
Preparar la instancia de base de datos MySQL de origen 3932
Copia de la base de datos 3934
Finalización de la exportación 3935
Opciones para MySQL 3938
Complemento de auditoría MariaDB 3939
memcached 3948
Parámetros de MySQL 3954
Tareas comunes de administración de bases de datos para MySQL 3957

Usuarios predefinidos ... 3957
Modelo de privilegios basado en roles ... 3958
Privilegios dinámicos ... 3961
Finalización de una sesión o una consulta ... 3965
Omisión del error de replicación actual ... 3966
Mejora de los tiempos de recuperación tras un bloqueo ... 3968
Administración del historial de estado global (Global Status History) ... 3971
Configuración del tamaño del grupo de búferes y la capacidad de registros redo ... 3973
Zona horaria local ... 3975
Problemas conocidos y limitaciones ... 3978
Palabra reservada InnoDB ... 3978
Comportamiento completo del almacenamiento ... 3978
Incoherencia en el tamaño del grupo de búfer de InnoDB ... 3979
La optimización de combinación de índice devuelve resultados incorrectos ... 3980
Excepciones en los parámetros de MySQL para las instancias de base de datos de Amazon RDS ... 3981
Límites de tamaño de archivo de MySQL en Amazon RDS ... 3982
Complemento de llavero de MySQL no compatible ... 3985
Puertos personalizados ... 3985
Limitaciones del procedimiento almacenado de MySQL ... 3985
Replicación basada en GTID con una instancia de origen externa ... 3985
Complemento de autenticación predeterminado de MySQL ... 3986
Anulación de innodb_buffer_pool_size ... 3986
Actualización de MySQL 5.7 a MySQL 8.4 ... 3987
Compresión de página de InnoDB ... 3987
Procedimientos almacenados de RDS para MySQL ... 3988
Recopilación y mantenimiento del historial de estado global ... 3989
Configuración, inicio y detención de la replicación del registro binario (binlog) ... 3992
Finalización de una sesión o una consulta ... 4037
Administración de clústeres activo-activo ... 4039
Administración de la replicación de varios orígenes ... 4044
Replicación de transacciones mediante GTID ... 4068
Rotación de los registros de consultas ... 4071
Establecimiento y muestra de la configuración del registro binario ... 4073
Calentamiento de caché de InnoDB ... 4078
Oracle en Amazon RDS ... 4080

Información general de Oracle 4081
Características de Oracle 4082
Versiones de Oracle 4086
Licencias de Oracle 4093
Usuarios y privilegios de Oracle 4097
Clases de instancia de Oracle 4099
Arquitectura de bases de datos de Oracle 4108
Parámetros de Oracle 4110
Conjuntos de caracteres de Oracle 4112
Limitaciones de Oracle 4116
Conexión a una instancia de base de datos de Oracle 4119
Búsqueda del punto de enlace 4119
SQL Developer 4121
SQL*Plus 4124
Consideraciones relativas al grupo de seguridad 4125
Procesos del servidor dedicados y compartidos 4126
Solución de problemas 4126
Modificación de parámetros sqlnet.ora de Oracle 4128
Protección de conexiones de Oracle 4134
Cifrado con SSL 4134
Uso de nuevos certificados de SSL/TLS 4135
Cifrado con NNE 4139
Configuración de la autenticación Kerberos 4140
Configuración del acceso UTL_HTTP 4161
Uso de CDB 4174
Descripción general de las CDB 4174
Configuración de una CDB 4181
Copia de seguridad y restauración de una CDB 4187
Conversión de una base de datos no CDB en una CDB 4188
Conversión de un solo inquilino a varios inquilinos 4192
Añadir una base de datos de inquilinos de RDS para Oracle a su instancia de CDB 4195
Modificación de una base de datos de inquilinos de RDS para Oracle 4198
Eliminar una base de datos de inquilinos de RDS para Oracle de su CDB 4200
Ver detalles de la base de datos de inquilinos 4203
Actualización de la CDB 4208
Administración de la instancia de base de datos de Oracle 4209

Tareas del sistema 4225
Tareas de bases de datos 4253
Tareas relacionadas con los registros 4286
Tareas de RMAN 4300
Tareas del programador de Oracle 4337
Diagnóstico de problemas 4348
Otras tareas 4358
Configuración de características avanzadas de RDS para Oracle 4374
Configuración del almacén de instancias 4374
Activación de páginas de gran tamaño 4387
Activación de tipos de datos extendidos 4391
Importación de datos en Oracle 4395
Importación mediante Oracle SQL Developer 4396
Migración mediante espacios de tabla transportables de Oracle 4396
Importación mediante Oracle Data Pump 4414
Importación mediante exportación/importación de Oracle 4433
Importación mediante Oracle SQL*Loader 4434
Migración de vistas materializadas de Oracle 4435
Trabajo con las réplicas de Oracle 4438
Información general sobre las réplicas de Oracle 4438
Requisitos y consideraciones sobre réplicas de Oracle 4441
Preparación para crear una réplica de Oracle 4445
Creación de una réplica de Oracle montada 4447
Modificación del modo de réplica 4449
Trabajo con copias de seguridad de réplicas de Oracle 4450
Realización de una conmutación de Oracle Data Guard 4453
Solución de problemas de réplicas de Oracle 4461
Opciones para Oracle 4464
Información general sobre las opciones de Oracle DB 4464
Integración de Amazon S3 4467
Oracle Application Express 4494
Integración de Amazon EFS 4519
Máquina virtual Java (JVM) 4537
Enterprise Manager 4542
Label security 4568
Locator 4572

Native Network Encryption (NNE) 4577
OLAP 4594
Capa de conexión segura (SSL) 4598
Spatial 4610
SQLT 4615
Statspack 4625
Zona horaria 4629
Actualización automática del archivo de zona horaria 4635
Cifrado de datos transparente (TDE) 4646
UTL_MAIL 4651
XML DB 4655
Actualización del motor de base de datos Oracle 4656
Información general sobre las actualizaciones de Oracle 4656
Actualizaciones de la versión principal 4664
Actualizaciones de la versión secundaria 4666
Consideraciones de actualización 4673
Comprobación de una actualización 4677
Actualización de una instancia de base de datos de RDS para Oracle 4678
Actualización de una instantánea de base de datos de Oracle 4680
Herramientas y software de terceros para Oracle 4683
Uso de Oracle GoldenGate 4684
Uso de Oracle Repository Creation Utility 4704
Configuración de CMAN 4712
Instalación de una base de datos de Siebel en Oracle en Amazon RDS 4715
Versiones del motor de Oracle Database 4720
PostgreSQL en Amazon RDS 4721
Tareas de administración comunes 4723
Trabajo con el entorno de vista previa de bases de datos 4728
Características no compatibles en el entorno de vista previa de bases de datos 4729
Versión 17 de PostgreSQL en el entorno de vista previa de bases de datos 4729
Creación de una nueva instancia de base de datos en el entorno de vista previa de bases de datos 4729
Nuevas versiones de PostgreSQL 4732
Versiones obsoletas de PostgreSQL 4732
Proceso de lanzamiento de RDS para PostgreSQL 4734
Ventajas del proceso de lanzamiento incremental de RDS para PostgreSQL 4734

Administración de actualizaciones de versiones 4734
Versiones de extensiones de PostgreSQL 4736
Restringir la instalación de extensiones de PostgreSQL 4736
Extensiones de confianza de PostgreSQL 4738
Características de PostgreSQL 4740
Tipos de datos personalizados y enumeraciones 4741
Desencadenadores de eventos 4741
Páginas de gran tamaño 4742
Realización de la replicación lógica 4743
Disco RAM para stats_temp_directory 4751
Espacios de tabla 4752
Intercalaciones para EBCDIC y otras migraciones de mainframe 4752
Administración de sincronización de ranuras lógicas 4759
Conexión a una instancia de PostgreSQL 4761
Instalación del cliente psql 4762
Busque la información de conexión: 4762
Uso de pgAdmin para conectarse a una instancia de base de datos de RDS for PostgreSQL 4765
Uso de psql para conectarse a una instancia de base de datos de RDS for PostgreSQL ... 4767
Conexión a RDS para PostgreSQL con el controlador JDBC de AWS 4769
Conexión a RDS para PostgreSQL con el controlador de Python de AWS 4769
Solución de problemas de conexiones a la instancia de RDS for PostgreSQL 4769
Protección de conexiones con SSL/TLS 4772
Uso de SSL con una instancia de base de datos PostgreSQL 4772
Actualización de aplicaciones para usar nuevos certificados SSL/TLS 4780
Uso de la autenticación Kerberos 4785
Disponibilidad en regiones y versiones 4786
Información general de la autenticación Kerberos 4786
Configuración 4787
Administración de una instancia de base de datos de RDS para PostgreSQL en un dominio de Active Directory 4802
Conexión con autenticación Kerberos 4803
Uso de un servidor de DNS personalizado para el acceso a la red de salida. 4807
Activación de la resolución de DNS personalizada 4807
Desactivación de la resolución de DNS personalizada 4807
Configuración de un servidor DNS personalizado 4807

Actualizaciones del motor de base de datos de PostgreSQL 4810
Consideraciones 4812
Búsqueda de objetivos de actualización válidos 4813
Números de versión de PostgreSQL 4814
Números de versión de RDS 4815
Elección de una actualización de versión principal 4816
Cómo realizar una actualización de versión principal 4831
Actualizaciones de versiones secundarias automáticas 4840
Actualización de las extensiones de PostgreSQL 4843
Actualización de una versión del motor de instantáneas de base de datos de PostgreSQL 4844
Uso de réplicas de lectura para RDS para PostgreSQL 4847
Decodificación lógica en una réplica de lectura 4847
Limitaciones de las réplicas de lectura con PostgreSQL 4851
Configuración de réplicas de lectura con PostgreSQL 4852
Uso de réplicas de lectura en cascada 4855
Creación de réplicas de lectura en cascada entre regiones 4857
Cómo funciona la replicación en diferentes versiones de RDS para PostgreSQL 4858
Supervisión y ajuste del proceso de replicación 4863
Solución de problemas de réplicas de lectura de RDS para PostgreSQL 4866
Mejora del rendimiento de las consultas con lecturas optimizadas de RDS 4868
Información general de las lecturas optimizadas para RDS en PostgreSQL 4868
Casos de uso 4869
Prácticas recomendadas 4870
Utilización 4870
Monitorización 4871
Limitaciones 4872
Importación de datos en PostgreSQL 4873
Importación de una base de datos de PostgreSQL desde una instancia Amazon EC2 4875
Uso del comando \copy para importar datos en una tabla en una instancia de base de datos PostgreSQL 4878
Importación de datos de Amazon S3 a RDS para PostgreSQL 4879
Transporte de bases de datos de PostgreSQL entre instancias de base de datos 4900
Exportación de datos de PostgreSQL a Amazon S3 4910
Instalación de la extensión 4911
Información general de la exportación a S3 4912
Especificación de la ruta del archivo de Amazon S3 a exportar 4913

Configuración del acceso a un bucket de Amazon S3 4914
Exportación de datos de consulta mediante la función aws_s3.query_export_to_s3 4919
Referencia de funciones 4922
Solución de errores de acceso a Amazon S3 4926
Invocar una Lambda función desde RDS para PostgreSQL 4928
Paso 1: configure las conexiones salientes 4929
Paso 2: configure IAM para su instancia y Lambda 4930
Paso 3: instale la extensión 4932
Paso 4: utilice las funciones auxiliares de Lambda 4933
Paso 5: invoque una función de Lambda 4934
Paso 6: Conceder permisos a los usuarios 4935
Ejemplos: invocar funciones de Lambda 4936
Mensajes de error de la función de Lambda 4939
Referencia de parámetros y funciones de Lambda 4940
Tareas comunes de DBA para RDS for PostgreSQL 4946
Intercalaciones admitidas en RDS para PostgreSQL 4947
Descripción de los roles y permisos de PostgreSQL 4948
Gestión de conexiones inactivas en PostgreSQL 4964
Trabajo con autovacuum de PostgreSQL 4967
Mecanismos de registro 5016
Administración de archivos temporales con PostgreSQL 5018
Uso de pgBadger para el análisis de registros con PostgreSQL 5024
Uso de PGSnapper para supervisar PostgreSQL 5024
Trabajo con parámetros 5024
Ajuste con eventos de espera de RDS para PostgreSQL 5046
Conceptos esenciales para el ajuste de RDS para PostgreSQL 5047
Eventos de espera de RDS para PostgreSQL 5052
Client:ClientRead 5054
Client:ClientWrite 5058
CPU 5060
IO:BufFileRead y IO:BufFileWrite 5067
IO:DataFileRead 5075
IO:WALWrite 5084
Eventos de espera IPC:parallel 5087
Lock:advisory 5094
Lock:extend 5097

Lock:Relation 5100
Lock:transactionid 5104
Lock:tuple 5107
LWLock:BufferMapping (LWLock:buffer_mapping) 5111
LWLock:BufferIO (IPC:BufferIO) 5114
LWLock:buffer_content (BufferContent) 5116
LWLock:lock_manager (LWLock:lockmanager) 5118
LWLock:pg_stat_statements 5124
Timeout:PgSleep 5128
Timeout:VacuumDelay 5129
Ajuste de RDS para PostgreSQL con información proactiva de Amazon DevOps Guru 5132
La base de datos lleva mucho tiempo inactiva en la conexión de la transacción 5132
Uso de extensiones PostgreSQL 5136
Uso de funciones de orafce 5137
Uso de la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL ... 5139
Administración de las particiones con la extensión pg_partman 5153
Uso de pgAudit para registrar la actividad de la base de datos 5160
Programación de mantenimiento con la extensión pg_cron 5174
Uso de pglogical para sincronizar datos 5185
Uso de pgactive para crear la replicación activa-activa 5200
Reducción de la sobrecarga con la extensión pg_repack 5277
Actualización y uso de PLV8 5283
Uso de PL/Rust para escribir funciones en lenguaje Rust 5286
Administración de datos espaciales con PostGIS 5291
Contenedores de datos externos compatibles en Amazon RDS para PostgreSQL 5301
Uso de la extensión log_fdw 5301
Uso de la extensión postgres_fdw para acceder a datos externos 5303
Uso de una base de datos MySQL 5304
Uso de una base de datos Oracle 5309
Uso de una base de datos de SQL Server 5313
Uso de Extensiones de lenguaje de confianza para PostgreSQL 5317
Terminología 5318
Requisitos para usar Extensiones de lenguaje de confianza 5319
Configuración de Extensiones de lenguaje de confianza 5322
Información general de Extensiones de lenguaje de confianza 5326
Creación de extensiones TLE 5328

Eliminar las extensiones TLE de una base de datos 5333
Desinstalación de Extensiones de lenguaje de confianza 5334
Uso de enlaces de PostgreSQL con sus extensiones TLE 5335
Uso de tipos de datos personalizados en Extensiones de lenguaje de confianza 5342
Referencia de funciones para Extensiones de lenguaje de confianza 5342
Referencia de enlaces para Extensiones de lenguaje de confianza 5356
Ejemplos de código 5360
Acciones 5371
`CreateDBInstance` 5372
`CreateDBParameterGroup` 5387
`CreateDBSnapshot` 5394
`DeleteDBInstance` 5402
`DeleteDBParameterGroup` 5411
`DescribeAccountAttributes` 5418
`DescribeDBEngineVersions` 5422
`DescribeDBInstances` 5430
`DescribeDBParameterGroups` 5440
`DescribeDBParameters` 5448
`DescribeDBSnapshots` 5458
`DescribeOrderableDBInstanceOptions` 5465
`GenerateRDSAuthToken` 5473
`ModifyDBInstance` 5475
`ModifyDBParameterGroup` 5481
`RebootDBInstance` 5487
Escenarios 5490
Comience a utilizar instancias de base de datos 5490
Ejemplos sin servidor 5588
Conexión a una base de datos de Amazon RDS en una función de Lambda 5588
Ejemplos de servicios cruzados 5605
Crear un rastreador de elementos de trabajo de Aurora Serverless 5605
Seguridad 5610
Autenticación de bases de datos 5612
Autenticación de contraseña 5613
Autenticación de bases de datos de IAM 5613
Autenticación Kerberos 5614
Administración de contraseñas con RDS y Secrets Manager 5616

Limitaciones ... 5616
Descripción general ... 5617
Ventajas ... 5618
Permisos ... 5619
Cumplimiento de la administración por parte de RDS ... 5620
Administración de la contraseña de la instancia de base de datos ... 5621
Administración de la contraseña de la base de datos de inquilinos ... 5625
Administración de la contraseña para un clúster de base de datos multi-AZ ... 5629
Rotación de secretos para la instancia de base de datos ... 5633
Rotación de secretos para clústeres de bases de datos multi-AZ ... 5635
Visualización de los detalles del secreto ... 5637
Visualización de los detalles del secreto para clústeres de base de datos multi-AZ ... 5640
Visualización de los detalles del secreto para las bases de datos de inquilinos ... 5644
Disponibilidad en regiones y versiones ... 5647
Protección de los datos ... 5647
Cifrado de datos ... 5648
Privacidad del tráfico entre redes ... 5681
Identity and Access Management ... 5683
Público ... 5683
Autenticación con identidades ... 5684
Administración de acceso mediante políticas ... 5688
Cómo funciona Amazon RDS con IAM ... 5690
Ejemplos de políticas basadas en identidades ... 5698
Políticas administradas por AWS ... 5721
Actualizaciones de políticas ... 5729
Prevención de la sustitución confusa entre servicios ... 5751
Autenticación de bases de datos de IAM ... 5754
Solución de problemas ... 5808
Registro y supervisión ... 5810
Validación de la conformidad ... 5813
Resiliencia ... 5814
Copia de seguridad y restauración ... 5814
Replicación ... 5814
Failover ... 5815
Seguridad de la infraestructura ... 5816
Grupos de seguridad ... 5816

Public accessibility (Accesibilidad pública) 5816
Puntos de enlace de la VPC (AWS PrivateLink) 5818
Consideraciones 1590
Disponibilidad 1590
Creación de un punto de enlace de la VPC de tipo interfaz 1591
Creación de una política de punto de enlace de la VPC 1591
Prácticas recomendadas de seguridad 5822
Control de acceso con grupos de seguridad 5823
Información general de los grupos de seguridad de VPC 5823
Escenario de grupos de seguridad 5824
Creación de un grupo de seguridad de VPC 5825
Asociación con una instancia de base de datos 5826
Privilegios de la cuenta de usuario maestro 5826
Roles vinculados a servicios 5831
Permisos de roles vinculados a servicios de Amazon RDS 5831
Permisos de roles vinculados a servicios para Amazon RDS Custom 5834
Permisos de roles vinculados a servicios para Amazon RDS Beta 5835
Rol vinculado a servicios para Amazon RDS Preview 5837
Uso de Amazon RDS con Amazon VPC 5839
Uso de una instancia de base de datos en una VPC 5839
Actualización de la VPC para una instancia de base de datos 5859
Escenarios de acceso a una instancia de base de datos en una VPC 5860
Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4) 5867
Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (modo de pila doble) 5875
Traslado de una instancia de base de datos a una VPC 5887
Cuotas y restricciones 5890
Cuotas en Amazon RDS 5890
Restricciones de la nomenclatura en Amazon RDS 5897
Número máximo de conexiones de base de datos 5898
Límites de tamaño de archivo en Amazon RDS 5901
Solución de problemas 5902
No puede conectarse a la instancia de base de datos de 5902
Comprobar la conexión a la instancia de base de datos 5905
Solución de problemas de autenticación de conexión 5906

Problemas de seguridad 5906
Mensaje de error "No se pudieron recuperar los atributos de cuenta. Determinadas funciones de la consola pueden estar deterioradas". 5906
Solución de problemas de estado de red incompatible 5907
Causas 5907
Resolución 5907
Restablecimiento de la contraseña del propietario de la instancia de base de datos 5909
Interrupción o reinicio de una instancia de base de datos 5910
Los cambios de parámetros no surten efecto 5911
Instancia de base de datos sin espacio de almacenamiento 5911
Instancias de bases de datos disponibles insuficientes 5913
Problemas de memoria que se puede liberar de RDS 5914
Problemas de MySQL y MariaDB 5915
Máximo de conexiones de MySQL y MariaDB 5915
Diagnóstico y resolución del estado de parámetros incompatibles para un límite de memoria 5916
Diagnóstico y resolución de retardos entre réplicas de lectura 5918
Diagnóstico y solución de un error de replicación de lectura de MySQL o MariaDB 5920
La creación de desencadenadores con registro binario habilitado exige privilegios SUPER 5922
Diagnóstico y resolución de errores de restauración a un momento dado 5924
Error de replicación detenida 5925
Se produce un error en la creación de la réplica de lectura o la replicación se interrumpe con el error grave 1236 5926
La replicación de réplicas de lectura no puede inicializar la estructura de metadatos 5926
No se puede establecer el período de retención de copia de seguridad en 0 5927
Referencia de la API de Amazon RDS 5928
Uso de la API de consulta 5928
Parámetros de consulta 5928
Autenticación de solicitudes de consulta 5929
Solución de problemas de aplicaciones 5929
Recuperación de errores 5929
Consejos para la solución de problemas 5930
Historial de revisión 5931
Actualizaciones anteriores 6123
Glosario de AWS 6161

¿Qué es Amazon Relational Database Service (Amazon RDS)?

Amazon Relational Database Service (Amazon RDS) es un servicio web que facilita la configuración, la operación y la escala de una base de datos relacional en Nube de AWS. Proporciona una capacidad rentable y de tamaño ajustable para una base de datos relacional estándar y se ocupa de las tareas de administración de bases de datos comunes.

> **Note**
>
> Esta guía cubre motores de base de datos de Amazon RDS que no sean de Amazon Aurora. Para obtener información acerca de cómo usar Amazon Aurora, consulte la Guía del usuario de Amazon Aurora.

Si es nuevo en AWS productos y servicios, empiece por obtener más información con los siguientes recursos:

- Para obtener una visión general de todos los AWS productos, consulte ¿Qué es la informática en la nube?
- Amazon Web Services ofrece diversos servicios de base de datos. Para obtener más información sobre la variedad de opciones de bases de datos disponibles en AWS, consulte Choosing an AWS database service (Elección de un servicio de base de datos de AWS) y Running databases on AWS (Ejecución de bases de datos en AWS).

Ventajas de Amazon RDS

Amazon RDS es un servicio de base de datos administrada. Es responsable de la mayoría de las tareas de administración. Amazon RDS elimina procesos manuales que resultan pesados, lo que le permite centrarse en la aplicación y en los usuarios.

Estas son las principales ventajas de Amazon RDS en comparación con implementaciones de bases de datos que no están completamente administradas:

- Puede utilizar los motores de base de datos que ya conoce: IBM Db2, MariaDB, Microsoft SQL Server, MySQL, Oracle Database y PostgreSQL.

- Amazon RDS administra las copias de seguridad, la aplicación de parches de software, la detección automática de errores y la recuperación.
- Puede activar las copias de seguridad automatizadas o crear manualmente sus propias instantáneas de copia de seguridad. Estas copias de seguridad se pueden utilizar para restaurar una base de datos. El proceso de restauración de Amazon RDS es fiable y eficaz.
- Puede obtener una alta disponibilidad gracias a una instancia de base de datos principal y una instancia de base de datos secundaria síncrona, a la que podrá acceder cuando haya algún error. También puede utilizar réplicas de lectura para aumentar el escalado de lectura.
- Además de la seguridad en el paquete de la base de datos, puede controlar el acceso usando AWS Identity and Access Management (IAM) para definir usuarios y permisos. Para ayudar a proteger sus bases de datos, también puede ponerlas en una nube virtual privada (VPC).

Comparación de responsabilidades con las implementaciones de Amazon EC2 y en las instalaciones

Recomendamos Amazon RDS como opción predeterminada para la mayoría de las implementaciones de bases de datos relacionales. La desventaja de las siguientes alternativas es que tendrá que dedicar más tiempo a administrar el software y el hardware:

Implementación en las instalaciones

: Cuando adquiere un servidor en las instalaciones, obtiene CPU, memoria, almacenamiento e IOPS, todo junto. Usted asume toda la responsabilidad relacionada con el software de la base de datos, el servidor y el sistema operativo.

Amazon EC2

: Amazon Elastic Compute Cloud (Amazon EC2) proporciona capacidad de computación escalable y segura en Nube de AWS. A diferencia de lo que ocurre con un servidor en las instalaciones, la CPU, la memoria, el almacenamiento y las IOPS están separadas, de modo que puede escalarlas de forma independiente. AWS administra las capas de hardware, lo que elimina parte de la carga implicada en la administración de un servidor de base de datos en las instalaciones.

  La desventaja de ejecutar una base de datos en Amazon EC2 es que es una opción más propensa a los errores de usuarios. Por ejemplo, cuando actualiza manualmente el sistema operativo o el software de la base de datos, podría provocar accidentalmente el tiempo de inactividad de la aplicación. Es posible que pase horas verificando cada cambio para identificar y solucionar un problema.

En la siguiente tabla, encontrará una comparación entre los modelos de administración para bases de datos Amazon EC2, Amazon RDS y en las instalaciones.

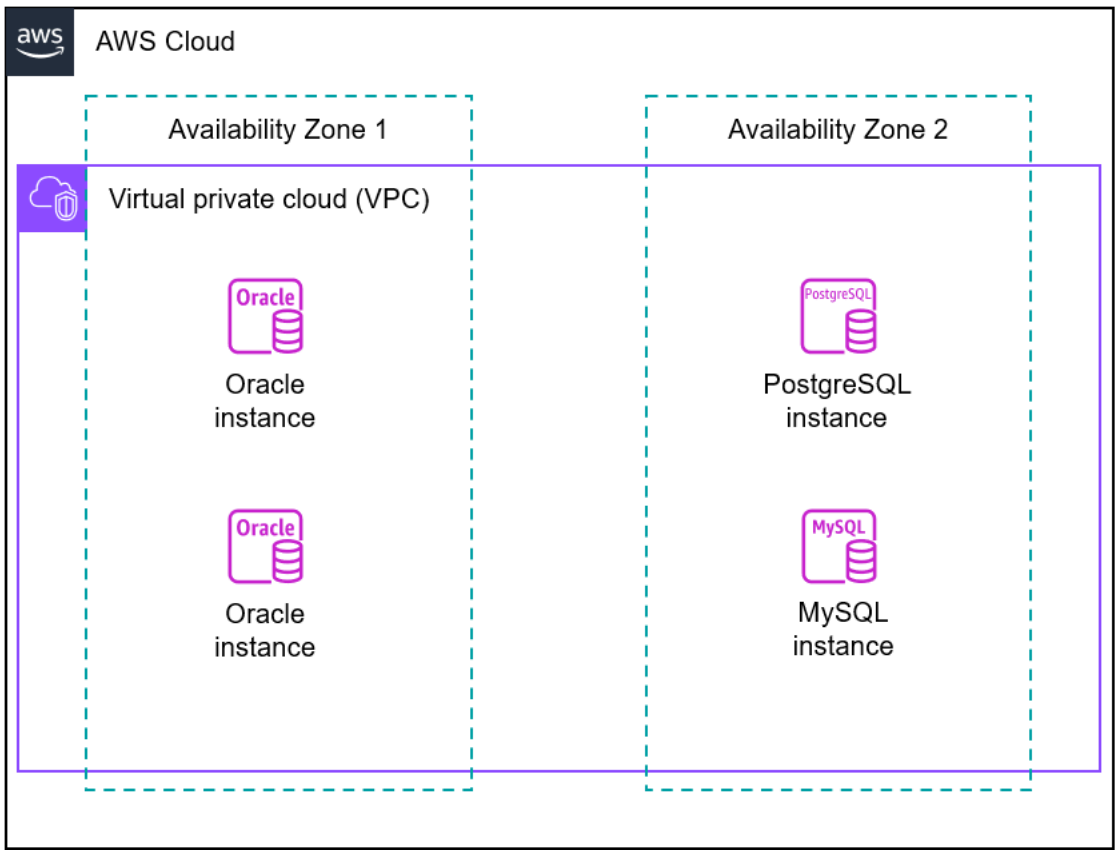
Característica	Administración en las instalaciones	Administración de Amazon EC2	Administración de Amazon RDS
Optimización de aplicaciones	Cliente	Cliente	Cliente
Escalado	Cliente	Cliente	AWS
Alta disponibilidad	Cliente	Cliente	AWS
Copias de seguridad de bases de datos	Cliente	Cliente	AWS
Revisiones de software de base de datos	Cliente	Cliente	AWS
Instalación de software de base de datos	Cliente	Cliente	AWS
Aplicación de revisiones del sistema operativo (SO)	Cliente	Cliente	AWS
Instalación del sistema operativo	Cliente	Cliente	AWS
Mantenimiento de servidores	Cliente	AWS	AWS
Ciclo de vida del hardware	Cliente	AWS	AWS
Alimentación, red y refrigeración	Cliente	AWS	AWS

Modelo de responsabilidad compartida de Amazon RDS

Amazon RDS es responsable de alojar los componentes de software y la infraestructura de las instancias de base de datos y los clústeres de bases de datos. Usted es responsable del ajuste de las consultas, que es el proceso de optimización de las consultas SQL para mejorar el rendimiento. El rendimiento de las consultas depende en gran medida del diseño de la base de datos, el tamaño de los datos, la distribución de los datos, la carga de trabajo de la aplicación y los patrones de consulta, que pueden variar considerablemente. La supervisión y el ajuste son procesos enormemente individualizados que usted posee para sus bases de datos de RDS. Puede utilizar Información de rendimiento de Amazon RDS y otras herramientas para identificar consultas problemáticas.

Instancias de base de datos de Amazon RDS

Una instancia de base de datos es un entorno de base de datos aislado en la Nube de AWS. El componente básico de Amazon RDS es la instancia de base de datos. Su instancia de base de datos puede contener una o más bases de datos creadas por el usuario. El siguiente diagrama muestra una nube privada virtual (VPC) que contiene dos zonas de disponibilidad; cada zona contiene dos instancias de base de datos.



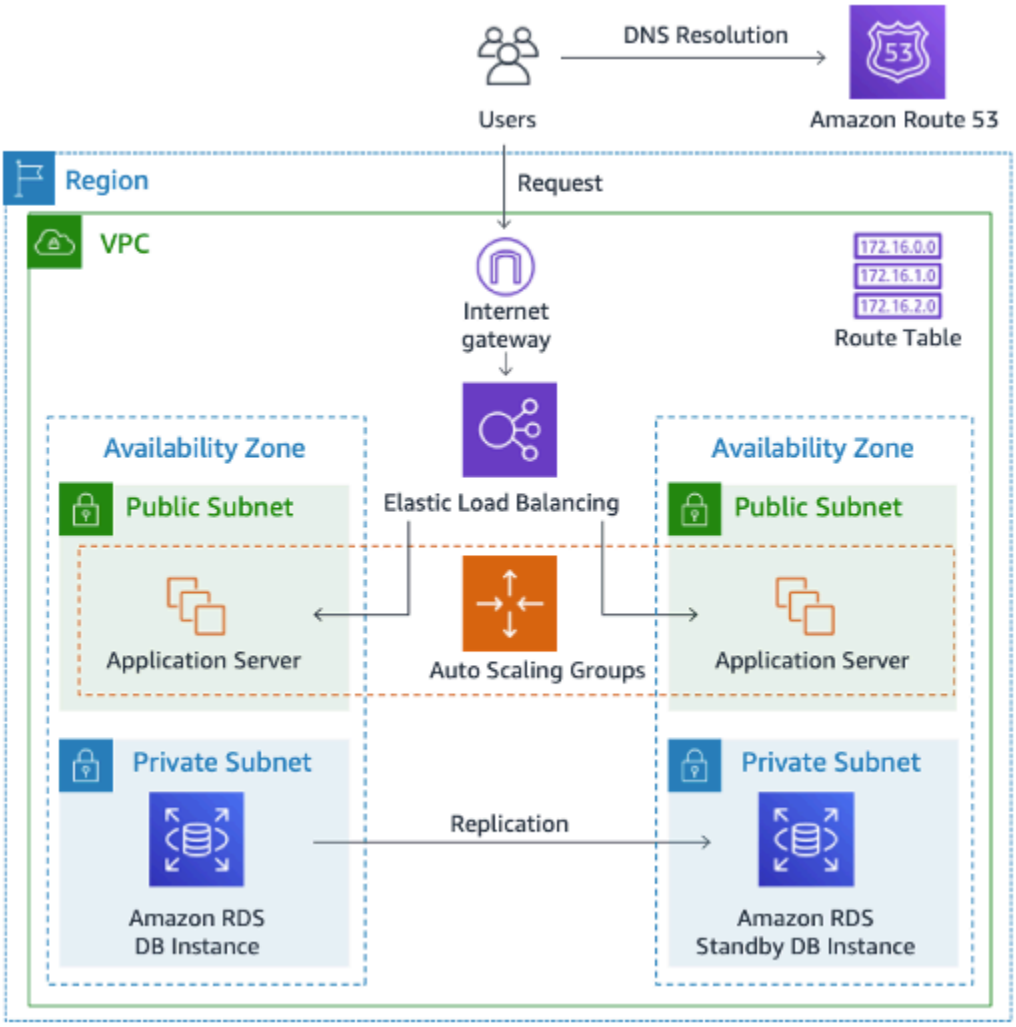
Puede acceder a las instancias de base de datos utilizando las mismas herramientas y aplicaciones que utiliza con una instancia de base de datos independiente. Puede crear y modificar una instancia de base de datos mediante AWS Command Line Interface (AWS CLI), la API de Amazon RDS o la AWS Management Console.

Temas

- Ejemplo de arquitectura de aplicaciones con Amazon RDS
- Motores de base de datos
- Clases de instancia de base de datos
- Almacenamiento de instancias de base de datos
- Instancias de base de datos en Amazon Virtual Private Cloud (Amazon VPC)

Ejemplo de arquitectura de aplicaciones con Amazon RDS

La siguiente imagen muestra un caso de uso típico de un sitio web dinámico que utiliza instancias de base de datos de Amazon RDS para el almacenamiento de bases de datos:



Los componentes principales de la arquitectura anterior son los siguientes:

Elastic Load Balancing

AWS enruta el tráfico de usuarios a través del equilibrador de carga elástico. Un equilibrador de carga distribuye cargas de trabajo a través de varios recursos informáticos, como, servidores virtuales. En este ejemplo de caso de uso, el equilibrador de carga elástico envía las solicitudes de los clientes a los servidores de aplicaciones.

Servidores de aplicaciones

Los servidores de aplicaciones interactúan con las instancias de base de datos de RDS. Por lo general, un servidor de aplicaciones en AWS se aloja en instancias EC2, que proporcionan una capacidad de computación escalable. Los servidores de aplicaciones residen en subredes públicas con diferentes zonas de disponibilidad (AZ) dentro de la misma nube privada virtual (VPC).

Instancias de base de datos de RDS

Los servidores de aplicaciones EC2 interactúan con instancias de base de datos de RDS. Las instancias de base de datos residen en subredes privadas dentro de diferentes zonas de disponibilidad (AZ) en la misma nube privada virtual (VPC). Como las subredes son privadas, no se permiten solicitudes desde Internet.

La instancia de base de datos principal se replica en otra instancia de base de datos, denominada réplica de lectura. Ambas instancias de base de datos se encuentran en subredes privadas dentro de la VPC, lo que significa que los usuarios de Internet no pueden acceder a ellas directamente.

Motores de base de datos

Un motor de base de datos es el software de base de datos relacional específico que se ejecuta en la instancia de base de datos. Amazon RDS es compatible con los siguientes motores de base de datos:

- IBM Db2

  Para obtener más información, consulte Amazon RDS para Db2.
- MariaDB

  Para obtener más información, consulte Amazon RDS para MariaDB.
- Microsoft SQL Server

  Para obtener más información, consulte Amazon RDS for Microsoft SQL Server.
- MySQL

  Para obtener más información, consulte Amazon RDS para MySQL.
- Oracle Database

  Para obtener más información, consulte Amazon RDS para Oracle.
- PostgreSQL

  Para obtener más información, consulte Amazon RDS para PostgreSQL.

Cada motor de base de datos cuenta con sus propias características compatibles y cada versión de un motor puede incluir características específicas. La compatibilidad con las características de Amazon RDS varía según las Regiones de AWS y las versiones específicas de cada motor de base de datos. Para comprobar la compatibilidad de características en las distintas versiones y regiones, consulte Funciones admitidas en Amazon RDS por Región de AWS y el motor de base de datos

Además, cada motor de base de datos tiene un conjunto de parámetros en un grupo de parámetros de base de datos que controlan el comportamiento de las bases de datos que administra. Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

Clases de instancia de base de datos

Una clase de instancia de base de datos determina la capacidad de cómputo y de memoria de una instancia de base de datos. Una clase de instancia de base de datos determina tanto el tamaño como el tipo de clase de instancia de base de datos. Amazon RDS es compatible con los siguientes tipos de clases de instancias; el asterisco (*) representa la generación, el atributo opcional y el tamaño:

- De uso general: db.m*
- Optimizadas para la memoria: db.z*, db.x*, db.r*
- Optimizadas para la computación: db.c*
- Rendimiento ampliable: db.t*

Cada clase de instancia ofrece diferentes capacidades de computación, memoria y almacenamiento. Por ejemplo, db.m7g es un tipo de clase de instancia de base de datos de uso general y de séptima generación, y cuenta con tecnología de procesadores Graviton3 de AWS. Al crear una instancia de base de datos, debe especificar una clase de instancia de base de datos, como db.m7g.2xlarge (2xlarge es el tamaño). Para obtener más información sobre las especificaciones de hardware de las diferentes clases de instancias, consulte Especificaciones de hardware para clases de instancia de base de datos .

Puede seleccionar la clase de instancia de base de datos que mejor se adapte a sus necesidades. Si sus necesidades van cambiando, puede cambiar la clase de instancia de base de datos. Por ejemplo, puede escalar verticalmente y pasar de la instancia db.m7g.2xlarge a la instancia db.m7g.4xlarge. Para obtener más información, consulte Clases de instancia de base de datos de .

> **Note**
>
> Para obtener información sobre precios de las clases de instancia de bases de datos, consulte la sección Precios de la página de productos de Amazon RDS.

Almacenamiento de instancias de base de datos

Amazon EBS ofrece volúmenes de almacenamiento permanente de nivel de bloque que se pueden adjuntar a una instancia en ejecución. El almacenamiento de instancias de base de datos viene en los siguientes tipos:

- Uso general (SSD)

  Este tipo de almacenamiento rentable es ideal para una amplia variedad de cargas de trabajo que se ejecutan en instancias de base de datos de tamaño medio. El almacenamiento de uso general es el más adecuado para entornos de desarrollo y pruebas.
- IOPS aprovisionadas (PIOPS)

  Este tipo de almacenamiento está diseñado para satisfacer las necesidades de las cargas de trabajo con uso intensivo de operaciones de E/S; especialmente, para las cargas de trabajo de bases de datos que requieren una latencia de E/S baja y un rendimiento constante de E/S. El almacenamiento de IOPS aprovisionadas es el más adecuado para los entornos de producción.
- Magnético

  Amazon RDS admite el almacenamiento magnético para garantizar la compatibilidad con versiones anteriores. Es recomendable utilizar volúmenes SSD de uso general o SSD de IOPS aprovisionadas para las nuevas necesidades de almacenamiento.

Los tipos de almacenamiento difieren en características de rendimiento y precio. Puede adaptar el rendimiento y el costo del almacenamiento a las necesidades de su base de datos.

Cada instancia de base de datos tiene requisitos de almacenamiento mínimos y máximos en función del tipo de almacenamiento y del motor de base de datos que admita. Es importante tener suficiente almacenamiento para que sus bases de datos tengan espacio para crecer. Además, un almacenamiento suficiente garantiza que las funciones del motor de base de datos tengan espacio para escribir contenido o registrar entradas. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Instancias de base de datos en Amazon Virtual Private Cloud (Amazon VPC)

Puede ejecutar una instancia de base de datos en una nube virtual privada (VPC) utilizando el servicio Amazon Virtual Private Cloud (Amazon VPC). Cuando utilice una VPC, puede controlar todos los aspectos del entorno de red virtual. Puede elegir su propio rango de direcciones IP, crear subredes y configurar listas de enrutamiento y control de acceso.

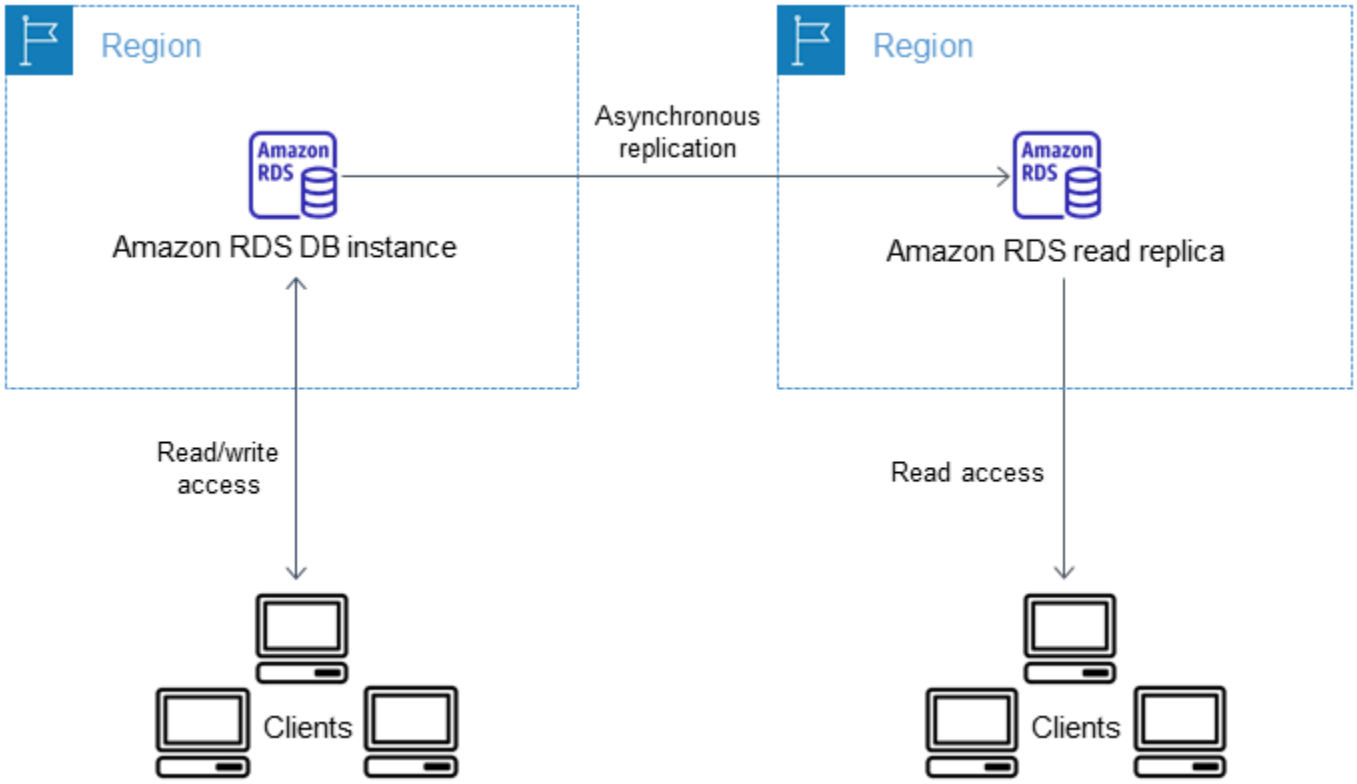
La funcionalidad básica de Amazon RDS es la misma, tanto si se ejecuta en una VPC como si no. Amazon RDS administra las copias de seguridad, la aplicación de parches de software, la detección automática de errores y la recuperación. Es posible ejecutar la instancia de base de datos en una VPC sin ningún costo adicional. Para obtener más información acerca del uso de Amazon VPC con RDS, consulte VPC de Amazon y Amazon RDS.

Amazon RDS usa el protocolo de tiempo de red (NTP) para sincronizar la hora en las instancias de base de datos.

Regiones de AWS y zonas de disponibilidad

Los recursos de informática en la nube de Amazon están alojados en instalaciones de centros de datos con alta disponibilidad, en diferentes zonas del mundo (por ejemplo, Norteamérica, Europa o Asia). Las ubicaciones del centro de datos se denominan regiones Región de AWS. Con Amazon RDS, puede crear instancias de base de datos en varias regiones.

El siguiente ejemplo muestra una instancia de base de datos de RDS en una región que se replica de forma asíncrona en una instancia de base de datos en espera de una región diferente. Si una región deja de estar disponible, la instancia de la otra región seguirá estando disponible.



Zonas de disponibilidad

Cada AWS región contiene varias ubicaciones distintas denominadas zonas de disponibilidad o AZ. Cada zona de disponibilidad está diseñada para quedar aislada en caso de error en otras zonas de disponibilidad. Cada una de ellas está diseñada para proporcionar conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma AWS región. Gracias a lanzar instancias de base de datos en distintas zonas de disponibilidad, puede proteger sus aplicaciones frente a los errores que ocurran en una única ubicación. Para obtener más información, consulte Regiones, zonas de disponibilidad y Local Zones.

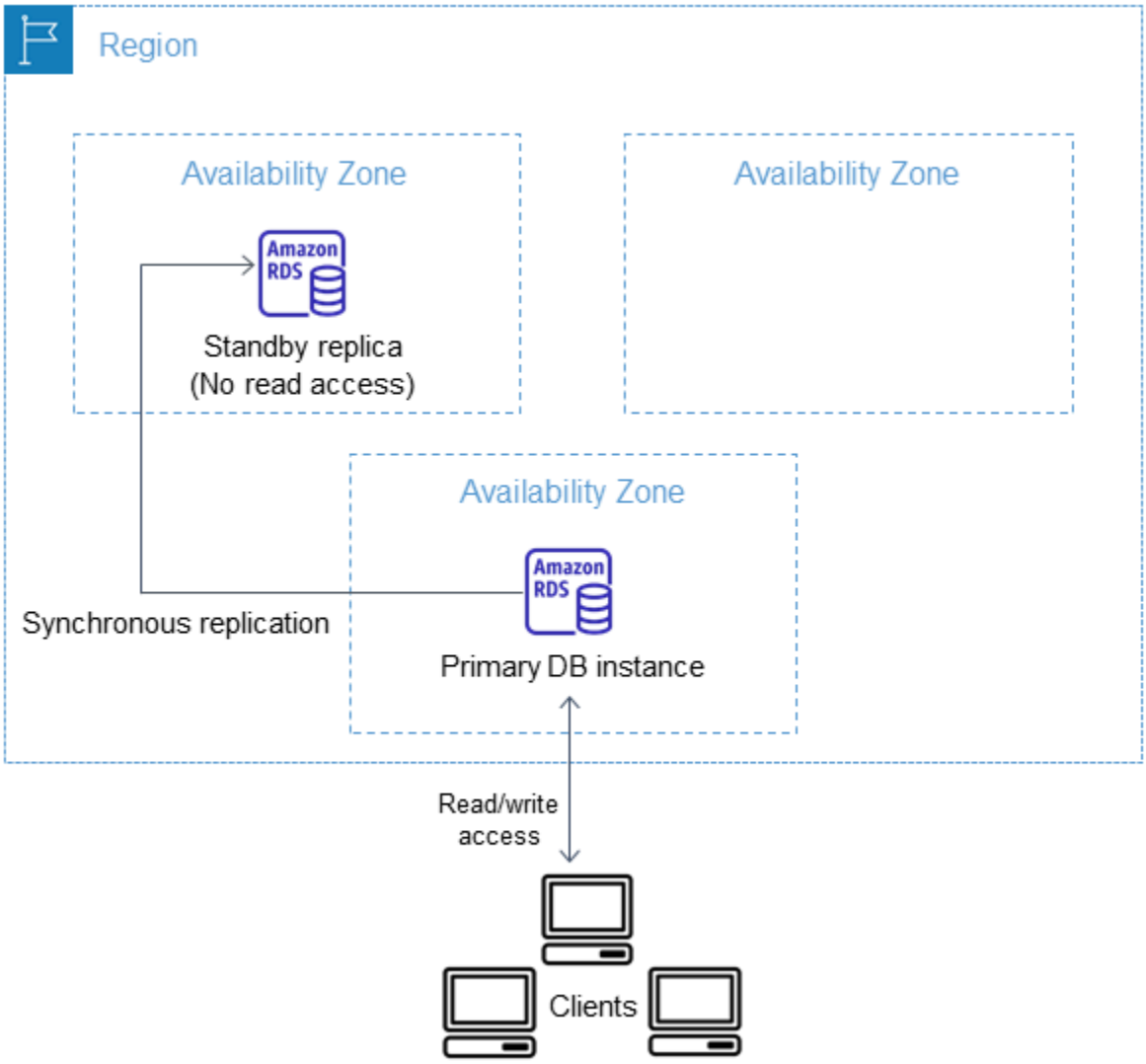
Implementaciones Multi-AZ

Puede ejecutar su instancia de base de datos en varias zonas de disponibilidad, lo que recibe el nombre de despliegue Multi-AZ. Cuando elige esta opción, Amazon aprovisiona automáticamente y mantiene una o más instancias de base de datos secundarias en espera en una zona de disponibilidad diferente. Su instancia de base de datos principal se replica en todas las zonas de disponibilidad para cada instancia de base de datos secundaria.

Una implementación Multi-AZ proporciona las siguientes ventajas:

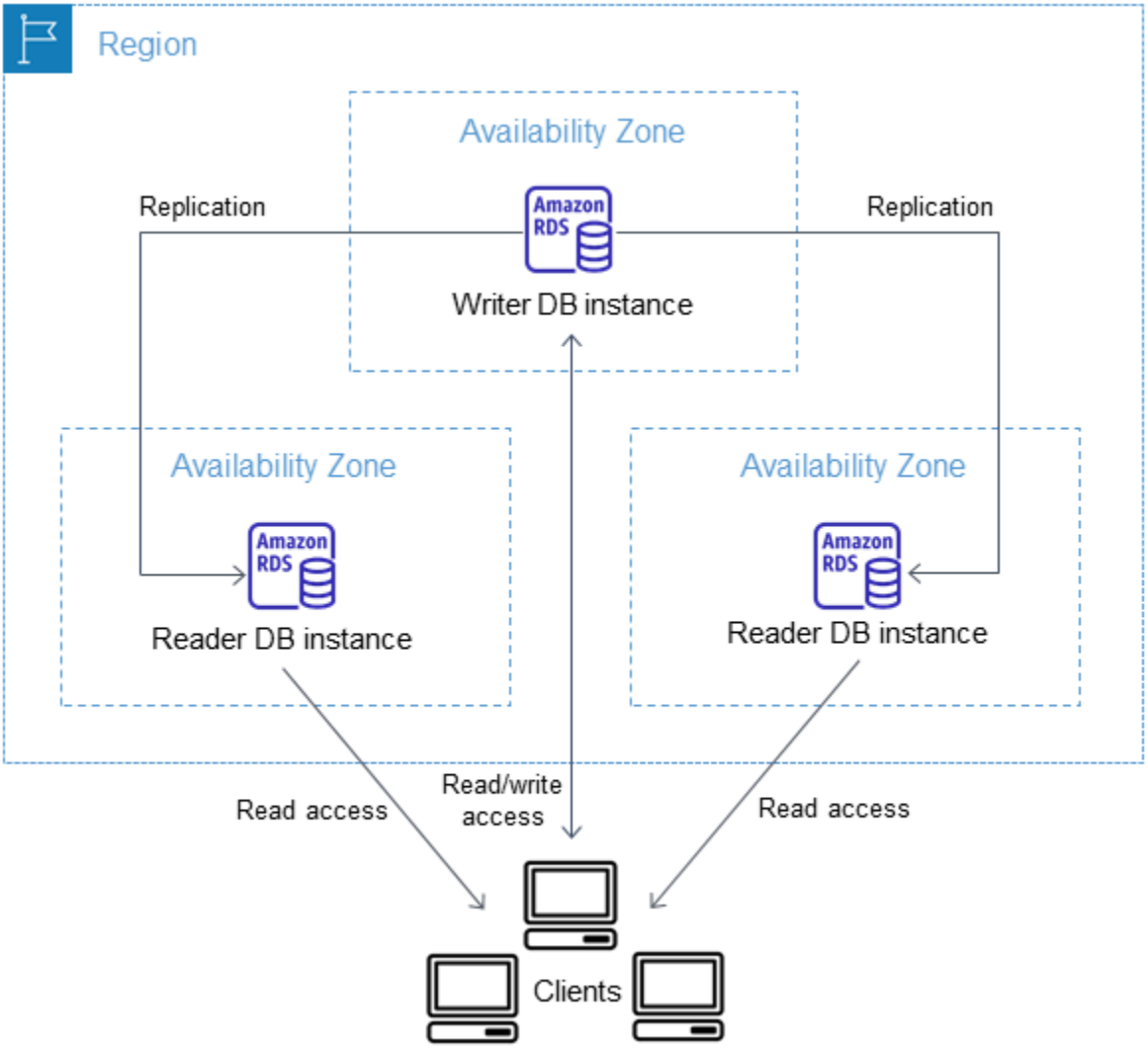
- Soporte de conmutación por error y redundancia de datos
- Eliminación de bloqueos de E/S
- Minimización de los picos de latencia durante las copias de seguridad del sistema
- Servicio de tráfico de lectura en instancias de base de datos secundarias (solo en implementación de clústeres de base de datos Multi-AZ)

El siguiente diagrama muestra una implementación de instancia de base de datos Multi-AZ donde Amazon RDS aprovisiona y mantiene automáticamente una réplica síncrona en espera dentro de una zona de disponibilidad diferente. La base de datos de réplica no gestiona tráfico de lectura.



El siguiente diagrama muestra una implementación de clúster de base de datos Multi-AZ que tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas

de disponibilidad diferentes dentro de la misma Región de AWS. Las tres instancias de base de datos pueden gestionar tráfico de lectura.



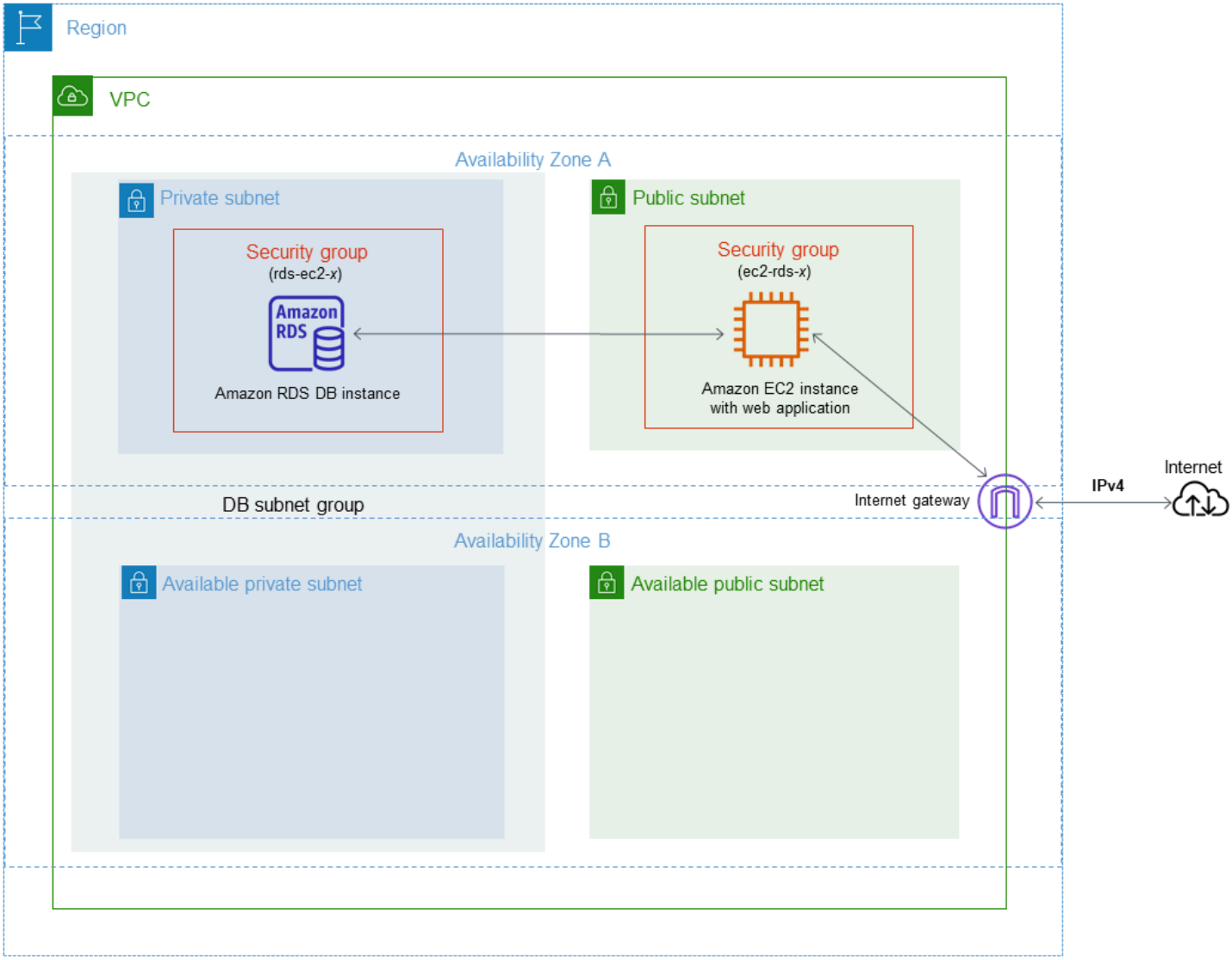
Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Control de acceso con grupos de seguridad

Un grupo de seguridad controla el acceso a una instancia de base de datos permitiendo el acceso a intervalos de direcciones IP o instancias de Amazon EC2 que usted especifique. Puede aplicar un grupo de seguridad en una o más instancias de base de datos.

Un uso común de una instancia de base de datos en una VPC consiste en compartir datos con un servidor de aplicaciones en la misma VPC. En el siguiente ejemplo, se usa un grupo de seguridad `ec2-rds-`*x* de VPC para definir reglas de entrada que utilicen las direcciones IP de la aplicación

cliente como origen. El servidor de aplicaciones pertenece a este grupo de seguridad. Un segundo grupo de seguridad denominado `rds-ec2-x` especifica a `ec2-rds-x` como origen y se conecta a una instancia de base de datos de RDS. De acuerdo con las reglas del grupo de seguridad, las aplicaciones cliente no pueden acceder directamente a la instancia de base de datos, pero la instancia EC2 sí que puede acceder.



Para obtener más información acerca de los grupos de seguridad, consulte Seguridad en Amazon RDS.

Supervisión de Amazon RDS

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon RDS y de otras soluciones de AWS. AWS ofrece diversas herramientas de

monitorización para vigilar a Amazon RDS, informar cuando algo no funciona y tomar medidas de manera automática cuando corresponda.

Puede hacer un seguimiento del rendimiento y el estado de sus instancias de base de datos con varias herramientas manuales y automatizadas:

Estado y recomendaciones de la instancia de base de datos de Amazon RDS

Consulte los detalles sobre el estado actual de su instancia mediante la consola de Amazon RDS, la AWS CLI o la API de RDS. También puede responder a recomendaciones automatizadas para recursos de base de datos, como instancias de base de datos, réplicas de lectura y grupos de parámetros de base de datos. Para obtener más información, consulte Recomendaciones para Amazon RDS.

Métricas de Amazon CloudWatch para Amazon RDS

Puede utilizar el servicio de Amazon CloudWatch para monitorear el rendimiento y el estado de una instancia de base de datos. Los gráficos de rendimiento de CloudWatch se muestran en la consola de Amazon RDS. Amazon RDS envía métricas automáticamente a CloudWatch cada minuto a todas las bases de datos activas. No se cobran cargos adicionales por métricas de Amazon RDS en CloudWatch.

Con las alarmas de Amazon CloudWatch puede ver una métrica determinada de Amazon RDS durante un periodo de tiempo específico. A continuación, puede realizar una o varias acciones en función del valor de la métrica en relación al umbral establecido. Para obtener más información, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.

Supervisión del sistema operativo e Información de rendimiento de Amazon RDS

Información de rendimiento evalúa la carga en su base de datos y determina cuándo y dónde tomar medidas. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS. La monitorización mejorada de Amazon RDS consulta las métricas en tiempo real para el sistema operativo. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Servicios de AWS integrados

Amazon RDS está integrado con Amazon EventBridge, Registros de Amazon CloudWatch y Amazon DevOps Guru. Para obtener más información, consulte Supervisión de métricas en una instancia de Amazon RDS.

Interfaces de usuario para Amazon RDS

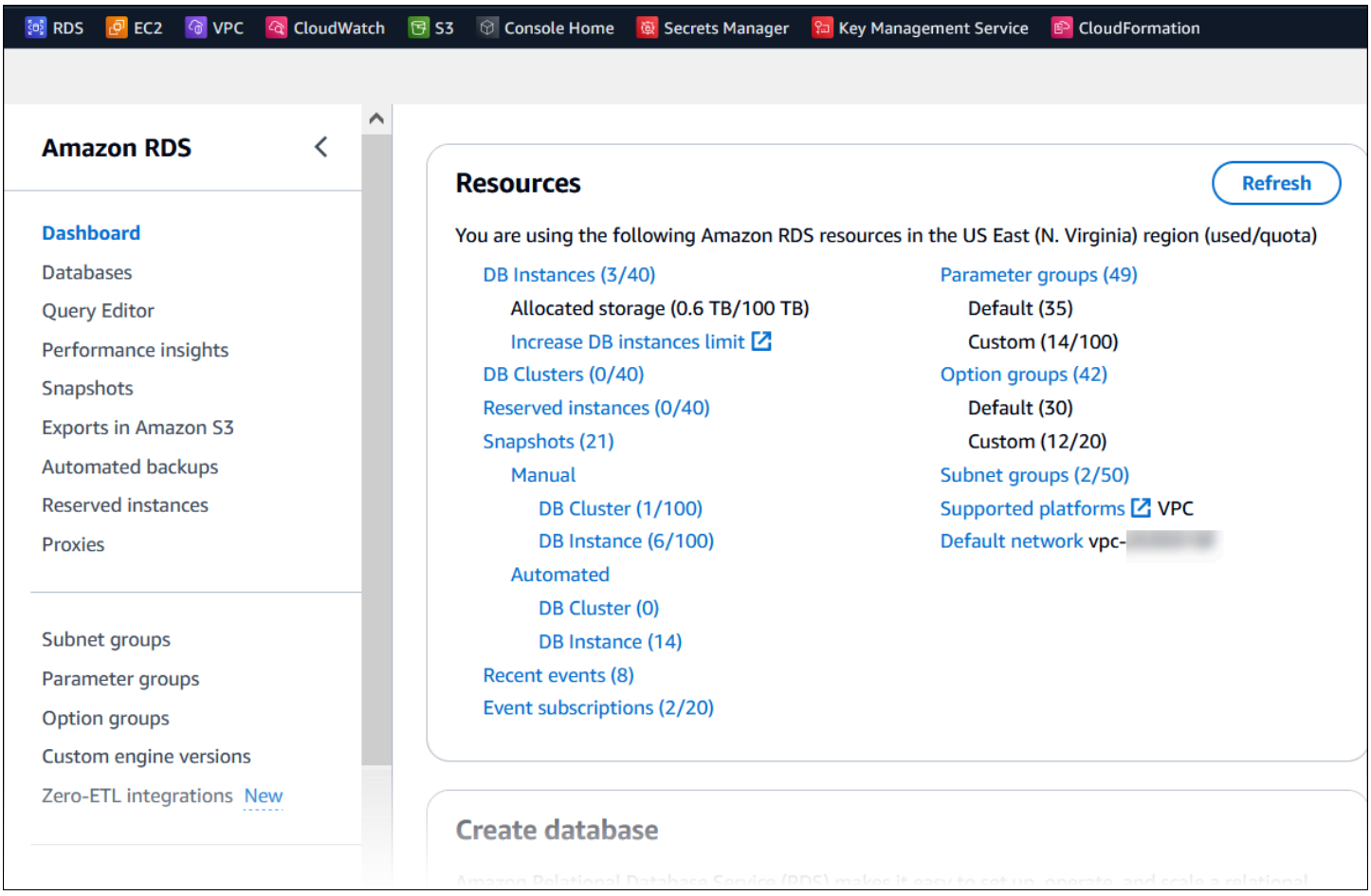
Puede interactuar con Amazon RDS de varias maneras.

Temas

- AWS Management Console
- La interfaz de línea de comandos
- API de Amazon RDS

AWS Management Console

La AWS Management Console es una interfaz de usuario sencilla y basada en web. Desde la consola puede administrar sus instancias de base de datos sin necesidad de programación. Para acceder a la consola de Amazon RDS, inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.



La interfaz de línea de comandos

Puede utilizar la AWS Command Line Interface (AWS CLI) para acceder a la API de Amazon RDS de forma interactiva. Para instalar el AWS CLI, consulte Instalación de la interfaz de línea de AWS comandos. Para empezar a utilizar la AWS CLI para RDS, consulte la referencia de la AWS Command Line Interface para Amazon RDS.

API de Amazon RDS

Si es desarrollador, puede acceder a Amazon RDS mediante programación con API. Para obtener más información, consulte Referencia de la API de Amazon RDS.

Para el desarrollo de aplicaciones le recomendamos que utilice uno de los kits de desarrollo de software (SDK) de AWS. Los AWS SDK gestionan detalles de bajo nivel como la autenticación, la lógica de reintento y la gestión de errores, para que pueda centrarse en la lógica de la aplicación. AWS Los SDK están disponibles en una amplia variedad de idiomas. Para obtener más información, consulte Herramientas para Amazon Web Services .

AWS también proporciona bibliotecas, código de muestra, tutoriales y otros recursos para ayudarlo a comenzar con mayor facilidad. Para obtener más información, consulte Código de muestra y bibliotecas.

Cómo se le cobra Amazon RDS

Cuando usa Amazon RDS, puede elegir instancias de base de datos bajo demanda o instancias de base de datos reservadas. Para obtener más información, consulte Facturación de instancia de base de datos para Amazon RDS.

Para obtener información acerca de los precios de Amazon RDS, consulte la página del producto de Amazon RDS.

capa gratuita de AWS en Amazon RDS

Puede usar capa gratuita de AWS en Amazon RDS con los siguientes motores y clases de instancias de base de datos:

- Tipos de motores: MariaDB, MySQL, PostgreSQL o SQL Server Express Edition

- Clases de instancia de base de datos
  - t3.micro: para todos los tipos de motores
  - t4g.micro: para todos los tipos de motores excepto SQL Server Express Edition

No puede utilizar las siguientes características, recursos y acciones con capa gratuita de AWS en Amazon RDS:

- Opciones de motor de Amazon RDS Custom
- Instancias de base de datos reservadas
- Opciones de implementación distintas a las de Single-AZ
- Migración de instantáneas
- Editor de consultas
- Creación de réplicas de lectura de Aurora

Estas limitaciones están sujetas a cambios a medida que el programa capa gratuita de AWS evoluciona. Para obtener más información acerca de capa gratuita de AWS, consulte Explorar los servicios de AWS con capa gratuita de AWS. Para obtener más información sobre el nivel gratuito de Amazon RDS, consulte Nivel gratuito de Amazon RDS.

Si era cliente de capa gratuita de AWS antes del 17 de julio de 2025, puede seguir utilizando el nivel gratuito de Amazon RDS hasta que expiren los 12 meses de uso gratuito. Durante este periodo, seguirá siendo elegible para el siguiente uso:

- 750 horas al mes de clases de instancias db.t3.micro y db.t4g.micro de Single-AZ que ejecutan MySQL, MariaDB o PostgreSQL en Amazon RDS
- 750 horas al mes de una clase de instancia db.t3.micro que ejecute SQL Server Express Edition en Amazon RDS

A partir del 17 de julio de 2025, los recursos de capa gratuita de AWS nuevos que cree en AWS utilizarán la nueva oferta de capa gratuita de AWS.

Siguientes pasos

En la sección anterior se han presentado los componentes de la infraestructura básica ofrecidos por RDS. ¿Qué debería hacer a continuación?

Introducción

Cree una instancia de base de datos siguiendo las instrucciones de Introducción a Amazon RDS.

Temas específicos de los motores de bases de datos

Puede revisar información específica de un motor de base de datos determinado en las siguientes secciones:

- Amazon RDS para Db2
- Amazon RDS para MariaDB
- Amazon RDS for Microsoft SQL Server
- Amazon RDS para MySQL
- Amazon RDS para Oracle
- Amazon RDS para PostgreSQL

Instancias de base de datos de Amazon RDS

Una instancia de base de datos es un entorno de base de datos aislado que se ejecuta en la nube. Es el componente básico de Amazon RDS. Una instancia de base de datos puede contener varias bases de datos creadas por el usuario y se puede obtener acceso a ella utilizando las mismas herramientas y aplicaciones cliente que podría usar para obtener acceso a una instancia de base de datos individual. Las instancias de base de datos se pueden crear y modificar fácilmente con las herramientas de línea de comandos AWS, las operaciones de la API de Amazon RDS o la AWS Management Console.

> **Note**
>
> Amazon RDS permite el acceso a las bases de datos mediante cualquier aplicación cliente de SQL estándar. Amazon RDS no permite el acceso directo de host excepto con RDS Custom.

Puede tener hasta 40 instancias de base de datos de Amazon RDS, con las siguientes limitaciones:

- 10 para cada edición de SQL Server (Enterprise, Standard, Web y Express) bajo el modelo «licencia incluida»
- 10 para Oracle bajo el modelo «licencia incluida»
- 40 para Db2 según el modelo de licencia “traiga su propia licencia” (BYOL).
- 40 para MySQL, MariaDB o PostgreSQL
- 40 para Oracle según el modelo de licencia "bring-your-own-license" (BYOL).

> **Note**
>
> Si su aplicación requiere más instancias de base de datos, puede solicitar instancias de base de datos adicionales usando este formulario.

Cada instancia de base de datos tiene un identificador de instancias de bases de datos. Este nombre suministrado por el cliente identifica de forma única la instancia de base de datos cuando se interactúa con la API de Amazon RDS y los comandos de la AWS CLI. El identificador de instancias de bases de datos debe ser único para ese cliente en una región de AWS.

El identificador de instancia de base de datos se utiliza como parte del nombre de host de DNS asignado por RDS a su instancia. Por ejemplo, si especifica db1 como identificador de instancia de base de datos, RDS asignará automáticamente un punto de conexión de DNS a su instancia. Un ejemplo de punto de conexión es *db1*.*abcdefghijkl*.*us-east-1*.rds.amazonaws.com, donde *db1* es su ID de instancia.

En el ejemplo de punto de conexión *db1*.*abcdefghijkl*.*us-east-1*.rds.amazonaws.com, la cadena *abcdefghijkl* es un identificador único para una combinación específica de Región de AWS y Cuenta de AWS. RDS genera internamente el identificador *abcdefghijkl* en el ejemplo, que no cambia para la combinación especificada de región y cuenta. Por lo tanto, todas las instancias de base de datos de esta región comparten el mismo identificador fijo. Tenga en cuenta las siguientes características del identificador fijo:

- Si cambia el nombre de la instancia de base de datos, el punto de conexión es diferente, pero el identificador fijo es el mismo. Por ejemplo, si cambia el nombre *db1* a *renamed-db1*, el punto de conexión de la nueva instancia es *renamed-db1*.*abcdefghijkl*.*us-east-1*.rds.amazonaws.com.
- Si elimina y vuelve a crear una instancia de base de datos con el mismo identificador de instancia de base de datos, el punto de conexión es el mismo.
- Si utiliza la misma cuenta para crear una instancia de base de datos en una región diferente, el identificador generado internamente es diferente porque la región es diferente, como en *db2*.*mnopqrstuvwx*.*us-west-1*.rds.amazonaws.com.

Cada instancia de base de datos admite un motor de base de datos. Amazon RDS es compatible actualmente con los motores de base de datos de Db2, MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server y Amazon Aurora.

Cuando se crea una instancia de base de datos, algunos motores de base de datos requieren que se especifique un nombre de base de datos. Una instancia de base de datos puede alojar varias bases de datos o una única base de datos de Oracle con varios esquemas. El valor del nombre de la base de datos depende del motor de base de datos:

- Para el motor de base de datos de Db2, el nombre de la base de datos es el nombre de una base de datos alojada en la instancia de base de datos. Este campo es opcional. Puede crear la base de datos más tarde llamando al procedimiento `rdsadmin.create_database` almacenado. Para obtener más información, consulte the section called “Creación de una base de datos”.

- Para los motores de base de datos de MySQL y MariaDB, el nombre de la base de datos es el nombre de una base de datos alojada en la instancia de base de datos. Las bases de datos alojadas en la misma instancia de base de datos deben tener un nombre único en esa instancia.
- Para el motor de base de datos de Oracle, el nombre de base de datos se usa para definir el valor de ORACLE_SID, que se debe suministrar al conectar a la instancia de RDS de Oracle.
- Para el motor de base de datos de Microsoft SQL Server, el nombre de base de datos no es un parámetro admitido.
- Para el motor de base de datos de PostgreSQL, el nombre de la base de datos es el nombre de una base de datos alojada en la instancia de base de datos. No se requiere un nombre de base de datos cuando se crea una instancia de base de datos. Las bases de datos alojadas en la misma instancia de base de datos deben tener un nombre único en esa instancia.

Amazon RDS crea una cuenta de usuario maestro para su instancia de base de datos como parte del proceso de creación. Este usuario maestro tiene permisos para crear bases de datos y para realizar operaciones de creación, eliminación, selección, actualización e inserción en las tablas que este crea. Debe definir la contraseña del usuario maestro cuando cree una instancia de base de datos, pero puede cambiarla en cualquier momento mediante la AWS CLI, las operaciones de la API de Amazon RDS o la AWS Management Console. También puede cambiar la contraseña del usuario maestro y administrar a los usuarios por medio de comandos SQL estándar.

> **Note**
>
> Esta guía cubre motores de base de datos de Amazon RDS que no sean de Aurora. Para obtener información acerca de cómo usar Amazon Aurora, consulte la Guía del usuario de Amazon Aurora.

Clases de instancia de base de datos de

La clase de instancia de base de datos determina la capacidad de computación y de memoria de una instancia de base de datos de Amazon RDS. La clase de instancia de base de datos que se necesite dependerá de la potencia de procesamiento y de los requisitos de memoria.

Una clase de instancia de base de datos determina tanto el tamaño como el tipo de clase de instancia de base de datos. Por ejemplo, db.r6g es una clase de instancia de base de datos de memoria optimizada con tecnología de procesadores Graviton2 de AWS. Dentro del tipo de clase de instancia db.r6g, db.r6g.2xlarge es una clase de instancia de base de datos. El tamaño de esta clase es 2xlarge.

Para obtener más información acerca de los precios de las clases de instancias, consulte Precios de Amazon RDS.

Para obtener más información sobre los tipos de clases de instancias de base de datos, los motores de base de datos compatibles, las Regiones de AWS compatibles, el cambio de la clase de instancia de base de datos, la configuración del procesador para RDS para Oracle o las especificaciones de hardware para las clases de instancias de base de datos, consulte las siguientes secciones.

Temas

- Tipos de clase de instancia de base de datos
- Motores de base de datos compatibles para clases de instancia de base de datos
- Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS
- Cambio de clase de instancia de base de datos
- Configuración del procesador de una clase de instancias de base de datos en RDS para Oracle
- Especificaciones de hardware para clases de instancia de base de datos

Tipos de clase de instancia de base de datos

Amazon RDS admite las clases de instancia de base de datos para los siguientes casos de uso:

- Uso general
- Optimizada para memoria
- Optimizada para computación
- Rendimiento ampliable

- Lecturas optimizadas

Para obtener más información sobre los tipos de instancias de Amazon EC2, consulte Tipos de instancia en la documentación de Amazon EC2.

Tipos de clases de instancias de uso general

A continuación, se indican las clases de instancias de bases de datos de uso general que hay disponibles:

- db.m8g: clases de instancia de base de datos de uso general con tecnología de procesadores Graviton4 de AWS. Estas clases de instancia ofrecen un conjunto equilibrado de recursos informáticos, de memoria y de redes para un rango amplio de cargas de trabajo de uso general. En comparación con las instancias M7g de séptima generación de AWS basadas en Graviton3, estas nuevas clases ofrecen tamaños de instancia más grandes con hasta tres veces más vCPU y memoria.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Graviton4 de AWS. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.m7i: clases de instancia de base de datos de uso general con procesadores Intel Xeon Scalable de cuarta generación. Las instancias db.m7i tienen la certificación de SAP y son ideales para aplicaciones empresariales que necesitan instancias de mayor tamaño o un uso continuo elevado de la CPU. Estas clases de instancia ofrecen un conjunto equilibrado de recursos informáticos, de memoria y de redes para un rango amplio de cargas de trabajo de uso general. Este tipo de clase de instancia ofrece un ancho de banda EBS de hasta 40 000 Mbps y un ancho de banda de la red de hasta 50 Gbps. Las instancias db.m7i ofrecen un rendimiento hasta un 15 % mejor en cuanto a precio en comparación con las instancias db.m6i.
- db.m7g: clases de instancias de base de datos de uso general con tecnología de procesadores AWS Graviton3. Estas clases de instancia ofrecen un conjunto equilibrado de recursos informáticos, de memoria y de redes para un rango amplio de cargas de trabajo de uso general.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores AWS Graviton3. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.m6g: clases de instancia de base de datos de uso general con tecnología de procesadores Graviton2 de AWS. Estas instancias ofrecen un conjunto equilibrado de recursos de computación,

de memoria y de redes para un rango amplio de cargas de trabajo de uso general. Las clases de instancia db.m6gd tienen almacenamiento local a nivel de bloque SSD basado en NVMe para aplicaciones que necesitan almacenamiento local de alta velocidad y baja latencia.

Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Graviton2 AWS. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.

- db.m6i: clases de instancia de base de datos de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación. Estas instancias cuentan con la certificación SAP y son ideales para cargas de trabajo como servidores backend compatibles con aplicaciones empresariales, servidores de juegos, flotas de almacenamiento en caché y entornos de desarrollo de aplicaciones. Las clases de instancia db.m6id y db.m6idn ofrecen hasta 7,6 TB de almacenamiento local SSD basado en NVMe, mientras que db.m6in ofrece almacenamiento solo para EBS. Las clases db.m6in y db.m6idn ofrecen hasta 200 Gbps de ancho de banda de la red.
- db.m5: clases de instancia de base de datos de uso general que proporcionan un equilibrio entre computación, memoria y recursos de red, y que son una buena elección para muchas aplicaciones. La clase de instancia db.m5d ofrece almacenamiento SSD basado en NVMe que está conectado físicamente al servidor host. Las clases de instancia db.m5 proporcionan más capacidad de computación que las clases de instancia db.m4 anteriores. Con tecnología del nuevo sistema Nitro AWS, una combinación de hardware dedicado e hipervisor ligero.
- db.m4: clases de instancia de base de datos de propósito general que proporcionan más capacidad informática que las clases de instancia db.m3 anteriores.

  En el caso de los motores de base de datos de RDS para Oracle, Amazon RDS ya no admite las clases de instancia de base de datos db.m4. Si ha creado anteriormente instancias de bases de datos db.m4 de RDS para Oracle, Amazon RDS actualiza automáticamente aquellas instancias de base de datos a clases de instancia de base de datos db.m5 equivalentes.

  Para los motores de base de datos RDS para MariaDB, RDS para MySQL, RDS para SQL Server y RDS para PostgreSQL, Amazon RDS ha iniciado el proceso de fin de soporte de esta clase de instancia de base de datos con el siguiente calendario. Para todas las instancias de base de datos de RDS que utilicen esta clase de instancia, recomendamos que actualice a una clase de instancia de base de datos de una generación posterior lo antes posible.

Acción o recomendación	Date
A partir de esta fecha, Amazon RDS comenzó a actualizar automáticamente las instancias que utilizan db.m4 a la clase de instancias db.m5 de generación posterior. Ya no se admite la creación de instancias de base de datos con la clase de instancias db.m4.	1 de junio de 2024
Amazon RDS finaliza el soporte para db.m4.	31 de diciembre de 2024

- db.m3: clases de instancia de base de datos de propósito general que proporcionan más capacidad informática que las clases de instancia db.m1 anteriores.

  Para los motores de base de datos RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL, Amazon RDS ha iniciado el proceso de fin de vida útil de las clases de instancia de base de datos de db.m3 con el siguiente calendario, que incluye recomendaciones de actualización. Para todas las instancias de base de datos de RDS que utilicen clases de instancia de base de datos db.m3, recomendamos que actualice a una clase de base de datos de una generación superior lo antes posible.

Acción o recomendación	Fechas
Ya no puede crear instancias de base de datos de RDS que utilicen las clases de instancia de base de datos db.m3.	Ahora
Amazon RDS ha iniciado las actualizaciones automáticas de instancias de base de datos de RDS que utilicen clases de instancia de base de datos db.m3 para clases de instancias de base de datos equivalentes a la db.m5.	1 de febrero de 2023

Tipos de clases de instancias optimizadas para memoria

La familia Z optimizada para memoria admite los siguientes tipos de clases de instancias:

- db.z1d: clases de instancia optimizadas para aplicaciones de uso intensivo de la memoria. Estas clases de instancia ofrecen una alta capacidad informática y recursos de alta memoria. Las instancias z1d de alta frecuencia ofrecen una frecuencia constante para todos los núcleos de hasta 4,0 GHz.

La familia X optimizada para memoria admite los siguientes tipos de clases de instancias:

- db.x2g: clases de instancia optimizadas para aplicaciones con gran uso de la memoria y con la tecnología de los procesadores Graviton2 de AWS. Estas clases de instancias ofrecen un bajo costo por GiB de memoria.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Graviton2 AWS. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.x2i: clases de instancia optimizadas para aplicaciones con uso intensivo de la memoria. Los tipos de clases de instancias db.x2iedn y db.x2idn cuentan con tecnología de procesadores Intel Xeon Scalable de tercera generación (Ice Lake). Incluyen hasta 3,8 TB de almacenamiento SSD NVMe local, hasta 100 Gbps de ancho de banda de la red y hasta 4 TiB (db.x2iden) o 2 TiB (db.x2idn) de memoria. El tipo db.x2iezn cuenta con procesadores Intel Xeon Scalable de segunda generación (Cascade Lake) con una frecuencia turbo para todos los núcleos de hasta 4,5 GHz y 1,5 TiB de memoria.
- db.x1 – Clases de instancia optimizadas para aplicaciones con uso intensivo de la memoria. Estas clases de instancia ofrecen uno de los precios más bajos por GiB de RAM de entre las clases de instancias de base de datos y hasta 1 952 GiB de memoria DRAM de la instancia. El tipo de clase de instancia db.x1e ofrece hasta 3 904 GiB de memoria de instancia basada en DRAM.

La familia R optimizada para memoria admite los siguientes tipos de clases de instancias:

- db.r8g: clases de instancia con tecnología de procesadores Graviton4 de AWS. Estas clases de instancia son idóneas para ejecutar cargas de trabajo de uso intensivo de memoria en bases de datos de código abierto como MySQL y PostgreSQL. Estas instancias ofrecen tamaños de instancia más grandes con hasta tres veces más vCPU y memoria que las instancias db.r7g de séptima generación basadas en Graviton3 de AWS.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Graviton4 de AWS. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.

- db.r7g: clases de instancias con tecnología de procesadores AWS Graviton3. Estas clases de instancia son idóneas para ejecutar cargas de trabajo de uso intensivo de memoria en bases de datos de código abierto como MySQL y PostgreSQL.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores AWS Graviton3. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.r7i: clases de instancia con tecnología de procesadores Intel Xeon Scalable de cuarta generación. Estas clases de instancia cuentan con certificación SAP y son idóneas para cargas de trabajo de uso intensivo de memoria en bases de datos de código abierto como MySQL y PostgreSQL. Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Intel Xeon Scalable de cuarta generación. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.r6g: clases de instancia con tecnología de procesadores Graviton2 de AWS. Estas clases de instancia son idóneas para ejecutar cargas de trabajo de uso intensivo de memoria en bases de datos de código abierto como MySQL y PostgreSQL. El tipo db.r6gd ofrece almacenamiento local a nivel de bloque SSD basado en NVMe para aplicaciones que necesitan almacenamiento local de alta velocidad y baja latencia.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Graviton2 AWS. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.r6i: clases de instancia con tecnología de procesadores Intel Xeon Scalable de 3.ª generación. Estas clases de instancia cuentan con certificación SAP y son idóneas para cargas de trabajo de uso intensivo de memoria en bases de datos de código abierto como MySQL y PostgreSQL. Las clases de instancias db.r6id, db.r6in y db.r6idn tienen una relación entre memoria y vCPU de 8:1 y una memoria máxima de 1 TiB. Las clases db.r6id y db.r6idn ofrecen hasta 7,6 TB de almacenamiento SSD basado en NVMe con conexión directa, mientras que db.r6in ofrece almacenamiento solo para EBS. Las clases db.r6idn y db.r6in ofrecen hasta 200 Gbps de ancho de banda de la red.
- db.r5b – Clases de instancia optimizadas destinadas a la memoria para aplicaciones que requieren un rendimiento intensivo. Con el sistema Nitro AWS, las instancias db.r5b ofrecen un ancho de banda de hasta 60 Gbps y 260 000 IOPS de rendimiento EBS. Este es el rendimiento de almacenamiento en bloques más rápido de EC2.

- db.r5d: clases de instancia optimizadas para una latencia baja, un rendimiento de E/S aleatorio muy alto y un alto rendimiento de lectura secuencial.
- db.r4: clases de instancia optimizadas para aplicaciones de uso intensivo de la memoria. Estas clases de instancia ofrecen un rendimiento mejorado en redes . Con tecnología del nuevo sistema Nitro AWS, una combinación de hardware dedicado e hipervisor ligero.
- db.r4: clases de instancia que proporcionan redes mejoradas en comparación con las clases de instancias db.r3 anteriores.

  En el caso de los motores de RDS para Oracle DB, Amazon RDS ha iniciado el proceso de fin de vida útil de las clases de instancia de base de datos db.r4 con el siguiente calendario, que incluye recomendaciones de actualización. Para las instancias de RDS para Oracle DB que utilicen clases de instancia db.r4, recomendamos que actualice a una clase de base de datos de una generación superior lo antes posible.

Acción o recomendación	Fechas
Ya no puede crear instancias de RDS para Oracle DB que utilicen las clases de instancia de base de datos db.r4.	Ahora
Amazon RDS ha iniciado actualizaciones automáticas de instancias de base de datos de RDS para Oracle que utilizan clases de instancia de base de datos db.r4 a clases de instancias de base de datos equivalentes a la db.r5.	17 de abril de 2023

  Para los motores de base de datos RDS para MariaDB, RDS para MySQL, RDS para SQL Server y RDS para PostgreSQL, Amazon RDS ha iniciado el proceso de fin de soporte de esta clase de instancia de base de datos con el siguiente calendario. Para todas las instancias de base de datos de RDS que utilicen esta clase de instancia, recomendamos que actualice a una clase de instancia de base de datos de una generación posterior lo antes posible.

Acción o recomendación	Fechas
A partir de esta fecha, Amazon RDS comenzó a actualizar automáticamente las instancias que utilizan db.r4 a la clase de instancias db.r5 de generación posterior. Ya no se admite la creación de instancias de base de datos con la clase de instancias db.m4.	1 de junio de 2024
Amazon RDS finaliza el soporte para db.r4.	31 de diciembre de 2024

- db.r3: clases de instancia que proporcionan optimización de la memoria.

  Para los motores de base de datos RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL, Amazon RDS ha iniciado el proceso de fin de vida útil de las clases de instancia de base de datos de db.r3 con el siguiente calendario, que incluye recomendaciones de actualización. Para todas las instancias de base de datos de RDS que utilicen clases de instancia de base de datos db.r3, recomendamos que actualice a una clase de base de datos de una generación superior lo antes posible.

Acción o recomendación	Fechas
Ya no puede crear instancias de base de datos de RDS que utilicen las clases de instancia de base de datos db.r3.	Ahora
Amazon RDS ha iniciado las actualizaciones automáticas de instancias de base de datos de RDS que utilicen clases de instancia de base de datos db.r3 a clases de instancias de base de datos equivalentes a la db.r5.	1 de febrero de 2023

Tipo de clase de instancia optimizada para la computación

Hay disponibles los siguientes tipos de clases de instancias optimizadas para la computación:

- db.c6gd: clases de instancias ideales para ejecutar cargas de trabajo de uso intensivo de computación. Este tipo de instancia, basado en los procesadores AWS Graviton2, ofrece almacenamiento por bloques SSD local basado en NVMe para aplicaciones que necesitan almacenamiento local de alta velocidad y baja latencia.

> **Note**
>
> Las clases de instancias c6gd solo se admiten para implementaciones de clústeres de base de datos multi-AZ. Son la única clase de instancia que se admite para clústeres de base de datos multi-AZ que ofrecen el tamaño de instancia `medium`. Para obtener más información, consulte the section called “Implementaciones de clústeres de base de datos Multi-AZ”.

Tipos de clases de instancias de rendimiento ampliable

A continuación, se indican los tipos de clase de instancia de base de datos de rendimiento ampliable disponibles:

- db.t4g: clases de instancia de uso general con la tecnología de los procesadores Graviton2 de AWS basados en ARM. Estas clases de instancia ofrecen un mejor rendimiento que las clases de instancia de base de datos de rendimiento ampliable anteriores para un amplio conjunto de cargas de trabajo de uso general ampliable. Las instancias db.t4g de Amazon RDS están configuradas para el modo ilimitado. Esto significa que pueden ampliarse más allá de la línea base en una ventana de 24 horas con cargo adicional.

  Puede modificar una instancia de base de datos para que utilice una de las clases de instancia de base de datos con tecnología de procesadores Graviton2 AWS. Para ello, siga los mismos pasos que con cualquier otra modificación de la instancia de base de datos.
- db.t3: clases de instancias que proporcionan un nivel de rendimiento de referencia con la capacidad de transmitir ráfagas que usen la totalidad de la CPU. Las instancias db.t3 están configuradas para el modo ilimitado. Las clases de instancia proporcionan más capacidad de computación que las clases de instancia db.t2 anteriores. Con tecnología del nuevo sistema Nitro AWS, una combinación de hardware dedicado e hipervisor ligero.
- db.t2: clases de instancias que proporcionan un nivel de desempeño de referencia con la capacidad de transmitir ráfagas que usen la totalidad de la CPU. Las instancias db.t2 están configuradas para el modo ilimitado. Recomendamos que se usen estas clases de instancia solo

para los servidores de desarrollo y de pruebas, o para otros servidores que no se utilicen para la producción.

Para los motores de base de datos RDS para MariaDB, RDS para MySQL, RDS para SQL Server y RDS para PostgreSQL, Amazon RDS ha iniciado el proceso de fin de soporte de esta clase de instancia de base de datos con el siguiente calendario. Para todas las instancias de base de datos de RDS que utilicen esta clase de instancia, recomendamos que actualice a una clase de instancia de base de datos de una generación posterior lo antes posible.

Acción o recomendación	Fechas
A partir de esta fecha, Amazon RDS comenzó a actualizar automáticamente las instancias que utilizan db.t2 a la clase de instancias db.t3 de nueva generación. Ya no se admite la creación de instancias de base de datos con la clase de instancias db.t2.	1 de junio de 2024
Amazon RDS finaliza el soporte para db.t2.	31 de diciembre de 2024

> **Note**
>
> Las clases de instancia de base de datos que utilizan el sistemaAWS Nitro (db.m5, db.r5, db.t3) se ven reguladas en la carga de trabajo combinada de lectura y escritura.

Para las especificaciones de hardware de clase de instancia de base de datos, consulte Especificaciones de hardware para clases de instancia de base de datos .

Tipos de clase de instancia de lecturas optimizadas

Los siguientes tipos de clases de instancia de lecturas optimizadas están disponibles:

- db.r6g: tipo de instancia con tecnología de procesadores Graviton2 de AWS. Estas clases de instancia son ideales para ejecutar cargas de trabajo con un gran uso de memoria, y ofrecen almacenamiento local en el nivel de bloque SSD basado en NVMe para aplicaciones que necesitan almacenamiento local de alta velocidad y baja latencia.

- db.r6id: clases de instancia con tecnología de procesadores Intel Xeon Scalable de 3.ª generación. Estas clases de instancias cuentan con certificación SAP y son idóneas para cargas de trabajo de uso intensivo de memoria en bases de datos de código abierto como MySQL y PostgreSQL. Ofrecen una memoria máxima de 1 TiB y hasta 7,6 TB de almacenamiento SSD basado en NVMe con conexión directa.

Motores de base de datos compatibles para clases de instancia de base de datos

A continuación se muestran las consideraciones específicas del motor de base de datos para las clases de instancia de base de datos:

Db2

La compatibilidad con la clase de instancia de base de datos varía en función de la versión y la edición de Db2. Para ver la clase de instancia admitida por versión y edición, consulte Amazon RDS para clases de instancia de Db2.

Microsoft SQL Server

La compatibilidad con la clase de instancia de base de datos varía en función de la versión y la edición de SQL Server. Para ver la clase de instancia admitida por versión y edición, consulte Compatibilidad con clases de instancia de base de datos para Microsoft SQL Server.

Oracle

La compatibilidad con la clase de instancia de base de datos varía en función de la versión y edición de Oracle Database. RDS para Oracle admite clases de instancias adicionales y optimizadas para la memoria. Estas clases tienen nombres con el formato db.r5.*instance_size*.tpc*threads_per_core*.mem*ratio*. Para obtener información sobre el recuento de vCPU y la asignación de memoria para cada clase optimizada, consulte Clases de instancias admitidas de RDS para Oracle.

RDS personalizado

Para obtener más información sobre las clases de instancia de bases de datos admitidas en RDS Custom, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle y Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL.

En la siguiente tabla, podrá encontrar detalles sobre las clases de instancia de base de datos de Amazon RDS compatibles para cada motor de base de datos de Amazon RDS. La celda de cada motor contiene uno de los siguientes valores:

Sí

La clase de instancia es compatible con todas las versiones del motor de base de datos.

No

La clase de instancia no es compatible con el motor de base de datos.

specific-versions

La clase de instancia es compatible solo con las versiones de base de datos especificadas del motor de base de datos.

Amazon RDS desactiva periódicamente las versiones principales y secundarias del motor de base de datos. Es posible que no todas las Regiones de AWS sean compatibles con versiones anteriores del motor. Para obtener más información sobre las versiones compatibles actualmente, consulte los temas de cada motor de base de datos: versiones de MariaDB, versiones de Microsoft SQL Server, versiones de MySQL, versiones de Oracle y versiones de PostgreSQL.

Temas

- Motores de base de datos compatibles para clases de instancias de uso general
- Motores de base de datos compatibles para clases de instancias optimizadas para memoria
- Motores de base de datos compatibles para clases de instancias optimizadas para la computación
- Motores de base de datos compatibles para clases de instancia de rendimiento ampliable
- Motores de base de datos compatibles para clases de instancias de lecturas optimizadas

Motores de base de datos compatibles para clases de instancias de uso general

En las tablas siguientes, se muestran las bases de datos y las versiones de bases de datos compatibles para las clases de instancias de uso general.

db.m7g: clases de instancias de uso general con tecnología de procesadores AWS Graviton3

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.m7g.1(xlarge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.m7g.1(xlarge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.m7g.8(large	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.m7g.4(large	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores,	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL,

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
		10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores				la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.m7g.2x large	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.m7g.xl arge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.m7g.la rge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)

db.m6g: clases de instancia de uso general con tecnología de procesadores Graviton2 de AWS.

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6g.1(xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.m6g.1: xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.m6g.8: large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL,

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
						la versión 12.7 y cualquier version 12 posterior
db.m6g.4x large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.m6g.2x large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.m6g.xl arge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.m6g.la rge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

db.m6g: clases de instancias de uso general con tecnología de procesadores Graviton2 de AWS y almacenamiento SSD

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6gd.16xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4
db.m6gd.12xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4
db.m6gd.8xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6gd.4xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4
db.m6gd.2xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4
db.m6gd.xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6gd.grande	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones de PostgreSQL 16, 15 y 14; las versiones 13.7 y versiones 13 posteriores, y la 13.4

db.m6id: clases de instancias de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación y almacenamiento SSD

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6id.32xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6id.24xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
		versiones 10.4 posterior es				13.7 (y cualquier versión 13 posterior)
db.m6id.16xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posterior es	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6id.12xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posterior es	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6id.8xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posterior es	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6id.4xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6id.2xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6id.xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.m6id.large	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

db.m6idn: clases de instancia de uso general con procesadores escalables Intel Xeon de tercera generación, almacenamiento SSD y optimización de red

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.m6idn.32xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6idn.24xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
		versiones 10.4 posterior es				
db.m6idn. 16xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posterior es	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6idn. 12xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posterior es	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6idn. 8xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posterior es	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.m6idn.4xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6idn.2xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.m6idn.xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.m6idn.large	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

db.m6in: clases de instancias de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación y optimización de red

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.m6in.32xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.m6in.24xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier

Clase de instancia	Db	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
		y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores				versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.m6in.16xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.m6in.12xlarge	No	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.m6in.8xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.m6in.4xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.m6in.2xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.m6in.x large	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.m6in.l arge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versión y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)

db.m6in: clases de instancias de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Db	MariaDB	Micros SQL Serve	MySQL	Oracle	PostgreSQL
db.m6i.32 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Oracle	PostgreSQL
		y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores				12.8 y la versión 11.13 (y cualquier versión 11 posterior)
db.m6i.24 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)
db.m6g.1 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Oracle	PostgreSQL
db.m6i.12 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)
db.m6i.8x large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Oracle	PostgreSQL
db.m6i.4x large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)
db.m6i.2x large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posterior es	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Oracle	PostgreSQL
db.m6i.xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posteriores	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)
db.m6i.large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.15 y versiones 10.5 posteriores y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL versió y posteriores	Oracle Databa 19c	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4, la versión 12.8 y la versión 11.13 (y cualquier versión 11 posterior)

db.m5d: clases de instancias de uso general con tecnología de procesadores Intel Xeon Platinum y almacenamiento SSD

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m5d.24xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.m5d.16xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.m5d.12xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.m5d.8xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y	Sí	MySQL 8.0 y	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
		versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores		posteriores		14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.m5d.4xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.m5d.2xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m5d.xlarge	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.m5d.large	No	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL 8.0 y posteriores	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

db.m5: clases de instancias de uso general con procesadores Intel Xeon Platinum de 2,5 GHz

Clase de instancia	Db2	Maria	Microsoft SQL Server	MyS	Oracl	PostgreSQL
db.m5.24x large	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.16x large	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier

Clase de instancia	Db2	Maria	Microsoft SQL Server	MyS	Oracl	PostgreSQL
						versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.12x large	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.8xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.4xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.2xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.m5.large	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)

db.m4: clases de instancias de uso general con procesadores Intel Xeon

Clase de instancia	Db	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m4.16 large	No	Obsoleto	Obsoleto	Obsoleto	Obsol	Obsoleto
db.m4.10 large	No	Obsoleto	Obsoleto	Obsoleto	Obsol	Obsoleto
db.m4.4x arge	No	Obsoleto	Obsoleto	Obsoleto	Obsol	Obsoleto
db.m4.2x arge	No	Obsoleto	Obsoleto	Obsoleto	Obsol	Obsoleto
db.m4.xla rge	No	Obsoleto	Obsoleto	Obsoleto	Obsol	Obsoleto
db.m4.lar ge	No	Obsoleto	Obsoleto	Obsoleto	Obsol	Obsoleto

db.m3: clases de instancia de uso general

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.m3.2xl arge	No	No	Obsoleto	Sí	Obsoleto	Obsoleto
db.m3.xla rge	No	No	Obsoleto	Sí	Obsoleto	Obsoleto
db.m3.lar ge	No	No	Obsoleto	Sí	Obsoleto	Obsoleto
db.m3.med ium	No	No	Obsoleto	Sí	Obsoleto	Obsoleto

Motores de base de datos compatibles para clases de instancias optimizadas para memoria

En las tablas siguientes, se muestran las bases de datos y las versiones de bases de datos compatibles para las clases de instancias optimizadas para memoria.

db.z1d: clases de instancia de memoria optimizada

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.z1d.1 xlarge	No	No	Sí	No	Sí	No
db.z1d.6 large	No	No	Sí	No	Sí	No
db.z1d.3 large	No	No	Sí	No	Sí	No
db.z1d.2 large	No	No	Sí	No	Sí	No
db.z1d.xl arge	No	No	Sí	No	Sí	No
db.z1d.la rge	No	No	Sí	No	Sí	No

db.x2g: clases de instancia optimizada para memoria con tecnología de procesadores Graviton2 de AWS

Clase de instancia	Db	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.x2g.1 xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.x2g.1 xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.x2g.8 large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.x2g.4 large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.x2g.2 large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.x2g.x arge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.x2g.l rge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

db.x2idn: clases de instancia optimizada para memoria con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Dl	MariaDB	Micros SQL Server	MySQL	Oracle	PostgreSQL
db.x2idn.32xlarge	No	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL y posterio es	Solo Enterp e Editior	PostgreSQL versiones 15, 14.6 y 13.9
db.x2idn.24xlarge	No	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL y posterio es	Solo Enterp e Editior	PostgreSQL versiones 15, 14.6 y 13.9
db.x2idn.16xlarge	No	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL y posterio es	Solo Enterp e Editior	PostgreSQL versiones 15, 14.6 y 13.9

db.x2iedn: clases de instancia optimizada para memoria con SSD local basado en NVMe y con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Dl	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x2iedn.32xlarge	Sí	Todas las versiones de MariaDB 10.11,	Solo ediciones	MySQL y	Solo Enterp	Todas las versiones 15 y 16 de PostgreSQ

Clase de instancia	DI	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
		MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Standard y Enterprise, SQL Server 2012.00 y posteriores	posterio es	e Editior	L, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.x2iedn .24xlarge	Sí	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Solo ediciones Standard y Enterprise, SQL Server 2012.00 y posteriores	MySQL y posterio es	Solo Enterp e Editior	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.x2iedn .16xlarge	Sí	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Solo ediciones Standard y Enterprise, SQL Server 2012.00 y posteriores	MySQL y posterio es	Solo Enterp e Editior	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.x2iedn .8xlarge	Sí	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Solo ediciones Standard y Enterprise, SQL Server 2012.00 y posteriores	MySQL y posterio es	Solo Enterp e Editior	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instancia	DI	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x2iedn .4xlarge	Sí	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Solo ediciones Standard y Enterprise, SQL Server 2012.00 y posteriores	MySQL 8.0.28 posteriores	Enterprise Edition y Standard Edition 2 (SE2)	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.x2iedn .2xlarge	Sí	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Solo ediciones Standard y Enterprise, SQL Server 2012.00 y posteriores	MySQL 8.0.28 posteriores	Enterprise Edition y Standard Edition 2 (SE2)	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.x2iedn .xlarge	Sí	Todas las versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	Solo ediciones Standard y Enterprise, SQL Server 2012.00 y posteriores	MySQL 8.0.28 posteriores	Enterprise Edition y Standard Edition 2 (SE2)	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

db.x2iezn: clases de instancia optimizada para memoria con tecnología de procesadores Intel Xeon Scalable de 2.ª generación

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x2iezn.8xlarge	No	No	No	No	Solo Enterprise Edition	No
db.x2iezn.6xlarge	No	No	No	No	Solo Enterprise Edition	No
db.x2iezn.4xlarge	No	No	No	No	Enterprise Edition y Standard Edition 2 (SE2)	No
db.x2iezn.2xlarge	No	No	No	No	Enterprise Edition y Standard Edition 2 (SE2)	No

db.x1e: clases de instancia optimizada para memoria

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x1e.32xlarge	No	No	Sí	No	Sí	No
db.x1e.16xlarge	No	No	Sí	No	Sí	No
db.x1e.8xlarge	No	No	Sí	No	Sí	No
db.x1e.4xlarge	No	No	Sí	No	Sí	No
db.x1e.2xlarge	No	No	Sí	No	Sí	No
db.x1e.xlarge	No	No	Sí	No	Sí	No

db.x1: clases de instancia optimizada para memoria

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.x1.32xlarge	No	No	Sí	No	Sí	No
db.x1.16xlarge	No	No	Sí	No	Sí	No

db.r7g: clases de instancia optimizada para memoria con tecnología de procesadores Graviton3 de AWS

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r7g.1 xlarge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.r7g.1 xlarge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.r7g.8 large	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la

Clase de instancia	DB	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
		posteriores y 10.4.26 y versiones 10.4 posteriores				versión 13.4 (y cualquier versión 13 posterior)
db.r7g.4 large	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.r7g.2 large	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.r7g.xl arge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)
db.r7g.la rge	No	Versiones de MariaDB 10.11, 10.6.10 y versiones 10.6 posteriores, 10.5.17 y versiones 10.5 posteriores y 10.4.26 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.4 (y cualquier versión 13 posterior)

db.r6g: clases de instancia optimizada para memoria con tecnología de procesadores Graviton2 de AWS

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6g.16 xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r6g.12 xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r6g.8x large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r6g.4x large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r6g.2x large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r6g.xl arge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
						12.7 y cualquier version 12 posterior
db.r6g.large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.23 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

db.r6gd: clases de instancia optimizada para memoria con tecnología de procesadores Graviton2 de AWS

Clase de instancia	D	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6gd.6xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.2xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instancia	DI	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6gd.8 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.4 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.2 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.x large	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instancia	Dl	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6gd.l arge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

db.r6id: clases de instancia optimizada para memoria con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6id.3 2xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.2 4xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6id.16xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.12xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.8xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.4xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6id.2xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.large	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

db.r6idn: clases de instancia optimizada para memoria con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6idn.32xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior	No	MySQL ver y	No	Todas las versiones 15 y 16 de PostgreSQ

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
		es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores		posterior es		L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6idn. 24xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6idn. 16xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6idn. 12xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6idn. 8xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6idn. 4xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6idn. 2xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6idn. xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ver y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

db.r6in: clases de instancia optimizada para memoria con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6in.32xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.r6in.24xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.r6in.16xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
						11.16 (y cualquier versión 11 posterior)
db.r6in.12xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.r6in.8xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6in.4xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.r6in.2xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)
db.r6in.xlarge	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6in.large	Sí	Versión de MariaDB 10.6.8 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL ve y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.3 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior), la versión 12.11 (y cualquier versión 12 posterior) y la versión 11.16 (y cualquier versión 11 posterior)

db.r6i: clases de instancia optimizada para memoria y preconfiguradas para alta memoria, almacenamiento y E/S

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6i.8xlarge.tpc2.mem4x	No	No	No	No	EE solo	No
db.r6i.8xlarge.tpc2.mem3x	No	No	No	No	EE solo	No
db.r6i.6xlarge.tpc2.mem4x	No	No	No	No	EE solo	No

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r6i.4xlarge.tpc2.mem4x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.4xlarge.tpc2.mem3x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.4xlarge.tpc2.mem2x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.2xlarge.tpc2.mem8x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.2xlarge.tpc2.mem4x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.2xlarge.tpc1.mem2x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.xlarge.tpc2.mem4x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.xlarge.tpc2.mem2x	No	No	No	No	EE y SE2 BYOL	No
db.r6i.large.tpc1.mem2x	No	No	No	No	EE y SE2 BYOL	No

db.r6i: clases de instancia optimizada para memoria

Clase de instanci	Dl	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.r6i.3 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL ver y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)
db.r6i.2 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL ver y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)
db.r6i.1 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL ver y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la

Clase de instanci	DI	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
						versión 10.21 (y cualquier versión 10 posterior)
db.r6g.1 xlarge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL vers y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)
db.r6i.8: large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL vers y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)

Clase de instanci	DI	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.r6i.4x large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL vers y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)
db.r6i.2x large	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL vers y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)
db.r6i.xl arge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL vers y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)

Clase de instanci	Dl	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.r6i.la rge	Sí	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.15 y versiones 10.5 posterior es y MariaDB 10.4.24 y versiones 10.4 posteriores	Sí	MySQL vers y posterior es	Sí	Todas las versiones 14, 15 y 16 de PostgreSQL, la versión 13.4 (y cualquier versión 13 posterior), la versión 12.8 (y cualquier versión 12 posterior), la versión 11.3 (y cualquier versión 11 posterior) y la versión 10.21 (y cualquier versión 10 posterior)

db.r5d: clases de instancia optimizada para memoria

Clase de instanci	Dl	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.r5d.2 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r5d.1 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instanci	DI	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.r5d.1 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r5d.8 large	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r5d.4 large	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r5d.2 large	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instanci	D	MariaDB	Micros SQL Serve	MySQL	Ora	PostgreSQL
db.r5d.x arge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r5d.la rge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	Sí	MySQL y posterio es	Sí	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

db.r5b: clases de instancia optimizada para memoria y preconfiguradas para alta memoria, almacenamiento y E/S

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5b.8x large.tpc 2.mem3x	No	No	No	No	Sí	No
db.r5b.6x large.tpc 2.mem4x	No	No	No	No	Sí	No

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5b.4xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5b.4xlarge.tpc2.mem3x	No	No	No	No	Sí	No
db.r5b.4xlarge.tpc2.mem2x	No	No	No	No	Sí	No
db.r5b.2xlarge.tpc2.mem8x	No	No	No	No	Sí	No
db.r5b.2xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5b.2xlarge.tpc1.mem2x	No	No	No	No	Sí	No
db.r5b.xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5b.xlarge.tpc2.mem2x	No	No	No	No	Sí	No
db.r5b.large.tpc1.mem2x	No	No	No	No	Sí	No

db.r5b: clases de instancia optimizada para memoria

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.r5b.24xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r5b.16xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r5b.12xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r5b.8xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	>Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

Clase de instancia	Db2	MariaDB	Micros SQL Server	MySQL	Orac	PostgreSQL
db.r5b.4xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r5b.2xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r5b.xlarge	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.r5b.large	No	Versiones de MariaDB 10.11, 10.6.5 y versiones 10.6 posteriores, 10.5.12 y versiones 10.5 posteriores, 10.4.24 y versiones 10.4 posteriores y 10.3.34 y versiones 10.3 posteriores	Sí	MySQL 8.0.25 y posteriores	Sí	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

db.r5: clases de instancia optimizada para memoria y preconfiguradas para alta memoria, almacenamiento y E/S

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5.12xlarge.tpc2.mem2x	No	No	No	No	Sí	No
db.r5.8xlarge.tpc2.mem3x	No	No	No	No	Sí	No
db.r5.6xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5.4xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5.4xlarge.tpc2.mem3x	No	No	No	No	Sí	No
db.r5.4xlarge.tpc2.mem2x	No	No	No	No	Sí	No
db.r5.2xlarge.tpc2.mem8x	No	No	No	No	Sí	No
db.r5.2xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5.2xlarge.tpc1.mem2x	No	No	No	No	Sí	No
db.r5.xlarge.tpc2.mem4x	No	No	No	No	Sí	No
db.r5.xlarge.tpc2.mem2x	No	No	No	No	Sí	No

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r5.large.tpc1.mem2x	No	No	No	No	Sí	No

db.r5: clases de instancia optimizada para memoria

Clase de instancia	Db2	MariaD	Microsoft SQL Server	MySC	Oracle	PostgreSQL
db.r5.24xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.r5.16xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.r5.12xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.r5.8xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.r5.4xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)

Clase de instancia	Db2	MariaD	Microsoft SQL Server	MySC	Oracle	PostgreSQL
db.r5.2xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.r5.xlarge	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)
db.r5.large	No	Sí	Sí	Sí	Sí	Todas las versiones 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 10.17 (y cualquier versión 10 posterior) y la versión 9.6.22 (y cualquier versión 9 posterior)

db.r4: clases de instancia optimizada para memoria

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r4.16xlarge	No	Obsoleto	Obsoleto	Obsoleto	Obsolet	Obsoleto
db.r4.8xlarge	No	Obsoleto	Obsoleto	Obsoleto	Obsolet	Obsoleto
db.r4.4xlarge	No	Obsoleto	Obsoleto	Obsoleto	Obsolet	Obsoleto
db.r4.2xlarge	No	Obsoleto	Obsoleto	Obsoleto	Obsolet	Obsoleto

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Oracle	PostgreSQL
db.r4.xlarge	No	Obsoleto	Obsoleto	Obsoleto	Obsolet	Obsoleto
db.r4.large	No	Obsoleto	Obsoleto	Obsoleto	Obsolet	Obsoleto

db.r3: clases de instancia optimizada para memoria

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQ	Oracle	PostgreSQL
db.r3.8xlarge**	No	Todas las versiones de MariaDB 10.6, 10.5, 10.4 y 10.3	Obsoleto	Sí	Obsoleto	Obsoleto
db.r3.4xlarge	No	Todas las versiones de MariaDB 10.6, 10.5, 10.4 y 10.3	Obsoleto	Sí	Obsoleto	Obsoleto
db.r3.2xlarge	No	Todas las versiones de MariaDB 10.6, 10.5, 10.4 y 10.3	Obsoleto	Sí	Obsoleto	Obsoleto
db.r3.xlarge	No	Todas las versiones de MariaDB 10.6, 10.5, 10.4 y 10.3	Obsoleto	Sí	Obsoleto	Obsoleto
db.r3.large	No	Todas las versiones de MariaDB 10.6, 10.5, 10.4 y 10.3	Obsoleto	Sí	Obsoleto	Obsoleto

Motores de base de datos compatibles para clases de instancias optimizadas para la computación

En las tablas siguientes, se muestran las bases de datos y las versiones de bases de datos compatibles para las clases de instancias optimizadas para la computación.

db.c6gd: clases de instancias optimizadas para la computación (solo para implementaciones de clústeres de bases de datos multi-AZ)

Clase de instancia	Db2	Maria	Microsoft SQL Server	MySQL	Orac	PostgreSQL
db.c6gd.16xlarge	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13
db.c6gd.12xlarge	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13
db.c6gd.8xlarge	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13
db.c6gd.4xlarge	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13

Clase de instancia	Db2	Maria	Microsoft SQL Server	MySQL	Orac	PostgreSQL
db.c6gd.2xlarge	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13
db.c6gd.xlarge	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13
db.c6gd.large	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13
db.c6gd.medium	No	No	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 16 y 15 de PostgreSQ; versión 14.5 y versiones posteriores a la 14; versiones 13.4 y 13.7 y versiones posteriores a la 13

Motores de base de datos compatibles para clases de instancia de rendimiento ampliable

En las tablas siguientes, se muestran las bases de datos y las versiones de bases de datos compatibles para las clases de instancias de rendimiento ampliable.

db.t4g: clases de instancia de rendimiento ampliable con la tecnología de los procesadores Graviton2 de AWS

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Orac	PostgreSQL
db.t4g: clases de instancia de rendimiento ampliable con la tecnología de los procesadores Graviton2 de AWS						
db.t4g.2xlarge*	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.t4g.xlarge	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.t4g.large	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.t4g.medium	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior
db.t4g.small	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

Clase de instancia	Db2	MariaDB	Microsoft SQL Server	MySQL	Orac	PostgreSQL
db.t4g.micro	No	Todas las versiones de MariaDB 10.11, 10.6, 10.5 y 10.4	No	MySQL 8.0.25 y posteriores	No	Todas las versiones 13, 14, 15 y 16 de PostgreSQL, la versión 12.7 y cualquier version 12 posterior

db.t3: clases de instancia de rendimiento ampliable

Clase de instancia	Db2	Maria	Microsoft SQL Server	MySQ	Oracle	PostgreSQL
db.t3.2xlarge	Sí	Sí	Sí	Sí	Sí	Todas las versiones 10, 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 9.6.22 y cualquier versión 9 posterior
db.t3.xlarge	Sí	Sí	Sí	Sí	Sí	Todas las versiones 10, 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 9.6.22 y cualquier versión 9 posterior
db.t3.large	Sí	Sí	Sí	Sí	Sí	Todas las versiones 10, 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 9.6.22 y cualquier versión 9 posterior
db.t3.medium	Sí	Sí	Sí	Sí	Sí	Todas las versiones 10, 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 9.6.22 y cualquier versión 9 posterior
db.t3.small	Sí	Sí	Sí	Sí	Sí	Todas las versiones 10, 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 9.6.22 y cualquier versión 9 posterior

Clase de instancia	Db2	Maria	Microsoft SQL Server	MySC	Oracle	PostgreSQL
db.t3.micro	No	Sí	Sí	Sí	Solo en Oracle Database 12c Release 1 (12.1.0.2), que está obsoleto	Todas las versiones 10, 11, 12, 13, 14, 15 y 16 de PostgreSQL, la versión 9.6.22 y cualquier versión 9 posterior

db.t2: clases de instancia de rendimiento ampliable

Clase de instancia	Db2	MariaDB	Microsof SQL Server	MySQL	Oracle	PostgreSQL
db.t2.2xlarge	No	Obsoleto	No	Obsoleto	Obsolet	Obsoleto
db.t2.xlarge	No	Obsoleto	No	Obsoleto	Obsolet	Obsoleto
db.t2.large	No	Obsoleto	Obsoletc	Obsoleto	Obsolet	Obsoleto
db.t2.medium	No	Obsoleto	Obsoletc	Obsoleto	Obsolet	Obsoleto
db.t2.small	No	Obsoleto	Obsoletc	Obsoleto	Obsolet	Obsoleto
db.t2.micro	No	Obsoleto	Obsoletc	Obsoleto	Obsolet	Obsoleto

Motores de base de datos compatibles para clases de instancias de lecturas optimizadas

En las tablas siguientes, se muestran las bases de datos y las versiones de bases de datos compatibles para las clases de instancias de lecturas optimizadas.

db.r6gd: clases de instancias optimizadas para memoria que admiten lecturas optimizadas y cuentan con la tecnología de procesadores Graviton2 de AWS

Clase de instancia	DI	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6gd.16xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.12xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.8xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

Clase de instancia	DI	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6gd.4 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.2 xlarge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.x large	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4
db.r6gd.l arge	N	Versiones de MariaDB 10.11, MariaDB 10.6.7 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior es y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL 8.0.28 y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior), la versión 13.7 (y cualquier versión 13 posterior) y la versión 13.4

db.r6id: clases de instancias optimizadas para memoria que admiten lecturas optimizadas y cuentan con la tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6id.32xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.24xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.16xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.12xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posterior	No	MySQL versió y posteriores	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
		es, y MariaDB 10.4.25 y versiones 10.4 posteriores				13.7 (y cualquier versión 13 posterior)
db.r6id.8xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.4xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.2xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)
db.r6id.xlarge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posteriores, MariaDB 10.5.16 y versiones 10.5 posteriores, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQL, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Clase de instancia	Db	MariaDB	Micros SQL Server	MySQL	Ora	PostgreSQL
db.r6id.l arge	No	Versión de MariaDB 10.6.10 y versiones 10.6 posterior es, MariaDB 10.5.16 y versiones 10.5 posterior es, y MariaDB 10.4.25 y versiones 10.4 posteriores	No	MySQL versió y posterior es	No	Todas las versiones 15 y 16 de PostgreSQ L, la versión 14.5 (y cualquier versión 14 posterior) y la versión 13.7 (y cualquier versión 13 posterior)

Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS

Para determinar las clases de instancia de base de datos admitidas por cada motor de base de datos en una Región de AWS específica, puede utilizar uno de varios métodos. Puede utilizar la AWS Management Console, la página de precios de Amazon RDS o el comando describe-orderable-db-instance-options para la AWS Command Line Interface (AWS CLI).

> **Note**
>
> Cuando realiza operaciones con la AWS Management Console, muestra automáticamente las clases de instancia de base de datos admitidas para un motor de base de datos específico, una versión del motor de base de datos y la Región de AWS. Entre los ejemplos de operaciones que puede realizar se incluyen la creación y modificación de una instancia de base de datos.

Contenido

- Uso de la página de precios de Amazon RDS para determinar la compatibilidad de las clases de instancia de base de datos en las Regiones de AWS
- Uso de la AWS CLI para determinar la compatibilidad de la clase de instancia de base de datos en las Regiones de AWS
  - Enumeración de las clases de instancia de base de datos compatibles con una versión específica del motor de base de datos en una Región de AWS

- Enumeración de las versiones del motor de base de datos que admiten una clase de instancia de base de datos específica en una Región de AWS
- Muestra de Regiones de AWS que admiten un motor de base de datos y una clase de instancia específicos

Uso de la página de precios de Amazon RDS para determinar la compatibilidad de las clases de instancia de base de datos en las Regiones de AWS

Puede utilizar la página Precios de Amazon RDS para determinar las clases de instancia de base de datos admitidas por cada motor de base de datos en una Región de AWS específica.

Para utilizar la página de precios para determinar las clases de instancia de base de datos admitidas por cada motor de una región

1. Vaya a Precios de Amazon RDS.
2. En la sección Calculadora de precios de AWS para Amazon RDS, seleccione Cree su presupuesto personalizado ahora.
3. En Elija una región, elija una Región de AWS.
4. En Buscar un servicio, introduzca **`Amazon RDS`**.
5. Elija Configurar para seleccionar la opción de configuración y el motor de base de datos.
6. Utilice la sección de instancias compatibles para ver las clases de instancias de base de datos compatibles.
7. (Opcional) Elija otras opciones en la calculadora y, a continuación, elija Guardar y ver resumen o Guardar y agregar servicio.

Uso de la AWS CLI para determinar la compatibilidad de la clase de instancia de base de datos en las Regiones de AWS

Puede utilizar la AWS CLI para determinar qué clases de instancia de base de datos se admiten para los motores de base de datos específicos y las versiones de motor de base de datos en una Región de AWS. En la tabla siguiente se muestran los valores válidos del motor de base de datos.

Nombres de motores	Valores del motor en comandos de CLI	Más información acerca de las versiones
Db2	`db2-ae` `db2-se`	Versiones de Db2 en Amazon RDS
MariaDB	`mariadb`	Versiones de MariaDB en Amazon RDS

Microsoft SQL Server	`sqlserver-ee`
	`sqlserver-se`
	`sqlserver-ex`
	`sqlserver-web`
		Versiones de Microsoft SQL Server en Amazon RDS

MySQL	`mysql`	Versiones de MySQL en Amazon RDS
Oracle	`oracle-ee` `oracle-se2`	Notas de la versión de Amazon RDS para Oracle
PostgreSQL	`postgres`	Versiones de base de datos de PostgreSQL disponibles

Para obtener más información sobre los nombres de la Región de AWS, consulte AWSRegiones de .

Los siguientes ejemplos muestran cómo determinar la compatibilidad de la clase de instancia de base de datos en una Región de AWS mediante el comando describe-orderable-db-instance-options de la AWS CLI.

> **Note**
>
> Para limitar la salida, en los siguientes ejemplos se muestran los resultados solo para el tipo de almacenamiento SSD de uso general (`gp2`). Si es necesario, puede cambiar el tipo de almacenamiento a SSD de uso general (`gp3`), IOPS aprovisionadas (`io1`), IOPS aprovisionadas Block Express (`io2`) o magnéticas (`standard`) en los comandos.

Temas

- Enumeración de las clases de instancia de base de datos compatibles con una versión específica del motor de base de datos en una Región de AWS
- Enumeración de las versiones del motor de base de datos que admiten una clase de instancia de base de datos específica en una Región de AWS
- Muestra de Regiones de AWS que admiten un motor de base de datos y una clase de instancia específicos

Enumeración de las clases de instancia de base de datos compatibles con una versión específica del motor de base de datos en una Región de AWS

Para enumerar las clases de instancia de base de datos compatibles con una versión específica del motor de base de datos en una Región de AWS, ejecute el siguiente comando.

Para Linux, macOS o Unix:

```
aws rds describe-orderable-db-instance-options --engine engine --engine-version version
 \
    --query "*[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[?
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" \
    --output text \
    --region region
```

Para Windows:

```
aws rds describe-orderable-db-instance-options --engine engine --engine-version version
 ^
    --query "*[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[?
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" ^
    --output text ^
    --region region
```

Por ejemplo, el siguiente comando enumera las clases de instancia de base de datos compatibles para la versión 13.6 del motor base de datos de RDS para PostgreSQL en Este de EE. UU. (Norte de Virginia).

Para Linux, macOS o Unix:

```
aws rds describe-orderable-db-instance-options --engine postgres --engine-version 15.4
 \
```

```
    --query "*[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[?
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" \
    --output text \
    --region us-east-1
```

Para Windows:

```
aws rds describe-orderable-db-instance-options --engine postgres --engine-version 15.4
 ^
    --query "*[].{DBInstanceClass:DBInstanceClass,StorageType:StorageType}|[?
StorageType=='gp2']|[].{DBInstanceClass:DBInstanceClass}" ^
    --output text ^
    --region us-east-1
```

Enumeración de las versiones del motor de base de datos que admiten una clase de instancia de base de datos específica en una Región de AWS

Para enumerar las versiones del motor de base de datos que admiten una clase de instancia de base de datos específica en una Región de AWS, ejecute el siguiente comando.

Para Linux, macOS o Unix:

```
aws rds describe-orderable-db-instance-options --engine engine --db-instance-
class DB_instance_class \
    --query "*[].{EngineVersion:EngineVersion,StorageType:StorageType}|[?
StorageType=='gp2']|[].{EngineVersion:EngineVersion}" \
    --output text \
    --region region
```

Para Windows:

```
aws rds describe-orderable-db-instance-options --engine engine --db-instance-
class DB_instance_class ^
    --query "*[].{EngineVersion:EngineVersion,StorageType:StorageType}|[?
StorageType=='gp2']|[].{EngineVersion:EngineVersion}" ^
    --output text ^
    --region region
```

Por ejemplo, el siguiente comando enumera las versiones del motor de base de datos del motor de base de datos RDS para PostgreSQL que admiten la clase de instancia de base de datos db.r5.large en US East (N. Virginia).

Para Linux, macOS o Unix:

```
aws rds describe-orderable-db-instance-options --engine postgres --db-instance-class
 db.m7g.large \
    --query "*[].{EngineVersion:EngineVersion,StorageType:StorageType}|[?
StorageType=='gp2']|[].{EngineVersion:EngineVersion}" \
    --output text \
    --region us-east-1
```

Para Windows:

```
aws rds describe-orderable-db-instance-options --engine postgres --db-instance-class
 db.m7g.large ^
    --query "*[].{EngineVersion:EngineVersion,StorageType:StorageType}|[?
StorageType=='gp2']|[].{EngineVersion:EngineVersion}" ^
    --output text ^
    --region us-east-1
```

Muestra de Regiones de AWS que admiten un motor de base de datos y una clase de instancia específicos

El siguiente script de bash muestra todas las Regiones de AWS que admiten la combinación especificada de motor de base de datos y clase de instancia.

```
#!/usr/bin/env bash
# Usage: check_region_support.sh <db-engine> <db-instance-class>

if [ $# -ne 2 ]; then
  echo "Usage: $0 <db-engine> <db-instance-class>"
  exit 1
fi
ENGINE="$1"
INSTANCE_CLASS="$2"
REGIONS=$(aws ec2 describe-regions --query "Regions[].RegionName" --output text)
for region in $REGIONS; do
  supported_count=$(aws rds describe-orderable-db-instance-options \
    --region "$region" \
    --engine "$ENGINE" \
    --db-instance-class "$INSTANCE_CLASS" \
    --query 'length(OrderableDBInstanceOptions)' \
    --output text 2>/dev/null || echo "0")
  if [ "$supported_count" -gt 0 ]; then
```

```
    echo "$region supports $INSTANCE_CLASS for $ENGINE."
  else
    echo "$region doesn't support $INSTANCE_CLASS for $ENGINE."
  fi
done
```

La siguiente salida de ejemplo comprueba la compatibilidad de la región con RDS para MySQL mediante la clase de instancia db.r8g.large.

```
./check_region_support.sh mysql db.r8g.large
ap-south-1 doesn't support db.r8g.large for mysql.
eu-north-1 doesn't support db.r8g.large for mysql.
eu-west-3 doesn't support db.r8g.large for mysql.
eu-west-2 doesn't support db.r8g.large for mysql.
eu-west-1 doesn't support db.r8g.large for mysql.
ap-northeast-3 doesn't support db.r8g.large for mysql.
ap-northeast-2 doesn't support db.r8g.large for mysql.
ap-northeast-1 doesn't support db.r8g.large for mysql.
ca-central-1 doesn't support db.r8g.large for mysql.
sa-east-1 doesn't support db.r8g.large for mysql.
ap-southeast-1 doesn't support db.r8g.large for mysql.
ap-southeast-2 doesn't support db.r8g.large for mysql.
eu-central-1 supports db.r8g.large for mysql.
us-east-1 supports db.r8g.large for mysql.
us-east-2 supports db.r8g.large for mysql.
us-west-1 doesn't support db.r8g.large for mysql.
us-west-2 supports db.r8g.large for mysql.
```

Cambio de clase de instancia de base de datos

Puede cambiar la CPU y la memoria disponible para la instancia de base de datos cambiando su clase de instancia de base de datos. Para cambiar la clase de instancia de base de datos, modifique su instancia de base de datos siguiendo las instrucciones en Modificación de una instancia de base de datos de Amazon RDS.

Configuración del procesador de una clase de instancias de base de datos en RDS para Oracle

Las clases de instancias de base de datos de Amazon RDS admiten la tecnología Intel Hyper-Threading, que permite la ejecución simultánea de varios subprocesos en un único núcleo de CPU

Intel Xeon. Cada subproceso está representado como una CPU virtual (vCPU) en la instancia de base de datos. Una instancia de base de datos tiene un número predeterminado de núcleos de CPU que varía en función de la clase de instancia. Por ejemplo, una clase de instancia de base de datos db.m4.xlarge tiene dos núcleos de CPU y dos subprocesos por núcleo de forma predeterminada, es decir, cuatro vCPU en total.

> **Note**
>
> Cada vCPU es un hiperproceso de un núcleo de CPU Intel Xeon.

Temas

- Descripción general de la configuración del procesador de RDS para Oracle
- Clases de instancia de base de datos que admiten la configuración del procesador
- Configuración de núcleos de CPU y subprocesos por núcleo de CPU para una clase de instancias de base de datos

Descripción general de la configuración del procesador de RDS para Oracle

Cuando usa RDS para Oracle, normalmente puede encontrar una clase de instancias de base de datos con la combinación de memoria y número de vCPU adecuada para sus cargas de trabajo. Sin embargo, también puede especificar las siguientes características del procesador para optimizar la instancia de base de datos de RDS para Oracle en función de cargas de trabajo o necesidades empresariales específicas:

- Número de núcleos de CPU: puede personalizar el número de núcleos de CPU de la instancia de base de datos. Esto le ofrecerá la posibilidad de optimizar los costos de licencias de software con una instancia de base de datos que disponga de la cantidad suficiente de memoria RAM para cargas de trabajo con uso intensivo de memoria pero menos núcleos de CPU.
- Subprocesos por núcleo: puede deshabilitar la tecnología Intel Hyper-Threading especificando un único subproceso por núcleo de CPU. Esto podría utilizarlo en determinadas cargas de trabajo, como las cargas de trabajo de informática de alto desempeño (HPC).

Puede controlar el número de núcleos de CPU y de subprocesos de cada núcleo por separado. Puede configurar uno o ambos en una solicitud. Una vez asociada una configuración a una instancia de base de datos, esta configuración se conserva hasta que la cambie.

La configuración del procesador de una instancia de base de datos está asociada a las instantáneas de la instancia de base de datos. Cuando se restaura una instantánea, su instancia de base de datos restaurada usa la configuración de características del procesador utilizada cuando se realizó la instantánea.

Si modifica la clase de instancia de base de datos para una instancia de base de datos con una configuración del procesador distinta de la predeterminada, especifique la configuración del procesador predeterminada o especifique explícitamente la configuración del procesador en el momento de la modificación. Este requisito garantiza que se conozcan los costos de licencias de terceros que se podrían aplicar al modificar la instancia de base de datos.

No se aplican cargos adicionales o reducidos al especificar características del procesador en una instancia de base de datos de RDS para Oracle. Se aplican los mismos cargos que en el caso de las instancias de base de datos que se lanzan con configuraciones de CPU predeterminadas.

Clases de instancia de base de datos que admiten la configuración del procesador

Puede configurar el número de núcleos de CPU y subprocesos por núcleo solo cuando se cumplan las siguientes condiciones:

- Está configurando una instancia de base de datos de RDS para Oracle. Para obtener información acerca de las clases de instancias de base de datos admitidas por las distintas ediciones de base de datos de Oracle, consulte Clases de instancias de base de datos de RDS para Oracle.
- Su instancia de base de datos utiliza la opción de licencia traiga su propia licencia (BYOL) de RDS para Oracle. Para obtener más información acerca de las opciones de licencias de Oracle, consulte Opciones de licencias de RDS para Oracle.
- Su instancia de base de datos no pertenece a una de las clases de instancia db.r5 o db.r5b que tienen configuraciones de procesador predefinidas. Estas clases de instancia se denominan db.r5.*instance_size*.tpc*threads_per_core*.mem*ratio* o db.r5b.*instance_size*.tpc*threads_per_core*.mem*ratio*. Por ejemplo, db.r5b.xlarge.tpc2.mem4x está preconfigurado con 2 subprocesos por núcleo (tpc2) y 4 veces más memoria que la clase de instancia db.r5b.xlarge estándar. No puede configurar las características del procesador de estas clases de instancia optimizadas. Para obtener más información, consulte Clases de instancias admitidas de RDS para Oracle.

Puede usar el siguiente comando de la AWS CLI para mostrar las vCPU predeterminadas, los núcleos, los subprocesos por núcleo y los números válidos de núcleos para una clase de instancia. Sustituya *r7i.48xlarge* en el comando de ejemplo por el nombre de la clase de instancia.

```
aws ec2 describe-instance-types \
    --instance-types r7i.48xlarge \
    --query '{
        DefaultVCPUs: InstanceTypes[0].VCpuInfo.DefaultVCpus,
        DefaultCores: InstanceTypes[0].VCpuInfo.DefaultCores,
        DefaultThreadsPerCore: InstanceTypes[0].VCpuInfo.DefaultThreadsPerCore,
        ValidCores: InstanceTypes[0].VCpuInfo.ValidCores
    }' \
    --output json
```

En la tabla siguiente, encontrará las clases de instancias de base de datos que permiten configurar el número de núcleos de CPU y subprocesos de CPU por núcleo. También encontrará el valor predeterminado y los valores válidos para el número de núcleos de CPU y subprocesos de CPU por núcleo para cada clase de instancias de base de datos.

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.m6i: clases de instancia optimizada para memoria					
db.m6i.large	2.	1	2	1	1, 2
db.m6i.xlarge	4	2	2	2	1, 2
db.m6i.2xlarge	8	4	2	2, 4	1, 2
db.m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.m6g.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
db.m5: clases de instancia de uso general					
db.m5.large	2	1	2	1	1, 2
db.m5.xlarge	4	2	2	2	1, 2
db.m5.2xlarge	8	4	2	2, 4	1, 2
db.m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.m5d: clases de instancia de uso general					
db.m5d.large	2	1	2	1	1, 2
db.m5d.xlarge	4	2	2	2	1, 2
db.m5d.2xlarge	8	4	2	2, 4	1, 2
db.m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.m4: clases de instancia de uso general					

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
db.m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r7i: clases de instancia optimizada para memoria					
db.r7i.large	2.	1	2	1	1, 2
db.r7i.xlarge	4	2	2	1, 2	1, 2
db.r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
db.r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
db.r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
db.r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
db.r6i: clases de instancia optimizada para memoria					
db.r6i.large	2.	1	2	1	1, 2
db.r6i.xlarge	4	2	2	1, 2	1, 2
db.r6i.2xlarge	8	4	2	2, 4	1, 2
db.r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.r6g.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
db.r5: clases de instancia optimizada para memoria					
db.r5.large	2	1	2	1	1, 2
db.r5.xlarge	4	2	2	2	1, 2
db.r5.2xlarge	8	4	2	2, 4	1, 2
db.r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r5: clases de instancia optimizada para memoria					
db.r5b.large	2	1	2	1	1, 2
db.r5b.xlarge	4	2	2	2	1, 2
db.r5b.2xlarge	8	4	2	2, 4	1, 2
db.r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r5b.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r5d: clases de instancia optimizada para memoria					
db.r5d.large	2	1	2	1	1, 2
db.r5d.xlarge	4	2	2	2	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.r5d.2xlarge	8	4	2	2, 4	1, 2
db.r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.r5d.12 xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.r5d.16 xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.r5d.24 xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.r4: clases de instancia optimizada para memoria					
db.r4.large	2	1	2	1	1, 2
db.r4.xlarge	4	2	2	1, 2	1, 2
db.r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
db.r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.r3: clases de instancia optimizada para memoria					
db.r3.large	2	1	2	1	1, 2
db.r3.xlarge	4	2	2	1, 2	1, 2
db.r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.x2idn: clases de instancia optimizada para memoria					
db.x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
db.x2iedn: clases de instancia optimizada para memoria					
db.x2iedn.xlarge	4	2	2	1, 2	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.x2iedn.2xlarge	8	4	2	2, 4	1, 2
db.x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
db.x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
db.x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
db.x2iezn: clases de instancia optimizada para memoria					
db.x2iezn.2xlarge	8	4	2	2, 4	1, 2
db.x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
db.x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
db.x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
db.x1: clases de instancia optimizada para memoria					
db.x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
db.x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
db.x1e: clases de instancia optimizada para memoria					
db.x1e.xlarge	4	2	2	1, 2	1, 2
db.x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
db.x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
db.x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
db.x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

DB instance class	vCPU predeterminadas	Núcleos de CPU predeterminados	Subprocesos por núcleo predeterminados	Número válido de núcleos de CPU	Número válido de subprocesos por núcleo
db.x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
db.z1d: clases de instancia de memoria optimizada					
db.z1d.large	2	1	2	1	1, 2
db.z1d.xlarge	4	2	2	2	1, 2
db.z1d.2xlarge	8	4	2	2, 4	1, 2
db.z1d.3xlarge	12	6	2	2, 4, 6	1, 2
db.z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
db.z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

> **Note**
>
> Puede utilizar AWS CloudTrail para monitorear y auditar cambios en la configuración de procesos de las instancias de base de datos de Amazon RDS para Oracle. Para obtener más información acerca del uso de CloudTrail, consulte Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail.

Configuración de núcleos de CPU y subprocesos por núcleo de CPU para una clase de instancias de base de datos

Puede configurar el número de núcleos de CPU y subprocesos por núcleo de la clase de instancias de base de datos cuando realiza las siguientes operaciones:

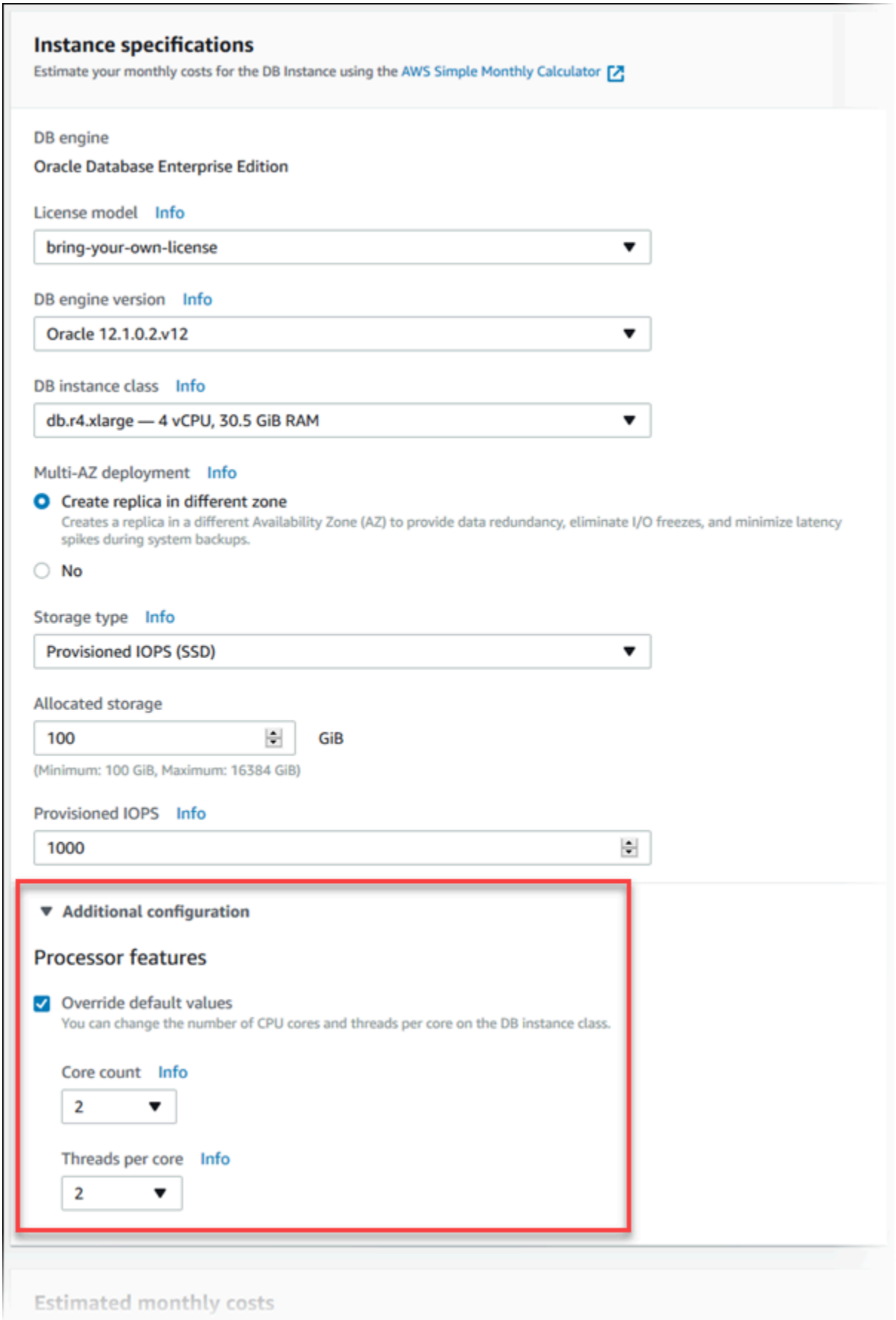
- Creación de una instancia de base de datos de Amazon RDS
- Modificación de una instancia de base de datos de Amazon RDS
- Restauración a una instancia de base de datos
- Restauración de una instancia de base de datos a un momento especificado para Amazon RDS

> **Note**
>
> Cuando modifica una instancia de base de datos para configurar el número de núcleos de CPU y subprocesos por núcleo, la instancia de base de datos se interrumpirá durante un breve periodo de tiempo.

Puede configurar el número de núcleos de CPU y los subprocesos por núcleo de CPU para una clase de instancias de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Cuando crea, modifica o restaura una instancia de base de datos, define la clase de instancias de base de datos en la AWS Management Console. En la sección Instance specifications (Especificaciones de la instancia) se muestran las opciones del procesador. La imagen siguiente muestra las opciones de características del procesador.

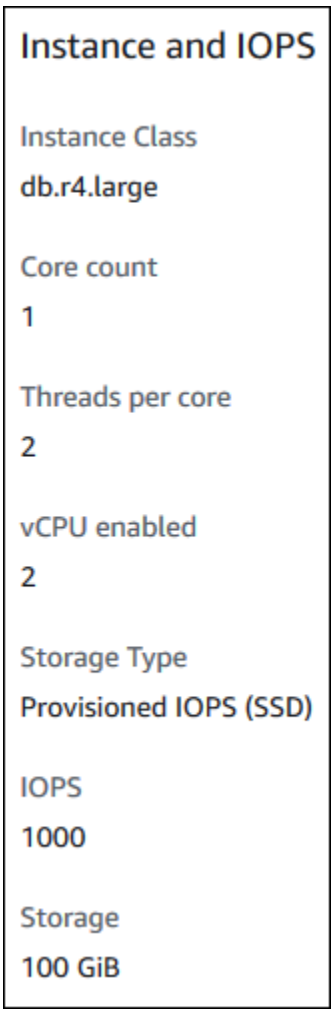

Instance specifications
Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator
DB engine
Oracle Database Enterprise Edition
License model Info
bring-your-own-license
DB engine version Info
Oracle 12.1.0.2.v12
DB instance class Info
db.r4.xlarge — 4 vCPU, 30.5 GiB RAM
Multi-AZ deployment Info
Create replica in different zone
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
No
Storage type Info
Provisioned IOPS (SSD)
Allocated storage
100
GiB
(Minimum: 100 GiB, Maximum: 16384 GiB)
Provisioned IOPS Info
1000
Additional configuration
Processor features
Override default values
You can change the number of CPU cores and threads per core on the DB instance class.
Core count Info
2
Threads per core Info
2
Estimated monthly costs

Establezca las siguientes opciones en los valores adecuados para su clase de instancias de base de datos en Processor features (Características del procesador):

- Core count (Número de núcleos): defina el número de núcleos de CPU con esta opción. El valor debe ser igual o inferior al número máximo de núcleos de CPU de la clase de instancias de base de datos.
- Threads per core (Subprocesos por núcleo): especifique 2 para habilitar varios subprocesos por núcleo o especifique 1 para deshabilitarlos.

Cuando modifica o restaura una instancia de base de datos, también puede establecer los núcleos de CPU y los subprocesos por núcleo de CPU en los valores predeterminados para la clase de instancia.

Cuando consulte los detalles de una instancia de base de datos en la consola, podrá ver la información del procesador para su clase de instancias de base de datos en la pestaña Configuration (Configuración). La imagen siguiente muestra una clase de instancias de base de datos con un núcleo de CPU y varios subprocesos por núcleo habilitados.



Para las instancias de base de datos de Oracle, la información del procesador solo aparece para las instancias de base de datos Bring Your Own License (BYOL).

AWS CLI

Puede definir las características del procesador para una instancia de base de datos con uno de los siguientes comandos de la AWS CLI:

- create-db-instance
- modify-db-instance
- restore-db-instance-from-db-snapshot
- restore-db-instance-from-s3
- restore-db-instance-to-point-in-time

Para configurar el procesador de una clase de instancias de base de datos para una instancia de base de datos mediante la AWS CLI, incluya la opción `--processor-features` en el comando. Especifique el número de núcleos de CPU con el nombre de característica `coreCount` y especifique si se van a habilitar varios subprocesos por núcleo con el nombre de característica `threadsPerCore`.

La opción presenta la siguiente sintaxis.

```
--processor-features "Name=coreCount,Value=<value>" "Name=threadsPerCore,Value=<value>"
```

A continuación se muestran ejemplos de configuración del procesador:

Ejemplos

- Configuración del número de núcleos de CPU de una instancia de base de datos
- Configuración del número de núcleos de CPU y desactivación de varios subprocesos para una instancia de base de datos
- Consulta de los valores de procesador válidos para una clase de instancias de base de datos
- Restauración de la configuración del procesador predeterminada de una instancia de base de datos
- Restauración del número de núcleos de CPU predeterminado de una instancia de base de datos
- Restauración del número predeterminado de subprocesos por núcleo de una instancia de base de datos

Configuración del número de núcleos de CPU de una instancia de base de datos

Example

El siguiente ejemplo modifica `mydbinstance` al establecer el número de núcleos de CPU en 4. Los cambios se aplican inmediatamente mediante `--apply-immediately`. Si desea aplicar los cambios durante el siguiente período de mantenimiento programado, omita la opción `--apply-immediately`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --processor-features "Name=coreCount,Value=4" \
```

```
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --processor-features "Name=coreCount,Value=4" ^
    --apply-immediately
```

Configuración del número de núcleos de CPU y desactivación de varios subprocesos para una instancia de base de datos

Example

El siguiente ejemplo modifica `mydbinstance` al establecer el número de núcleos de CPU en `4` y deshabilitar el uso de varios subprocesos por núcleo. Los cambios se aplican inmediatamente mediante `--apply-immediately`. Si desea aplicar los cambios durante el siguiente período de mantenimiento programado, omita la opción `--apply-immediately`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --processor-features "Name=coreCount,Value=4" "Name=threadsPerCore,Value=1" \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --processor-features "Name=coreCount,Value=4" "Name=threadsPerCore,Value=1" ^
    --apply-immediately
```

Consulta de los valores de procesador válidos para una clase de instancias de base de datos

Example

Puede consultar los valores de procesador válidos para una determinada clase de instancias de base de datos ejecutando el comando describe-orderable-db-instance-options y especificando la clase de

instancias para la opción `--db-instance-class`. Por ejemplo, la salida del siguiente comando muestra las opciones del procesador para la clase de instancias db.r3.large.

```
aws rds describe-orderable-db-instance-options --engine oracle-ee --db-instance-class
 db.r3.large
```

A continuación se muestra una salida de ejemplo del comando en formato JSON.

```
    {
                "SupportsIops": true,
                "MaxIopsPerGib": 50.0,
                "LicenseModel": "bring-your-own-license",
                "DBInstanceClass": "db.r3.large",
                "SupportsIAMDatabaseAuthentication": false,
                "MinStorageSize": 100,
                "AvailabilityZones": [
                    {
                        "Name": "us-west-2a"
                    },
                    {
                        "Name": "us-west-2b"
                    },
                    {
                        "Name": "us-west-2c"
                    }
                ],
                "EngineVersion": "12.1.0.2.v2",
                "MaxStorageSize": 32768,
                "MinIopsPerGib": 1.0,
                "MaxIopsPerDbInstance": 40000,
                "ReadReplicaCapable": false,
                "AvailableProcessorFeatures": [
                    {
                        "Name": "coreCount",
                        "DefaultValue": "1",
                        "AllowedValues": "1"
                    },
                    {
                        "Name": "threadsPerCore",
                        "DefaultValue": "2",
                        "AllowedValues": "1,2"
                    }
                ],
```

```
                "SupportsEnhancedMonitoring": true,
                "SupportsPerformanceInsights": false,
                "MinIopsPerDbInstance": 1000,
                "StorageType": "io1",
                "Vpc": false,
                "SupportsStorageEncryption": true,
                "Engine": "oracle-ee",
                "MultiAZCapable": true
    }
```

Asimismo, puede ejecutar los siguientes comandos para obtener información sobre el procesador de la clase de instancias de base de datos:

- describe-db-instances: muestra la información del procesador para la instancia de base de datos especificada.
- describe-db-snapshots: muestra la información del procesador para la instantánea de base de datos especificada.
- describe-valid-db-instance-modifications: muestra las modificaciones válidas del procesador para la instancia de base de datos especificada.

En la salida de los comandos anteriores, los valores de las características del procesador no son nulos solo si se cumplen las siguientes condiciones:

- Está utilizando una instancia de base de datos de RDS para Oracle.
- Su instancia de base de datos de RDS para Oracle admite cambios en los valores del procesador.
- La configuración actual del núcleo y el subproceso de CPU están establecidos en valores no predeterminados.

Si no se cumplen las condiciones anteriores, puede obtener el tipo de instancia mediante describe-db-instances. Puede obtener la información del procesador de este tipo de instancia ejecutando la operación de EC2 describe-instance-types.

Restauración de la configuración del procesador predeterminada de una instancia de base de datos

Example

El siguiente ejemplo modifica `mydbinstance` restaurando la clase de instancias de bases de datos a los valores del procesador predeterminados para dicha clase. Los cambios se aplican

inmediatamente mediante `--apply-immediately`. Si desea aplicar los cambios durante el siguiente período de mantenimiento programado, omita la opción `--apply-immediately`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --use-default-processor-features \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --use-default-processor-features ^
    --apply-immediately
```

Restauración del número de núcleos de CPU predeterminado de una instancia de base de datos

Example

El siguiente ejemplo modifica `mydbinstance` restaurando la clase de instancias de bases de datos al número predeterminado de núcleos de CPU para dicha clase. La configuración de subprocesos por núcleo no cambia. Los cambios se aplican inmediatamente mediante `--apply-immediately`. Si desea aplicar los cambios durante el siguiente período de mantenimiento programado, omita la opción `--apply-immediately`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --processor-features "Name=coreCount,Value=DEFAULT" \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --processor-features "Name=coreCount,Value=DEFAULT" ^
    --apply-immediately
```

Restauración del número predeterminado de subprocesos por núcleo de una instancia de base de datos

Example

El siguiente ejemplo modifica `mydbinstance` restaurando la clase de instancias de base de datos al número predeterminado de subprocesos por núcleo para dicha clase. La configuración del número de núcleos de CPU no cambia. Los cambios se aplican inmediatamente mediante `--apply-immediately`. Si desea aplicar los cambios durante el siguiente período de mantenimiento programado, omita la opción `--apply-immediately`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --processor-features "Name=threadsPerCore,Value=DEFAULT" \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --processor-features "Name=threadsPerCore,Value=DEFAULT" ^
    --apply-immediately
```

API de RDS

Puede definir las características del procesador para una instancia de base de datos llamando a una de las siguientes operaciones de la API de Amazon RDS:

- CreateDBInstance
- ModifyDBInstance
- RestoreDBInstanceFromDBSnapshot
- RestoreDBInstanceFromS3
- RestoreDBInstanceToPointInTime

Para configurar las características del procesador de una clase de instancias de base de datos para una instancia de base de datos mediante la API de Amazon RDS, incluya el parámetro `ProcessFeatures` en la llamada.

El parámetro presenta la siguiente sintaxis.

```
ProcessFeatures "Name=coreCount,Value=<value>" "Name=threadsPerCore,Value=<value>"
```

Especifique el número de núcleos de CPU con el nombre de característica `coreCount` y especifique si se van a habilitar varios subprocesos por núcleo con el nombre de característica `threadsPerCore`.

Puede consultar los valores de procesador válidos para una determinada clase de instancia de base de datos ejecutando la operación DescribeOrderableDBInstanceOptions y especificando la clase de instancias en el parámetro `DBInstanceClass`. También puede utilizar las siguientes operaciones:

- DescribeDBInstances: muestra la información del procesador para la instancia de base de datos especificada.
- DescribeDBSnapshots: muestra la información del procesador para la instantánea de base de datos especificada.
- DescribeValidDBInstanceModifications: muestra las modificaciones válidas del procesador para la instancia de base de datos especificada.

En la salida de las operaciones anteriores, los valores de las características del procesador no son nulos solo si se cumplen las siguientes condiciones:

- Está utilizando una instancia de base de datos de RDS para Oracle.
- Su instancia de base de datos de RDS para Oracle admite cambios en los valores del procesador.
- La configuración actual del núcleo y el subproceso de CPU están establecidos en valores no predeterminados.

Si no se cumplen las condiciones anteriores, puede obtener el tipo de instancia mediante DescribeDBInstances. Puede obtener la información del procesador de este tipo de instancia ejecutando la operación de EC2 DescribeInstanceTypes.

Especificaciones de hardware para clases de instancia de base de datos

En las tablas de esta sección, podrá encontrar información de hardware sobre las clases de instancias de base de datos de Amazon RDS para.

Para obtener información sobre la compatibilidad del motor de base de datos de Amazon RDS para cada clase de instancia de base de datos, consulte Motores de base de datos compatibles para clases de instancia de base de datos.

Temas

- Terminología de hardware para clases de instancias de base de datos
- Especificaciones de hardware para las clases de instancias de uso general
- Especificaciones de hardware para las clases de instancia optimizada para memoria
- Especificaciones de hardware para las clases de instancia optimizada para la computación
- Especificaciones de hardware para las clases de instancias de rendimiento ampliable

Terminología de hardware para clases de instancias de base de datos

La siguiente terminología se utiliza para describir las especificaciones de hardware para clases de instancia de base de datos:

vCPU

El número de unidades de procesamiento central (CPU) virtuales. Una CPU virtual es una unidad de capacidad que se puede usar para comparar clases de instancia de base de datos. En lugar de comprar o arrendar un procesamiento concreto para usarlo durante varios meses o años, la capacidad se alquila por horas. Nuestro objetivo es proporcionar una cantidad constante y específica de capacidad de CPU dentro de los límites del hardware subyacente real.

ECU

La medida relativa de la potencia de procesamiento íntegra de una instancia de Amazon EC2. Para facilitar a los desarrolladores la comparación de la capacidad de la CPU entre distintas clases de instancia, hemos definido una unidad de computación Amazon EC2. La cantidad de CPU asignada a una instancia concreta se expresa en términos de estas unidades informáticas EC2. Actualmente, una ECU proporciona capacidad de CPU equivalente a un procesador 2007 Opteron o 2007 Xeon de 1,0–1,2 GHz.

Memoria (GiB)

La RAM, en gibibytes, asignada a la instancia de base de datos. A menudo, hay una relación coherente entre memoria y vCPU. Como ejemplo, seleccione la clase de instancia db.r4, que dispone de una memoria en la relación de vCPU similar a la clase de instancia db.r5. Sin

embargo, para la mayoría de casos de uso, la clase de instancia db.r5 proporciona un mejor rendimiento y más coherente que la clase de instancia db.r4.

Optimizado para EBS

Una instancia de base de datos utiliza una pila de configuración optimizada y proporciona capacidad adicional y dedicada para las E/S. Esta optimización proporciona el mejor rendimiento, ya que reduce al mínimo la contención entre las E/S y otro tráfico procedente de la instancia. Para obtener más información acerca de las instancias optimizadas para Amazon EBS, consulte Instancias optimizadas para Amazon EBS en la guía del usuario de Amazon EC2.

Las instancias optimizadas para EBS tienen una tasa de IOPS máxima y de referencia. La tasa de IOPS máxima se aplica en el nivel de instancia de base de datos. Si se combina un conjunto de volúmenes de EBS para tener una tasa de IOPS superior a la máxima, este no puede superar el umbral a nivel de instancia. Por ejemplo, si el número máximo de IOPS para una clase de instancia de base de datos determinada es de 40 000 y se asocian cuatro volúmenes de EBS de 64 000 IOPS, el número máximo de IOPS será de 40 000 en lugar de 256 000. Para obtener el máximo de IOPS de cada tipo de instancia de EC2, consulte Tipos de instancias admitidos en la Guía del usuario de instancias de Linux de Amazon EC2.

Ancho de banda Ancho de banda de EBS (MB/s)

El ancho de banda máximo de EBS en megabits por segundo. Divídalo entre 8 para obtener el rendimiento esperado en megabytes por segundo.

> **Important**
>
> Los volúmenes SSD de uso general (gp2) para instancias de bases de datos de Amazon RDS tienen un límite de velocidad de 250 MiB/s en la mayoría de los casos. Sin embargo, su límite de velocidad puede variar en función del tamaño del volumen. Para obtener más información, consulte Tipos de volúmenes de Amazon EBS en la Guía del usuario de Amazon EC2.

Ancho de banda de red

La velocidad de red relativa a otras clases de instancia de base de datos.

Especificaciones de hardware para las clases de instancias de uso general

En las siguientes tablas, aparecen las especificaciones de computación, memoria, almacenamiento y ancho de banda para las clases de instancias de uso general.

db.m8g: clases de instancia de uso general con tecnología de procesadores AWS Graviton4

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m8g.48xlarge	192	—	768	Solo optimizado para EBS	40 000	50
db.m8g.24xlarge	96	—	512	Solo optimizado para EBS	30.000	40
db.m8g.16xlarge	64	—	384	Solo optimizado para EBS	20 000	30
db.m8g.12xlarge	48	—	256	Solo optimizado para EBS	15.000	22,5
db.m8g.8xlarge	32	—	128	Solo optimizado para EBS	10 000	15
db.m8g.4xlarge*	16	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.m8g.2xlarge*	8	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 15

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m8g.xlarge*	4	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m8g.large*	2	—	8	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.m7i: clases de instancia de uso general con tecnología de procesadores Intel Xeon Scalable de 4.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m7i.48xlarge	192	—	768	Solo optimizado para EBS	40 000	50
db.m7i.24xlarge	96	—	384	Solo optimizado para EBS	30.000	37,5
db.m7i.16xlarge	64	—	256	Solo optimizado para EBS	20 000	25
db.m7i.12xlarge	48	—	192	Solo optimizado para EBS	15.000	18,75

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m7i.8xlarge	32	—	128	Solo optimizado para EBS	10 000	12,5
db.m7i.4xlarge	16	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m7i.2xlarge	8	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m7i.xlarge	4	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m7i.large	2	—	8	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.m7g: clases de instancias de uso general con tecnología de procesadores AWS Graviton3

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m7g.16xlarge	64	—	256	Solo optimizado para EBS	20 000	30

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m7g.12xlarge	48	—	192	Solo optimizado para EBS	15.000	22,5
db.m7g.8xlarge	32	—	128	Solo optimizado para EBS	10 000	15
db.m7g.4xlarge	16	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.m7g.2xlarge*	8	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.m7g.xlarge*	4	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m7g.large*	2	—	8	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.m6g: clases de instancia de uso general con tecnología de procesadores Graviton2 de AWS.

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6g.16xlarge	64	—	256	Solo optimizado para EBS	19 000	25
db.m6g.12xlarge	48	—	192	Solo optimizado para EBS	13 500	20
db.m6g.8xlarge	32	—	128	Solo optimizado para EBS	9,000	12
db.m6g.4xlarge	16	—	64	Solo optimizado para EBS	4750	Hasta 10
db.m6g.2xlarge*	8	—	32	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.m6g.xlarge*	4	—	16	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.m6g.large*	2	—	8	Solo optimizado para EBS	Hasta 4750.	Hasta 10

db.m6g: clases de instancias de uso general con tecnología de procesadores Graviton2 de AWS y almacenamiento SSD

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6gd.16xlarge	64	—	256	SSD NVMe de 2 x 1900	19 000	25
db.m6gd.12xlarge	48	—	192	SSD NVMe de 2 x 1425	13 500	20
db.m6gd.8xlarge	32	—	128	SSD NVMe de 1 x 1900	9,000	12
db.m6gd.4xlarge*	16	—	64	SSD NVMe de 1 x 950	4750	Hasta 10
db.m6gd.2xlarge*	8	—	32	SSD NVMe de 1 x 474	Hasta 4750.	Hasta 10
db.m6gd.xlarge*	4	—	16	SSD NVMe de 1 x 237	Hasta 4750.	Hasta 10
db.m6gd.large*	2	—	8	SSD NVMe de 1 x 118	Hasta 4750.	Hasta 10

db.m6id: clases de instancias de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación y almacenamiento SSD

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6id.32xlarge	128	—	512	SSD NVMe de 4 x 1900	40 000	50

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6id.24xlarge	96	—	384	SSD NVMe de 4 x 1425	30.000	37,5
db.m6id.16xlarge	64	—	256	SSD NVMe de 2 x 1900	20 000	25
db.m6id.12xlarge	48	—	192	SSD NVMe de 2 x 1425	15.000	18,75
db.m6id.8xlarge	32	—	128	SSD NVMe de 1 x 1900	10 000	12,5
db.m6id.4xlarge*	16	—	64	SSD NVMe de 1 x 950	Hasta 10 000	Hasta 12,5
db.m6id.2xlarge*	8	—	32	SSD NVMe de 1 x 474	Hasta 10 000	Hasta 12,5
db.m6id.xlarge*	4	—	16	SSD NVMe de 1 x 237	Hasta 10 000	Hasta 12,5
db.m6id.large*	2	—	8	SSD NVMe de 1 x 118	Hasta 10 000	Hasta 12,5

db.m6idn: clases de instancia de uso general con procesadores escalables Intel Xeon de tercera generación, almacenamiento SSD y optimización de red

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6idn.32xlarge	128	—	512	SSD NVMe de 4 x 1900	80 000	200
db.m6idn.24xlarge	96	—	384	SSD NVMe de 4 x 1425	60 000	150
db.m6idn.16xlarge	64	—	256	SSD NVMe de 2 x 1900	40 000	100
db.m6idn.12xlarge	48	—	192	SSD NVMe de 2 x 1425	30.000	75
db.m6idn.8xlarge	32	—	128	SSD NVMe de 1 x 1900	20 000	50
db.m6idn.4xlarge*	16	—	64	SSD NVMe de 1 x 950	Hasta 20 000	Hasta 50
db.m6idn.2xlarge*	8	—	32	SSD NVMe de 1 x 474	Hasta 20 000	Hasta 40
db.m6idn.xlarge*	4	—	16	SSD NVMe de 1 x 237	Hasta 20 000	Hasta 30
db.m6idn.large*	2	—	8	SSD NVMe de 1 x 118	Hasta 20 000	Hasta 25

db.m6in: clases de instancias de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación y optimización de red

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6in.32xlarge	128	—	512	Solo optimizado para EBS	80 000	200
db.m6in.24xlarge	96	—	384	Solo optimizado para EBS	60 000	150
db.m6in.16xlarge	64	—	256	Solo optimizado para EBS	40 000	100
db.m6in.12xlarge	48	—	192	Solo optimizado para EBS	30.000	75
db.m6in.8xlarge	32	—	128	Solo optimizado para EBS	20 000	50
db.m6in.4xlarge*	16	—	64	Solo optimizado para EBS	Hasta 20 000	Hasta 50
db.m6in.2xlarge*	8	—	32	Solo optimizado para EBS	Hasta 20 000	Hasta 40
db.m6in.xlarge*	4	—	16	Solo optimizado para EBS	Hasta 20 000	Hasta 30

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6in.large*	2	—	8	Solo optimizado para EBS	Hasta 20 000	Hasta 25

db.m6in: clases de instancias de uso general con tecnología de procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6i.32xlarge	128	—	512	Solo optimizado para EBS	40 000	50
db.m6i.24xlarge	96	—	384	Solo optimizado para EBS	30.000	37,5
db.m6g.16xlarge	64	—	256	Solo optimizado para EBS	20 000	25
db.m6i.12xlarge	48	—	192	Solo optimizado para EBS	15.000	18,75
db.m6i.8xlarge	32	—	128	Solo optimizado para EBS	10 000	12,5

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m6i.4xlarge*	16	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m6i.2xlarge*	8	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m6i.xlarge*	4	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.m6i.large*	2	—	8	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.m5d: clases de instancias de uso general con tecnología de procesadores Intel Xeon Platinum y almacenamiento SSD

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m5d.24xlarge	96	345	384	SSD NVMe de 4 x 900	19 000	25
db.m5d.16xlarge	64	262	256	SSD NVMe de 4 x 600	13 600	20
db.m5d.12xlarge	48	173	192	SSD NVMe de 2 x 900	9500	10

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m5d.8xlarge	32	131	128	SSD NVMe de 2 x 600	6800	10
db.m5d.4xlarge	16	61	64	SSD NVMe de 2 x 300	4750	Hasta 10
db.m5d.2xlarge*	8	31	32	SSD NVMe de 1 x 300	Hasta 4750.	Hasta 10
db.m5d.xlarge*	4	15	16	SSD NVMe de 1 x 150	Hasta 4750.	Hasta 10
db.m5d.large*	2	10	8	SSD NVMe de 1 x 75	Hasta 4750.	Hasta 10

db.m5: clases de instancia de uso general con procesadores Intel Xeon Platinum

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m5.24xlarge	96	345	384	Solo optimizado para EBS	19 000	25
db.m5.16xlarge	64	262	256	Solo optimizado para EBS	13 600	20

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m5.12xlarge	48	173	192	Solo optimizado para EBS	9500	10
db.m5.8xlarge	32	131	128	Solo optimizado para EBS	6800	10
db.m5.4xlarge	16	61	64	Solo optimizado para EBS	4750	Hasta 10
db.m5.2xlarge*	8	31	32	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.m5.xlarge*	4	15	16	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.m5.large*	2	10	8	Solo optimizado para EBS	Hasta 4750.	Hasta 10

db.m4: clases de instancia de uso general con procesadores escalables Intel Xeon

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m4.16xlarge	64	188	256	Solo optimizado para EBS	10 000	25
db.m4.10xlarge	40	124.5	160	Solo optimizado para EBS	4.000	10
db.m4.4xlarge	16	53.5	64	Solo optimizado para EBS	2,000	Alta
db.m4.2xlarge	8	25.5	32	Solo optimizado para EBS	1 000	Alta
db.m4.xlarge	4	13	16	Solo optimizado para EBS	750	Alta
db.m4.large	2	6.5	8	Solo optimizado para EBS	450	Moderado

db.m3: clases de instancia de uso general

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.m3.2xlarge	8	26	30	Solo optimizado para EBS	1 000	Alta
db.m3.xlarge	4	13	15	Solo optimizado para EBS	500	Alta
db.m3.large	2	6.5	7.5	EBS solo	—	Moderado
db.m3.medium	1	3	3.75	EBS solo	—	Moderado

* Estos tipos de clases de instancia de base de datos pueden admitir un rendimiento máximo durante 30 minutos una vez cada 24 horas, como mínimo. Para obtener más información sobre el rendimiento de referencia de estos tipos de instancia de EC2 subyacentes, consulte Instancias optimizadas de Amazon EBS en la Guía del usuario de Amazon EC2.

Especificaciones de hardware para las clases de instancia optimizada para memoria

En las siguientes tablas, aparecen las especificaciones de computación, memoria, almacenamiento y ancho de banda para las clases de instancia optimizada para memoria.

db.z1d: clases de instancia de memoria optimizada

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.z1d.12xlarge	48	271	384	SSD NVMe de 2 x 900	14 000	25

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.z1d.6xlarge	24	134	192	SSD NVMe de 1 x 900	7000	10
db.z1d.3xlarge	12	75	96	SSD NVMe de 1 x 450	3500	Hasta 10
db.z1d.2xlarge	8	53	64	SSD NVMe de 1 x 300	2333	Hasta 10
db.z1d.xlarge*	4	28	32	SSD NVMe de 1 x 150	Hasta 2333	Hasta 10
db.z1d.large*	2	15	16	SSD NVMe de 1 x 75	Hasta 2333	Hasta 10

db.x2g: clases de instancia optimizada para memoria con procesadores Graviton2 de AWS

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2g.16xlarge	64	—	1024	Solo optimizado para EBS	19 000	25
db.x2g.12xlarge	48	—	768	Solo optimizado para EBS	14 250	20

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2g.8xlarge	32	—	512	Solo optimizado para EBS	9500	12
db.x2g.4xlarge	16	—	256	Solo optimizado para EBS	4750	Hasta 10
db.x2g.2xlarge	8	—	128	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.x2g.xlarge	4	—	64	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.x2g.large	2	—	32	Solo optimizado para EBS	Hasta 4750.	Hasta 10

db.x2idn: clases de instancia optimizada para memoria con procesadores escalables Intel Xeon de 3.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2idn.32xlarge	128	—	2048	SSD NVMe de 2 x 1900	80 000	100

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2idn.24xlarge	96	—	1536	SSD NVMe de 2 x 1425	60 000	75
db.x2idn.16xlarge	64	—	1 024	SSD NVMe de 1 x 1900	40 000	50

db.x2iedn: clases de instancia optimizada para memoria con SSD local basado en NVMe y con procesadores escalables Intel Xeon de 3.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2iedn.32xlarge	128	—	4.096	SSD NVMe de 2 x 1900	80 000	100
db.x2iedn.24xlarge	96	—	3072	SSD NVMe de 2 x 1425	60 000	75
db.x2iedn.16xlarge	64	—	2048	SSD NVMe de 1 x 1900	40 000	50
db.x2iedn.8xlarge	32	—	1 024	SSD NVMe de 1 x 950	20 000	25
db.x2iedn.4xlarge	16	—	512	SSD NVMe de 1 x 475	Hasta 20 000	Hasta 25
db.x2iedn.2xlarge	8	—	256	SSD NVMe de 1 x 237	Hasta 20 000	Hasta 25

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2iedn.xlarge	4	—	128	SSD NVMe de 1 x 118	Hasta 20 000	Hasta 25

db.x2iezn: clases de instancia optimizada para memoria con procesadores escalables Intel Xeon de 2.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x2iezn.12xlarge	>48	—	1536	Solo optimizado para EBS	19 000	100
db.x2iezn.8xlarge	32	—	1 024	Solo optimizado para EBS	12 000	75
db.x2iezn.6xlarge	24	—	768	Solo optimizado para EBS	Hasta 9500	50
db.x2iezn.4xlarge	16	—	512	Solo optimizado para EBS	Hasta 4750.	Hasta 25
db.x2iezn.2xlarge	8	—	256	Solo optimizado para EBS	Hasta 3170	Hasta 25

db.x1e: clases de instancia optimizada para memoria

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x1e.32xlarge	128	340	3,904	Solo optimizado para EBS	14 000	25
db.x1e.16xlarge	64	179	1,952	Solo optimizado para EBS	7000	10
db.x1e.8xlarge	32	91	976	Solo optimizado para EBS	3500	Hasta 10
db.x1e.4xlarge	16	47	488	Solo optimizado para EBS	1.750	Hasta 10
db.x1e.2xlarge	8	23	244	Solo optimizado para EBS	1 000	Hasta 10
db.x1e.xlarge	4	12	122	Solo optimizado para EBS	500	Hasta 10

db.x1: clases de instancia optimizada para memoria

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.x1.32xlarge	128	349	1,952	Solo optimizado para EBS	14 000	25
db.x1.16xlarge	64	174,5	976	Solo optimizado para EBS	7000	10

db.r8g: clases de instancia optimizada para memoria con procesadores Graviton4 de AWS

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r8g.48xlarge	192	—	1536	Solo optimizado para EBS	40 000	50
db.r8g.24xlarge	96	—	768	Solo optimizado para EBS	30.000	40
db.r8g.16xlarge	64	—	512	Solo optimizado para EBS	20 000	30
db.r8g.12xlarge	48	—	384	Solo optimizado para EBS	15.000	22,5

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r8g.8xlarge	32	—	256	Solo optimizado para EBS	10 000	15
db.r8g.4xlarge*	16	—	128	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.r8g.2xlarge*	8	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.r8g.xlarge*	4	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r8g.large*	2	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.r7i: clases de instancia optimizada para memoria con tecnología de procesadores Intel Xeon Scalable de 4.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r7i.48xlarge	192	—	1536	Solo optimizado para EBS	40 000	50

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r7i.24xlarge	96	—	768	Solo optimizado para EBS	30.000	37,5
db.r7i.16xlarge	64	—	512	Solo optimizado para EBS	20 000	25
db.r7i.12xlarge	48	—	384	Solo optimizado para EBS	15.000	18,75
db.r7i.8xlarge	32	—	256	Solo optimizado para EBS	10 000	12,5
db.r7i.4xlarge	16	—	128	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r7i.2xlarge	8	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r7i.xlarge	4	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r7i.large	2	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.r7g: clases de instancia optimizada para memoria con procesadores Graviton3 de AWS

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r7g.16xlarge	64	—	512	Solo optimizado para EBS	20 000	30
db.r7g.12xlarge	48	—	384	Solo optimizado para EBS	15.000	22,5
db.r7g.8xlarge	32	—	256	Solo optimizado para EBS	10 000	15
db.r7g.4xlarge	16	—	128	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.r7g.2xlarge*	8	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 15
db.r7g.xlarge*	4	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r7g.large*	2	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.r6g - clases de instancia optimizada para memoria con procesadores Graviton2 de AWS

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6g.16xlarge	64	—	512	Solo optimizado para EBS	19 000	25
db.r6g.12xlarge	48	—	384	Solo optimizado para EBS	13 500	20
db.r6g.8xlarge	32	—	256	Solo optimizado para EBS	9,000	12
db.r6g.4xlarge	16	—	128	Solo optimizado para EBS	4750	Hasta 10
db.r6g.2xlarge*	8	—	64	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.r6g.xlarge*	4	—	32	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.r6g.large*	2	—	16	Solo optimizado para EBS	Hasta 4750.	Hasta 10

db.r6gd: clases de instancia optimizada para memoria con procesadores Graviton2 de AWS y almacenamiento SSD

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6gd.16xlarge	64	—	512	SSD NVMe de 2 x 1900	19 000	25
db.r6gd.12xlarge	48	—	384	SSD NVMe de 2 x 1425	13 500	20
db.r6gd.8xlarge	32	—	256	SSD NVMe de 1 x 1900	9,000	12
db.r6gd.4xlarge	16	—	128	SSD NVMe de 1 x 950	4750	Hasta 10
db.r6gd.2xlarge	8	—	64	SSD NVMe de 1 x 474	Hasta 4750.	Hasta 10
db.r6gd.xlarge	4	—	32	SSD NVMe de 1 x 237	Hasta 4750.	Hasta 10
db.r6gd.large	2	—	16	SSD NVMe de 1 x 118	Hasta 4750.	Hasta 10

db.r6id: clases de instancia optimizada para memoria con procesadores escalables Intel Xeon de 3.ª generación y almacenamiento SSD

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6id.32xlarge	128	—	1 024	SSD NVMe de 4 x 1900	40 000	50

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6id.24xlarge	96	—	768	SSD NVMe de 4 x 1425	30.000	37,5
db.r6id.16xlarge	64	—	512	SSD NVMe de 2 x 1900	20 000	25
db.r6id.12xlarge	48	—	384	SSD NVMe de 2 x 1425	15.000	18,75
db.r6id.8xlarge	32	—	256	SSD NVMe de 1 x 1900	10 000	12,5
db.r6id.4xlarge*	16	—	128	SSD NVMe de 1 x 950	Hasta 10 000	Hasta 12,5
db.r6id.2xlarge*	8	—	64	SSD NVMe de 1 x 474	Hasta 10 000	Hasta 12,5
db.r6id.xlarge*	4	—	32	SSD NVMe de 1 x 237	Hasta 10 000	Hasta 12,5
db.r6id.large*	2	—	16	SSD NVMe de 1 x 118	Hasta 10 000	Hasta 12,5

db.r6idn: clases de instancia optimizada para memoria con procesadores escalables Intel Xeon de 3.ª generación, almacenamiento SSD y optimización de red

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6idn.32xlarge	128	—	1 024	SSD NVMe de 4 x 1900	80 000	200
db.r6idn.24xlarge	96	—	768	SSD NVMe de 4 x 1425	60 000	150
db.r6idn.16xlarge	64	—	512	SSD NVMe de 2 x 1900	40 000	100
db.r6idn.12xlarge	48	—	384	SSD NVMe de 2 x 1425	30.000	75
db.r6idn.8xlarge	32	—	256	SSD NVMe de 1 x 1900	20 000	50
db.r6idn.4xlarge*	16	—	128	SSD NVMe de 1 x 950	Hasta 20 000	Hasta 50
db.r6idn.2xlarge*	8	—	64	SSD NVMe de 1 x 474	Hasta 20 000	Hasta 40
db.r6idn.xlarge*	4	—	32	SSD NVMe de 1 x 237	Hasta 20 000	Hasta 30
db.r6idn.large*	2	—	16	SSD NVMe de 1 x 118	Hasta 20 000	Hasta 25

db.r6in: clases de instancia optimizada para memoria con procesadores escalables Intel Xeon de 3.ª generación y optimización de red

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6in.32xlarge	128	—	1 024	Solo optimizado para EBS	80 000	200
db.r6in.24xlarge	96	—	768	Solo optimizado para EBS	60 000	150
db.r6in.16xlarge	64	—	512	Solo optimizado para EBS	40 000	100
db.r6in.12xlarge	48	—	384	Solo optimizado para EBS	30.000	75
db.r6in.8xlarge	32	—	256	Solo optimizado para EBS	20 000	50
db.r6in.4xlarge*	16	—	128	Solo optimizado para EBS	Hasta 20 000	Hasta 50
db.r6in.2xlarge*	8	—	64	Solo optimizado para EBS	Hasta 20 000	Hasta 40
db.r6in.xlarge*	4	—	32	Solo optimizado para EBS	Hasta 20 000	Hasta 30

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6in.large*	2	—	16	Solo optimizado para EBS	Hasta 20 000	Hasta 25

db.r6i: clases de instancia optimizada para memoria de Oracle y preconfiguradas para alta memoria, almacenamiento y E/S

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6i.8xlarge.tpc2.mem4x	32	—	1024	Solo optimizado para EBS	40 000	50
db.r6i.8xlarge.tpc2.mem3x	32	—	768	Solo optimizado para EBS	30.000	37,5
db.r6i.6xlarge.tpc2.mem4x	24	—	768	Solo optimizado para EBS	30.000	37,5
db.r6i.4xlarge.tpc2.mem4x	16	—	512	Solo optimizado para EBS	20 000	25
db.r6i.4xlarge.tpc2.mem3x	16	—	384	Solo optimizado para EBS	15.000	18,75

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6i.4xlarge.tpc2.mem2x	16	—	256	Solo optimizado para EBS	10 000	12,5
db.r6i.2xlarge.tpc2.mem8x	8	—	512	Solo optimizado para EBS	20 000	12,5
db.r6i.2xlarge.tpc2.mem4x	8	—	256	Solo optimizado para EBS	10 000	12,5
db.r6i.2xlarge.tpc1.mem2x	8	—	128	Solo optimizado para EBS	Hasta 10 000	12,5
db.r6i.xlarge.tpc2.mem4x	4	—	128	Solo optimizado para EBS	Hasta 10 000	12,5
db.r6i.xlarge.tpc2.mem2x	4	—	64	Solo optimizado para EBS	Hasta 10 000	12,5
db.r6i.large.tpc1.mem2x	2	—	32	Solo optimizado para EBS	Hasta 10 000	12,5

db.r6i: clases de instancia optimizada para memoria con procesadores Intel Xeon Scalable de 3.ª generación

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6i.32xlarge	128	—	1 024	Solo optimizado para EBS	40 000	50
db.r6i.24xlarge	96	—	768	Solo optimizado para EBS	30.000	37,5
db.r6i.16xlarge	64	—	512	Solo optimizado para EBS	20 000	25
db.r6g.12xlarge	48	—	384	Solo optimizado para EBS	15.000	18,75
db.r6i.8xlarge	32	—	256	Solo optimizado para EBS	10 000	12,5
db.r6i.4xlarge*	16	—	128	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r6i.2xlarge*	8	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5
db.r6i.xlarge*	4	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r6i.large*	2	—	16	Solo optimizado para EBS	Hasta 10 000	Hasta 12,5

db.r5d: clases de instancia optimizada para memoria con procesadores Intel Xeon Platinum y almacenamiento SSD

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5d.24xlarge	96	347	768	SSD NVMe de 4 x 900	19 000	25
db.r5d.16xlarge	64	264	512	SSD NVMe de 4 x 600	13 600	20
db.r5d.12xlarge	48	173	384	SSD NVMe de 2 x 900	9500	10
db.r5d.8xlarge	32	132	256	SSD NVMe de 2 x 600	6800	10
db.r5d.4xlarge	16	71	128	SSD NVMe de 2 x 300	4750	Hasta 10
db.r5d.2xlarge*	8	38	64	SSD NVMe de 1 x 300	Hasta 4750.	Hasta 10
db.r5d.xlarge*	4	19	32	SSD NVMe de 1 x 150	Hasta 4750.	Hasta 10

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5d.large*	2	10	16	SSD NVMe de 1 x 75	Hasta 4750.	Hasta 10

db.r5b: clases de instancia optimizada para memoria y preconfiguradas para alta memoria, almacenamiento y E/S

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5b.8xlarge.tpc2.mem3x	32	—	768	Solo optimizado para EBS	60 000	25
db.r5b.6xlarge.tpc2.mem4x	24	—	768	Solo optimizado para EBS	60 000	25
db.r5b.4xlarge.tpc2.mem4x	16	—	512	Solo optimizado para EBS	40 000	20
db.r5b.4xlarge.tpc2.mem3x	16	—	384	Solo optimizado para EBS	30.000	10
db.r5b.4xlarge.tpc2.mem2x	16	—	256	Solo optimizado para EBS	20 000	10

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5b.2xlarge.tpc2.mem8x	8	—	512	Solo optimizado para EBS	40 000	20
db.r5b.2xlarge.tpc2.mem4x	8	—	256	Solo optimizado para EBS	20 000	10
db.r5b.2xlarge.tpc1.mem2x	8	—	128	Solo optimizado para EBS	10 000	Hasta 10
db.r5b.xlarge.tpc2.mem4x	4	—	128	Solo optimizado para EBS	10 000	Hasta 10
db.r5b.xlarge.tpc2.mem2x	4	—	64	Solo optimizado para EBS	Hasta 10 000	Hasta 10
db.r5b.large.tpc1.mem2x	2	—	32	Solo optimizado para EBS	Hasta 10 000	Hasta 10

db.r5b: clases de instancia optimizada para memoria con procesadores Intel Xeon Platinum y optimización EBS

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5b.24xlarge	96	347	768	Solo optimizado para EBS	60 000	25
db.r5b.16xlarge	64	264	512	Solo optimizado para EBS	40 000	20
db.r5b.12xlarge	48	173	384	Solo optimizado para EBS	30.000	10
db.r5b.8xlarge	32	132	256	Solo optimizado para EBS	20 000	10
db.r5b.4xlarge	16	71	128	Solo optimizado para EBS	10 000	Hasta 10
db.r5b.2xlarge*	8	38	64	Solo optimizado para EBS	Hasta 10 000	Hasta 10
db.r5b.xlarge*	4	19	32	Solo optimizado para EBS	Hasta 10 000	Hasta 10
db.r5b.large*	2	10	16	Solo optimizado para EBS	Hasta 10 000	Hasta 10

db.r5: clases de instancia optimizada para memoria y preconfiguradas para alta memoria, almacenamiento y E/S

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5.12xlarge.tpc2.mem2x	48	—	768	Solo optimizado para EBS	19 000	25
db.r5.8xlarge.tpc2.mem3x	32	—	768	Solo optimizado para EBS	19 000	25
db.r5.6xlarge.tpc2.mem4x	24	—	768	Solo optimizado para EBS	19 000	25
db.r5.4xlarge.tpc2.mem4x	16	—	512	Solo optimizado para EBS	13 600	20
db.r5.4xlarge.tpc2.mem3x	16	—	384	Solo optimizado para EBS	9500	10
db.r5.4xlarge.tpc2.mem2x	16	—	256	Solo optimizado para EBS	6800	10
db.r5.2xlarge.tpc2.mem8x	8	—	512	Solo optimizado para EBS	13 600	20

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5.2xlarge.tpc2.mem4x	8	—	256	Solo optimizado para EBS	6800	10
db.r5.2xlarge.tpc1.mem2x	8	—	128	Solo optimizado para EBS	4750	Hasta 10
db.r5.xlarge.tpc2.mem4x	4	—	128	Solo optimizado para EBS	4750	Hasta 10
db.r5.xlarge.tpc2.mem2x	4	—	64	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.r5.large.tpc1.mem2x	2	—	32	Solo optimizado para EBS	Hasta 4750.	Hasta 10

db.r5: clases de instancia optimizada para memoria

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5.24xlarge	96	347	768	Solo optimizado para EBS	19 000	25

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r5.16xlarge	64	264	512	Solo optimizado para EBS	13 600	20
db.r5.12xlarge	48	173	384	Solo optimizado para EBS	9500	12
db.r5.8xlarge	32	132	256	Solo optimizado para EBS	6800	10
db.r5.4xlarge	16	71	128	Solo optimizado para EBS	4750	Hasta 10
db.r5.2xlarge*	8	38	64	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.r5.xlarge*	4	19	32	Solo optimizado para EBS	Hasta 4750.	Hasta 10
db.r5.large*	2	10	16	Solo optimizado para EBS	Hasta 4750.	Hasta 10

db.r4: clases de instancia optimizada para memoria con procesadores Intel Xeon Scalable

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r4.16xlarge	64	195	488	Solo optimizado para EBS	14 000	25
db.r4.8xlarge	32	99	244	Solo optimizado para EBS	7000	10
db.r4.4xlarge	16	53	122	Solo optimizado para EBS	3500	Hasta 10
db.r4.2xlarge	8	27	61	Solo optimizado para EBS	1.700	Hasta 10
db.r4.xlarge	4	13.5	30.5	Solo optimizado para EBS	850	Hasta 10
db.r4.large	2	7	15.25	Solo optimizado para EBS	425	Hasta 10

db.r3: clases de instancia optimizada para memoria

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r3.8xlarge**	32	104	244	EBS solo	—	10

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.r3.4xlarge	16	52	122	Solo optimizado para EBS	2,000	Alta
db.r3.2xlarge	8	26	61	Solo optimizado para EBS	1 000	Alta
db.r3.xlarge	4	13	30.5	Solo optimizado para EBS	500	Moderado
db.r3.large	2	6.5	15.25	Solo optimizado para EBS	—	Moderado

* Estos tipos de clases de instancia de base de datos pueden admitir un rendimiento máximo durante 30 minutos una vez cada 24 horas, como mínimo. Para obtener más información sobre el rendimiento de referencia de estos tipos de instancia de EC2 subyacentes, consulte Instancias optimizadas de Amazon EBS en la Guía del usuario de Amazon EC2.

** La clase de instancia de base de datos r3.8xlarge no tiene ancho de banda de EBS dedicado y, por lo tanto, no ofrece optimización de EBS. Para esta clase de instancia, el tráfico de red y el tráfico de Amazon EBS comparten la misma interfaz de red de 10 gigabits.

Especificaciones de hardware para las clases de instancia optimizada para la computación

En las siguientes tablas, aparecen las especificaciones de computación, memoria, almacenamiento y ancho de banda para las clases de instancia optimizada para la computación.

db.c6gd: clases de instancias optimizadas para la computación (solo para implementaciones de clústeres de bases de datos multi-AZ)

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.c6gd.16xlarge	64	—	128	SSD NVMe de 2 x 1900	19 000	25
db.c6gd.12xlarge	48	—	96	SSD NVMe de 2 x 1425	13 500	20
db.c6gd.8xlarge	32	—	64	SSD NVMe de 1 x 1900	9,000	12
db.c6gd.4xlarge	16	—	32	SSD NVMe de 1 x 950	4750	Hasta 10
db.c6gd.2xlarge	8	—	16	SSD NVMe de 1 x 474	Hasta 4750.	Hasta 10
db.c6gd.xlarge	4	—	8	SSD NVMe de 1 x 237	Hasta 4750.	Hasta 10
db.c6gd.large	2	—	4	SSD NVMe de 1 x 118	Hasta 4750.	Hasta 10
db.c6gd.medium	1	—	2	SSD NVMe de 1 x 59	Hasta 4750.	Hasta 10

Especificaciones de hardware para las clases de instancias de rendimiento ampliable

En las siguientes tablas, aparecen las especificaciones de computación, memoria, almacenamiento y ancho de banda para las clases de instancia de rendimiento ampliable.

db.t4g: clases de instancia de rendimiento ampliable con la tecnología de los procesadores Graviton2 de AWS

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.t4g.2xlarge*	8	—	32	Solo optimizado para EBS	Hasta 2048.	Hasta 5
db.t4g.xlarge*	4	—	16	Solo optimizado para EBS	Hasta 2048.	Hasta 5
db.t4g.large*	2	—	8	Solo optimizado para EBS	Hasta 2048.	Hasta 5
db.t4g.medium*	2	—	4	Solo optimizado para EBS	Hasta 2085	Hasta 5
db.t4g.small*	2	—	2.	Solo optimizado para EBS	Hasta 2085	Hasta 5
db.t4g.micro*	2.	—	1	Solo optimizado para EBS	Hasta 2085	Hasta 5

db.t3: clases de instancia de rendimiento ampliable

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.t3.2xlarge*	8	Variab	32	Solo optimizado para EBS	Hasta 2048.	Hasta 5
db.t3.xlarge*	4	Variab	16	Solo optimizado para EBS	Hasta 2048.	Hasta 5
db.t3.large*	2	Variab	8	Solo optimizado para EBS	Hasta 2048.	Hasta 5
db.t3.medium*	2	Variab	4	Solo optimizado para EBS	Hasta 1536.	Hasta 5
db.t3.small*	2	Variab	2	Solo optimizado para EBS	Hasta 1536.	Hasta 5
db.t3.micro	2	Variab	1	Solo optimizado para EBS	Hasta 1536.	Hasta 5

db.t2: clases de instancia de rendimiento ampliable

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.t2.2xlarge	8	Variab	32	EBS solo	—	Moderado

Clase de instancia	vCPU	ECU	Memoria (GiB)	Almacenamiento de la instancia (GiB)	Ancho de banda Ancho de banda de EBS (MB/s)	Ancho de banda de la red (Gbps)
db.t2.xlarge	4	Variab	16	EBS solo	—	Moderado
db.t2.large	2	Variab	8	EBS solo	—	Moderado
db.t2.medium	2	Variab	4	EBS solo	—	Moderado
db.t2.small	1	Variab	2	EBS solo	—	Baja
db.t2.micro	1	Variab	1	EBS solo	—	Bajo

* Estos tipos de clases de instancia de base de datos pueden admitir un rendimiento máximo durante 30 minutos una vez cada 24 horas, como mínimo. Para obtener más información sobre el rendimiento de referencia de estos tipos de instancia de EC2 subyacentes, consulte Instancias optimizadas de Amazon EBS en la Guía del usuario de Amazon EC2.

Almacenamiento de instancias de base de datos de Amazon RDS

Las instancias de base de datos de Amazon RDS para Bd2, MariaDB, MySQL, PostgreSQL, Oracle y Microsoft SQL Server usan volúmenes de Amazon Elastic Block Store (Amazon EBS) para el almacenamiento de bases de datos y archivos de registro.

En algunos casos, es posible que la carga de trabajo de base de datos no logre el 100 por cien de las IOPS que ha aprovisionado. Para obtener más información, consulte Factores que afectan al rendimiento del almacenamiento.

Para obtener más información acerca de los precios de almacenamiento de instancias, consulte Precios de Amazon RDS.

Tipos de almacenamiento de Amazon RDS

Amazon RDS ofrece tres tipos de almacenamiento: SSD de IOPS aprovisionadas (denominado también io1 y io2 Block Express), SSD de uso general (denominado también gp2 y gp3) y magnético (también conocido como estándar). Se diferencian por las características de desempeño y en el precio, lo que quiere decir que puede adaptar el desempeño y el costo del almacenamiento a las necesidades de la carga de trabajo de su base de datos. Puede crear instancias de base de datos de Db2, MySQL, MariaDB, Oracle, SQL Server y PostgreSQL RDS con hasta 64 TiB de almacenamiento. RDS para Db2 no admite los tipos gp2 y de almacenamiento magnético.

En la lista siguiente se describen brevemente los tres tipos de almacenamiento:

- SSD de IOPS aprovisionadas: el almacenamiento de IOPS aprovisionadas está diseñado para satisfacer las necesidades de las cargas de trabajo con uso intensivo de operaciones de E/S, en especial de las cargas de trabajo de bases de datos, que requieren una latencia de E/S baja y un rendimiento de E/S constante. El almacenamiento de IOPS aprovisionadas es el más adecuado para los entornos de producción.

  Para obtener más información sobre el almacenamiento de IOPS aprovisionadas, incluidos los rangos de tamaños de almacenamiento, consulte Almacenamiento de SSD de IOPS aprovisionadas.
- SSD de uso general: los volúmenes SSD de uso general ofrecen un almacenamiento rentable que resulta idóneo para una amplia variedad de cargas de trabajo en instancias de base de datos de tamaño medio. El almacenamiento de uso general es el más adecuado para entornos de desarrollo y pruebas.

Para obtener más información sobre el almacenamiento de SSD de uso general, incluidos los intervalos de tamaño de almacenamiento, consulte Almacenamiento de SSD de uso general.

- Magnético: Amazon RDS también admite el almacenamiento magnético para garantizar la compatibilidad con versiones anteriores. Es recomendable utilizar volúmenes SSD de uso general o SSD de IOPS aprovisionadas para las nuevas necesidades de almacenamiento. La cantidad máxima de almacenamiento que se permite para instancias de base de datos en el almacenamiento magnético es de 3 TiB. Para obtener más información, consulte Almacenamiento magnético (heredado, no recomendado).

Al seleccionar SSD de uso general o SSD de IOPS aprovisionadas, según el motor elegido y la cantidad de almacenamiento solicitada, Amazon RDS distribuye automáticamente varios volúmenes para mejorar el rendimiento, tal como se muestra en la siguiente tabla.

Motor de base de datos	Tamaño de almacenamiento de Amazon RDS	Número de volúmenes aprovisionados
Db2	Menos de 400 GiB	1
Db2	400–65 536 GiB	4
MariaDB, MySQL y PostgreSQL	Menos de 400 GiB	1
MariaDB, MySQL y PostgreSQL	400–65 536 GiB	4
Oracle	Menos de 200 GiB	1
Oracle	200–65 536 GiB	4
SQL Server	Cualquiera	1

Al modificar un volumen de SSD de uso general o de SSD de IOPS aprovisionadas, este pasa por una serie de estados. Mientras el volumen está en el estado `optimizing`, el rendimiento del volumen estará entre las especificaciones de las configuraciones de origen y de destino. El rendimiento del volumen transitorio estará por encima del de las dos especificaciones bajas.

> **Important**
>
> Al modificar el almacenamiento de una instancia para que pase de un volumen a cuatro, o al modificar una instancia mediante el almacenamiento magnético, Amazon RDS no utiliza la característica Volúmenes elásticos. En cambio, Amazon RDS aprovisiona nuevos volúmenes y mueve los datos del volumen anterior a los nuevos volúmenes de forma transparente. Esta operación consume una cantidad significativa de IOPS y de rendimiento tanto del volumen antiguo como de los nuevos. Según el tamaño del volumen y la cantidad de carga de trabajo de la base de datos presente durante la modificación, esta operación puede consumir una gran cantidad de IOPS, aumentar significativamente la latencia de E/S y tardar varias horas en completarse, mientras la instancia de RDS permanezca en el estado `Modifying`.

Almacenamiento de SSD de IOPS aprovisionadas

Para cualquier aplicación de producción que requiera un rendimiento de E/S rápido y coherente, recomendamos el almacenamiento de IOPS aprovisionadas. El almacenamiento de IOPS aprovisionadas es un tipo de almacenamiento que ofrece un desempeño predecible y una latencia baja en todo momento. El almacenamiento de IOPS aprovisionadas está optimizado para las cargas de trabajo de procesamiento de transacciones online (OLTP) que tienen requisitos de rendimiento coherentes. Las IOPS aprovisionadas ayudan a ajustar el desempeño de estas cargas de trabajo.

Cuando se crea una instancia de base de datos, se especifica la velocidad de IOPS y el tamaño del volumen. Amazon RDS proporciona esa tasa de IOPS para la instancia de base de datos hasta que la cambie.

Amazon RDS ofrece dos tipos de almacenamiento SSD de IOPS aprovisionadas: Almacenamiento io2 Block Express (recomendado) y Almacenamiento io1 (generación anterior).

Almacenamiento io2 Block Express (recomendado)

Para las cargas de trabajo con uso intensivo de E/S y sensibles a la latencia, puede utilizar el almacenamiento io2 Block Express de IOPS aprovisionadas y lograr hasta 256 000 operaciones de E/S por segundo (IOPS). El rendimiento de los volúmenes de io2 Block Express varía en función de la cantidad de IOPS aprovisionadas por volumen y del tamaño de las operaciones de E/S que se estén ejecutando.

Todos los volúmenes io2 de RDS basados en AWS Nitro System son volúmenes de io2 Block Express y ofrecen una latencia media inferior a un milisegundo. Las instancias de base de datos que no están basadas en AWS Nitro System son volúmenes io2.

En la siguiente tabla se muestra el intervalo de IOPS aprovisionadas y de rendimiento máximo para el motor de base de datos y el rango de tamaño de almacenamiento.

Motor de base de datos	Rango de tamaño de almacenamiento	Rango de IOPS aprovisionadas	Rendimiento máximo
Db2, MariaDB, MySQL y PostgreSQL	100–65 536 GiB	De 1000 a 256 000 IOPS	16 000 MiB/s
Oracle	100–199 GiB	1000–199 000 IOPS	16 000 MiB/s
Oracle	200–65 536 GiB	De 1000 a 256 000 IOPS	16 000 MiB/s
SQL Server	20–65 536 GiB	De 1000 a 256 000 IOPS	16 000 MiB/s

Las IOPS y los rangos de tamaño de almacenamiento presentan las siguientes restricciones:

- La relación entre IOPS y almacenamiento asignado (en GiB) no debe ser mayor de 1000:1. Para las instancias de bases de datos que no están basadas en AWS Nitro System, la relación es de 500:1.
- Las IOPS máximas se pueden aprovisionar con volúmenes de 256 GiB y más grandes (1000 IOPS × 256 GiB = 256 000 IOPS). Para las instancias de base de datos que no están basadas en AWS Nitro System, las IOPS máximas se alcanzan a 512 GiB (500 IOPS x 512 GiB = 256 000 IOPS).
- El rendimiento se escala de manera proporcional hasta 0,256 MiB/s por IOPS provisionadas. Se puede lograr un rendimiento máximo de 4000 MiB/s a 256 000 IOPS con un tamaño de E/S de 16 KiB y 16 000 IOPS o más con un tamaño de E/S de 256 KiB. Para las instancias de base de datos que no están basadas en AWS Nitro System, se puede lograr un rendimiento máximo de 2000 MiB/s a 128 000 IOPS con un tamaño de E/S de 16 KiB.
- Si utilizas el escalado automático de almacenamiento, también se aplican las mismas relaciones entre IOPS y el umbral máximo de almacenamiento (en GiB). Para obtener más información sobre

el escalado automático del almacenamiento, consulte Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS.

Los volúmenes de io2 Block Express de Amazon RDS están disponibles en las siguientes:Regiones de AWS

- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europe (Londres)
- Europa (Estocolmo)
- Medio Oriente (Baréin)
- US East (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)

Almacenamiento io1 (generación anterior)

Para las cargas de trabajo con uso intensivo de E/S, puede utilizar el almacenamiento SSD io1 de IOPS aprovisionadas y lograr hasta 256 000 operaciones de E/S por segundo (IOPS). El rendimiento de los volúmenes io1 varía en función de la cantidad de IOPS aprovisionadas por volumen y del tamaño de las operaciones de IO que se estén ejecutando. Recomendamos utilizar el almacenamiento io2 Block Express cuando esté disponible.

En la siguiente tabla se muestra el intervalo de IOPS aprovisionadas y de rendimiento máximo para el motor de base de datos y el rango de tamaño de almacenamiento.

Motor de base de datos	Rango de tamaño de almacenamiento	Rango de IOPS aprovisionadas	Rendimiento máximo
Db2, MariaDB, MySQL y PostgreSQL	100–399 GiB	De 1000 a 19 950 IOPS	500 MiB/s
Db2, MariaDB, MySQL y PostgreSQL	400–65 536 GiB	De 1000 a 256 000 IOPS	4000 MiB/s
Oracle	100–199 GiB	De 1000 a 9950 IOPS	500 MiB/s
Oracle	200–65 536 GiB	1000–256 000 IOPS[1]	4000 MiB/s
SQL Server	20–16 384 GiB	1000–64 000 IOPS[2]	1000 MiB/s

Note

[1] Para Oracle, puede aprovisionar el máximo de 256 000 IOPS solo en el tipo de instancia r5b.
[2] Para SQL Server, el máximo de 64 000 IOPS solo está garantizado en instancias basadas en Nitro que se encuentran en los tipos de instancias m5*, m6i, r5*, r6i y z1d. Otros tipos de instancias garantizan un rendimiento de hasta 32 000 IOPS.

Las IOPS y los rangos de tamaño de almacenamiento presentan las siguientes restricciones:

- La relación entre IOPS y almacenamiento asignado (en GiB) debe ser de 1 a 50 en RDS para SQL Server y de 0,5 a 50 en otros motores de base de datos de RDS.
- Si utilizas el escalado automático de almacenamiento, también se aplican las mismas relaciones entre IOPS y el umbral máximo de almacenamiento (en GiB).

  Para obtener más información sobre el escalado automático del almacenamiento, consulte Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS.

Combinación del almacenamiento de IOPS aprovisionadas con implementaciones Multi-AZ o réplicas de lectura

Para los casos de uso de OLTP de producción, es recomendable usar implementaciones Multi-AZ para mejorar la tolerancia a errores con IOPS aprovisionadas con el fin de obtener un desempeño rápido y predecible.

También puede usar el almacenamiento de IOPS aprovisionadas con réplicas de lectura para MySQL, MariaDB o PostgreSQL. El tipo de almacenamiento de una réplica de lectura es independiente del de la instancia de base de datos principal. Por ejemplo, es posible que use SSD de uso general para réplicas de lectura con una instancia de base de datos principal que utilice el almacenamiento de SSD de IOPS aprovisionadas para reducir los costos. Sin embargo, en este caso, el rendimiento de sus réplicas de lectura es posible que difiera del de una configuración en la que tanto la instancia de base de datos principal como las réplicas de lectura usen almacenamiento de IOPS aprovisionadas.

Costos de almacenamiento de IOPS aprovisionadas

Con el almacenamiento de IOPS aprovisionadas, se le cobra por los recursos aprovisionados tanto si los usa como si no en un mes dado.

Para obtener más información acerca de los precios, consulte Precios de Amazon RDS.

Obtención del mejor rendimiento del almacenamiento de IOPS aprovisionadas de Amazon RDS

Si su carga de trabajo tiene restricciones de E/S, el uso del almacenamiento de IOPS aprovisionadas puede aumentar el número de solicitudes de E/S que el sistema puede procesar de forma simultánea. El aumento de la simultaneidad permite reducir la latencia, ya que las solicitudes de E/S pasan menos tiempo en una cola. Una latencia menor se traduce en confirmaciones más rápidas en la base de datos, lo que mejora el tiempo de respuesta y permite obtener un rendimiento más alto en la base de datos.

El almacenamiento de IOPS aprovisionadas proporciona una forma de reservar capacidad de E/S mediante la especificación de IOPS. Sin embargo, al igual que cualquier otro atributo de capacidad del sistema, su rendimiento máximo con carga quedará restringido por el recurso que se agote antes. Ese recurso podría ser el ancho de banda de la red, la CPU, la memoria o los recursos internos de la base de datos.

Almacenamiento de SSD de uso general

El almacenamiento de uso general ofrece un almacenamiento rentable que es aceptable para la mayoría de las cargas de trabajo de bases de datos no sensibles a la latencia o al rendimiento.

> **Note**
>
> Las instancias de base de datos que utilizan almacenamiento de uso general pueden experimentar una latencia mucho más larga que las instancias que utilizan almacenamiento de IOPS aprovisionadas. Si necesita una instancia de base de datos con latencia mínima después de estas operaciones, se recomienda utilizar Almacenamiento de SSD de IOPS aprovisionadas.

Amazon RDS ofrece dos tipos de almacenamiento de uso general: Almacenamiento gp3 (recomendado) y Almacenamiento pg2 (generación anterior).

Almacenamiento gp3 (recomendado)

Al utilizar volúmenes de almacenamiento gp3 de uso general, puede personalizar el rendimiento del almacenamiento independientemente de la capacidad de almacenamiento. El rendimiento de almacenamiento es la combinación de operaciones de E/S por segundo (IOPS) y la rapidez con que el volumen de almacenamiento puede realizar lecturas y escrituras (rendimiento de almacenamiento). En los volúmenes de almacenamiento gp3, Amazon RDS proporciona un rendimiento de almacenamiento de referencia de 3000 IOPS y 125 MiB/s.

Para cada motor de base de datos de RDS, excepto RDS para SQL Server, cuando el tamaño de almacenamiento para los volúmenes gp3 alcanza un umbral determinado, el rendimiento de almacenamiento de referencia aumenta. Esto se debe a la fragmentación de volúmenes, en la que el almacenamiento utiliza cuatro volúmenes en lugar de uno. RDS para SQL Server no admite la fragmentación de volúmenes y, por lo tanto, no tiene un valor de umbral. En los volúmenes fragmentados, Amazon RDS proporciona un rendimiento de almacenamiento de referencia de 12 000 IOPS y 500 MiB/s.

El rendimiento del almacenamiento de los volúmenes gp3 en los motores de base de datos de Amazon RDS, incluido el umbral, se muestra en la siguiente tabla.

Motor de base de datos	Tamaño del almacenamiento	Rendimiento del almacenamiento de referencia	Rango de IOPS aprovisionadas	Rango de rendimiento del almacenamiento aprovisionado
Db2, MariaDB, MySQL y PostgreSQL	20–399 GiB	3000 IOPS/125 MiB/s	N/A	N/A
Db2, MariaDB, MySQL y PostgreSQL	400–65 536 GiB	12 000 IOPS/500 MiB/s	De 12 000 a 64 000 IOPS	De 500 a 4000 MiB/s
Oracle	20–199 GiB	3000 IOPS/125 MiB/s	N/A	N/A
Oracle	200–65 536 GiB	12 000 IOPS/500 MiB/s	De 12 000 a 64 000 IOPS	De 500 a 4000 MiB/s
SQL Server	20–16 384 GiB	3000 IOPS/125 MiB/s	3000–16 000 IOPS	De 125 a 1000 MiB/s

Para cada motor de base de datos, excepto RDS para SQL Server, puede aprovisionar IOPS y rendimiento de almacenamiento adicionales cuando el tamaño del almacenamiento sea igual o superior al valor umbral. Para RDS para SQL Server, puede aprovisionar IOPS y rendimiento de almacenamiento adicionales para cualquier tamaño de almacenamiento disponible. Para todos los motores de base de datos, solo se paga por el rendimiento de almacenamiento aprovisionado adicional. Para obtener más información, consulte Precios de Amazon RDS.

Si bien las IOPS aprovisionadas y el rendimiento del almacenamiento añadidos no dependen del tamaño del almacenamiento, están relacionados entre sí. Cuando se elevan las IOPS por encima de 32 000 para MariaDB y MySQL, el valor del rendimiento del almacenamiento aumenta automáticamente desde los 500 MiBps. Por ejemplo, si establece el IOPS en 40 000 en RDS para MySQL, el rendimiento del almacenamiento debe ser de al menos 625 MiBps. El aumento automático no se produce para instancias de base de datos Db2, Oracle, PostgreSQL y SQL Server.

Para los clústeres de bases de datos multi-AZ, Amazon RDS establece automáticamente el valor de rendimiento en función de las IOPS que aprovisione. No puede modificar el valor de rendimiento.

Los valores de rendimiento del almacenamiento de los volúmenes gp3 en RDS tienen las siguientes restricciones:

- La proporción máxima entre el rendimiento del almacenamiento y las IOPS es de 0,25 para todos los motores de base de datos compatibles.
- La proporción mínima entre IOPS y el almacenamiento asignado (en GiB) es de 0,5 en RDS para SQL Server. No hay una proporción mínima para los demás motores de base de datos compatibles.
- La proporción máxima entre IOPS y el almacenamiento asignado es de 500 para todos los motores de base de datos compatibles.
- Si utilizas el escalado automático de almacenamiento, también se aplican las mismas relaciones entre IOPS y el umbral máximo de almacenamiento (en GiB).

  Para obtener más información sobre el escalado automático del almacenamiento, consulte Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS.

Almacenamiento pg2 (generación anterior)

Cuando sus aplicaciones no necesiten un alto rendimiento de almacenamiento, puede utilizar el almacenamiento gp2 de SSD de uso general. El rendimiento de E/S de referencia para almacenamiento gp2 es de 3 IOPS por cada GiB, con un mínimo de 100 IOPS. Esta relación implica que los volúmenes más grandes tendrán un mejor rendimiento. Por ejemplo, el rendimiento de referencia para un volumen de 100 GiB es de 300 IOPS. El rendimiento de referencia para un volumen de 1000 GiB es de 3000 IOPS.

Los volúmenes gp2 individuales inferiores a 1000 GiB en tamaño también podrán llegar a 3000 IOPS durante periodos de tiempo prolongados. El saldo de créditos de E/S del volumen determina el rendimiento por ráfagas. Para obtener una descripción más detallada de cómo afectan el rendimiento de referencia y el saldo de créditos de E/S al rendimiento, consulte el artículo de Comparación del rendimiento por ráfagas y de referencia con Amazon RDS y gp2 en el blog de AWS Database.

Muchas cargas de trabajo nunca agotan el balance de ráfagas. Sin embargo, algunas cargas de trabajo pueden agotar el saldo de créditos de almacenamiento de ráfagas de 3000 IOPS, por lo que debería planificar su capacidad de almacenamiento para dar respuesta a las necesidades de sus cargas de trabajo.

Para volúmenes gp2 superiores a 4000 GiB, el rendimiento de referencia es mayor que el rendimiento por ráfagas. Para estos volúmenes, la ráfaga es irrelevante porque el rendimiento de referencia es mejor que el rendimiento por ráfagas de 3000 IOPS. Sin embargo, para las instancias de base de datos de ciertos motores y tamaños, el almacenamiento se fragmenta en cuatro volúmenes, lo que proporciona cuatro veces el rendimiento inicial y cuatro veces la ráfaga de IOPS de un solo volumen.

En la siguiente tabla se muestra el rendimiento del almacenamiento de los volúmenes gp2 de varios tamaños de almacenamiento en los motores de base de datos de Amazon RDS.

Motor de base de datos	Tamaño de almacenamiento de RDS	Rango de IOPS de referencia	Rango de rendimiento de referencia	IOPS por ráfagas
MariaDB, MySQL y PostgreSQL	5–399 GiB[1]	De 100 a 1197 IOPS	De 128 a 250 MiB/s	3000
MariaDB, MySQL y PostgreSQL	400–1335 GiB	De 1200 a 4005 IOPS	512-1000 MiB/s	12 000
MariaDB, MySQL y PostgreSQL	1336–3999 GiB	De 4008 a 11 997 IOPS	1000 MiB/s	12 000
MariaDB, MySQL y PostgreSQL	4000–65 536 GiB	De 12 000 a 64 000 IOPS	1000 MiB/s	N/A[2]
Oracle	20–199 GiB	De 100 a 597 IOPS	De 128 a 250 MiB/s	3000
Oracle	200–1335 GiB	De 600 a 4005 IOPS	De 500 a 1000 MiB/s	12 000
Oracle	1336–3999 GiB	De 4008 a 11 997 IOPS	1000 MiB/s	12 000

Motor de base de datos	Tamaño de almacenamiento de RDS	Rango de IOPS de referencia	Rango de rendimiento de referencia	IOPS por ráfagas
Oracle	4000–65 536 GiB	De 12 000 a 64 000 IOPS	1000 MiB/s	N/A[2]
SQL Server	20–333 GiB	De 100 a 999 IOPS	De 128 a 250 MiB/s	3000
SQL Server	334–999 GiB	De 1002 a 2997 IOPS	250 MiB/s	3000
SQL Server	1000–16 384 GiB	De 3000 a 16 000 IOPS	250 MiB/s	N/A[2]

> **Note**
>
> [1] Con la AWS Management Console, puede crear instancias de base de datos con un tamaño de almacenamiento mínimo de 5 GiB en el nivel gratuito para las clases de instancias de base de datos db.t3.micro y db.t4g.micro. De lo contrario, el tamaño mínimo de almacenamiento es 20 GiB. Esta limitación no se aplica a la AWS CLI y la API de RDS.
> [2] El rendimiento de referencia del volumen excede el rendimiento por ráfagas máximo.

Comparación de tipos de almacenamiento de unidades de estado sólido (SSD)

La siguiente tabla muestra los casos de uso y las características de rendimiento de los volúmenes de almacenamiento SSD que usa Amazon RDS.

Característica	IOPS aprovisionadas (io2 Block Express)	IOPS aprovisionadas (io1)	Uso general (gp3)	Uso general (gp2)
Descripción	El rendimiento más alto dentro	Rendimiento de almacenam	Flexibilidad para aprovisionar el	Proporciona IOPS ampliables

Característica	IOPS aprovisionadas (io2 Block Express)	IOPS aprovisionadas (io1)	Uso general (gp3)	Uso general (gp2)
	de la gama de almacenamiento de RDS (IOPS, rendimiento, latencia) Diseñado para cargas de trabajo transaccionales sensibles a la latencia	iento uniforme (IOPS, rendimiento, latencia) Diseñado para cargas de trabajo transaccionales sensibles a la latencia	almacenamiento, las IOPS y el rendimiento de forma independiente Combinan precio y rendimiento para una gran variedad de cargas de trabajo transaccionales	Combinan precio y rendimiento para una gran variedad de cargas de trabajo transaccionales
Casos de uso	Cargas de trabajo transaccionales críticas para la empresa que requieren una latencia inferior a un milisegundo y un rendimiento de IOPS sostenido de hasta 256 000 IOPS	Cargas de trabajo transaccionales que requieren un rendimiento de IOPS sostenido de hasta 256 000 IOPS	Amplia gama de cargas de trabajo que se ejecutan en bases de datos relacionales de tamaño mediano en entornos de desarrollo y pruebas	Amplia gama de cargas de trabajo que se ejecutan en bases de datos relacionales de tamaño mediano en entornos de desarrollo y pruebas

Característica	IOPS aprovisionadas (io2 Block Express)	IOPS aprovisionadas (io1)	Uso general (gp3)	Uso general (gp2)
Latencia	Por debajo del milisegundo, proporcionado de forma constante el 99,9 % del tiempo	Milisegundo de un dígito, proporcionado de forma consistente el 99,9 % del tiempo	Milisegundo de un dígito, proporcionado de forma consistente el 99 % del tiempo	Milisegundo de un dígito, proporcionado de forma consistente el 99 % del tiempo
Tamaño del volumen	100–65 536 GiB	100–65 536 GiB (20–16 384 GiB en RDS para SQL Server)	20–65 536 GiB (16 384 GiB en RDS para SQL Server)	20–65 536 GiB (16 384 GiB en RDS para SQL Server)

Característica	IOPS aprovisionadas (io2 Block Express)	IOPS aprovisionadas (io1)	Uso general (gp3)	Uso general (gp2)
IOPS máximo	256 000	256 000 (64 000 en RDS para SQL Server)	64 000 (16 000 en RDS para SQL Server)	64 000 (16 000 en RDS para SQL Server) **Note** No puede aprovisionar IOPS directamente en el almacenamiento de gp2. Las IOPS varían según el tamaño de almacenamiento asignado.

Característica	IOPS aprovisionadas (io2 Block Express)	IOPS aprovisionadas (io1)	Uso general (gp3)	Uso general (gp2)
Rendimiento máximo	Escala en función de las IOPS aprovisionadas hasta 4000 Mb/s El rendimiento se escala de manera proporcional hasta 0,256 MiB/s por IOPS provisionadas. Se puede lograr un rendimiento máximo de 4000 MiB/s a 256 000 IOPS con un tamaño de E/S de 16 KiB y 16 000 IOPS o más con un tamaño de E/S de 256 KiB. Para las instancias que no están basadas en AWS Nitro System, se puede lograr un rendimien	Escala en función de las IOPS aprovisionadas hasta 4000 Mb/s	Proporciona rendimiento adicional de hasta 4000 Mb/s (1000 MB/s en RDS para SQL Server)	1000 Mb/s (250 Mb/s en RDS para SQL Server)

Característica	IOPS aprovisionadas (io2 Block Express)	IOPS aprovisionadas (io1)	Uso general (gp3)	Uso general (gp2)
	to máximo de 2000 MiB/s a 128 000 IOPS con un tamaño de E/S de 16 KiB.			
AWS CLI y nombre de la API de RDS	io2	io1	gp3	gp2

Almacenamiento magnético (heredado, no recomendado)

Amazon RDS también admite el almacenamiento magnético para garantizar la compatibilidad con versiones anteriores. Es recomendable utilizar volúmenes SSD de uso general o SSD de IOPS aprovisionadas para las nuevas necesidades de almacenamiento. A continuación se indican algunas limitaciones del almacenamiento magnético:

- No permite escalar el almacenamiento cuando se utiliza el motor de base de datos de SQL Server.
- No permite convertir a un tipo de almacenamiento diferente cuando se utiliza el motor de base de datos de SQL Server.
- No admite el escalado automático del almacenamiento.
- No admite volúmenes elásticos.
- Está limitado a un tamaño máximo de 3 TiB.
- Está limitado a un máximo de 1 000 IOPS.

Volumen de registro específico (DLV)

Puede utilizar un volumen de registro específico (DLV) para una instancia de base de datos que utilice el almacenamiento de IOPS aprovisionadas (PIOPS) mediante la consola de Amazon RDS, la AWS CLI o la API de Amazon RDS. Un DLV transporta los registros de transacciones de la base

de datos de PostgreSQL y los registros redo y registros binarios de MySQL/MariaDB a un volumen de almacenamiento independiente del volumen que contiene las tablas de la base de datos. Un DLV hace que el registro de escritura de transacciones sea más eficiente y uniforme. Los DLV son ideales para bases de datos con gran capacidad de almacenamiento asignado, requisitos elevados de E/S por segundo (IOPS) o cargas de trabajo donde la latencia es muy importante.

Los DLV son compatibles con el almacenamiento PIOPS (io1 y io2 Block Express) y se crean con un tamaño fijo de 1000 GiB y 3000 IOPS aprovisionadas.

> **Note**
>
> Los DLV no se admiten con el almacenamiento de uso general (gp2 y gp3).

Amazon RDS es compatible con los DLV en todas las Regiones de AWS para las siguientes versiones:

- MariaDB 10.6.7 y versiones 10 superiores
- MySQL 8.0.28 y versiones 8 superiores
- Versiones de PostgreSQL 13.10 y posteriores a 13, versiones 14.7 y posteriores a 14, versiones 15.2 y posteriores a 15 y versiones 16.1 y posteriores a 16

RDS es compatible con DLV con implementaciones Multi-AZ Al modificar o crear una instancia Multi-AZ, se crea un DLV tanto para la instancia principal como para la secundaria.

RDS admite DLV con réplicas de lectura. Si la instancia de base de datos principal tiene un DLV habilitado, todas las réplicas de lectura creadas después de habilitar el DLV también tendrán un DLV. Las réplicas de lectura creadas antes del cambio a DLV no la tendrán habilitada, a menos que se modifiquen explícitamente para ello. Es recomendable que todas las réplicas de lectura conectadas a una instancia principal antes de activar el DLV también se modifiquen manualmente para que tengan un DLV.

Una vez que haya modificado la configuración de DLV de una instancia de base de datos, esta se debe reiniciar.

Para obtener más información sobre cómo habilitar un DLV, consulte Uso de un volumen de registro específico (DLV).

Monitoreo del desempeño de almacenamiento

Amazon RDS proporciona varias métricas que se pueden usar para determinar el desempeño de la instancia de base de datos. Puede ver las métricas en la página de resumen de su instancia en la Management Console de Amazon RDS. También puede utilizar Amazon CloudWatch para monitorizar estas métricas. Para obtener más información, consulte Consulta de métricas en la consola de Amazon RDS. La monitorización mejorada proporciona unas métricas de E/S más detalladas. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Las siguientes métricas son útiles para monitorear el almacenamiento de una instancia de base de datos:

- IOPS: el número de operaciones de E/S que se completan por segundo. Esta métrica se indica como el promedio de IOPS para un intervalo de tiempo dado. Amazon RDS indica las IOPS de lectura y escritura por separado en intervalos de 1 minuto. El valor total de IOPS es la suma de las IOPS de lectura y escritura. Los valores típicos de IOPS van de cero a decenas de miles por segundo.
- Latencia: el tiempo transcurrido entre el envío de una solicitud de E/S y su finalización. Esta métrica se indica como la latencia promedio para un intervalo de tiempo dado. Amazon RDS indica la latencia de lectura y escritura por separado, en intervalos de 1 minuto. Los valores típicos de latencia están en milisegundos (ms).
- Rendimiento: número de bytes por segundo transferidos al disco o desde él. Esta métrica se indica como el rendimiento promedio para un intervalo de tiempo dado. Amazon RDS indica el rendimiento de lectura y escritura por separado en intervalos de 1 minuto y en unidades de bytes por segundo (B/s). Los valores típicos del rendimiento van desde cero al ancho de banda máximo del canal de E/S.
- Profundidad de la cola: el número de solicitudes de E/S de la cola en espera para ser respondidas. Son las solicitudes de E/S que ha enviado la aplicación pero no se han enviado al dispositivo porque este está ocupado respondiendo a otras solicitudes de E/S. El tiempo transcurrido esperando en la cola es un componente del tiempo de latencia y servicio (no disponible como métrica). Esta métrica se indica como la profundidad promedio de la cola para un intervalo de tiempo dado. Amazon RDS indica la profundidad de la cola en intervalos de 1 minuto. Los valores típicos de la profundidad de la cola van desde cero a varios cientos.

Los valores de IOPS medidos son independientes del tamaño de la operación de E/S específica. Esto significa que cuando mida el rendimiento de E/S, debería examinar el rendimiento de la instancia y no simplemente el número de operaciones de E/S.

Factores que afectan al rendimiento del almacenamiento

Tanto las actividades del sistema como la carga de trabajo de la base de datos y las clases de instancia de base de datos pueden afectar al rendimiento del almacenamiento.

Actividades del sistema

Las siguientes actividades relacionadas con el sistema consumen capacidad de E/S y podrían reducir el rendimiento de la instancia de base de datos mientras se llevan a cabo:

- Creación de instancias en espera en varias zonas de disponibilidad Multi-AZ
- Creación de réplicas de lectura
- Cambio de tipo de almacenamiento

Carga de trabajo de base de datos

En algunos casos, el diseño de la base de datos o de la aplicación provoca problemas de simultaneidad, bloqueo u otras formas de contención de la base de datos. En esos casos, es posible que no pueda usar directamente todo el ancho de banda aprovisionado. Además, se puede encontrar con las siguientes situaciones relacionadas con la carga de trabajo:

- Se ha alcanzado el límite de rendimiento del tipo de instancia subyacente.
- La profundidad de la cola es sistemáticamente inferior a 1 porque la aplicación no está produciendo suficientes operaciones de E/S.
- Existe contención de las consultas de la base de datos aunque hay capacidad de E/S sin usar.

En algunos casos, no hay un recurso del sistema que esté en un límite o se acerca a él y al agregar subprocesos no se incrementa la velocidad de las transacciones en la base de datos. En tales casos, el cuello de botella es probablemente una contención en la base de datos. Las formas más habituales son la contención de bloqueo de filas y de bloqueo de páginas de índice, pero hay muchas otras posibilidades. Si este es su caso, pida consejo a un experto en ajuste del rendimiento de base de datos.

Clase de instancia de base de datos

Para obtener el máximo rendimiento de su instancia de base de datos de Amazon RDS, elija un tipo de instancia de la generación actual con suficiente ancho de banda para permitir el tipo de almacenamiento elegido. Por ejemplo, puede elegir instancias optimizadas para Amazon EBS e instancias con una conectividad de red de 10 gigabits.

> **Important**
>
> Según la clase de instancia que esté utilizando, es posible que vea un rendimiento de IOPS menor que el máximo que RDS le permite aprovisionar. Para obtener información específica sobre el rendimiento de IOPS para clases de instancia de base de datos, consulte Instancias optimizadas para Amazon EBS en la Guía del usuario de Amazon EC2. Se recomienda determinar el máximo de IOPS para la clase de instancia antes de establecer un valor de IOPS aprovisionadas para la instancia de base de datos.

Le sugerimos que utilice la última generación de instancias para disfrutar del mejor rendimiento. Las instancias de base de datos de generaciones anteriores también pueden tener un máximo de almacenamiento menor.

Algunos sistemas de archivos antiguos de 32 bits podrían tener capacidades de almacenamiento más bajas. Para determinar la capacidad de almacenamiento de la instancia de base de datos, puede utilizar el comando de la AWS CLI describe-valid-db-instance-modificaciones.

La siguiente lista muestra el almacenamiento máximo al que pueden escalar la mayoría de las clases de instancia de base de datos para cada motor de base de datos:

- DB2: 64 TiB
- MariaDB: 64 TiB
- Microsoft SQL Server: 64 TiB
- MySQL: 64 TiB
- Oracle: 64 TiB
- PostgreSQL: 64 TiB

En la siguiente tabla, se muestran algunas excepciones para el almacenamiento máximo (en TiB). Todas las instancias de base de datos de RDS para Microsoft SQL Server, aparte del

almacenamiento io2 Block Express, tienen un almacenamiento máximo de 16 TiB, por lo que no hay entradas para SQL Server.

Clase de instancia	Db2	MariaDB	MySQL	Oracle	PostgreSQL
db.m3 – Clases de instancia estándar					
db.t4g: clases de instancia de rendimiento ampliable					
db.t4g.medium	N/A	16	16	N/A	32
db.t4g.small	N/A	16	16	N/A	16
db.t4g.micro	N/A	6	6	N/A	6
db.t3: clases de instancia de rendimiento ampliable					
db.t3.medium	32	16	16	32	32
db.t3.small	32	16	16	32	16
db.t3.micro	N/A	6	6	32	6
db.t2: clases de instancia de rendimiento ampliable					

Para obtener más información sobre todas las clases de instancias compatibles, consulte Instancias de base de datos de generación anterior.

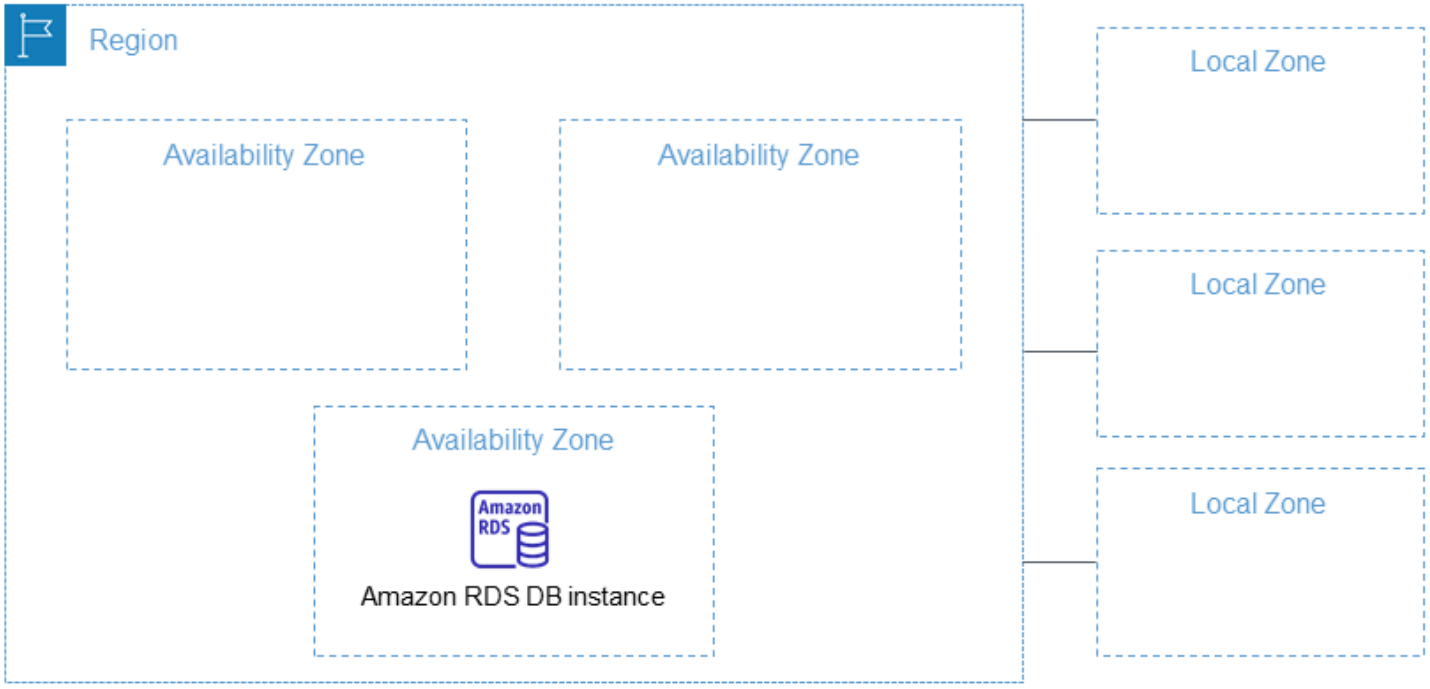
Regiones, zonas de disponibilidad y Local Zones

Los recursos de informática en la nube de Amazon están alojados en varias ubicaciones de todo el mundo. Dichas ubicaciones se componen de regiones de AWS, zonas de disponibilidad y zonas locales. Cada región de AWS es un área geográfica independiente. Cada región de AWS tiene varias ubicaciones aisladas conocidas como zonas de disponibilidad.

> **Note**
>
> Para obtener información acerca de cómo encontrar las zonas de disponibilidad de una región de AWS, consulte el tema donde se describen las zonas de disponibilidad en la documentación de Amazon EC2.

Las Local Zones le permiten colocar recursos, como de cómputo y de almacenamiento, en varias ubicaciones más cercanas a los usuarios finales. Amazon RDS le permite colocar recursos, como instancias de base de datos y datos en varias ubicaciones. Los recursos no se replican en las regiones de AWS, a menos que usted decida hacerlo específicamente.

Amazon opera centros de datos de alta disponibilidad con tecnología de vanguardia. Aunque es infrecuente, puede suceder que se produzcan errores que afecten a la disponibilidad de las instancias de bases de datos que están en la misma ubicación. Si aloja todas sus instancias de base de datos en una ubicación que se ve afectada por dicho error, ninguna de sus instancias de base de datos estará disponible.



Es importante recordar que cada región de AWS es completamente independiente. Cualquier actividad de Amazon RDS; que se inicie (por ejemplo, la creación de instancias de base de datos o la enumeración de las instancias de base de datos disponibles) se ejecuta solo en la región de AWS predeterminada actual. La Región de AWS por defecto se puede cambiar en la consola, o estableciendo la variable de entorno `AWS_DEFAULT_REGION`. O bien, se puede anular utilizando el parámetro `--region` con la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Configurar la AWS Command Line Interface, específicamente las secciones relativas a las variables de entorno y las opciones de la línea de comandos.

Amazon RDS admite las regiones especiales de AWS denominadas AWS GovCloud (US). Estas se han diseñado para permitir a los clientes y los organismos del Gobierno de Estados Unidos que traspasen cargas de trabajo más confidenciales a la nube. Mediante las regiones AWS GovCloud (US) se atienden las necesidades reglamentarias y de cumplimiento propias del Gobierno de Estados Unidos. Para obtener más información, consulte ¿Qué es AWS GovCloud (US)?

Para crear una instancia de base de datos de Amazon RDS o trabajar con ella en una región concreta de AWS, use el punto de enlace de servicio regional correspondiente.

AWSRegiones de

Cada región de AWS se ha diseñado para que esté totalmente aislada de las demás regiones de AWS. Este diseño logra la mayor tolerancia a errores y estabilidad posibles.

Cuando se consultan los recursos, solo se ven los recursos vinculados a la región de AWS especificada. Esto se debe a que las regiones de AWSestán aisladas entre sí y no replicamos automáticamente los recursos en distintas regiones de AWS.

Disponibilidad por región

En la tabla siguiente, se muestran las regiones de AWS donde Amazon RDS está disponible actualmente y el punto de enlace de cada región.

Nombre de la región	Región	Punto de conexión	Protocolo
Este de EE. UU. (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS
		rds-fips.us-east-2.api.aws	HTTPS
		rds.us-east-2.api.aws	HTTPS
		rds-fips.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS
		rds-fips.us-east-1.api.aws	HTTPS
		rds-fips.us-east-1.amazonaws.com	HTTPS
		rds.us-east-1.api.aws	HTTPS
Oeste de EE. UU. (Norte de California)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS
		rds.us-west-1.api.aws	HTTPS
		rds-fips.us-west-1.amazonaws.com	HTTPS
		rds-fips.us-west-1.api.aws	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS
		rds-fips.us-west-2.amazonaws.com	HTTPS
		rds.us-west-2.api.aws	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
		rds-fips.us-west-2.api.aws	HTTPS
África (Ciudad del Cabo)	af-south-1	rds.af-south-1.amazonaws.com rds.af-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	rds.ap-east-1.amazonaws.com rds.ap-east-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com rds.ap-south-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Yakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com rds.ap-southeast-3.api.aws	HTTPS HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	rds.ap-southeast-4.amazonaws.com rds.ap-southeast-4.api.aws	HTTPS HTTPS
Asia-Pacífico (Bombay)	ap-south-1	rds.ap-south-1.amazonaws.com rds.ap-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com rds.ap-northeast-3.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Seúl)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com rds.ap-northeast-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com rds.ap-southeast-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com rds.ap-southeast-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com rds.ap-northeast-1.api.aws	HTTPS HTTPS
Canadá (centro)	ca-central-1	rds.ca-central-1.amazonaws.com rds.ca-central-1.api.aws rds-fips.ca-central-1.api.aws rds-fips.ca-central-1.amazonaws.com	HTTPS HTTPS HTTPS HTTPS
Oeste de Canadá (Calgary)	ca-west-1	rds.ca-west-1.amazonaws.com rds-fips.ca-west-1.amazonaws.com	HTTPS HTTPS
Europa (Fráncfort)	eu-central-1	rds.eu-central-1.amazonaws.com rds.eu-central-1.api.aws	HTTPS HTTPS
Europa (Irlanda)	eu-west-1	rds.eu-west-1.amazonaws.com rds.eu-west-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Londres)	eu-west-2	rds.eu-west-2.amazonaws.com rds.eu-west-2.api.aws	HTTPS HTTPS
Europa (Milán)	eu-south-1	rds.eu-south-1.amazonaws.com rds.eu-south-1.api.aws	HTTPS HTTPS
Europa (París)	eu-west-3	rds.eu-west-3.amazonaws.com rds.eu-west-3.api.aws	HTTPS HTTPS
Europa (España)	eu-south-2	rds.eu-south-2.amazonaws.com rds.eu-south-2.api.aws	HTTPS HTTPS
Europa (Estocolmo)	eu-north-1	rds.eu-north-1.amazonaws.com rds.eu-north-1.api.aws	HTTPS HTTPS
Europa (Zúrich)	eu-central-2	rds.eu-central-2.amazonaws.com rds.eu-central-2.api.aws	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	rds.il-central-1.amazonaws.com rds.il-central-1.api.aws	HTTPS HTTPS
Medio Oriente (Baréin)	me-south-1	rds.me-south-1.amazonaws.com rds.me-south-1.api.aws	HTTPS HTTPS
Medio Oriente (EAU)	me-central-1	rds.me-central-1.amazonaws.com rds.me-central-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
América del Sur (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com rds.sa-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com rds.us-gov-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (Oeste de EE.UU.)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com rds.us-gov-west-1.api.aws	HTTPS HTTPS

Si no especifica expresamente un punto de enlace, el punto de enlace de EE.UU. Oeste (Oregón) es el ajuste predeterminado.

Cuando trabaje con una instancia de base de datos utilizando las operaciones de la AWS CLI o de la API, asegúrese de especificar su punto de enlace regional.

Zonas de disponibilidad

Cuando crea una instancia de base de datos, puede elegir una zona de disponibilidad o hacer que Amazon RDS elija una al azar. Una zona de disponibilidad está representada por un código de región de AWSseguido de un identificador de letra (por ejemplo, `us-east-1a`).

Utilice el comando describe-availability-zones de Amazon EC2, tal y como se indica a continuación, para describir las zonas de disponibilidad dentro de la región especificada que están habilitadas para su cuenta.

```
aws ec2 describe-availability-zones --region region-name
```

Por ejemplo, para describir las zonas de disponibilidad de la región Este de EE. UU. (Norte de Virginia) (us-east-1) que están habilitadas para su cuenta, ejecute el siguiente comando:

```
aws ec2 describe-availability-zones --region us-east-1
```

No puede elegir las zonas de disponibilidad para las instancias de base de datos primaria y secundaria en una implementación de base de datos Multi-AZ. Amazon RDS las elige de forma aleatoria. Para obtener más información sobre las implementaciones Multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

> **Note**
>
> La selección aleatoria de zonas de disponibilidad de RDS no garantiza una distribución uniforme de instancias de base de datos entre las zonas de disponibilidad dentro de una sola cuenta o grupo de subred de base de datos. Puede solicitar una zona de disponibilidad específica cuando crea o modifica una instancia Single-AZ y puede utilizar grupos de subred de base de datos más específicos para instancias Multi-AZ. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS y Modificación de una instancia de base de datos de Amazon RDS.

Zonas locales

Una Zona local es una extensión de una región de AWS que está geográficamente cerca de sus usuarios. Puede ampliar cualquier VPC de la región de AWS principal a las zonas locales. Para ellos, cree una nueva subred y asígnela a la zona local de AWS. Cuando crea una subred en una zona local, la VPC también se amplía a dicha zona local. La subred de la zona local funciona igual que otras subredes de su VPC.

Al crear una instancia de base de datos, puede elegir una subred en una zona local. Las zonas locales tienen sus propias conexiones a internet y admiten AWS Direct Connect. Por lo tanto, los recursos creados en una zona local pueden prestar servicio a los usuarios locales con comunicaciones de muy baja latencia. Para obtener más información, consulte AWS Local Zones.

Una zona local se representa mediante un código de región de AWS seguido de un identificador que indica la ubicación, por ejemplo, `us-west-2-lax-1a`.

> **Note**
>
> Las zonas locales no se pueden incluir en una implementación Multi-AZ.

Para utilizar una zona local

1. Habilite la zona local en la consola de Amazon EC2.

   Para obtener más información, consulte Habilitación de Local Zones en la Guía del usuario de Amazon EC2.
2. Cree una subred en la zona local.

   Para obtener más información, consulte Creación de una subred en la VPC en la Guía del usuario de Amazon VPC.
3. Cree un grupo de subredes de base de datos en la zona local.

   Al crear un grupo de subredes de base de datos, elija el grupo de zonas de disponibilidad para la zona local.

   Para obtener más información, consulte Creación de una instancia de base de datos en una VPC.
4. Cree una instancia de base de datos que utilice el grupo de subredes de base de datos en la zona local.

   Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

> **Important**
>
> Actualmente, la única zona local de AWS donde Amazon RDS está disponible es Los Ángeles, en la región Oeste de EE. UU. (Oregón).

Funciones admitidas en Amazon RDS por Región de AWS y el motor de base de datos

Compatibilidad con las características y opciones de Amazon RDS según las Regiones de AWS y las versiones específicas de cada motor de base de datos. Para identificar la compatibilidad y la disponibilidad de la versión del motor de base de datos RDS en una Región de AWS determinada, puede utilizar las siguientes secciones.

Las características nativas de Amazon RDS son diferentes de las características y opciones nativas del motor. Para obtener más información acerca de características y opciones nativas del motor, consulte Funciones nativas del motor.

Regiones y motores de base de datos admitidos

- Convenciones de tabla
- Referencia rápida de características
- Regiones y motores de base de datos admitidos para implementaciones azul/verde de Amazon RDS
- Regiones y motores de bases de datos admitidos para copias de seguridad automatizadas entre regiones en Amazon RDS
- Regiones y motores de bases de datos admitidos para réplicas de lectura entre regiones en Amazon RDS
- Regiones y motores de base de datos admitidos para los flujos de actividad de bases de datos en Amazon RDS
- Regiones y motores de bases de datos admitidos para el modo de doble pila en Amazon RDS
- Regiones y motores de base de datos admitidos para exportar instantáneas a S3 en Amazon RDS
- Regiones y motores de base de datos admitidos para autenticación de base de datos IAM en Amazon RDS
- Regiones y motores de base de datos admitidos para autenticación de Kerberos en Amazon RDS
- Regiones y motores de base de datos admitidos para clústeres de bases de datos Multi-AZ en Amazon RDS
- Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS
- Regiones y motores de base de datos admitidos para RDS Custom

- Regiones y motores de base de datos para Amazon RDS Proxy
- Regiones y motores de bases de datos admitidos para la integración de Secrets Manager con Amazon RDS
- Regiones y motores de base de datos admitidos para las integraciones sin ETL de Amazon RDS
- Características nativas del motor en Amazon RDS

Convenciones de tabla

Las tablas en las secciones de características utilizan estos patrones para especificar los números de versión y el nivel de disponibilidad:

- Versión x.y: solo está disponible la versión específica.
- Versión x.y y posteriores: se admiten la versión especificada y todas las versiones secundarias posteriores. Por ejemplo, “versión 10.11 y posteriores” significa que están disponibles las versiones 10.11, 10.11.1 y 10.12.

Referencia rápida de características

La siguiente tabla de referencia rápida incluye cada característica y motor de base de datos RDS que hay disponible. La disponibilidad en regiones y versiones específicas se indica en las secciones posteriores sobre las características.

Caract stica	RDS para Db2	RDS para MariaDB	RDS para MySQL	RDS para Oracle	RDS para PostgreSQL	RDS para SQL Server
Implen acione azul/ verd e	No disponibl e	Disponible	Disponible	No disponibl e	Disponible	No disponibl e
Copias de seguri autom adas	Disponible	Disponible	Disponible	Disponible	Disponible	Disponible

Caract stica	RDS para Db2	RDS para MariaDB	RDS para MySQL	RDS para Oracle	RDS para PostgreSQL	RDS para SQL Server
entre region						
Réplic de lectura entre region	No disponibl e	Disponible	Disponible	Disponible	Disponible	Disponible
Secue s de activid es de la base de datos	No disponibl e	No disponibl e	No disponibl e	Disponible	No disponibl e	Disponible
Modo de pila doble	No disponibl e	Disponible	Disponible	Disponible	Disponible	Disponible
Export instant eas a Amazo S3	No disponibl e	Disponible	Disponible	No disponibl e	Disponible	No disponibl e

Caract stica	RDS para Db2	RDS para MariaDB	RDS para MySQL	RDS para Oracle	RDS para PostgreSQL	RDS para SQL Server
AWS Identit and Acces Manag tAuten ación de base de datos de (IAM)	No disponibl e	Disponible	Disponible	No disponibl e	Disponible	No disponibl e
Autent ción de Kerbe	Disponible	No disponibl e	Disponible	Disponible	Disponible	Disponible
Clúste de base de datos Multi-AZ	No disponibl e	No disponibl e	Disponible	No disponibl e	Disponible	No disponibl e
Perfor ce Insight	No disponibl e	Disponible	Disponible	Disponible	Disponible	Disponible
RDS persor zado	No disponibl e	No disponibl e	No disponibl e	Disponible	No disponibl e	Disponible

Caract stica	RDS para Db2	RDS para MariaDB	RDS para MySQL	RDS para Oracle	RDS para PostgreSQL	RDS para SQL Server
RDS Proxy	No disponibl e	Disponible	Disponible	No disponibl e	Disponible	Disponible
Integra ón de Secret Manag	Disponible	Disponible	Disponible	Disponible	Disponible	Disponible

Regiones y motores de base de datos admitidos para implementaciones azul/verde de Amazon RDS

Una implementación azul/verde copia un entorno de base de datos de producción en un entorno de almacenamiento provisional sincronizado e independiente. Con las implementaciones azul/verde de Amazon RDS, puede realizar cambios en la base de datos en el entorno de almacenamiento provisional sin que eso afecte al entorno de producción. Por ejemplo, puede actualizar la versión principal o secundaria del motor de base de datos, cambiar los parámetros de la base de datos o realizar cambios de esquema en el entorno de almacenamiento provisional. Cuando esté listo, puede promocionar el entorno de almacenamiento provisional para que sea el nuevo entorno de base de datos de producción. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Las implementaciones azules/verdes se admiten en todas las Regiones de AWS.

La implementación azul/verde no se admite en los siguientes motores:

- RDS para Db2
- RDS para SQL Server
- RDS para Oracle

Temas

- Implementaciones azul/verde con RDS para MariaDB
- Implementaciones azules/verdes con RDS para MySQL

- Implementaciones azules/verdes con Aurora PostgreSQL

Implementaciones azul/verde con RDS para MariaDB

Para RDS para MariaDB, las implementaciones azul/verde son compatibles con las siguientes versiones:

- RDS para MariaDB 11.4 (todas las versiones disponibles)
- RDS para MariaDB 10.2 y versiones 10 posteriores

Implementaciones azules/verdes con RDS para MySQL

Para RDS para MySQL, las implementaciones azul/verde son compatibles con las siguientes versiones:

- RDS para MySQL 8.4 (todas las versiones disponibles)
- RDS para MySQL 8.0 (todas las versiones disponibles)
- RDS para MySQL 5.7 (todas las versiones disponibles)

Implementaciones azules/verdes con Aurora PostgreSQL

En el caso de RDS para PostgreSQL, las implementaciones azules/verdes son compatibles con la versión 11.1 y todas las versiones superiores, principales y secundarias.

> **Note**
>
> En determinadas condiciones, RDS para PostgreSQL utiliza la replicación lógica en lugar de la replicación física para mantener el entorno verde sincronizado con el entorno azul. Para obtener más información, consulte ???.

Regiones y motores de bases de datos admitidos para copias de seguridad automatizadas entre regiones en Amazon RDS

Al usar la replicación de copias de seguridad en Amazon RDS, puede configurar su instancia de base de datos de RDS para que replique las instantáneas y los registros de transacciones en una región

de destino. Cuando se configura la replicación de copia de seguridad para una instancia de base de datos, RDS inicia una copia entre regiones de todas las instantáneas y registros de transacciones cuando están listos. Para obtener más información, consulte Replicación de las copias de seguridad automatizadas en otra Región de AWS.

Para obtener información sobre las Regiones de AWS en las que está disponible la replicación de copia de seguridad, consulte Replicación de las copias de seguridad automatizadas en otra Región de AWS.

Temas

- Replicación de copias de seguridad con RDS para Db2
- Replicación de copias de seguridad con RDS para MariaDB
- Replicación de copias de seguridad con RDS para MySQL
- Replicación de copias de seguridad con RDS para Oracle
- Replicación de copias de seguridad con RDS para PostgreSQL
- Replicación de copias de seguridad con RDS para SQL Server

Replicación de copias de seguridad con RDS para Db2

Amazon RDS admite la replicación de copias de seguridad para todas las versiones de RDS para Db2 disponibles actualmente.

Replicación de copias de seguridad con RDS para MariaDB

Amazon RDS admite la replicación de copias de seguridad para todas las versiones de RDS para MariaDB disponibles actualmente.

Replicación de copias de seguridad con RDS para MySQL

Amazon RDS admite la replicación de copias de seguridad para todas las versiones de RDS para MySQL disponibles actualmente.

Replicación de copias de seguridad con RDS para Oracle

Amazon RDS admite la replicación de copias de seguridad para todas las versiones de RDS para Oracle disponibles actualmente.

Replicación de copias de seguridad con RDS para PostgreSQL

Amazon RDS admite la replicación de copias de seguridad para todas las versiones de RDS para PostgreSQL disponibles actualmente.

Replicación de copias de seguridad con RDS para SQL Server

Amazon RDS admite la replicación de copias de seguridad para todas las versiones de RDS para SQL Server disponibles actualmente.

Regiones y motores de bases de datos admitidos para réplicas de lectura entre regiones en Amazon RDS

Con las réplicas de lectura entre regiones en Amazon RDS, puede crear una réplica de lectura de MariaDB, MySQL, Oracle, PostgreSQL o SQL Server en una región diferente a la de la instancia de base de datos de origen. Para obtener información sobre las réplicas de lectura entre regiones, incluidas las réplicas de lectura entre regiones, consulte Creación de una réplica de lectura en una Región de AWS distinta.

Las réplicas de lectura entre regiones no están disponibles para los siguientes motores:

- RDS para Db2

Temas

- Réplicas de lectura entre regiones con RDS para MariaDB
- Réplicas de lectura entre regiones con RDS para MySQL
- Réplicas de lectura entre regiones con RDS para Oracle
- Réplicas de lectura entre regiones con RDS para PostgreSQL
- Réplicas de lectura entre regiones con RDS para SQL Server

Réplicas de lectura entre regiones con RDS para MariaDB

Las réplicas de lectura entre regiones con RDS para MariaDB están disponibles en todas las regiones para las siguientes versiones:

- RDS para MariaDB 11.4 (todas las versiones disponibles)
- RDS para MariaDB 10.11 (todas las versiones disponibles)

- RDS para MariaDB 10.6 (todas las versiones disponibles)
- RDS para MariaDB 10.5 (todas las versiones disponibles)
- RDS para MariaDB 10.4 (todas las versiones disponibles)

Réplicas de lectura entre regiones con RDS para MySQL

Las réplicas de lectura entre regiones con RDS para MySQL están disponibles en todas las regiones para las siguientes versiones:

- RDS para MySQL 8.4 (todas las versiones disponibles)
- RDS para MySQL 8.0 (todas las versiones disponibles)
- RDS para MySQL 5.7 (todas las versiones disponibles)

Réplicas de lectura entre regiones con RDS para Oracle

Las réplicas de lectura entre regiones con RDS para Oracle están disponibles en todas las Regiones de AWS para todas las versiones de bases de datos compatibles con Enterprise Edition. Las réplicas se admiten únicamente en entornos que no son CDB y en la configuración de un solo inquilino de la arquitectura CDB. Las réplicas de lectura entre regiones no se admiten en la configuración de varios inquilinos de la arquitectura CDB.

Para obtener más información sobre los requisitos adicionales para las réplicas de lectura entre regiones con RDS para Oracle, consulte Requisitos y consideraciones sobre réplicas de RDS para Oracle.

Réplicas de lectura entre regiones con RDS para PostgreSQL

Las réplicas de lectura entre regiones con RDS para PostgreSQL están disponibles en todas las regiones para las siguientes versiones:

- RDS para PostgreSQL 17 (todas las versiones disponibles)
- RDS para PostgreSQL 16 (todas las versiones disponibles)
- RDS para PostgreSQL 15 (todas las versiones disponibles)
- RDS para PostgreSQL 14 (todas las versiones disponibles)
- RDS para PostgreSQL 13 (todas las versiones disponibles)
- RDS para PostgreSQL 12 (todas las versiones disponibles)

- RDS para PostgreSQL 11 (todas las versiones disponibles)
- RDS para PostgreSQL 10 (todas las versiones disponibles)

Réplicas de lectura entre regiones con RDS para SQL Server

Las réplicas de lectura entre regiones con RDS para SQL Server están disponibles en todas las regiones excepto:

- Africa (Cape Town)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Oeste de Canadá (Calgary)
- Europa (Milán)
- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)

Las réplicas de lectura entre regiones con RDS para SQL Server están disponibles para las siguientes versiones que usen Microsoft SQL Server Enterprise Edition:

- RDS para SQL Server 2022
- RDS para SQL Server 2019 (versión 15.00.4073.23 y posteriores)
- RDS para SQL Server 2017 (versión 14.00.3281.6 y posteriores)
- RDS para SQL Server 2016 (versión 13.00.6300.2 y posteriores)

Regiones y motores de base de datos admitidos para los flujos de actividad de bases de datos en Amazon RDS

Con los flujos de actividad de la base de datos en Amazon RDS, puede supervisar y configurar alarmas para la actividad de auditoría en su base de datos Oracle y su base de datos SQL Server. Para obtener más información, consulte Información general sobre flujos de actividad de la base de datos.

Los flujos de actividades de la base de datos no están disponibles con los siguientes motores:

- RDS para Db2
- RDS para MariaDB
- RDS para MySQL
- RDS para PostgreSQL

Temas

- Secuencias de actividades de la base de datos con RDS para Oracle
- Flujos de actividad de bases de datos con RDS para SQL Server

Secuencias de actividades de la base de datos con RDS para Oracle

A continuación se detallan las regiones y las versiones de motores que están disponibles para secuencias de actividades de base de datos con RDS para Oracle.

Para obtener más información acerca de los requisitos adicionales para los flujos de actividades de la base de datos con RDS para Oracle, consulte Información general sobre flujos de actividad de la base de datos.

Región	RDS para Oracle 21c	RDS para Oracle 19c
Este de EE. UU. (Norte de Virginia)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Este de EE. UU. (Ohio)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando

Región	RDS para Oracle 21c	RDS para Oracle 19c
		la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Oeste de EE. UU. (Norte de California)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Oeste de EE. UU. (Oregón)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
África (Ciudad del Cabo)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Hong Kong)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Hyderabad)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Yakarta)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Malasia)	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible

Región	RDS para Oracle 21c	RDS para Oracle 19c
Asia Pacific (Bombay)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Osaka)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Seúl)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Singapur)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Sídney)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Asia-Pacífico (Tokio)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Canadá (centro)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)

Región	RDS para Oracle 21c	RDS para Oracle 19c
Oeste de Canadá (Calgary)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
China (Pekín)	No disponible	No disponible
China (Ningxia)	No disponible	No disponible
Europa (Fráncfort)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Europa (Irlanda)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Europa (Londres)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Europa (Milán)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Europa (París)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)

Región	RDS para Oracle 21c	RDS para Oracle 19c
Europa (España)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Europa (Estocolmo)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Europa (Zúrich)	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible
Medio Oriente (Baréin)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
Medio Oriente (EAU)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
América del Sur (São Paulo)	No disponible	Oracle Database 19.0.0.0.ru-2019-07.rur-2019-07.r1 y posteriores utilizando la Enterprise Edition (EE) o la Standard Edition 2 (SE2)
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible
AWS GovCloud (Oeste de EE.UU.)	No disponible	No disponible

Flujos de actividad de bases de datos con RDS para SQL Server

A continuación se detallan las regiones y las versiones de motores que están disponibles para secuencias de actividades de base de datos con RDS para SQL Server.

Para obtener más información acerca de los requisitos adicionales para los flujos de actividad de la base de datos con RDS para SQL Server, consulte Información general sobre flujos de actividad de la base de datos.

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible
Asia Pacific (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	No disponible	No disponible	No disponible
China (Ningxia)	No disponible	No disponible	No disponible
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE.UU.)	No disponible	No disponible	No disponible

Regiones y motores de bases de datos admitidos para el modo de doble pila en Amazon RDS

Al utilizar el modo de pila doble en RDS, los recursos pueden comunicarse con una instancia de base de datos a través del protocolo de Internet versión 4 (IPv4), del protocolo de Internet versión 6 (IPv6) o de ambos. Para obtener más información, consulte Modo de pila doble.

Temas

- Modo de doble pila con RDS para Db2
- Modo de pila doble con RDS para MariaDB
- Modo de pila doble con RDS para MySQL
- Modo de pila doble con RDS para Oracle
- Modo de pila doble con RDS para PostgreSQL
- Modo de pila doble con RDS para SQL Server

IPv6 no es compatible con ningún motor de base de datos de Amazon RDS en las siguientes Regiones de AWS:

- Asia-Pacífico (Hyderabad)
- Medio Oriente (EAU)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Melbourne)
- Oeste de Canadá (Calgary)
- Europa (Zúrich)
- Israel (Tel Aviv)

Modo de doble pila con RDS para Db2

A continuación, se detallan las regiones y las versiones de motores disponibles para el modo de doble pila con RDS para Db2.

Región	RDS para Db2 11.5				
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles				
Este de EE. UU. (Ohio)	Todas las versiones disponibles				
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles				
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles				
África (Ciudad del Cabo)	Todas las versiones disponibles				
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles				
Asia-Pacífico (Hyderabad)	No disponible				
Asia-Pacífico (Yakarta)	Todas las versiones disponibles				
Asia-Pacífico (Malasia)	No disponible				

Región	RDS para Db2 11.5				
Asia-Pacífico (Melbourne)	No disponible				
Asia-Pacífico (Bombay)	Todas las versiones disponibles				
Asia-Pacífico (Osaka)	Todas las versiones disponibles				
Asia-Pacífico (Seúl)	Todas las versiones disponibles				
Asia-Pacífico (Singapur)	Todas las versiones disponibles				
Asia-Pacífico (Sídney)	Todas las versiones disponibles				
Asia-Pacífico (Tokio)	Todas las versiones disponibles				
Canadá (centro)	Todas las versiones disponibles				
Oeste de Canadá (Calgary)	No disponible				
China (Pekín)	No disponible				

Región	RDS para Db2 11.5				
China (Ningxia)	No disponible				
Europa (Fráncfort)	Todas las versiones disponibles				
Europa (Irlanda)	Todas las versiones disponibles				
Europa (Londres)	Todas las versiones disponibles				
Europa (Milán)	Todas las versiones disponibles				
Europa (París)	Todas las versiones disponibles				
Europa (España)	No disponible				
Europa (Estocolmo)	Todas las versiones disponibles				
Europa (Zúrich)	No disponible				
Israel (Tel Aviv)	No disponible				

Región	RDS para Db2 11.5				
Medio Oriente (Baréin)	Todas las versiones disponibles				
Medio Oriente (EAU)	No disponible				
América del Sur (São Paulo)	Todas las versiones disponibles				
AWS GovCloud (Este de EE. UU.)	No disponible				
AWS GovCloud (Oeste de EE. UU.)	No disponible				

Modo de pila doble con RDS para MariaDB

A continuación, se detallan las regiones y las versiones de motores disponibles para el modo de doble pila con RDS para MariaDB.

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Este de EE. UU.	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
(Norte de Virginia)					
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible	No disponible	No disponible

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible	No disponible	No disponible

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	No disponible	No disponible	No disponible	No disponible	No disponible
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Europa (Zúrich)	No disponible	No disponible	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	No disponible	No disponible	No disponible	No disponible	No disponible
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Modo de pila doble con RDS para MySQL

A continuación, se detallan las regiones y las versiones de motores disponibles para el modo de doble pila con RDS para MySQL.

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	No disponible	No disponible	No disponible
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	No disponible	No disponible	No disponible
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	No disponible	No disponible	No disponible
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Modo de pila doble con RDS para Oracle

A continuación, se detallan las regiones y las versiones de motores disponibles para el modo de doble pila con RDS para Oracle.

Región	RDS para Oracle 21c	RDS para Oracle 19c
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para Oracle 21c	RDS para Oracle 19c
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	No disponible	No disponible
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para Oracle 21c	RDS para Oracle 19c
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	No disponible	No disponible
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	No disponible	No disponible
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible

Región	RDS para Oracle 21c	RDS para Oracle 19c
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	No disponible	No disponible
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles

Modo de pila doble con RDS para PostgreSQL

A continuación, se detallan las regiones y las versiones de motores disponibles para el modo de doble pila con RDS para PostgreSQL.

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Modo de pila doble con RDS para SQL Server

A continuación, se detallan las regiones y las versiones de motores disponibles para el modo de doble pila con RDS para SQL Server.

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	No disponible	No disponible	No disponible
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	No disponible	No disponible	No disponible
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	No disponible	No disponible	No disponible
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Regiones y motores de base de datos admitidos para exportar instantáneas a S3 en Amazon RDS

Puede exportar datos de instantáneas de bases de datos de RDS a un bucket de Amazon S3. Puede exportar todos los tipos de instantáneas de base de datos, como instantáneas manuales, instantáneas del sistema automatizadas o instantáneas creadas por AWS Backup. Después de exportar los datos, puede analizar los datos exportados directamente con herramientas como Amazon Athena o Amazon Redshift Spectrum. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS.

La exportación de instantáneas a S3 no está disponible para los siguientes motores:

- RDS para Db2
- RDS para Oracle
- RDS para SQL Server

Temas

- Exportar instantáneas a S3 con RDS para MariaDB
- Exportar instantáneas a S3 con RDS para MySQL
- Exportar instantáneas a S3 con RDS para PostgreSQL

Exportar instantáneas a S3 con RDS para MariaDB

A continuación, se detallan las regiones y las versiones de motores para exportar instantáneas a S3 con RDS para MariaDB.

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible

Exportar instantáneas a S3 con RDS para MySQL

Estas son las regiones y las versiones de motor disponibles para exportar instantáneas a S3 con RDS para MySQL.

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7 (con RDS Extended Support)
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	No disponible	No disponible	No disponible

Exportar instantáneas a S3 con RDS para PostgreSQL

A continuación, se detallan las regiones y las versiones de motores para exportar instantáneas a S3 con RDS para PostgreSQL.

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible

Regiones y motores de base de datos admitidos para autenticación de base de datos IAM en Amazon RDS

Al usar la autenticación de base de datos de IAM en Amazon RDS, puede autenticarse sin una contraseña al conectarse a una instancia de base de datos. En su lugar, puede usar un token de autenticación. Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

La autenticación de bases de datos de IAM no está disponible para los siguientes motores:

- RDS para Db2
- RDS para Oracle
- RDS para SQL Server

Temas

- Autenticación de bases de datos de IAM con RDS para MariaDB
- Autenticación de bases de IAM con RDS para MySQL
- Autenticación de bases de datos de IAM con RDS para PostgreSQL

Autenticación de bases de datos de IAM con RDS para MariaDB

A continuación, se detallan las regiones y las versiones de motores para la autenticación de bases de datos de IAM con RDS para MariaDB.

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Hyderabad)	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Malasia)	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (España)	No disponible	No disponible	No disponible	No disponible	No disponible
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (Zúrich)	No disponible	No disponible	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Medio Oriente (EAU)	No disponible	No disponible	No disponible	No disponible	No disponible
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible

Autenticación de bases de IAM con RDS para MySQL

La autenticación de bases de datos de IAM con RDS para MySQL está disponible en todas las regiones para las siguientes versiones:

- RDS para MySQL 8.4: todas las versiones disponibles
- RDS para MySQL 8.0: todas las versiones disponibles
- RDS para MySQL 5.7: todas las versiones disponibles

Autenticación de bases de datos de IAM con RDS para PostgreSQL

La autenticación de bases de datos de IAM con RDS para PostgreSQL está disponible en todas las regiones para las siguientes versiones:

- RDS para PostgreSQL 17: todas las versiones disponibles
- RDS para PostgreSQL 16: todas las versiones disponibles
- RDS para PostgreSQL 15: todas las versiones disponibles
- RDS para PostgreSQL 14: todas las versiones disponibles
- RDS para PostgreSQL 13: todas las versiones disponibles
- RDS para PostgreSQL 12: todas las versiones disponibles
- RDS para PostgreSQL 11: todas las versiones disponibles

- RDS para PostgreSQL 10: todas las versiones disponibles

Regiones y motores de base de datos admitidos para autenticación de Kerberos en Amazon RDS

Con la autenticación Kerberos en Amazon RDS, puede admitir la autenticación externa de usuarios de bases de datos mediante Kerberos y Microsoft Active Directory. El uso de Kerberos y Microsoft Active Directory permite usar el inicio de sesión único y la autenticación centralizada de usuarios de bases de datos.

La autenticación Kerberos no está disponible para los siguientes motores:

- RDS para MariaDB

Aunque la mayoría de las regiones de AWS están activas de forma predeterminada en su cuenta de AWS, algunas regiones solo se activan cuando las selecciona manualmente. Estas regiones se denominan regiones registradas. En cambio, las regiones que están activas de forma predeterminada, en cuanto se crea su cuenta de AWS, se denominan regiones comerciales o, simplemente, regiones. En el caso de las regiones registradas, debe utilizar una entidad principal de servicio regionalizado con el formato `directoryservice.rds.region_name.amazonaws.com`. Por ejemplo, para África (Ciudad del Cabo), debe agregar la entidad principal de servicio `directoryservice.rds.region-af-south-1.amazonaws.com` a su política de confianza. Para obtener más información, consulte Autenticación Kerberos.

Temas

- Autenticación Kerberos con RDS para Db2
- Autenticación Kerberos con RDS para MySQL
- Autenticación Kerberos con RDS para Oracle
- Autenticación Kerberos con RDS para PostgreSQL
- Autenticación Kerberos con RDS para SQL Server

Autenticación Kerberos con RDS para Db2

A continuación, se detallan las regiones y las versiones de motores que están disponibles para la autenticación Kerberos con RDS para Db2.

Región	RDS para Db2 11.5
Este de EE. UU. (Ohio)	Todas las versiones
Este de EE. UU. (Norte de Virginia)	Todas las versiones
Oeste de EE. UU. (Norte de California)	Todas las versiones
Oeste de EE. UU. (Oregón)	Todas las versiones
África (Ciudad del Cabo)	No disponible
Asia-Pacífico (Hong Kong)	No disponible
Asia-Pacífico (Hyderabad)	No disponible
Asia-Pacífico (Yakarta)	No disponible
Asia-Pacífico (Melbourne)	No disponible
Asia-Pacífico (Bombay)	Todas las versiones
Asia-Pacífico (Osaka)	No disponible
Asia-Pacífico (Seúl)	Todas las versiones
Asia-Pacífico (Singapur)	Todas las versiones
Asia-Pacífico (Sídney)	Todas las versiones
Asia-Pacífico (Tokio)	Todas las versiones
Canadá (centro)	Todas las versiones
Oeste de Canadá (Calgary)	No disponible
China (Pekín)	Todas las versiones
China (Ningxia)	Todas las versiones
Europa (Fráncfort)	Todas las versiones

Región	RDS para Db2 11.5
Europa (Irlanda)	Todas las versiones
Europa (Londres)	Todas las versiones
Europa (Milán)	No disponible
Europa (París)	No disponible
Europa (España)	No disponible
Europa (Estocolmo)	Todas las versiones
Europa (Zúrich)	No disponible
Israel (Tel Aviv)	No disponible
Medio Oriente (Baréin)	No disponible
Medio Oriente (EAU)	No disponible
América del Sur (São Paulo)	Todas las versiones
AWS GovCloud (Este de EE. UU.)	No disponible
AWS GovCloud (Oeste de EE.UU.)	No disponible

Autenticación Kerberos con RDS para MySQL

A continuación, se detallan las regiones y las versiones de motores que están disponibles para la autenticación Kerberos con RDS para MySQL.

Región	RDS para MySQL 8.0	RDS para MySQL 5.7	RDS para MySQL 5.6
Este de EE. UU. (Ohio)	Todas las versiones	Todas las versiones	Todas las versiones
Este de EE. UU. (Norte de Virginia)	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para MySQL 8.0	RDS para MySQL 5.7	RDS para MySQL 5.6
Oeste de EE. UU. (Norte de California)	Todas las versiones	Todas las versiones	Todas las versiones
Oeste de EE. UU. (Oregón)	Todas las versiones	Todas las versiones	Todas las versiones
África (Ciudad del Cabo)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Hong Kong)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Hyderabad)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Yakarta)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Melbourne)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Bombay)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Osaka)	No disponible	No disponible	No disponible
Asia-Pacífico (Seúl)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Singapur)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Sídney)	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Tokio)	Todas las versiones	Todas las versiones	Todas las versiones
Canadá (centro)	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para MySQL 8.0	RDS para MySQL 5.7	RDS para MySQL 5.6
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible
China (Pekín)	Todas las versiones	Todas las versiones	Todas las versiones
China (Ningxia)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Fráncfort)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Irlanda)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Londres)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Milán)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (París)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (España)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Estocolmo)	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Zúrich)	Todas las versiones	Todas las versiones	Todas las versiones
Israel (Tel Aviv)	Todas las versiones	Todas las versiones	Todas las versiones
Medio Oriente (Baréin)	Todas las versiones	Todas las versiones	Todas las versiones
Medio Oriente (EAU)	Todas las versiones	Todas las versiones	Todas las versiones
América del Sur (São Paulo)	Todas las versiones	Todas las versiones	Todas las versiones
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE.UU.)	No disponible	No disponible	No disponible

Autenticación Kerberos con RDS para Oracle

A continuación, se detallan las regiones y las versiones de motores para la autenticación Kerberos con RDS para Oracle.

Región	RDS para Oracle 21c	RDS para Oracle 19c
Este de EE. UU. (Ohio)	Todas las versiones	Todas las versiones
Este de EE. UU. (Norte de Virginia)	Todas las versiones	Todas las versiones
Oeste de EE. UU. (Norte de California)	Todas las versiones	Todas las versiones
Oeste de EE. UU. (Oregón)	Todas las versiones	Todas las versiones
África (Ciudad del Cabo) (región registrada)	Todas las versiones	Todas las versiones
Asia-Pacífico (Hong Kong) (región registrada)	Todas las versiones	Todas las versiones
Asia-Pacífico (Hyderabad) (región registrada)	Todas las versiones	Todas las versiones
Asia-Pacífico (Yakarta) (región registrada)	Todas las versiones	Todas las versiones
Asia-Pacífico (Melbourne) (región registrada)	Todas las versiones	Todas las versiones
Asia-Pacífico (Bombay)	Todas las versiones	Todas las versiones
Asia-Pacífico (Osaka)	No disponible	No disponible
Asia-Pacífico (Seúl)	Todas las versiones	Todas las versiones
Asia-Pacífico (Singapur)	Todas las versiones	Todas las versiones
Asia-Pacífico (Sídney)	Todas las versiones	Todas las versiones

Región	RDS para Oracle 21c	RDS para Oracle 19c
Asia-Pacífico (Tokio)	Todas las versiones	Todas las versiones
Canadá (centro)	Todas las versiones	Todas las versiones
Oeste de Canadá (Calgary)	No disponible	No disponible
China (Pekín)	No disponible	No disponible
China (Ningxia)	No disponible	No disponible
Europa (Fráncfort)	Todas las versiones	Todas las versiones
Europa (Irlanda)	Todas las versiones	Todas las versiones
Europa (Londres)	Todas las versiones	Todas las versiones
Europa (Milán) (región registrada)	Todas las versiones	Todas las versiones
Europa (París)	No disponible	No disponible
Europa (España) (región registrada)	Todas las versiones	Todas las versiones
Europa (Estocolmo)	Todas las versiones	Todas las versiones
Europa (Zúrich) (región registrada)	Todas las versiones	Todas las versiones
Israel (Tel Aviv) (región registrada)	Todas las versiones	Todas las versiones
Medio Oriente (Baréin) (región registrada)	Todas las versiones	Todas las versiones
Medio Oriente (EAU) (región registrada)	Todas las versiones	Todas las versiones
América del Sur (São Paulo)	Todas las versiones	Todas las versiones

Región	RDS para Oracle 21c	RDS para Oracle 19c
AWS GovCloud (Este de EE. UU.)	Todas las versiones	Todas las versiones
AWS GovCloud (Oeste de EE.UU.)	Todas las versiones	Todas las versiones

Autenticación Kerberos con RDS para PostgreSQL

A continuación, se detallan las regiones y las versiones de motores para la autenticación Kerberos con RDS para PostgreSQL.

Región	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Este de EE. UU. (Ohio)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Este de EE. UU. (Norte de Virginia)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Oeste de EE. UU. (Norte de California)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Oeste de EE. UU. (Oregón)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
África (Ciudad del Cabo)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Hong Kong)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Hyderabad)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Yakarta)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Melbourne)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Bombay)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Osaka)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible

Región	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Seúl)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Singapur)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Sídney)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Tokio)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Canadá (centro)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
China (Pekín)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
China (Ningxia)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Fráncfort)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Europa (Irlanda)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Londres)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Milán)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (París)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (España)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Estocolmo)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Zúrich)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Israel (Tel Aviv)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Medio Oriente (Baréin)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Medio Oriente (EAU)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
América del Sur (São Paulo)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE.UU.)	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible	No disponible

Autenticación Kerberos con RDS para SQL Server

A continuación, se detallan las regiones y las versiones de motores para la autenticación Kerberos con RDS para SQL Server.

Región	RDS para SQL Server 2022	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Este de EE. UU. (Ohio)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Este de EE. UU. (Norte de Virginia)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para SQL Server 2022	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Oeste de EE. UU. (Norte de California)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Oeste de EE. UU. (Oregón)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
África (Ciudad del Cabo)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Hong Kong)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Hyderabad)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Yakarta)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Melbourne)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Bombay)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Osaka)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Seúl)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Singapur)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Asia-Pacífico (Sídney)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para SQL Server 2022	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Asia-Pacífico (Tokio)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Canadá (centro)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible	No disponible
China (Pekín)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
China (Ningxia)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Fráncfort)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Irlanda)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Londres)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Milán)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (París)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (España)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Europa (Estocolmo)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Región	RDS para SQL Server 2022	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Europa (Zúrich)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Israel (Tel Aviv)	No disponible	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
Medio Oriente (EAU)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
América del Sur (São Paulo)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
AWS GovCloud (Este de EE. UU.)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones
AWS GovCloud (Oeste de EE.UU.)	Todas las versiones	Todas las versiones	Todas las versiones	Todas las versiones

Regiones y motores de base de datos admitidos para clústeres de bases de datos Multi-AZ en Amazon RDS

La implementación de un clúster de bases de datos Multi-AZ en Amazon RDS proporciona un modo de implementación de alta disponibilidad de Amazon RDS con dos instancias de base de datos en espera legibles. Un clúster de base de datos Multi-AZ tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas de disponibilidad diferentes en la misma región de . Los clústeres de base de datos Multi-AZ proporcionan alta disponibilidad, mayor capacidad para cargas de trabajo de lectura y menor latencia de escritura en comparación con las implementaciones de las instancias de base de datos Multi-AZ. Para obtener más información, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

Los clústeres de base de datos Multi-AZ no están disponibles con los siguientes motores:

- RDS para Db2
- RDS para MariaDB
- RDS para Oracle
- RDS para SQL Server

Temas

- Clústeres Multi-AZ con RDS para MySQL
- Clústeres de base de datos Multi-AZ con RDS para PostgreSQL

Clústeres Multi-AZ con RDS para MySQL

A continuación, se detallan las regiones y las versiones de motores para los clústeres de base de datos multi-AZ con RDS para MySQL.

Región	RDS para MySQL 8.4	RDS para MySQL 8.0
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	No disponible	No disponible
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	No disponible	No disponible

Puede enumerar las versiones disponibles en una región para una clase de instancia de base de datos determinada utilizando la AWS CLI. Cambie la clase de instancia de base de datos para mostrar las versiones de motor disponibles para ella.

Para Linux, macOS o Unix:

```
aws rds describe-orderable-db-instance-options \
--engine mysql \
--db-instance-class db.r5d.large \
--query '*[]|[?SupportsClusters == `true`].[EngineVersion]'  \
--output text
```

Para Windows:

```
aws rds describe-orderable-db-instance-options ^
--engine mysql ^
--db-instance-class db.r5d.large ^
--query "*[]|[?SupportsClusters == `true`].[EngineVersion]"  ^
--output text
```

Clústeres de base de datos Multi-AZ con RDS para PostgreSQL

A continuación, se detallan las regiones y las versiones de motores para los clústeres de base de datos multi-AZ con RDS para PostgreSQL.

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13
Este de EE. UU.	Todas las versiones 17	Todas las versiones 16	Todas las versiones	Versión 14.5 y posteriores	Versión 13.4 y versión

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13
(Norte de Virginia)	de PostgreSQL	de PostgreSQL	15 de PostgreSQL		13.7 y posteriores
Este de EE. UU. (Ohio)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Oeste de EE. UU. (Norte de California)	No disponible	No disponible	No disponible	No disponible	No disponible
Oeste de EE. UU. (Oregón)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
África (Ciudad del Cabo)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Hong Kong)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Hyderabad)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13
Asia-Pacífico (Yakarta)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Malasia)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Melbourne)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Bombay)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Osaka)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Seúl)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Singapur)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13
Asia-Pacífico (Sídney)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Asia-Pacífico (Tokio)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Canadá (centro)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Oeste de Canadá (Calgary)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
China (Pekín)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
China (Ningxia)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (Fráncfort)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13
Europa (Irlanda)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (Londres)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (Milán)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (París)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (España)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (Estocolmo)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Europa (Zúrich)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13
Israel (Tel Aviv)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Medio Oriente (Baréin)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
Medio Oriente (EAU)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
América del Sur (São Paulo)	Todas las versiones 17 de PostgreSQL	Todas las versiones 16 de PostgreSQL	Todas las versiones 15 de PostgreSQL	Versión 14.5 y posteriores	Versión 13.4 y versión 13.7 y posteriores
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	No disponible	No disponible	No disponible	No disponible	No disponible

Puede enumerar las versiones disponibles en una región para una clase de instancia de base de datos determinada utilizando la AWS CLI. Cambie la clase de instancia de base de datos para mostrar las versiones de motor disponibles para ella.

Para Linux, macOS o Unix:

```
aws rds describe-orderable-db-instance-options \
--engine postgres \
--db-instance-class db.r5d.large \
--query '*[]|[?SupportsClusters == `true`].[EngineVersion]'  \
--output text
```

Para Windows:

```
aws rds describe-orderable-db-instance-options ^
--engine postgres ^
--db-instance-class db.r5d.large ^
--query "*[]|[?SupportsClusters == `true`].[EngineVersion]"  ^
--output text
```

Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS.

Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Performance Insights en Amazon RDS amplía las características de supervisión de Amazon RDS existentes para informarle y ayudarle a analizar el rendimiento de su base de datos. En el panel de Performance Insights, puede visualizar la carga de la base de datos en su instancia de base de datos de Amazon RDS. También puede filtrarla por esperas, instrucciones SQL, hosts o usuarios. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.

Información de rendimiento está disponible para todos los motores de base de datos de RDS, excepto RDS para Db2.

Para los motores de bases de datos disponibles, Información de rendimiento está disponible con todas las versiones de motores disponibles y en todas las Regiones de AWS.

Para obtener información sobre la compatibilidad de las características de la Información de rendimiento por región, motor de base de datos y clase de instancia, consulte Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento.

Regiones y motores de base de datos admitidos para RDS Custom

Amazon RDS Custom automatiza las tareas y las operaciones de administración de bases de datos. Al utilizar RDS Custom, como administrador de la base de datos puede acceder y personalizar su entorno de base de datos y su sistema operativo. Con RDS Custom, puede personalizarlo para cumplir con los requisitos de las aplicaciones heredadas, personalizadas y empaquetadas. Para obtener más información, consulte Amazon RDS Custom.

RDS Custom solo es compatible con los siguientes motores de base de datos:

Temas

- Regiones y motores de base de datos admitidos para RDS Custom para Oracle
- Regiones y motores de base de datos admitidos para RDS Custom para SQL Server

Regiones y motores de base de datos admitidos para RDS Custom para Oracle

A continuación, se detallan las regiones y las versiones de motores para RDS Custom para Oracle.

Región	Oracle Database 19c	Oracle Database 18c	Oracle Database 12c
Este de EE. UU. (Norte de Virginia)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Este de EE. UU. (Ohio)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Oeste de EE. UU. (Norte de California)	No disponible	No disponible	No disponible
Oeste de EE. UU. (Oregón)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
África (Ciudad del Cabo)	No disponible	No disponible	No disponible
Asia-Pacífico (Hong Kong)	No disponible	No disponible	No disponible
Asia-Pacífico (Yakarta)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible

Región	Oracle Database 19c	Oracle Database 18c	Oracle Database 12c
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible
Asia-Pacífico (Bombay)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Asia-Pacífico (Osaka)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Asia-Pacífico (Seúl)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Asia-Pacífico (Singapur)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Asia-Pacífico (Sídney)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Asia-Pacífico (Tokio)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Canadá (centro)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible
China (Pekín)	No disponible	No disponible	No disponible
China (Ningxia)	No disponible	No disponible	No disponible

Región	Oracle Database 19c	Oracle Database 18c	Oracle Database 12c
Europa (Fráncfort)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Europa (Irlanda)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Europa (Londres)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Europa (Milán)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Europa (París)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Europa (Estocolmo)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
Israel (Tel Aviv)	No disponible	No disponible	No disponible
Medio Oriente (Baréin)	No disponible	No disponible	No disponible
Medio Oriente (EAU)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
América del Sur (São Paulo)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior

Región	Oracle Database 19c	Oracle Database 18c	Oracle Database 12c
AWS GovCloud (Este de EE. UU.)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior
AWS GovCloud (Oeste de EE. UU.)	19c con el RU/RUR de enero de 2021 o posterior	18c con el RU/RUR de enero de 2021 o posterior	12.1 y 12.2 con el RU/RUR de enero de 2021 o posterior

Regiones y motores de base de datos admitidos para RDS Custom para SQL Server

Puede implementar RDS Custom para SQL Server con una versión de motor proporcionada por RDS (RPEV, por sus siglas en inglés) o una versión de motor personalizada (CEV, por sus siglas en inglés):

- Si usa una RPEV, esta incluye la instalación predeterminada de la Imagen de máquina de Amazon (AMI, por sus siglas en inglés) y SQL Server. Si personaliza o modifica el sistema operativo (SO), es posible que los cambios no se mantengan durante las revisiones, la restauración de instantáneas o la recuperación automática.
- Si usa una CEV, debe elegir su propia AMI con Microsoft SQL Server preinstalada o SQL Server instalada con sus propios medios. Al utilizar una CEV proporcionada por AWS, debe elegir la imagen de Amazon EC2 (AMI) más reciente disponible para AWS, que tenga la actualización acumulativa (CU, por sus siglas en inglés) compatible con RDS Custom para SQL Server. Con una CEV, puede personalizar la configuración del sistema operativo y de SQL Server para satisfacer las necesidades de su empresa.

A continuación, se detallan las Regiones de AWS y las versiones de motor de base de datos para RDS Custom para SQL Server. La compatibilidad de la versión del motor depende de si utiliza RDS Custom para SQL Server con una RPEV, una CEV proporcionado por AWS o una CEV proporcionada por el cliente.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Este de EE. UU. (Norte de Virginia)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Este de EE. UU. (Ohio)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Oeste de EE. UU. (Norte de California)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
	SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Oeste de EE. UU. (Oregón)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
África (Ciudad del Cabo)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Asia-Pacífico (Hong Kong)	No disponible	No disponible	No disponible
Asia-Pacífico (Hyderabad)	No disponible	No disponible	No disponible
Asia-Pacífico (Yakarta)	No disponible	No disponible	No disponible
Asia-Pacífico (Malasia)	No disponible	No disponible	No disponible
Asia-Pacífico (Melbourne)	No disponible	No disponible	No disponible

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Asia-Pacífico (Bombay)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Asia-Pacífico (Osaka)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Asia-Pacífico (Seúl)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Asia-Pacífico (Singapur)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Asia-Pacífico (Sídney)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Asia-Pacífico (Tokio)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Canadá (centro)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible
China (Pekín)	No disponible	No disponible	No disponible
China (Ningxia)	No disponible	No disponible	No disponible
Europa (Fráncfort)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Europa (Irlanda)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Europa (Londres)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Europa (Milán)	No disponible	No disponible	No disponible

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Europa (París)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Europa (España)	No disponible	No disponible	No disponible
Europa (Estocolmo)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
Europa (Zúrich)	No disponible	No disponible	No disponible
Israel (Tel Aviv)	No disponible	No disponible	No disponible

Región	PREV	CEV proporcionada AWS	CEV proporcionada por el cliente
Medio Oriente (Baréin)	No disponible	No disponible	No disponible
Medio Oriente (EAU)	No disponible	No disponible	No disponible
América del Sur (São Paulo)	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.	SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19. SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
AWS GovCloud (Este de EE. UU.)	No disponible	No disponible	No disponible
AWS GovCloud (Oeste de EE. UU.)	No disponible	No disponible	No disponible

Regiones y motores de base de datos para Amazon RDS Proxy

El proxy de Amazon RDS es un proxy de base de datos totalmente administrado y de alta disponibilidad que hace que las aplicaciones sean más escalables al agrupar y compartir conexiones de base de datos establecidas. Para obtener más información, consulte Amazon RDS Proxy .

RDS Proxy no está disponible para los siguientes motores:

- RDS para Db2

- RDS para Oracle

Temas

- RDS Proxy con RDS para MariaDB
- RDS Proxy con RDS para MySQL
- RDS Proxy con RDS para PostgreSQL
- RDS Proxy con RDS para SQL Server

RDS Proxy con RDS para MariaDB

Estas son las regiones y versiones del motor disponibles para el proxy de RDS con RDS para MariaDB.

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tailandia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MariaDB 11.4	RDS para MariaDB 10.11	RDS para MariaDB 10.6	RDS para MariaDB 10.5	RDS para MariaDB 10.4
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
México (central)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

RDS Proxy con RDS para MySQL

A continuación, se detallan las regiones y las versiones de motores para el proxy de RDS con RDS para MySQL.

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tailandia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para MySQL 8.4	RDS para MySQL 8.0	RDS para MySQL 5.7
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
México (central)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

RDS Proxy con RDS para PostgreSQL

A continuación se detallan las regiones y las versiones del motor que están disponibles para el proxy de RDS con RDS para PostgreSQL.

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Asia-Pacífico (Tailandia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
México (central)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para PostgreSQL 17	RDS para PostgreSQL 16	RDS para PostgreSQL 15	RDS para PostgreSQL 14	RDS para PostgreSQL 13	RDS para PostgreSQL 12	RDS para PostgreSQL 11	RDS para PostgreSQL 10
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

RDS Proxy con RDS para SQL Server

A continuación, se detallan las regiones y las versiones de motores para el proxy de RDS con RDS para SQL Server.

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Este de EE. UU. (Norte de Virginia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Norte de California)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de EE. UU. (Oregón)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Asia-Pacífico (Hyderabad)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Yakarta)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Malasia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Melbourne)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Bombay)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Osaka)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tailandia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Oeste de Canadá (Calgary)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Pekín)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
China (Ningxia)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Fráncfort)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londres)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (España)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Estocolmo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Israel (Tel Aviv)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	RDS para SQL Server 2019	RDS para SQL Server 2017	RDS para SQL Server 2016
Medio Oriente (Baréin)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Medio Oriente (EAU)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
México (central)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
América del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Este de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovCloud (Oeste de EE. UU.)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Regiones y motores de bases de datos admitidos para la integración de Secrets Manager con Amazon RDS

Con AWS Secrets Manager, puede reemplazar las credenciales con codificación rígida (incluidas las contraseñas de bases de datos), con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. Para obtener más información acerca de Secrets Manager, consulte la Guía del usuario de AWS Secrets Manager.

Puede especificar que Amazon RDS administre la contraseña de usuario maestro en Secrets Manager para una instancia de base de datos de Amazon RDS o un clúster de base de datos Multi-AZ . RDS genera la contraseña, la almacena en Secrets Manager y la rota periódicamente. Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.

La integración de Secrets Manager está disponible en todas las Regiones de AWS.

Regiones y motores de base de datos admitidos para las integraciones sin ETL de Amazon RDS

Las integraciones sin ETL de RDS son una solución totalmente administrada que permite que los datos transaccionales estén disponibles en Amazon Redshift o Amazon SageMaker después de escribirlos en una instancia de base de datos de Amazon RDS. Para obtener más información, consulte Integraciones sin ETL.

Temas

- Integraciones sin ETL con RDS para MySQL

Integraciones sin ETL con RDS para MySQL

Las siguientes regiones y versiones de motores están disponibles para las integraciones sin ETL de RDS para MySQL con Amazon Redshift y Amazon SageMaker.

Región	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.4	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.0	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.4	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.0
Este de EE. UU. (Norte de Virginia	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Este de EE. UU. (Ohio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.4	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.0	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.4	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.0
Oeste de EE. UU (Norte de Californ a)	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Oeste de EE. UU (Oregó	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
África (Ciudad del Cabo)	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Hong Kong)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Hyderad)	No disponible	No disponible	No disponible	No disponible

Región	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.4	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.0	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.4	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.0
Asia-Pacífico (Yakart	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Malasi	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Melbo e)	No disponible	No disponible	No disponible	No disponible
Asia-Pacífico (Bomba	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Osaka	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Asia-Pacífico (Seúl)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles

Región	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.4	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.0	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.4	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.0
Asia-Pacífico (Singapur)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Sídney)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Asia-Pacífico (Tokio)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Canadá (centro)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Oeste de Canadá (Calgary)	No disponible	No disponible	No disponible	No disponible
China (Pekín)	No disponible	No disponible	No disponible	No disponible
China (Ningxi	No disponible	No disponible	No disponible	No disponible

Región	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.4	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.0	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.4	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.0
Europa (Francf t)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Irlanda	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Londre	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Milán)	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (París)	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Europa (Españ	No disponible	No disponible	No disponible	No disponible
Europa (Estocc o)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
Europa (Zúrich	No disponible	No disponible	No disponible	No disponible

Región	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.4	Integración sin ETL con Amazon Redshift para RDS para MySQL 8.0	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.4	Integración sin ETL con Amazon SageMaker para RDS para MySQL 8.0
Israel (Tel Aviv)	No disponible	No disponible	No disponible	No disponible
Medio Oriente (Baréin	Todas las versiones disponibles	Todas las versiones disponibles	No disponible	No disponible
Medio Oriente (EAU)	No disponible	No disponible	No disponible	No disponible
Américc del Sur (São Paulo)	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles	Todas las versiones disponibles
AWS GovClc (Este de EE. UU	No disponible	No disponible	No disponible	No disponible
AWS GovClc (Oeste de EE. UU	No disponible	No disponible	No disponible	No disponible

Características nativas del motor en Amazon RDS

Los motores de base de datos de Amazon RDS también admiten muchas de las características y funcionalidades nativas del motor más comunes. Estas características son diferentes a las características nativas de Amazon RDS que se indican en esta página. Algunas características nativas del motor pueden disponer de una compatibilidad limitada o de privilegios restringidos.

Para obtener más información sobre las características nativas del motor, consulte:

- Características de Amazon RDS para Db2
- Compatibilidad de características de MariaDB en Amazon RDS
- Compatibilidad con características de MySQL en Amazon RDS
- Características de RDS para Oracle
- Uso de las características de PostgreSQL admitidas por Amazon RDS para PostgreSQL
- Características de Microsoft SQL Server en Amazon RDS

Facturación de instancia de base de datos para Amazon RDS

Las instancias de Amazon RDS se facturan en función de los siguientes componentes:

- Horas de instancia de base de datos (por hora): en función de la clase de instancia de base de datos (por ejemplo, db.t2.small o db.m4.large). Los precios se muestran por hora, pero las facturas se ajustan hasta el segundo y muestran las horas en formato decimal. El uso de RDS se factura por incrementos de un segundo, con un mínimo de 10 minutos. Para obtener más información, consulte Clases de instancia de base de datos de .
- Almacenamiento (por GiB al mes): la capacidad de almacenamiento que ha aprovisionado para su instancia de base de datos. Si escala la capacidad de almacenamiento aprovisionada durante el mes, la factura se prorratea. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.
- Solicitudes de entrada/salida (E/S) (por millón de solicitudes): número total de solicitudes de E/S de almacenamiento realizadas en un ciclo de facturación, solo para el almacenamiento magnético de Amazon RDS.
- IOPS aprovisionadas (por IOPS al mes): cantidad de IOPS aprovisionadas, independientemente de las IOPS consumidas (para el almacenamiento de Amazon RDS de IOPS aprovisionadas (SSD) y de uso general (SSD) gp3). El almacenamiento aprovisionado para volúmenes de EBS se factura en incrementos de un segundo, con un mínimo de 10 minutos.
- Almacenamiento de copias de seguridad (por GiB al mes): el almacenamiento de copias de seguridad es el almacenamiento asociado a copias de seguridad de base de datos automatizadas y cualquier instantánea de base de datos activa que haya realizado. Aumentar el período de retención de copia de seguridad u obtener instantáneas de base de datos adicionales aumenta el almacenamiento de copias de seguridad consumido por su base de datos. La facturación por segundo no se aplica al almacenamiento de copia de seguridad (medido en GB/mes).

  Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.
- Transferencia de datos (por GB): las transferencias de datos de entrada y de salida de su instancia de base de datos, desde y hacia Internet y otras regiones de AWS. Para ver ejemplos útiles, consulte la entrada del blog de AWS Exploring Data Transfer Costs for AWS Managed Databases.

Amazon RDS proporciona las siguientes opciones de compra para que pueda optimizar los costos en función de sus necesidades:

- On-Demand Instances (Instancias bajo demanda): pague por las horas de instancia de base de datos que use. Los precios se muestran por hora, pero las facturas se ajustan hasta el segundo y muestran las horas en formato decimal. El uso de RDS ahora se factura por incrementos de un segundo, con un mínimo de 10 minutos.
- Reserved Instances (Instancias reservadas): reserve una instancia de base de datos durante un plazo de uno a tres años y obtenga descuentos importantes en comparación con los precios de instancias de base de datos bajo demanda. Cuando use instancias reservadas, podrá lanzar, eliminar, iniciar o detener varias instancias dentro de una misma hora y obtener el beneficio de instancia reservada para todas las instancias.

Para obtener información acerca de los precios de Amazon RDS, consulte la página Precios de Amazon RDS.

Temas

- Instancias de base de datos bajo demanda para Amazon RDS
- Instancias de base de datos reservadas para Amazon RDS

Instancias de base de datos bajo demanda para Amazon RDS

Las instancias de base de datos bajo demanda de Amazon RDS se facturan en función de la clase de instancia de base de datos (por ejemplo, db.t3.small o db.m5.large). Para obtener información acerca de los precios de Amazon RDS, consulte la página del producto de Amazon RDS.

La facturación de una instancia de base de datos comienza en cuanto la instancia está disponible. Los precios se muestran por hora, pero las facturas se ajustan hasta el segundo y muestran las horas en formato decimal. El uso de Amazon RDS se factura por incrementos de un segundo, con un mínimo de 10 minutos. En caso de un cambio de configuración facturable, como el escalado informático o la capacidad de almacenamiento, se le cobrará un mínimo de 10 minutos. La facturación continúa hasta que se termina la instancia de base de datos, lo que tiene lugar cuando se elimina la instancia de base de datos o produce un error.

Si ya no desea que se le cobre por su instancia de base de datos, debe detenerla o eliminarla para evitar que se le cobren horas de instancia de base de datos adicionales. Para obtener más información acerca de los estados de instancias de base de datos que se le cobran, consulte Visualización del estado de la instancia de base de datos de en un clúster de Aurora.

Instancias de base de datos detenidas

Mientras la instancia de base de datos está detenida, se le cobra el almacenamiento provisionado, incluidas las IOPS provisionadas. También se le cobra el almacenamiento de copias de seguridad, incluido el almacenamiento de las instantáneas manuales y las copias de seguridad automatizadas en el periodo de retención especificado. No se le cobrarán las horas de instancia de base de datos.

Instancias de base de datos Multi-AZ

Una configuración multi-AZ mejora la durabilidad y disponibilidad de los datos al aprovisionar y mantener automáticamente una réplica en espera sincrónica dentro de una zona de disponibilidad diferente. Debido a los recursos adicionales y al aumento de la disponibilidad, las implementaciones multi-AZ tienen un precio más alto que las implementaciones en AZ única y pueden costar aproximadamente el doble debido a la instancia de reserva adicional y a los recursos asociados.

Tenga en cuenta los siguientes detalles importantes acerca de los precios de multi-AZ:

- Costos informáticos: se facturan por hora de instancia de base de datos para instancias principales y en espera.
- Costos de almacenamiento: se cobran por GB al mes por el almacenamiento aprovisionado para las instancias principales y en espera.

- Costos de transferencia de datos: la replicación entre las instancias principales y en espera está incluida en el costo, pero es posible que se apliquen otros cargos por transferencia de datos en función del uso.

Para estimar con precisión los costos mensuales en función del caso de uso específico y Región de AWS, puede usar Calculadora de precios de AWS. Esta herramienta le permite ingresar los detalles de configuración y proporciona un desglose completo de los costos.

> **Note**
>
> Los precios están sujetos a cambios. Consulte la página de precios de Amazon RDS para obtener la información más actualizada.

Instancias de base de datos reservadas para Amazon RDS

Puede reservar una instancia de base de datos durante un periodo de un año o de tres años mediante instancias de base de datos reservadas. Las instancias de base de datos reservadas ofrecen un descuento importante en comparación con los precios de las instancias de base de datos bajo demanda. Las instancias de base de datos reservadas no son instancias físicas sino más bien un descuento de facturación que se aplica al uso de determinadas instancias de base de datos bajo demanda en su cuenta. Los descuentos están vinculados al tipo de instancia y a la Región de AWS.

El proceso general de trabajo con instancias de base de datos reservadas es el siguiente: en primer lugar, obtener información sobre las ofertas de instancias de base de datos reservadas; en segundo lugar, comprar una oferta y, por último, obtener información sobre las instancias de base de datos reservadas.

Para obtener información sobre la compra de instancias de base de datos reservadas y sobre la consulta de la facturación de dichas instancias, consulte las siguientes secciones.

- Compra de instancias de base de datos reservadas para Amazon RDS
- Visualización de la facturación de las instancias de bases de datos reservadas para Amazon RDS

Información general sobre instancias de base de datos reservadas

Cuando adquiere una instancia de base de datos reservada en Amazon RDS, adquiere un compromiso para obtener una tarifa con descuento en un tipo de instancia de base de datos específico durante el periodo de duración de la instancia de base de datos reservada. Para usar una instancia de base de datos reservada de Amazon RDS, debe crear una instancia de base de datos nueva, tal como haría para una instancia bajo demanda.

La nueva instancia de base de datos que cree deberá tener las mismas especificaciones que la instancia de base de datos reservada, es decir:

- Región de AWS
- Motor de base de datos (no es necesario que el número de versión del motor de base de datos coincida).
- Tipo de instancia de base de datos
- Tamaño de la instancia de base de datos (RDS para Microsoft SQL Server y Amazon RDS para Oracle License Included)

- Edición (RDS para SQL Server y RDS para Oracle)
- Tipo de licencia (con licencia o traiga su propia licencia)

Si las especificaciones de la nueva instancia de base de datos nueva coinciden con una instancia reservada existente para su cuenta, se le facturará con la tarifa con descuento ofrecida para la instancia reservada. De lo contrario, la instancia de base de datos se factura con una tarifa bajo demanda.

Puede modificar una instancia de base de datos que utilice como instancia de base de datos reservada. Si la modificación está dentro de las especificaciones de la instancia de base de datos reservada, parte o todo el descuento seguirá siendo aplicable a la instancia de base de datos modificada. Si la modificación está fuera de las especificaciones, como cambiar la clase de instancia, el descuento ya no se aplica. Para obtener más información, consulte Flexibilidad del tamaño de las instancias de base de datos reservadas.

Temas

- Tipos de ofertas
- Flexibilidad del tamaño de las instancias de base de datos reservadas
- Ejemplo de facturación de instancias de base de datos reservadas
- Instancias de base de datos reservadas para un clúster de base de datos multi-AZ
- Eliminación de una instancia de base de datos reservada

Para obtener más información acerca de las instancias de base de datos reservadas, incluidos los precios, consulte Instancias reservadas de Amazon RDS.

Tipos de ofertas

Las instancias de base de datos reservadas están disponibles en tres variedades: sin pago inicial, pago inicial parcial y pago inicial total, lo cual le permite optimizar sus costos de Amazon RDS en función del uso previsto.

> **Note**
>
> No todas las clases de instancias de RDS admiten todos los tipos de ofertas de instancias reservadas. Por ejemplo, es posible que algunas clases de instancias no ofrezcan la opción Sin pago inicial. Para confirmar la disponibilidad, revise las ofertas de instancias reservadas

en AWS Management Console o use el comando `describe-reserved-db-instances-offerings` de la AWS CLI.

Sin pago inicial

Esta opción proporciona acceso a una instancia de base de datos reservada sin que haya que hacer un pago inicial. Su instancia de base de datos reservada sin pago inicial le cobra una tarifa por hora con descuento por cada hora dentro del plazo, independientemente del uso. No es necesario realizar ningún pago inicial. Esta opción solo está disponible en la modalidad de reserva de un año.

Pago inicial parcial

Esta opción exige que parte de la instancia de base de datos reservada se pague por adelantado. Las horas restantes del plazo se cobran a una tarifa por hora con descuento, independientemente del uso que haga. Esta opción sustituye la anterior opción de utilización intensa.

Pago inicial total

Se realiza un pago total al comienzo del plazo, y no se aplicará ningún otro costo el resto del plazo, independientemente del número de horas de uso.

Si está utilizando la facturación unificada, todas las cuentas de la organización se tratan como una sola. Esto quiere decir que todas las cuentas de la organización pueden beneficiarse del precio por hora reducido de las instancias de base de datos reservadas adquiridas por otra cuenta. Para obtener más información sobre la facturación unificada, consulte Instancias de base de datos reservadas de Amazon RDS en la Guía del usuario de Administración de costos y facturación de AWS.

Flexibilidad del tamaño de las instancias de base de datos reservadas

Al comprar una instancia de base de datos reservada, una de las cosas que especifica es la clase de instancia, por ejemplo, db.r5.large. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

Si tiene una instancia de base de datos y debe escalarla para aumentar la capacidad, la instancia de base de datos reservada se aplica automáticamente a la instancia de base de datos escalada. Es decir que las instancias de base de datos reservadas se aplican automáticamente entre todos los

tamaños de clase de instancia de base de datos. Las instancias de base de datos reservadas con flexibilidad de tamaño están disponibles para las instancias de base de datos de la misma Región de AWS y motor de base de datos. Las instancias de base de datos reservadas con flexibilidad de tamaño solo se pueden escalar en su tipo de clase de instancia. Por ejemplo, una instancia de base de datos reservada para una db.r5.large se puede utilizar en una db.r5.xlarge, pero no en una db.r6g.large, ya que db.r5 y db.r6g son clases distintas de instancias.

Otro de los beneficios de las instancias de base de datos reservadas es que se aplican a las configuraciones multi-AZ y single-AZ. Esto significa que puede moverse libremente entre configuraciones dentro del mismo tipo de clase de instancia de base de datos. Por ejemplo, puede pasar de una implementación single-AZ que se ejecuta en una sola instancia de base de datos grande (cuatro unidades normalizadas por hora) a una implementación multi-AZ que se ejecuta en dos instancias de base de datos medianas (2+2 = 4 unidades normalizadas por hora).

Las instancias de base de datos reservadas con flexibilidad de tamaño están disponibles para los siguientes motores de base de datos de Amazon RDS:

- RDS para MariaDB
- RDS para MySQL
- RDS para Oracle, traiga su propia licencia
- RDS para PostgreSQL

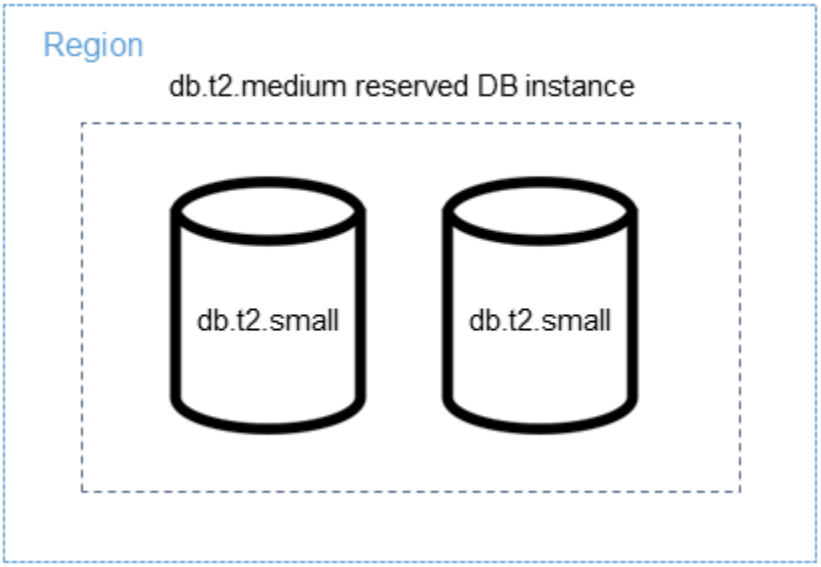
La flexibilidad de tamaño no se aplica a RDS para SQL Server ni a RDS para Oracle License Included.

Para obtener más información acerca de cómo utilizar las instancias reservadas con flexibilidad de tamaño con Aurora, consulte Instancias de bases de datos reservadas de Aurora.

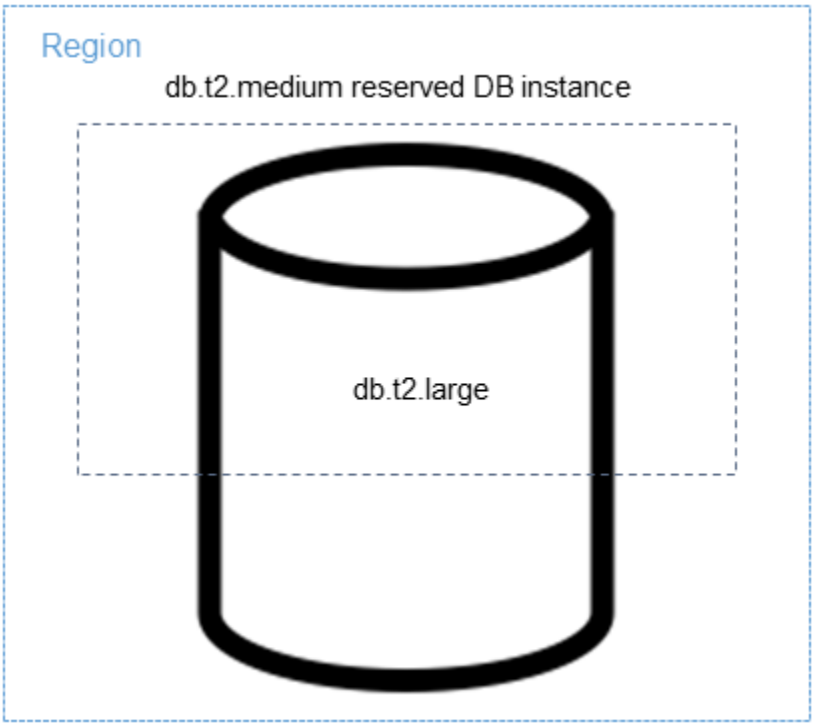
Puede comparar el uso de diferentes tamaños de instancias de base de datos reservadas utilizando unidades normalizadas por hora. Por ejemplo, una unidad de uso en dos instancias de base de datos db.r3.large equivale a ocho unidades de uso normalizadas por hora en una db.r3.small. En la tabla siguiente se muestra el número de unidades normalizadas por hora por cada tamaño de instancia de base de datos.

Tamaño de instancia	Unidades normalizadas single-AZ por hora (implementación con una instancia de base de datos)	Unidades normalizadas de instancias de base de datos multi-AZ por hora (implementación con una instancia de base de datos y una en espera)	Unidades normalizadas de clústeres de base de datos multi-AZ por hora (implementación con una instancia de base de datos y dos en espera)
micro	0,5	1	1.5
small	1	2	3
medium	2	4	6
large	4	8	12
xlarge	8	16	24
2xlarge	16	32	48
4xlarge	32	64	96
6xlarge	48	96	144
8xlarge	64	128	192
10xlarge	80	160	240
12xlarge	96	192	288
16xlarge	128	256	384
24xlarge	192	384	576
32xlarge	256	512	768

Por ejemplo, suponga que adquiere una instancia de base de datos reservada `db.t2.medium` y tiene dos instancias de base de datos `db.t2.small` en ejecución en su cuenta en la misma Región de AWS. En este caso, el beneficio de facturación se aplica en su totalidad a las dos instancias.



De forma alternativa, si tiene una instancia `db.t2.large` en ejecución en su cuenta en la misma Región de AWS, el beneficio de facturación se aplica al 50 % del uso de la instancia de base de datos.



Ejemplo de facturación de instancias de base de datos reservadas

El precio de una instancia de base de datos reservada no incluye ningún descuento en los costos asociados al almacenamiento, las copias de seguridad y las E/S. Es un descuento únicamente sobre el uso por hora de la instancia bajo demanda. En el siguiente ejemplo se ilustra el costo total mensual de una instancia de base de datos reservada:

- Una clase de instancia de base de datos reservada db.r5.large Single-AZ de RDS para MySQL en Este de EE. UU. (Norte de Virginia) con la opción sin pago inicial con un costo de 0,12 USD para la instancia o de 90 USD al mes
- 400 GiB de almacenamiento SSD de propósito general (gp2) con un costo de 0,115 USD por GiB al mes o de 45,60 USD al mes
- 600 GiB de almacenamiento de copia de seguridad a 0,095 USD o 19 USD al mes (400 GiB gratis)

Sume todos estos cargos (90 USD + 45,60 USD + 19 USD) a la instancia de base de datos reservada. El costo total mensual es de 154,60 USD.

Si elige una instancia de base de datos bajo demanda en lugar de una instancia de base de datos reservada, una clase de instancia de base de datos reservada db.r5.large Single-AZ de RDS para MySQL en Este de EE. UU. (Norte de Virginia) cuesta 0,1386 USD por hora 101,18 USD al mes. Así que para una instancia de base de datos bajo demanda, sume todas estas opciones (101,18 USD + 45,60 USD + 19 USD) y el costo total mensual es de 165,78 USD. Ahorra algo más de 11 USD al mes al utilizar la instancia de base de datos reservada.

> **Note**
>
> Los precios que aparecen aquí son ejemplos y podrían no coincidir con los precios reales. Para obtener información acerca de los precios de Amazon RDS, consulte Precios de Amazon RDS.

Instancias de base de datos reservadas para un clúster de base de datos multi-AZ

Para comprar instancias de base de datos reservadas equivalentes para un clúster de base de datos multi-AZ, puede realizar una de las siguientes acciones:

- Reserve tres instancias de base de datos Single-AZ que tengan el mismo tamaño que las instancias del clúster.

- Reserve una instancia de base de datos multi-AZ y una instancia de base de datos single-AZ que tengan el mismo tamaño que las instancias de base de datos del clúster.

Por ejemplo, suponga que tiene un clúster que consta de tres instancias de base de datos db.m6gd.large. En este caso, puede comprar tres instancias de base de datos reservadas single-AZ db.m6gd.large, o bien una instancia de base de datos reservada multi-AZ db.m6gd.large y una instancia de base de datos reservada single-AZ db.m6gd.large. Con cualquiera de estas opciones, se reserva el descuento máximo de instancias reservadas para el clúster de base de datos multi-AZ.

Como alternativa, puede utilizar instancias de base de datos de tamaño flexible y comprar una instancia de base de datos más grande para cubrir las instancias de base de datos más pequeñas en uno o más clústeres. Por ejemplo, si tiene dos clústeres con seis instancias de base de datos db.m6gd.large en total, puede comprar tres instancias de base de datos reservadas Single-AZ db.m6gd.xl. Al hacerlo, se reservan las seis instancias de base de datos en los dos clústeres. Para obtener más información, consulte Flexibilidad del tamaño de las instancias de base de datos reservadas.

Puede reservar instancias de base de datos que tengan el mismo tamaño que las instancias de base de datos del clúster, pero reservar menos instancias de base de datos que el número total de instancias de base de datos del clúster. Sin embargo, si lo hace, el clúster solo estará reservado parcialmente. Por ejemplo, supongamos que tiene un clúster con tres instancias de base de datos db.m6gd.large y compra una instancia de base de datos reservada multi-AZ db.m6gd.large. En este caso, el clúster solo está reservado parcialmente, porque solo dos de las tres instancias del clúster están cubiertas por instancias de base de datos reservadas. La instancia de base de datos restante se cobra a la tarifa por horas de db.m6gd.large bajo demanda.

Para obtener más información acerca de los clústeres de base de datos multi-AZ, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

Eliminación de una instancia de base de datos reservada

Los términos de una instancia de base de datos reservada implican un compromiso de un año o de tres años. No tiene autorización para cancelar una instancia de base de datos reservada. Sin embargo, puede eliminar una instancia de base de datos que tenga un descuento de instancia de base de datos reservada. El proceso para eliminar una instancia de base de datos con un descuento de instancia de base de datos reservada es el mismo que para cualquier otra instancia de base de datos.

Los costos iniciales se facturarán independientemente de si utiliza los recursos.

Si elimina una instancia de base de datos con un descuento de instancia de base de datos reservada, puede lanzar otra instancia de base de datos con especificaciones compatibles. En este caso, sigue disfrutando de la tarifa de descuento mientras dure la reserva (de uno o tres años).

Compra de instancias de base de datos reservadas para Amazon RDS

Puede utilizar la AWS Management Console, la AWS CLI y la API de RDS para trabajar con instancias de base de datos reservadas.

Consola

Puede utilizar la AWS Management Console para trabajar con instancias de base de datos reservadas, tal como se muestra en los siguientes procedimientos.

Para obtener precios e información sobre ofertas de instancias de base de datos reservadas disponibles

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Reserved instances (Instancias reservadas).
3. Elija Purchase Reserved DB Instance.
4. En Product description (Descripción de producto), elija el motor de base de datos y el tipo de licencia.
5. En DB instance class (Clase de instancia de base de datos), elija la clase de instancia de base de datos.
6. En Opción de implementación, elija si quiere una implementación de instancias single-AZ o multi-AZ.

   > **Note**
   >
   > Para comprar las instancias de base de datos reservadas equivalentes para una implementación de un clúster de base de datos multi-AZ, compre tres instancias de base de datos reservadas single-AZ, o bien una instancia de base de datos reservada multi-AZ y otra single-AZ. Para obtener más información, consulte Instancias de base de datos reservadas para un clúster de base de datos multi-AZ.

7. En Periodo, elija el tiempo durante el cual desea que se reserve la instancia de base de datos.

8. En Offering type (Tipo de oferta), elija el tipo de oferta.

   Después de seleccionar el tipo de oferta, podrá ver la información sobre los precios.

   > **Important**
   >
   > Elija Cancel (Cancelar) para evitar comprar la instancia de base de datos reservada y generar cargos.

Después de recibir la información sobre las ofertas disponibles de instancias de base de datos reservadas, podrá utilizar dicha información para adquirir una oferta, tal como se explica a continuación.

Para comprar una instancia de base de datos reservada

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Reserved instances (Instancias reservadas).
3. Elija Purchase Reserved DB Instance (Comprar instancia de base de datos reservada).
4. En Product description (Descripción de producto), elija el motor de base de datos y el tipo de licencia.
5. En DB instance class (Clase de instancia de base de datos), elija la clase de instancia de base de datos.
6. En Implementación multi-AZ, elija si quiere una implementación de instancias de base de datos sinle-AZ o multi-AZ.

   > **Note**
   >
   > Para comprar las instancias de base de datos reservadas equivalentes para una implementación de un clúster de base de datos multi-AZ, compre tres instancias de base de datos reservadas single-AZ, o bien una instancia de base de datos reservada multi-AZ y otra single-AZ. Para obtener más información, consulte Instancias de base de datos reservadas para un clúster de base de datos multi-AZ.

7. En Term, elija el tiempo durante el cual desea que se reserve la instancia de base de datos.
8. En Offering type (Tipo de oferta), elija el tipo de oferta.

Después de seleccionar el tipo de oferta, podrá ver la información sobre los precios.

9. (Opcional) Puede asignar su propio identificador a las instancias de base de datos reservadas que adquiera para poder realizar un seguimiento de estas. En Reserved Id, escriba un identificador para la instancia de base de datos reservada.
10. Seleccione Submit (Enviar).

    La instancia de base de datos reservada se compra y, a continuación, se muestra en la lista de Reserved instances (Instancias reservadas).

Después de adquirir las instancias de base de datos reservadas, podrá obtener información sobre las instancias de base de datos reservadas, tal como se muestra a continuación.

Para obtener información sobre instancias de base de datos reservadas para su cuenta de AWS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel Navigation (Navegación), elija Reserved instances (Instancias reservadas).

   Aparecerán las instancias de base de datos reservadas de la cuenta. Para ver información detallada sobre la instancia de base de datos reservada particular, elija dicha instancia de la lista. Entonces, podrá ver información detallada sobre esa instancia en el panel de detalles ubicado en la parte inferior de la consola.

AWS CLI

Puede utilizar la AWS CLI para trabajar con instancias de base de datos reservadas, tal como se muestra en los siguientes ejemplos.

Example de obtener ofertas de instancias de base de datos reservadas disponibles

Para obtener información sobre las ofertas disponibles de instancias de base de datos reservadas, llame al comando AWS CLI de la `describe-reserved-db-instances-offerings`.

```
aws rds describe-reserved-db-instances-offerings
```

Esta llamada devuelve un resultado similar al siguiente:

```
OFFERING  OfferingId                            Class         Multi-AZ  Duration  Fixed
 Price  Usage Price  Description  Offering Type
OFFERING  438012d3-4052-4cc7-b2e3-8d3372e0e706  db.r3.large   y         1y
 1820.00 USD  0.368 USD    mysql        Partial  Upfront
OFFERING  649fd0c8-cf6d-47a0-bfa6-060f8e75e95f  db.r3.small   n         1y
 227.50 USD  0.046 USD    mysql        Partial  Upfront
OFFERING  123456cd-ab1c-47a0-bfa6-12345667232f  db.r3.small   n         1y
 162.00 USD   0.00 USD    mysql        All      Upfront
    Recurring Charges:   Amount  Currency  Frequency
    Recurring Charges:   0.123   USD       Hourly
OFFERING  123456cd-ab1c-37a0-bfa6-12345667232d  db.r3.large   y         1y
 700.00 USD   0.00 USD    mysql        All      Upfront
    Recurring Charges:   Amount  Currency  Frequency
    Recurring Charges:   1.25    USD       Hourly
OFFERING  123456cd-ab1c-17d0-bfa6-12345667234e  db.r3.xlarge  n         1y
 4242.00 USD   2.42 USD    mysql        No       Upfront
```

Después de recibir la información sobre las ofertas disponibles de instancias de base de datos reservadas, podrá utilizar dicha información para adquirir una oferta.

Para adquirir una instancia de base de datos reservada, use el comando AWS CLI de la `purchase-reserved-db-instances-offering` con los siguientes parámetros:

- `--reserved-db-instances-offering-id` – El ID de la oferta que desea adquirir. Consulte el ejemplo anterior para obtener el ID de la oferta.
- `--reserved-db-instance-id` – Puede asignar su propio identificador a las instancias de base de datos reservadas que adquiera para poder realizar un seguimiento de estas.

Example de adquirir una instancia de base de datos reservada

El siguiente ejemplo adquiere la oferta de instancia de base de datos reservada con el ID *649fd0c8-cf6d-47a0-bfa6-060f8e75e95f* y le asigna el identificador *MyReservation*.

Para Linux, macOS, o:Unix

```
aws rds purchase-reserved-db-instances-offering \
    --reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f \
    --reserved-db-instance-id MyReservation
```

En:Windows

```
aws rds purchase-reserved-db-instances-offering ^
    --reserved-db-instances-offering-id 649fd0c8-cf6d-47a0-bfa6-060f8e75e95f ^
    --reserved-db-instance-id MyReservation
```

El comando devuelve un resultado similar al siguiente:

```
RESERVATION  ReservationId      Class        Multi-AZ  Start Time
 Duration  Fixed Price  Usage Price  Count  State           Description  Offering Type
RESERVATION  MyReservation      db.r3.small  y         2011-12-19T00:30:23.247Z  1y
    455.00 USD   0.092 USD    1      payment-pending  mysql        Partial  Upfront
```

Después de adquirir las instancias de base de datos reservadas, podrá obtener información sobre las instancias de base de datos reservadas.

Para obtener información sobre las instancias de base de datos reservadas de su cuenta de AWS, llame al comando de AWS CLI`describe-reserved-db-instances`, como se muestra en el siguiente ejemplo.

Example de obtener sus instancias de base de datos reservadas

```
aws rds describe-reserved-db-instances
```

El comando devuelve un resultado similar al siguiente:

```
RESERVATION  ReservationId     Class        Multi-AZ  Start Time
 Duration  Fixed Price  Usage Price  Count  State    Description  Offering Type
RESERVATION  MyReservation     db.r3.small  y         2011-12-09T23:37:44.720Z  1y
   455.00 USD   0.092 USD    1      retired  mysql        Partial  Upfront
```

API de RDS

Puede usar la API de RDS para trabajar con instancias de base de datos reservadas:

- Para obtener información sobre las ofertas de instancias de base de datos reservadas disponibles, llame a la operación de API de Amazon RDS `DescribeReservedDBInstancesOfferings`.
- Después de recibir la información sobre las ofertas disponibles de instancias de base de datos reservadas, podrá utilizar dicha información para adquirir una oferta. Llame a la operación de API de RDS `PurchaseReservedDBInstancesOffering` con los siguientes parámetros:
  - `--reserved-db-instances-offering-id` – El ID de la oferta que desea adquirir.

- `--reserved-db-instance-id` – Puede asignar su propio identificador a las instancias de base de datos reservadas que adquiera para poder realizar un seguimiento de estas.
- Después de adquirir las instancias de base de datos reservadas, podrá obtener información sobre las instancias de base de datos reservadas. Llame a la operación de la API de RDS `DescribeReservedDBInstances`.

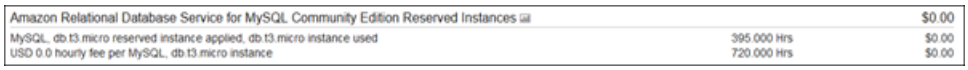
Visualización de la facturación de las instancias de bases de datos reservadas para Amazon RDS

Puede ver la facturación de las instancias de base de datos reservadas en Billing Dashboard (Panel de facturación) en la AWS Management Console.

Para ver la facturación de una instancia de base de datos reservada

1. Inicie sesión en la AWS Management Console.
2. Desde el account menu (menú de cuenta) en la parte superior derecha, elija Billing Dashboard (Panel de facturación).
3. Elija Bill Details (Detalles de la factura) que aparece en la parte superior derecha del panel.
4. En AWSService Charges (Cargos de servicio), expanda Relational Database Service (Servicio de base de datos relacional).
5. Expanda la Región de AWS en la que se encuentran las instancias de base de datos reservadas, por ejemplo, US West (Oregon) (Oeste de EE. UU. [Oregón]).

   Las instancias de base de datos reservadas y sus cargos por hora del mes en curso se muestran en Amazon Relational Database Service for ***Database Engine*** Reserved Instances (Amazon Relational Database Service para Instancias reservadas del motor de base de datos).

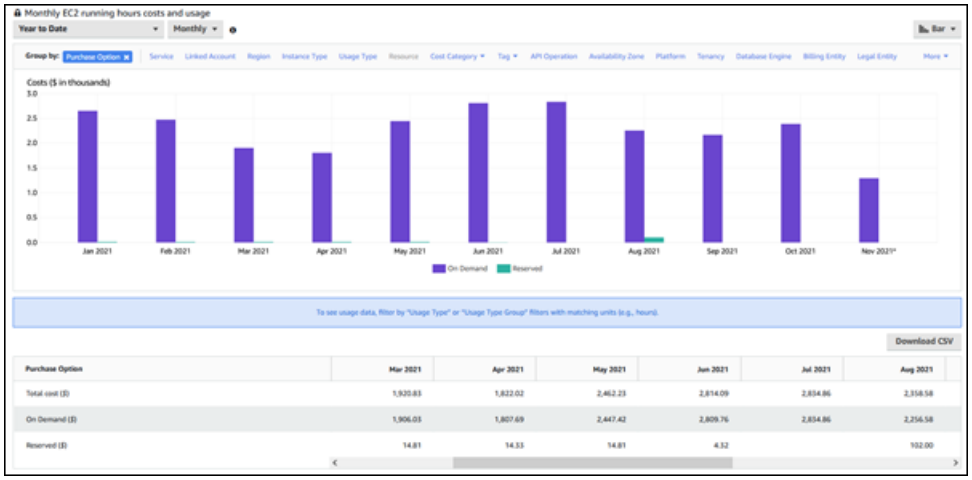
   

   La instancia de base de datos reservada en este ejemplo se compró con un pago total por adelantado, por lo que no hay cargos por hora.
6. Elija el icono Cost Explorer (gráfico de barras) que aparece junto al encabezado de Reserved Instances (Instancias reservadas).

   Cost Explorer muestra el gráfico Monthly EC2 running hours costs and usage (Uso y costos por horas de ejecución de EC2 mensuales).
7. Borre el filtro Usage Type Group (Grupo de tipo de uso) a la derecha del gráfico.

8. Elija el periodo y la unidad de tiempo para los que quiere examinar los costos de uso.

   En el siguiente ejemplo se muestran los costos de uso de las instancias de base de datos bajo demanda y reservadas para el año hasta la fecha por mes.



   Los costos de las instancias de base de datos reservadas de enero a junio de 2021 son cargos mensuales para una instancia parcial inicial, mientras que el costo de agosto de 2021 es un cargo único para una instancia de pago total por adelantado.

   El descuento de la instancia reservada para la instancia de pago inicial parcial venció en junio de 2021, pero la instancia de base de datos no se eliminó. Después de la fecha de vencimiento, simplemente se cobró según la tarifa bajo demanda.

Configuración del entorno para Amazon RDS

Esta página proporciona una guía completa para configurar Amazon Relational Database Service, lo que incluye la configuración de cuentas, la seguridad y la administración de recursos. Le explica los pasos esenciales para crear, administrar y proteger sus entornos de bases de datos de manera eficiente. Tanto si es la primera vez que utiliza Amazon RDS como si lo está configurando para cumplir requisitos específicos, estas secciones ayudan a garantizar que su configuración esté optimizada y siga las prácticas recomendadas.

Temas

- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo
- Conceder acceso programático
- Determinar las necesidades
- Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad

Si ya tiene una cuenta de Cuenta de AWS, conoce los requisitos de Amazon RDS y prefiere usar los valores predeterminados para los grupos de seguridad de IAM y VPC, vaya directo a Introducción a Amazon RDS.

Cómo crear una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Procedimiento para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica

recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación cuando complete el proceso de registro. Puede ver la actividad de la cuenta y administrarla en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no usar el usuario raíz en las tareas cotidianas.

Protección de Usuario raíz de la cuenta de AWS

1. Inicie sesión en AWS Management Console como propietario de la cuenta; para ello, elija Usuario raíz e introduzca el correo electrónico de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitación de un dispositivo MFA virtual para su usuario raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre cómo usar Directorio de IAM Identity Center como origen de identidad, consulte Configuración del acceso de los usuarios con el Directorio de IAM Identity Center predeterminado en la Guía del usuario de AWS IAM Identity Center.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, consulte Inicio de sesión en el portal de acceso de AWS en la Guía del usuario de AWS Sign-In.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center.
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center.

Conceder acceso programático

Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Utiliza credenciales temporales para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK y las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para utilizar la AWS CLI, consulte Configuring the AWS CLI to usa AWS

¿Qué usuario necesita acceso programático?	Para	Mediante
		IAM Identity Center en la Guía del usuario de AWS Command Line Interface. • Para usar AWS SDK, las herramientas y las API de AWS, consulta IAM Identity Center authentication en la Guía de referencia del SDK y las herramientas de AWS.
IAM	Utiliza credenciales temporales para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK y las API de AWS.	Siguiendo las instrucciones de Uso de credenciales temporales con recursos de AWS de la Guía del usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilizar credenciales a largo plazo para firmar las solicitudes programáticas a la AWS CLI, los AWS SDK o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para ver los AWS SDK y las herramientas, consulte Autenticar mediante credenciales a largo plazo en la Guía de referencia de AWS SDK y herramientas. • Para las API de AWS, consulta Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

Determinar las necesidades

El componente básico de Amazon RDS es la instancia de base de datos. En una instancia de base de datos, usted crea sus bases de datos. Una instancia de base de datos proporciona una dirección de red llamada punto de enlace. Sus aplicaciones usarán este punto de enlace para conectarse a su instancia de base de datos. Al crear una instancia de base de datos, especifica detalles como el almacenamiento, la memoria, el motor de base de datos y la versión, la configuración de red, la seguridad y los periodos de mantenimiento. Controla el acceso de red a una instancia de base de datos mediante un grupo de seguridad.

Antes de crear una instancia de base de datos y un grupo de seguridad, debe conocer su instancia de base de datos y las necesidades de la red. Aquí se indican algunos aspectos importantes que se deben tener en cuenta:

- Requisitos de recursos: ¿cuáles son los requisitos de memoria y de procesador para su aplicación o su servicio? Use esta configuración como ayuda para determinar la clase de instancia de base de datos que se usará. Para conocer las especificaciones de las clases de instancia de base de datos, consulte Clases de instancia de base de datos de .
- VPC, subred y grupo de seguridad–: es muy probable que la instancia de base de datos se encuentre en una nube virtual privada (VPC). Para conectarse a su instancia de base de datos, debe configurar reglas de grupo de seguridad. Estas reglas se configuran de forma diferente según el tipo de VPC que utilice y cómo la utilice. Por ejemplo, puede utilizar: una VPC predeterminada o una VPC definida por el usuario.

  En la siguiente lista se describen las reglas de cada opción de VPC:

  - VPC predeterminada: si la cuenta de AWS tiene una VPC predeterminada en la región de AWS actual, esa VPC está configurada para admitir instancias de base de datos. Si especifica la VPC predeterminada al crear la instancia de base de datos, haga lo siguiente:
    - Asegúrese de crear un grupo de seguridad de VPC que autorice conexiones desde la aplicación o el servicio a la instancia de base de datos de Amazon RDS. Use la opción Security Group (Grupo de seguridad) de la consola de VPC o la AWS CLI para crear grupos de seguridad de VPC. Para obtener información, consulte Paso 3: Crear un grupo de seguridad de VPC.
    - Especifique el grupo de subredes de base de datos predeterminado. Si se trata de la primera instancia de base de datos que ha creado en esta región de AWS, Amazon RDS crea el grupo de subred de base de datos predeterminado cuando crea la instancia de base de datos.
  - VPC definida por el usuario: si desea especificar una VPC definida por el usuario al crear una instancia de base de datos, tenga en cuenta lo siguiente:
    - Asegúrese de crear un grupo de seguridad de VPC que autorice conexiones desde la aplicación o el servicio a la instancia de base de datos de Amazon RDS. Use la opción Security Group (Grupo de seguridad) de la consola de VPC o la AWS CLI para crear grupos de seguridad de VPC. Para obtener información, consulte Paso 3: Crear un grupo de seguridad de VPC.
    - La VPC debe cumplir ciertos requisitos para alojar instancias de base de datos, como tener al menos dos subredes, cada una en una zona de disponibilidad independiente. Para obtener información, consulte VPC de Amazon y Amazon RDS.

    - Asegúrese de que especifica un grupo de subredes de base de datos que defina qué subredes de esa VPC puede usar la instancia de base de datos. Para obtener información, consulte la sección DB subnet group (Grupo de subred de base de datos) de Uso de una instancia de base de datos en una VPC.
- Alta disponibilidad: ¿necesita compatibilidad con conmutación por error? En Amazon RDS una implementación Multi-AZ crea una réplica de instancia de base de datos principal y una instancia de base de datos en espera secundaria en otra zona de disponibilidad para permitir la conmutación por error. Es recomendable usar implementaciones Multi-AZ para las cargas de trabajo de producción con el objeto de mantener una alta disponibilidad. Para fines de desarrollo y de pruebas, puede utilizar una implementación no Multi-AZ. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.
- Políticas de IAM: ¿tiene la cuenta de AWS políticas que conceden los permisos necesarios para realizar operaciones de Amazon RDS? Si se conecta a AWS con credenciales de IAM, la cuenta de IAM debe tener políticas de IAM que concedan los permisos necesarios para realizar operaciones de Amazon RDS. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.
- Puertos abiertos: ¿en qué puerto TCP/IP escucha la base de datos? Los firewall de algunas empresas podrían bloquear las conexiones al puerto predeterminado para el motor de base de datos. Si el firewall de su compañía bloquea el puerto predeterminado, elija otro puerto para la nueva instancia de base de datos. Cuando crea una instancia de base de datos que escuche en un puerto especificado, puede cambiar el puerto modificando la instancia de base de datos.
- Región de AWS: ¿en qué región de AWS desea que esté la base de datos? Tener la base de datos cerca de la aplicación o el servicio web puede reducir la latencia de la red. Para obtener más información, consulte Regiones, zonas de disponibilidad y Local Zones.
- Subsistema de disco de base de datos: ¿cuáles son sus requisitos de almacenamiento? Amazon RDS proporciona tres tipos de almacenamiento:
    - Uso general (SSD)
    - IOPS aprovisionadas (PIOPS)
    - Magnético (también conocido como almacenamiento estándar)

    Para obtener más información acerca del almacenamiento de Amazon RDS, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Cuando tenga la información que necesita para crear el grupo de seguridad y la instancia de base de datos, vaya al siguiente paso.

Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad

Los grupos de seguridad de VPC proporcionan acceso a las instancias de base de datos en una VPC. Actúan como firewall para la instancia de base de datos asociada, controlan el tráfico entrante y saliente a nivel de instancia de base de datos. Las instancias de base de datos se crean de manera predeterminada con un firewall y un grupo de seguridad predeterminado que protege la instancia de base de datos.

Para poder conectarse a la instancia de base de datos, debe agregar reglas a un grupo de seguridad que permitan conectarse. Use la información de red y de configuración para crear reglas que permitan el acceso a la instancia de base de datos.

Por ejemplo, supongamos que tiene una aplicación que accede a una base de datos en su instancia de base de datos en una VPC. En este caso, debe añadir una regla de TCP personalizada que especifique el rango de puertos y direcciones IP que la aplicación utiliza para obtener acceso a la base de datos. Si tiene una aplicación en una instancia Amazon EC2, puede usar el grupo de seguridad que configuró para la instancia Amazon EC2.

Puede configurar la conectividad entre una instancia de Amazon EC2 y una instancia de base de datos al crear la instancia de base de datos. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2.

> **Tip**
>
> Puede configurar la conectividad de red entre una instancia de Amazon EC2 y una instancia de base de datos automáticamente al crear la instancia de base de datos. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2.

Para obtener información sobre cómo conectar los recursos en Amazon Lightsail a las instancias de base de datos, consulte Conecte los recursos Servicios de AWS de Lightsail a los servicios mediante el peering VPC.

Para obtener información sobre situaciones comunes del acceso a una instancia de base de datos, consulte Escenarios de acceso a una instancia de base de datos en una VPC.

Para crear un grupo de seguridad de VPC

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc.

   > **Note**
   >
   > Asegúrese de estar en la consola de VPC, no en la consola de RDS.

2. En la esquina superior derecha de la AWS Management Console, elija la AWS región en la que desea crear el grupo de seguridad de VPC y la instancia de base de datos. En la lista de recursos de Amazon VPC para esa región de AWS, debería ver al menos una VPC y varias subredes. Si no es así, no tiene una VPC predeterminada en esa AWS región.
3. En el panel de navegación, elija Grupos de seguridad.
4. Elija Create Security Group (Creación de grupo de seguridad).

   Aparece la página Create security group (Crear grupo de seguridad).
5. En Basic details (Detalles básicos), ingrese el Security group name (Nombre del grupo de seguridad) y la Description (Descripción). Para VPC, elija la VPC en la que desea crear su instancia de base de datos.
6. En Inbound rules (Reglas de entrada), elija Add rule (Agregar regla).

   a. En Type (Tipo), elija Custom TCP (TCP personalizada).

   b. En Port range (Rango de puertos), escriba el valor de puerto que se va a utilizar para la instancia de base de datos.

   c. En Source (Origen), elija un nombre de grupo de seguridad o escriba el rango de direcciones IP (valor CIDR) desde donde accede a la instancia de base de datos. Si elige My IP (Mi IP), esto permite el acceso a la instancia de base de datos desde la dirección IP detectada en su navegador.
7. Si necesita agregar más direcciones IP o distintos rangos de puertos, elija Add rule (Agregar regla) e ingrese la información de la regla.
8. (Opcional) En Outbound rules (Reglas de salida), agregue reglas para el tráfico saliente. De forma predeterminada, se permite todo el tráfico de salida.
9. Elija Create Security Group (Crear grupo de seguridad).

Puede usar el grupo de seguridad de VPC que acaba de crear como grupo de seguridad de la instancia de base de datos cuando la cree.

> **Note**
>
> Si se usa una VPC predeterminada, se crea un grupo de subredes predeterminado que abarca todas las subredes de la VPC. Al crear una instancia de base de datos, puede seleccionar la VPC predeterminada y usar default (valor predeterminado) para DB Subnet Group (Grupo de subred de base de datos).

Una vez que haya completado los requisitos de configuración, puede crear una instancia de base de datos con sus requisitos y grupo de seguridad. Para ello, siga las instrucciones que se indican en Creación de una instancia de base de datos de Amazon RDS. Para obtener información sobre cómo empezar a crear una instancia de base de datos que utiliza un motor de base de datos específico, consulte la documentación pertinente en la siguiente tabla.

Motor de base de datos	Documentación
MariaDB	Creación y conexión a una instancia de base de datos de MariaDB
Microsoft SQL Server	Creación de una instancia de base de datos de Microsoft SQL Server y conexión a ella
MySQL	Creación de una instancia de base de datos MySQL y conexión a ella
Oracle	Creación y conexión a una instancia de base de datos de Oracle
PostgreSQL	Creación de una instancia de base de datos de PostgreSQL y conexión a ella

> **Note**
>
> Si no puede conectarse a una instancia de base de datos después de crearla, consulte la información de solución de problemas en No puede conectarse a la instancia de base de datos de Amazon RDS.

Introducción a Amazon RDS

En los siguientes ejemplos, aprenderá cómo crear y conectarse a una instancia de base de datos utilizando Amazon Relational Database Service (Amazon RDS). Puede crear una instancia de base de datos que utilice Db2, MariaDB, MySQL, Microsoft SQL Server, Oracle o PostgreSQL.

> **Important**
>
> Debe completar las tareas que aparecen en Configuración del entorno para Amazon RDS antes de crear una instancia de base de datos o conectarse a ella.

La creación de una instancia de base de datos y la conexión a una base de datos en una instancia de base de datos son ligeramente diferentes para cada uno de los motores de base de datos. Elija uno de los siguientes motores de base de datos que desee usar para obtener información detallada acerca de la creación y la conexión a la instancia de base de datos. Una vez que ha creado su instancia de base de datos y se ha conectado a esta, hay instrucciones para ayudarle a eliminar la instancia.

Temas

- Creación y conexión a una instancia de base de datos de MariaDB
- Creación de una instancia de base de datos de Microsoft SQL Server y conexión a ella
- Creación de una instancia de base de datos MySQL y conexión a ella
- Creación y conexión a una instancia de base de datos de Oracle
- Creación de una instancia de base de datos de PostgreSQL y conexión a ella
- Explicación: crear un servidor web y una instancia de base de datos de Amazon RDS
- Tutorial: Uso de una función de Lambda para obtener acceso a la base de datos de Amazon RDS

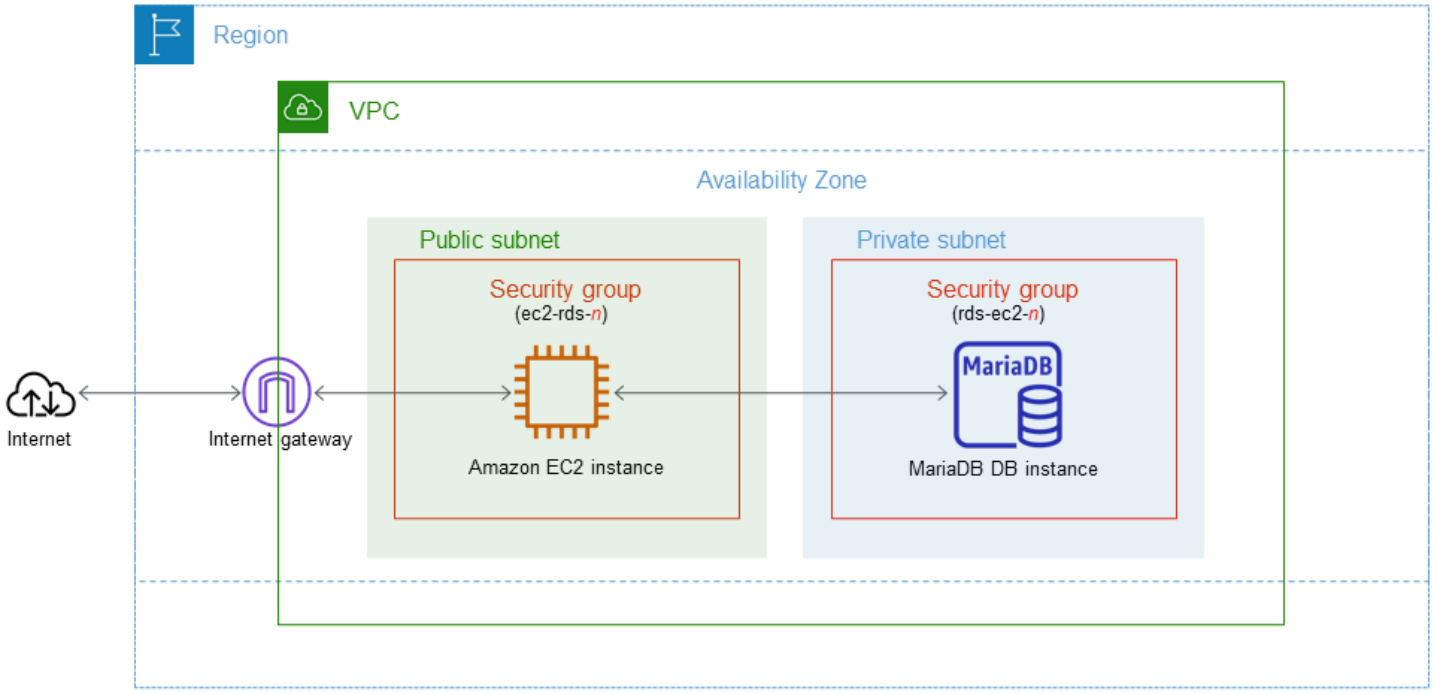
Creación y conexión a una instancia de base de datos de MariaDB

En este tutorial, se crea una instancia de EC2 y una instancia de base de datos de RDS para MariaDB. El tutorial muestra cómo acceder a la instancia de base de datos desde la instancia de EC2 mediante un cliente de MySQL estándar. Como práctica recomendada, este tutorial crea una instancia de base de datos privada en una nube privada virtual (VPC). En la mayoría de los casos, otros recursos de la misma VPC, como las instancias de EC2, pueden acceder a la instancia de base de datos, pero los recursos ajenos a la VPC no pueden acceder a ella.

Tras completar el tutorial, habrá una subred pública y una privada en cada zona de disponibilidad de la VPC. En una zona de disponibilidad, la instancia de EC2 está en la subred pública y la instancia de base de datos está en la subred privada.

> **Important**
>
> La creación de una Cuenta de AWS no supone ningún coste. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

El siguiente diagrama muestra la configuración cuando el tutorial se completa.



Este tutorial le permite crear sus recursos mediante uno de los métodos siguientes:

1. Use la AWS Management Console: Crear una instancia de EC2 y Creación de una instancia de base de datos de MariaDB
2. Use AWS CloudFormation para crear la instancia de base de datos y la instancia de EC2: (Opcional) Crear una VPC, una instancia EC2 y una instancia MariaDB mediante AWS CloudFormation

El primer método utiliza Creación sencilla para crear una instancia de base de datos MariaDB privada con la AWS Management Console. Con Creación sencilla, únicamente debe especificar el tipo de motor de base de datos, el tamaño de la instancia de base de datos y el identificador de instancias de base de datos. Easy create (Creación sencilla) utiliza los ajustes predeterminados para otras opciones de configuración.

Cuando usa Creación estándar, se especifican más opciones de configuración al crear una instancia de base de datos. Estas opciones incluyen la configuración de la disponibilidad, la seguridad, las copias de seguridad y el mantenimiento. Para crear una instancia de base de datos pública, debe utilizar Creación estándar. Para obtener más información, consulta Creación de una instancia de base de datos de Amazon RDS.

Temas

- Requisitos previos
- Crear una instancia de EC2
- Creación de una instancia de base de datos de MariaDB
- (Opcional) Crear una VPC, una instancia EC2 y una instancia MariaDB mediante AWS CloudFormation
- Conectarse a una instancia de base de datos MariaDB
- Eliminación de la instancia de EC2 y la instancia de base de datos
- (Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation
- (Opcional) Conecte la instancia de base de datos a una función de Lambda

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

- Cómo crear una Cuenta de AWS

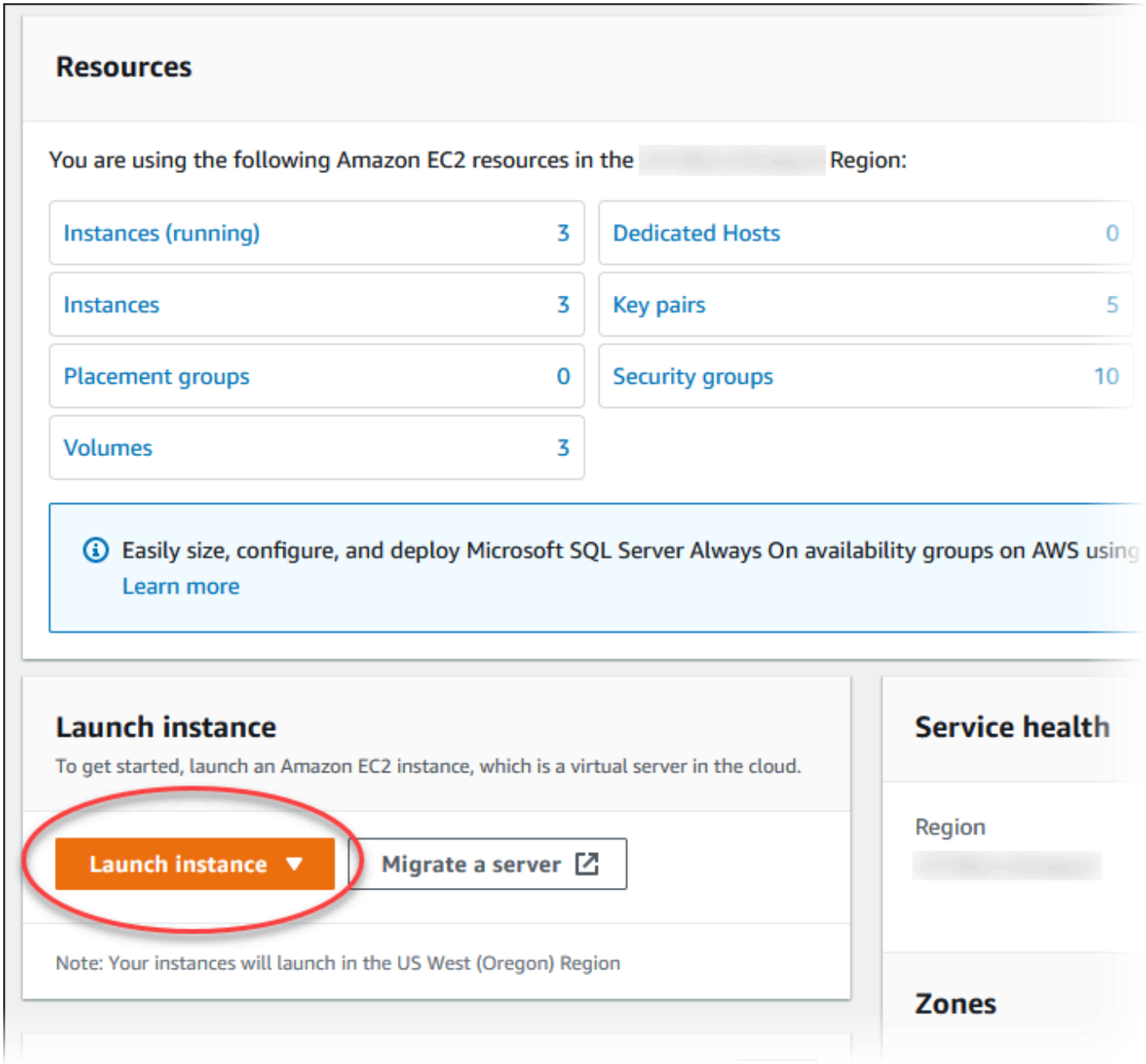
- Creación de un usuario con acceso administrativo

Crear una instancia de EC2

Cree una instancia de Amazon EC2 que utilicará para conectarse a la base de datos.

Para crear una instancia EC2;

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS en la que desea crear la instancia de EC2.
3. Elija Panel de EC2 y, a continuación, Lanzar instancia, como se muestra en la siguiente imagen.

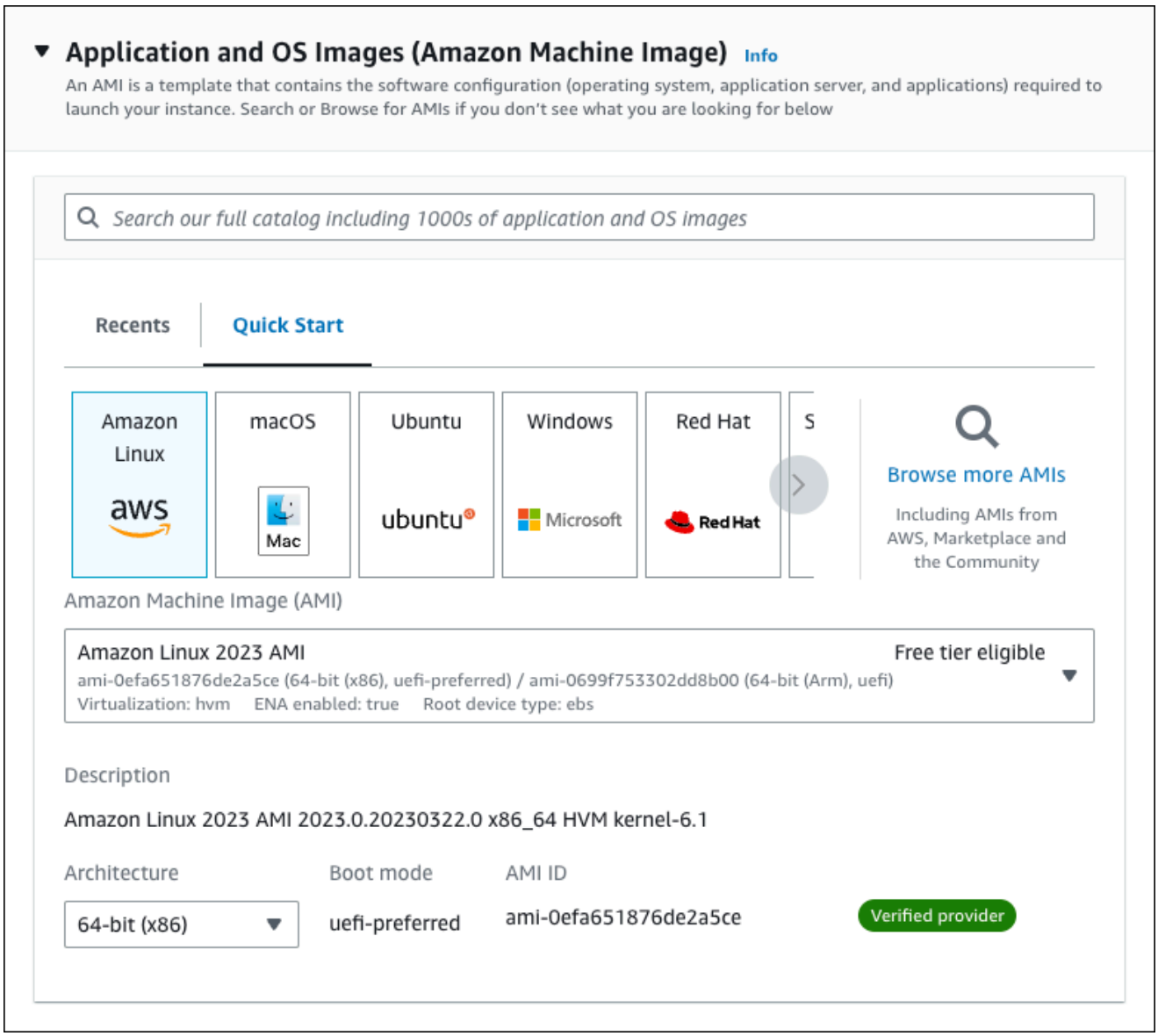


Se abre la página Lanzar una instancia.

4. Elija los siguientes ajustes en la página Lanzar una instancia.

   a. En Name and tags (Nombre y etiquetas), en Name (Nombre), introduzca **`ec2-database-connect`**.

   b. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija Amazon Linux y, a continuación, AMI de Amazon Linux 2023. Mantenga los valores predeterminados para las demás opciones.



c. En Instance type (Tipo de instancia), elija t2.micro.

d. En Key pair (login) [Par de claves (inicio)], elija Key pair name (Nombre de par de claves) para utilizar un par de claves existente. Para crear un nuevo par de claves para la instancia de Amazon EC2, que se muestra a continuación, elija Create new key pair (Crear nuevo par de claves) y, a continuación, utilice la ventana Create key pair (Crear un par de claves).

   Para obtener más información sobre la creación de un nuevo par de claves, consulte Crear un par de claves en la Guía del usuario de Amazon EC2.

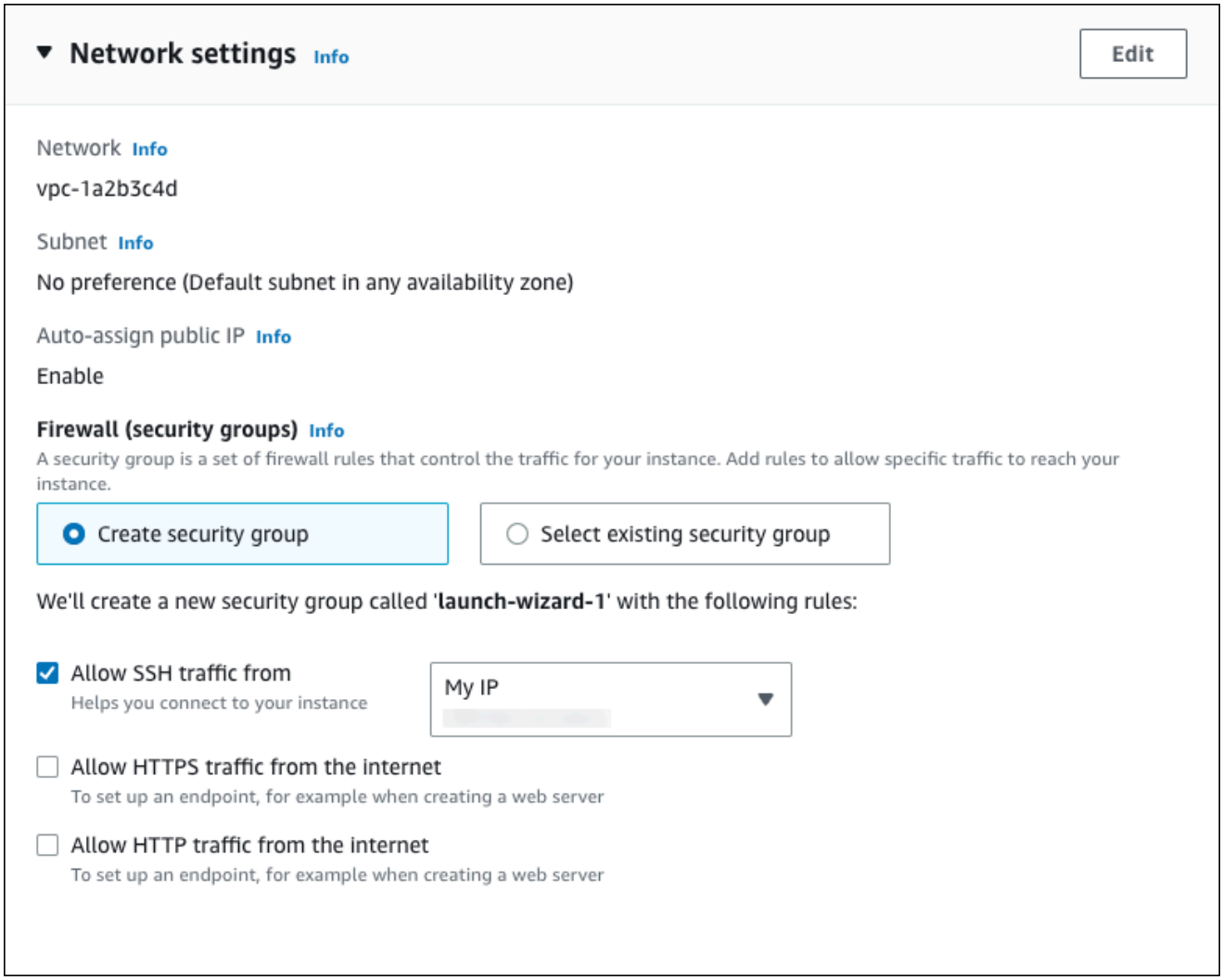
e. En Permitir tráfico de SSH en Configuraciones de red, elija el origen de las conexiones SSH a la instancia de EC2.

Puede elegir My IP (Mi IP) si la dirección IP que se muestra es correcta para las conexiones SSH. De lo contrario, puede determinar la dirección IP que usará para conectarse a las instancias de EC2 en su VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, asegúrese de identificar el rango de direcciones IP que utilizan los equipos cliente.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

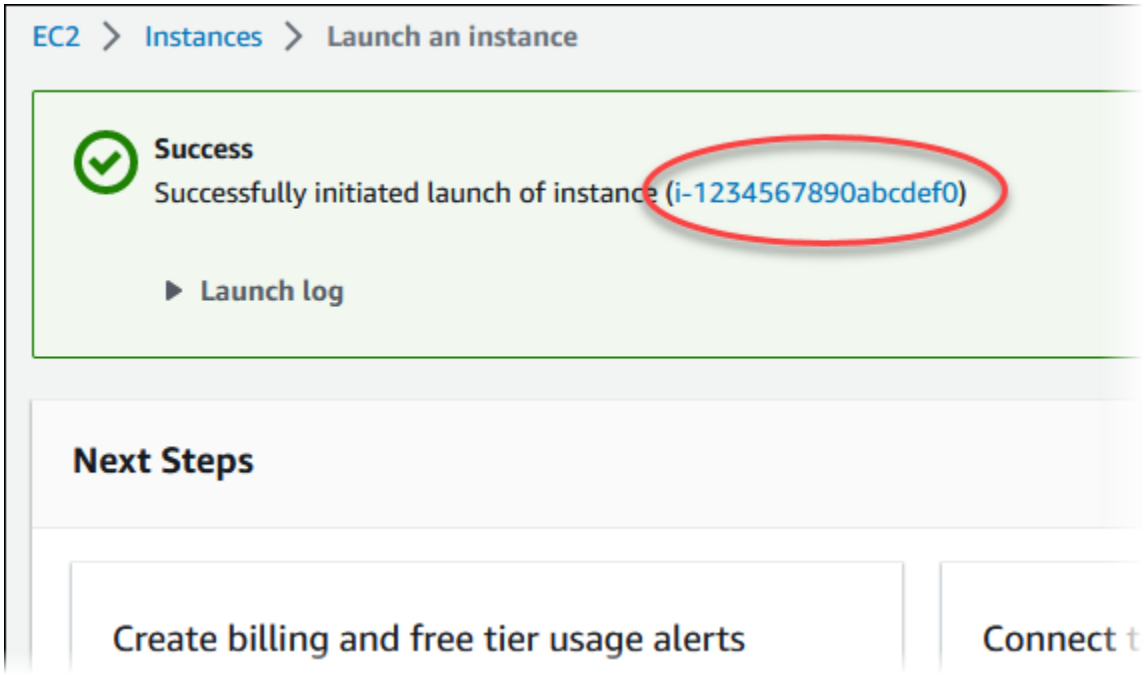
La siguiente imagen muestra un ejemplo de la sección Configuraciones de red.



f. No cambie los valores predeterminados del resto de las secciones.

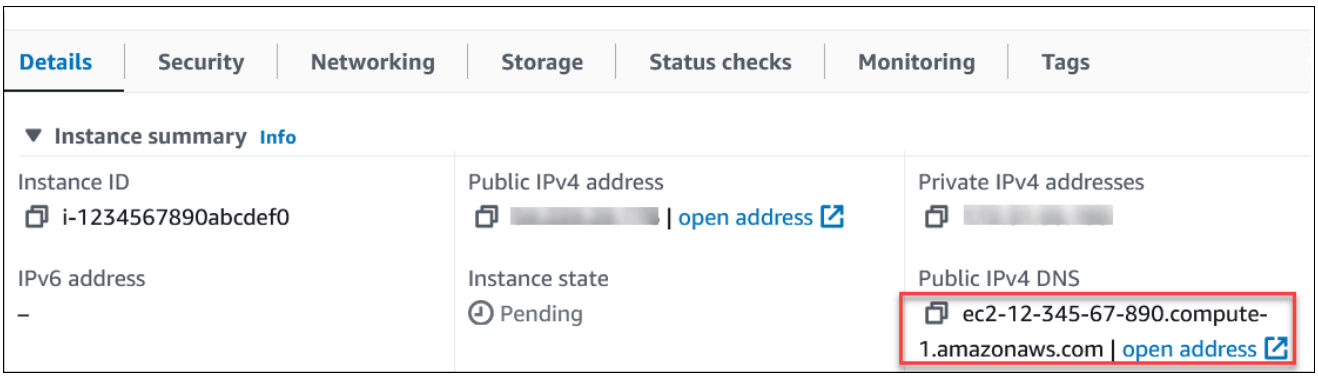
g. Revise un resumen de la configuración de su instancia de EC2 en el panel Resumen; cuando haya terminado, elija Lanzar instancia.

5. En la página Launch Status, que se muestra a continuación, anote el identificador de la nueva instancia de EC2, por ejemplo, `i-1234567890abcdef0`.

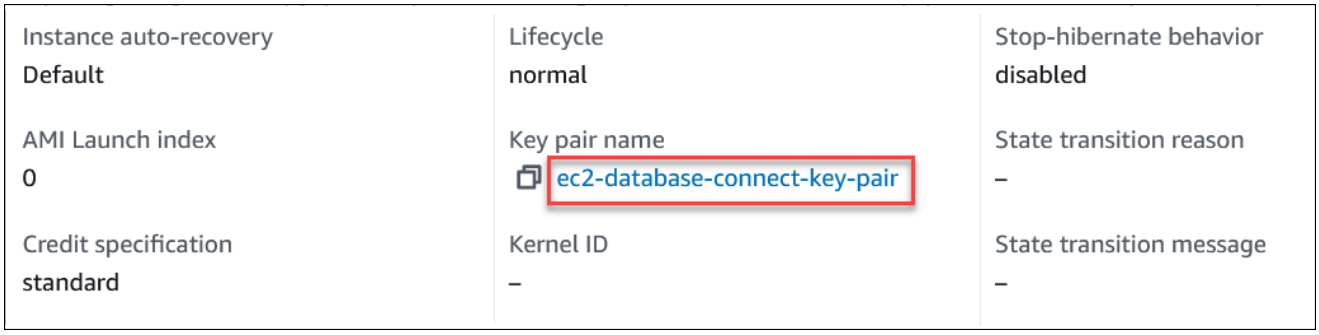


6. Elija el identificador de instancia de EC2 para abrir la lista de instancias de EC2 y, a continuación, seleccione su instancia de EC2.
7. En la pestaña Detalles, anote los siguientes valores, ya que los necesitará cuando se conecte mediante SSH:

   a. En Resumen de la instancia, anote el valor del DNS IPv4 público.



   b. En Detalles de la instancia, anote el valor de Nombre del par de claves.



8. Espere hasta que el Estado de la instancia de su instancia de EC2 tenga el estado En ejecución antes de continuar.

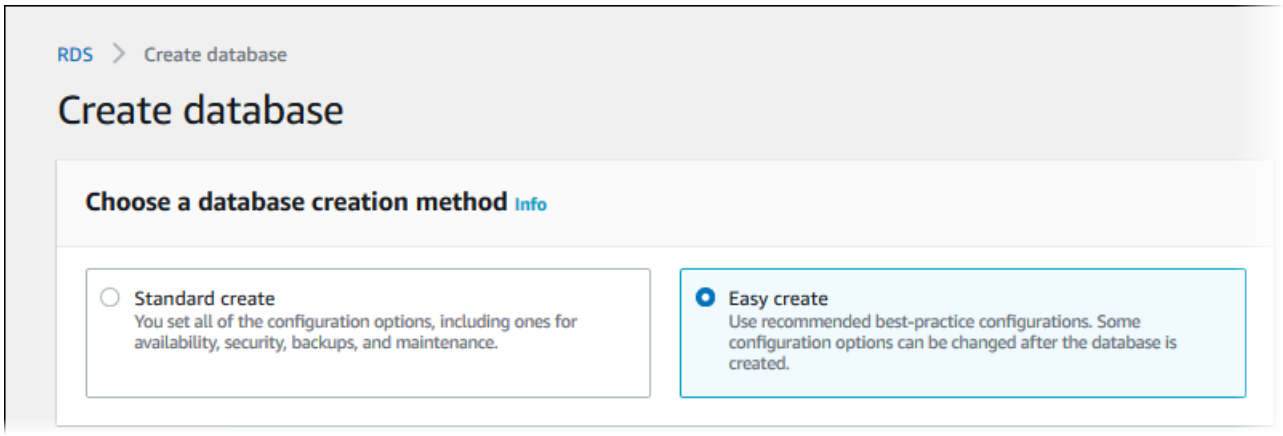
Creación de una instancia de base de datos de MariaDB

El componente básico de Amazon RDS es la instancia de base de datos. Este es el entorno en el que ejecuta las bases de datos MariaDB.

En este ejemplo, utilice la opción Creación sencilla para crear una instancia de base de datos que ejecute el motor de base de datos de MariaDB con una clase de instancia de base de datos db.t4g.micro.

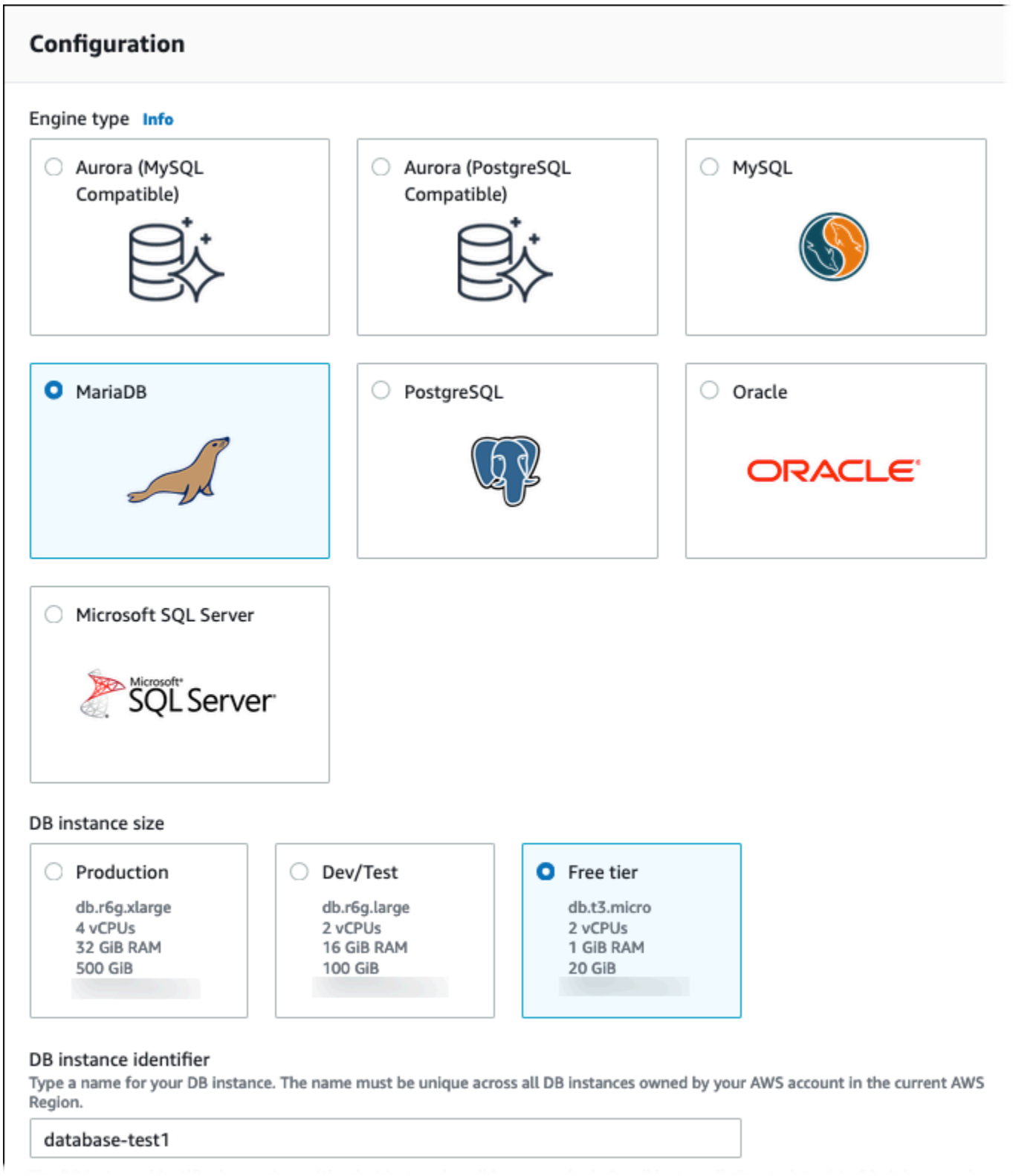
Para crear una instancia de base de datos de MariaDB con la opción Easy Create (Creación sencilla)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija Crear base de datos y seleccione Creación sencilla.



5. En Configuration (Configuración), seleccione MariaDB.
6. Para el tamaño de instancia de base de datos, elija Nivel gratuito o Entorno de pruebas. El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.
7. En DB instance identifier (Identificador de instancia de base de datos), ingrese **`database-test1`**.
8. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro o deje el nombre predeterminado.

   La página Create database (Crear base de datos) debe ser similar a la siguiente imagen. Para las cuentas del plan gratuito, aparece Nivel gratuito. Para las cuentas de planes de pago, aparece Entorno de pruebas.

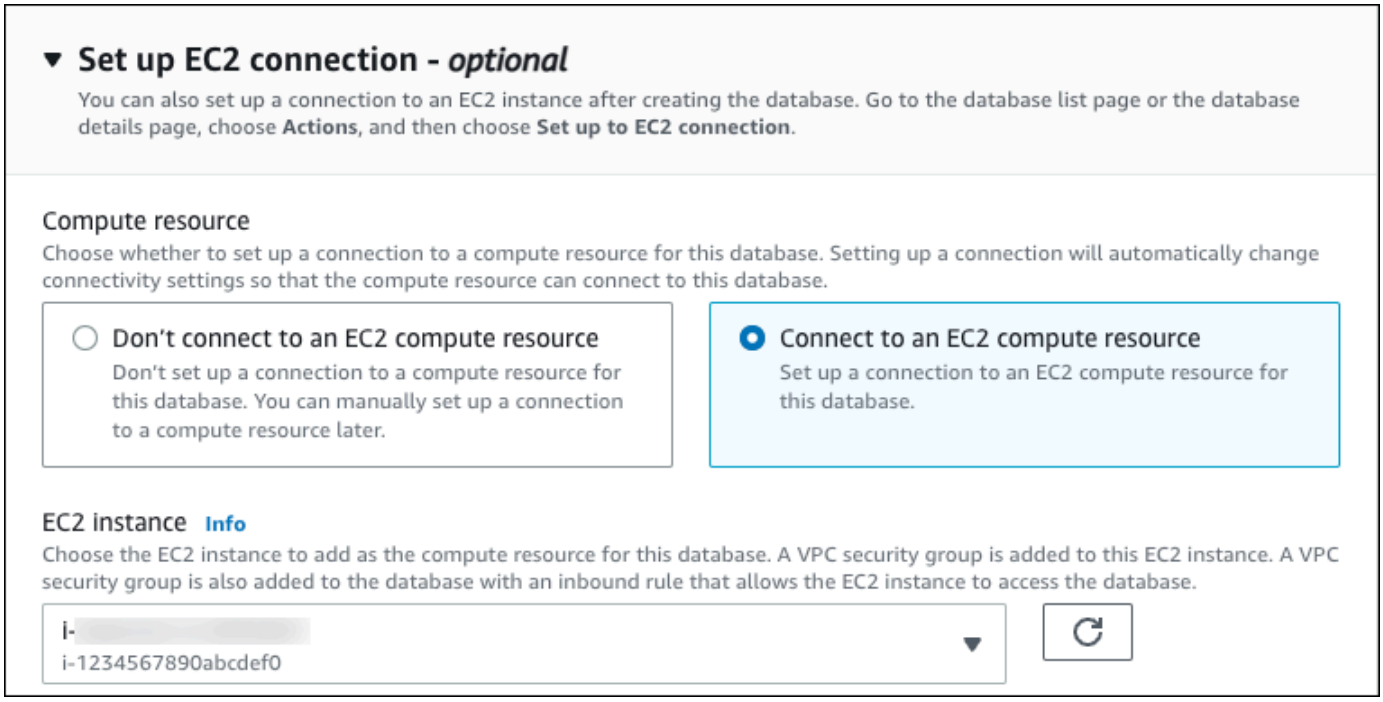


9. Para utilizar una contraseña maestra generada automáticamente para la instancia de base de datos, seleccione Generación automática de contraseña.

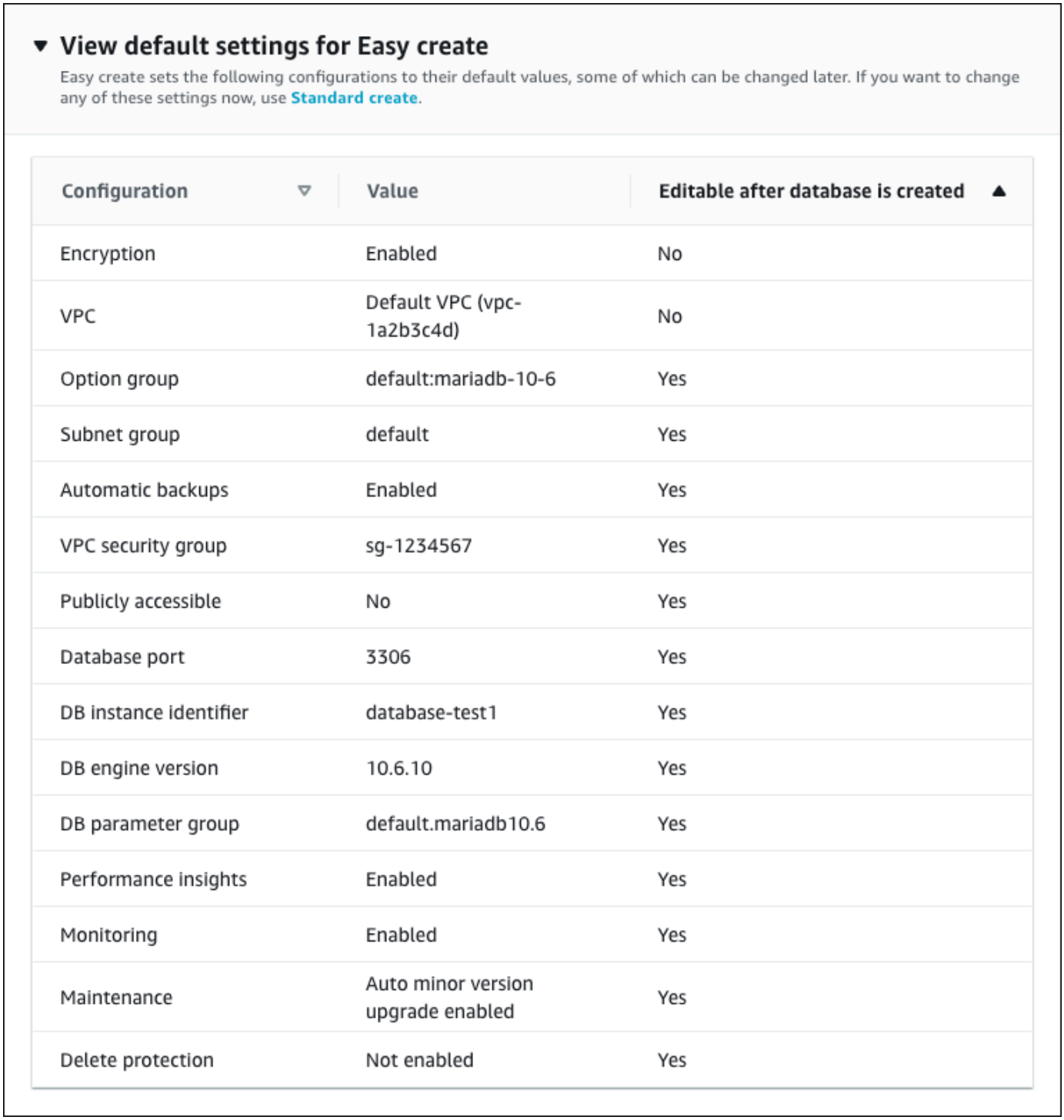
Para introducir la contraseña maestra, desactive la casilla Generar automáticamente una contraseña y luego introduzca la misma contraseña en Contraseña maestra y Confirmar contraseña.

10. Para configurar una conexión con la instancia de EC2 que ha creado anteriormente, abra Configurar conexión a EC2 (opcional).

    Seleccione Conectarse a un recurso informático de EC2. Elija la instancia de EC2 que ha creado anteriormente.



11. Expanda Ver la configuración predeterminada de la creación sencilla.



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:mariadb-10-6	Yes
Subnet group	default	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-1234567	Yes
Publicly accessible	No	Yes
Database port	3306	Yes
DB instance identifier	database-test1	Yes
DB engine version	10.6.10	Yes
DB parameter group	default.mariadb10.6	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Puede examinar la configuración predeterminada utilizada con Easy create (Creación sencilla). La columna Editable después de crear la base de datos muestra las opciones que puede cambiar después de crear la base de datos.

- Si una configuración tiene No en esa columna y desea una configuración diferente, puede usar Creación estándar para crear la instancia de base de datos.
- Si una configuración tiene Sí en esa columna y desea una configuración diferente, puede utilizar Creación estándar para crear la instancia de base de datos o modificar la instancia de base de datos después de crearla para cambiar la configuración.

12. Elija Creación de base de datos.

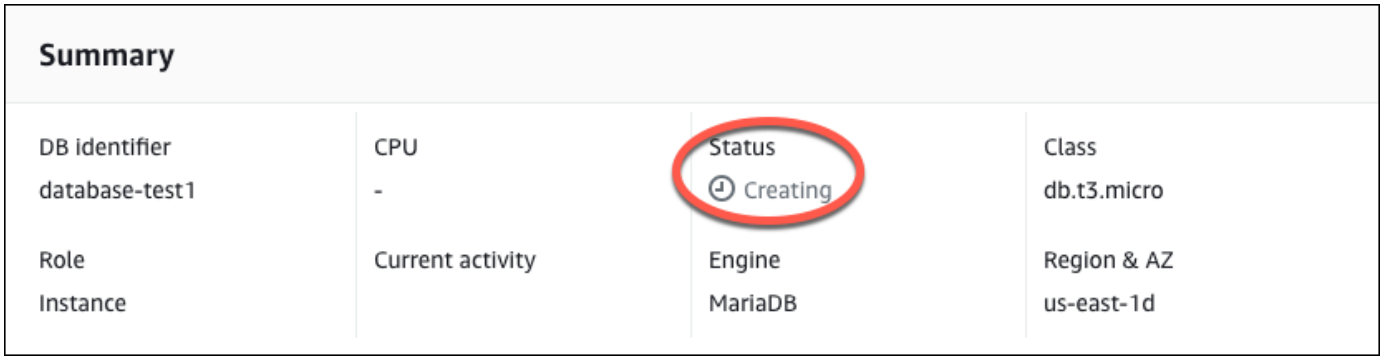
    Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales).

    Puede utilizar la contraseña y el nombre de usuario que aparecen para conectarse a la instancia de base de datos como el usuario maestro.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla.
    > Si tiene que cambiar la contraseña de usuario maestro después de que la instancia de base de datos esté disponible, puede modificar la instancia de base de datos para ello. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

13. En la lista Bases de datos, seleccione el nombre de la nueva instancia de base de datos de MariaDB para ver sus detalles.

    La instancia de base de datos tiene el estado Creando hasta que está lista para usarse.



Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de la base de datos. Dependiendo de la clase de instancia de la base de datos y de la cantidad de almacenamiento, es posible que la nueva instancia tarde hasta 20 minutos en estar disponible.

(Opcional) Crear una VPC, una instancia EC2 y una instancia MariaDB mediante AWS CloudFormation

En lugar de utilizar la consola para crear la VPC, la instancia de EC2 y la instancia de MariaDB, puede utilizar AWS CloudFormation para aprovisionar recursos de AWS tratando la infraestructura como código. Para ayudarle a organizar sus recursos de AWS en unidades más pequeñas y fáciles de administrar, puede utilizar la funcionalidad de pila anidada de AWS CloudFormation. Para obtener más información, consulte Creación de una pila en la consola AWS CloudFormation y Uso de pilas anidadas.

> **Important**
>
> AWS CloudFormation es gratuito, pero los recursos que CloudFormation crea están activos. Se le facturan las tarifas de uso estándar por estos recursos hasta que los finalice. Para obtener más información, consulte Precios de RDS para MariaDB.

- Descargar la plantilla de CloudFormation
- Configurar los recursos mediante CloudFormation

Descargar la plantilla de CloudFormation

Una plantilla de CloudFormation es un archivo de texto con formato JSON o YAML que contiene la información de configuración de los recursos que desea crear en la pila. Esta plantilla también crea una VPC y un host bastión para usted junto con la instancia de RDS.

Para descargar el archivo de plantilla, abra el enlace MariaDB CloudFormation template.

En la página de Github, haga clic en el botón Descargar archivo sin procesar para guardar el archivo YAML de la plantilla.

Configurar los recursos mediante CloudFormation

> **Note**
>
> Antes de iniciar este proceso, asegúrese de tener un par de claves para una instancia EC2 en su Cuenta de AWS. Para obtener más información, consulte Pares de claves de Amazon EC2 e instancias Linux.

Al utilizar la plantilla de AWS CloudFormation, debe seleccionar los parámetros correctos para asegurarse de que los recursos se crean correctamente. Siga los pasos que se indican a continuación:

1. Inicie sesión en la AWS Management Console y abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Elija Crear pila.
3. En la sección Especificar la plantilla, seleccione Cargar un archivo de plantilla desde el ordenador y Siguiente.
4. En la página Especificar detalles de la pila, introduzca los siguientes parámetros:
   a. Ponga el nombre de pila en MariaDBTestStack.
   b. En Parámetros, defina las zonas de disponibilidad seleccionando tres zonas de disponibilidad.
   c. En Configuración de host bastión de Linux, en Nombre de la clave, seleccione un par de claves para iniciar sesión en su instancia de EC2.
   d. En los ajustes de Configuración de host bastión de Linux, ponga el rango de IP permitido en su dirección IP. Para conectarse a las instancias de EC2 de su VPC mediante Secure Shell (SSH), determine su dirección IP pública mediante el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección

IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

e. En Configuración general de la base de datos, ponga la Clase de instancia de base de datos en db.t3.micro.

f. Ponga el Nombre de la base de datos en **`database-test1`**.

g. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro.

h. Ponga Administrar contraseña de usuario maestro de base de datos con Secrets Manager en `false` para este tutorial.

i. En Contraseña de base de datos, ponga la contraseña que desee. Recuerde esta contraseña para poder ver los pasos adicionales del tutorial.

j. En Configuración de almacenamiento de base de datos, ponga el Tipo de almacenamiento de base de datos en gp2.

k. En la Configuración de supervisión de base de datos, ponga Habilitar RDS Performance Insights en falso.

l. Deje el resto de la configuración con los valores predeterminados. Haga clic en Siguiente para continuar.

5. En la página Revisar la pila, seleccione Enviar después de comprobar las opciones de base de datos y de host bastión de Linux.

Una vez finalizado el proceso de creación de la pila, visualice las pilas con los nombres BastionStack y RDSNS para anotar la información que necesita para conectarse a la base de datos. Para obtener más información, consulte Viewing AWS CloudFormation stack data and resources on the AWS Management Console.

Conectarse a una instancia de base de datos MariaDB

Puede usar cualquier aplicación cliente de SQL estándar para conectarse a la instancia de base de datos. En este ejemplo, se conecta a una instancia de base de datos de MariaDB mediante el cliente de línea de comandos mysql.

Para conectarse a una instancia de base de datos de MariaDB

1. Busque el punto de enlace (nombre de DNS) y el número de puerto de la instancia de base de datos.

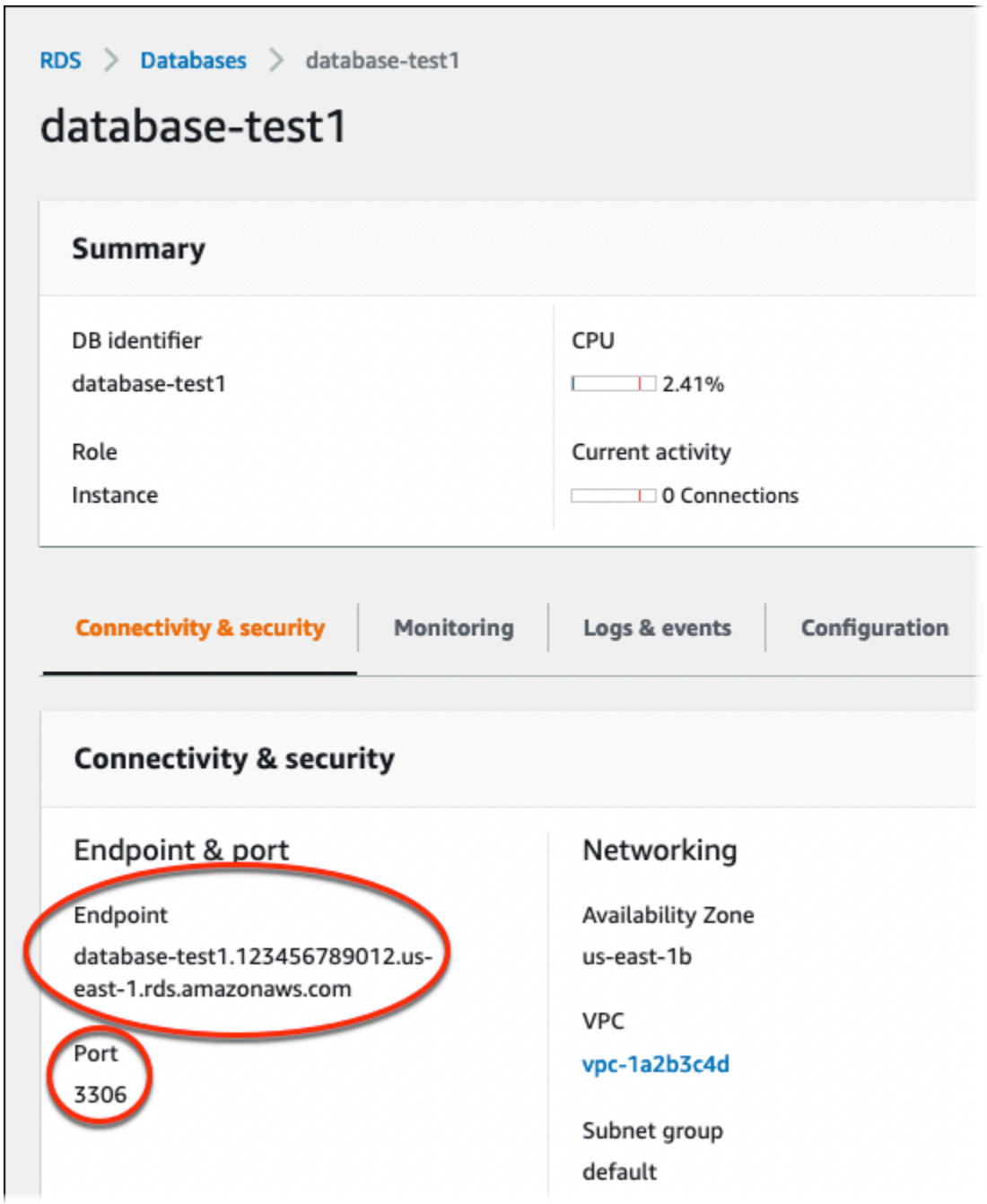
a. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

b. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS de la instancia de base de datos.

c. En el panel de navegación, elija Databases (Bases de datos).

d. Seleccione el nombre de la instancia de base de datos MariaDB para mostrar sus detalles.

e. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



2. Conéctese a la instancia de EC2 que ha creado anteriormente siguiendo los pasos que se indican en Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2.

   Le recomendamos que se conecte a la instancia de EC2 mediante SSH. Si la utilidad de cliente SSH está instalada en Windows, Linux o Mac, puede conectarse a la instancia con el siguiente formato de comando:

   ```
   ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
   ```

Por ejemplo, suponga que `ec2-database-connect-key-pair.pem` está almacenado en `/dir1` en Linux y que el DNS IPv4 público de su instancia de EC2 es `ec2-12-345-678-90.compute-1.amazonaws.com`. Su comando SSH tendría el siguiente aspecto:

```
ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
user@ec2-12-345-678-90.compute-1.amazonaws.com
```

3. Obtenga las correcciones de errores y las actualizaciones de seguridad más recientes actualizando el software en su instancia de EC2. Para ello, utilice el siguiente comando.

> **Note**
>
> La opción `-y` instala las actualizaciones sin necesidad de confirmación. Para examinar las actualizaciones antes de la instalación, omita esta opción.

```
sudo dnf update -y
```

4. Instale el cliente de línea de comandos mysql desde MariaDB.

   Para instalar el cliente de línea de comandos de MariaDB en Amazon Linux 2023, ejecute el siguiente comando:

```
sudo dnf install mariadb105
```

5. Conéctese a la instancia de base de datos de MariaDB. Por ejemplo, introduzca el siguiente comando. Esta acción le permite conectarse a la instancia de base de datos de MariaDB mediante el cliente de MySQL.

   Sustituya el punto de conexión de la instancia de base de datos (nombre de DNS) por *`endpoint`* y sustituya el nombre de usuario maestro que utilizó por *`admin`*. Proporcione la contraseña maestra que utilizó cuando se le solicite una contraseña.

```
mysql -h endpoint -P 3306 -u admin -p
```

   Una vez especificada la contraseña del usuario, debería ver un resultado similar al siguiente.

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 156
Server version: 10.6.10-MariaDB-log managed by https://aws.amazon.com/rds/

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Para obtener más información acerca de cómo conectarse a la instancia de base de datos MariaDB, consulte Conexión a la instancia de base de datos de MariaDB. Si no puede conectarse a la instancia de base de datos, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Por motivos de seguridad, se recomienda utilizar conexiones cifradas. Utilice solo una conexión de MariaDB sin cifrar cuando el cliente y el servidor están en la misma VPC y la red es de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte Conexión a la instancia de base de datos de MariaDB en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado).

6. Ejecutar comandos SQL.

   Por ejemplo, el siguiente comando de SQL muestra la fecha y la hora actuales:

   ```
   SELECT CURRENT_TIMESTAMP;
   ```

Eliminación de la instancia de EC2 y la instancia de base de datos

Después de conectarse y explorar la instancia de EC2 de muestra y la instancia de base de datos que creó, elimínelas para que no le sigan cobrando por ellas.

Si ha utilizado AWS CloudFormation para crear recursos, omita este paso y vaya al siguiente.

Para eliminar la instancia de EC2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).

3. Seleccione la instancia de EC2 y elija Estado de la instancia y Terminar instancia.
4. Cuando se le indique que confirme, elija Terminar.

Para obtener más información sobre la eliminación de una instancia de EC2, consulte Terminar la instancia en la Guía del usuario de Amazon EC2.

Para eliminar una instancia de base de datos sin instantánea de base de datos final

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. Desactive Crear la instantánea final y Conservar copias de seguridad automatizadas.
6. Complete la confirmación y seleccione Eliminar.

(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation

Si ha utilizado AWS CloudFormation para crear recursos, elimine la pila de CloudFormation después de conectarse a la instancia de EC2 y a la instancia de base de datos de muestra y de explorarlas; de este modo, ya no se le cobrará por ellas.

Para eliminar los recursos de CloudFormation

1. Abra la consola de AWS CloudFormation.
2. En la página Pilas de la consola de CloudFormation, seleccione la pila raíz (la pila sin el nombre VPCStack, BastionStack o RDSNS).
3. Elija Eliminar.
4. Cuando se le pida confirmación, seleccione Eliminar pila.

Para obtener información sobre cómo eliminar una pila en CloudFormation, consulte Eliminación de una pila en la consola de AWS CloudFormation, en la Guía del usuario de AWS CloudFormation.

(Opcional) Conecte la instancia de base de datos a una función de Lambda

También puede conectar la instancia de base de datos de RDS para MariaDB a un recurso de computación sin servidor de Lambda. Las funciones de Lambda permiten ejecutar código sin aprovisionar ni administrar la infraestructura. Una función de Lambda también permite responder automáticamente a las solicitudes de ejecución de código a cualquier escala, desde una docena de eventos al día hasta cientos de eventos por segundo. Para obtener más información, consulte Conexión automática de una función de Lambda y una instancia de base de datos.

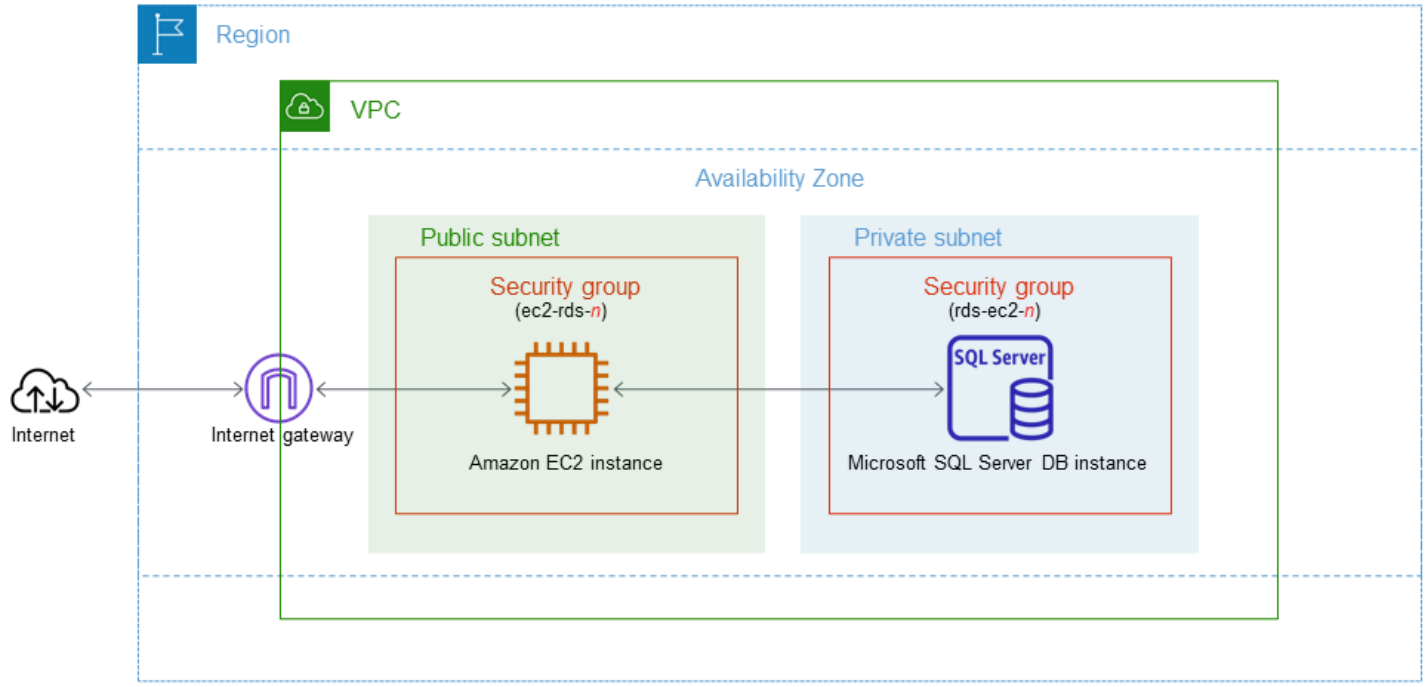
Creación de una instancia de base de datos de Microsoft SQL Server y conexión a ella

En este tutorial, se crea una instancia de EC2 y una instancia de base de datos de RDS para Microsoft SQL Server. El tutorial muestra cómo acceder a la instancia de base de datos desde la instancia de EC2 mediante el cliente Microsoft SQL Server Management Studio. Como práctica recomendada, este tutorial crea una instancia de base de datos privada en una nube privada virtual (VPC). En la mayoría de los casos, otros recursos de la misma VPC, como las instancias de EC2, pueden acceder a la instancia de base de datos, pero los recursos ajenos a la VPC no pueden acceder a ella.

Tras completar el tutorial, habrá una subred pública y una privada en cada zona de disponibilidad de la VPC. En una zona de disponibilidad, la instancia de EC2 está en la subred pública y la instancia de base de datos está en la subred privada.

> **Important**
>
> La creación de una cuenta de AWS no supone ningún costo. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de AWS que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

El siguiente diagrama muestra la configuración cuando el tutorial se completa.



Este tutorial le permite crear sus recursos mediante uno de los métodos siguientes:

1. Use la AWS Management Console: Creación de una instancia de base de datos de SQL Server y Crear una instancia de EC2
2. Use AWS CloudFormation para crear la instancia de base de datos y la instancia de EC2: (Opcional) Crear una VPC, una instancia EC2 y una instancia de SQL Server mediante AWS CloudFormation

El primer método utiliza Creación sencilla para crear una instancia de base de datos privada de SQL Server con la AWS Management Console. Con Creación sencilla, únicamente debe especificar el tipo de motor de base de datos, el tamaño de la instancia de base de datos y el identificador de instancias de base de datos. Easy create (Creación sencilla) utiliza los ajustes predeterminados para otras opciones de configuración.

Cuando usa Creación estándar, se especifican más opciones de configuración al crear una instancia de base de datos. Estas opciones incluyen la configuración de la disponibilidad, la seguridad, las copias de seguridad y el mantenimiento. Para crear una instancia de base de datos pública, debe utilizar Creación estándar. Para obtener más información, consulta Creación de una instancia de base de datos de Amazon RDS.

Temas

- Requisitos previos
- Crear una instancia de EC2
- Creación de una instancia de base de datos de SQL Server
- (Opcional) Crear una VPC, una instancia EC2 y una instancia de SQL Server mediante AWS CloudFormation
- Conexión a una instancia de base de datos de SQL Server
- Exploración de una instancia de base de datos de SQL Server de ejemplo
- Eliminación de la instancia de EC2 y la instancia de base de datos
- (Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation
- (Opcional) Conecte la instancia de base de datos a una función de Lambda

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

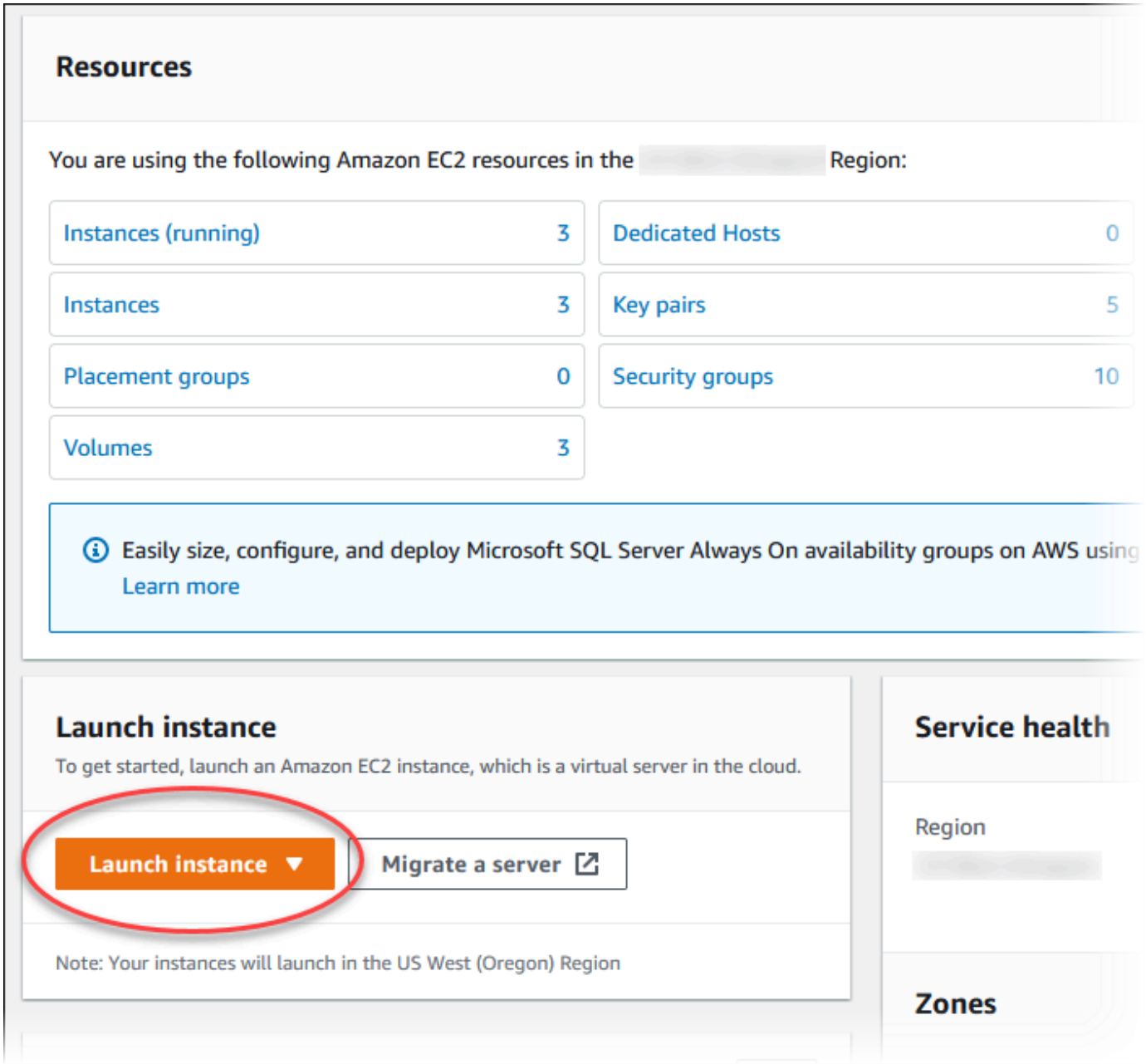
- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Crear una instancia de EC2

Cree una instancia de Amazon EC2 que utilicará para conectarse a la base de datos.

Para crear una instancia EC2;

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS que ha utilizado anteriormente para la base de datos.
3. Elija Panel de EC2 y, a continuación, Lanzar instancia, como se muestra en la siguiente imagen.

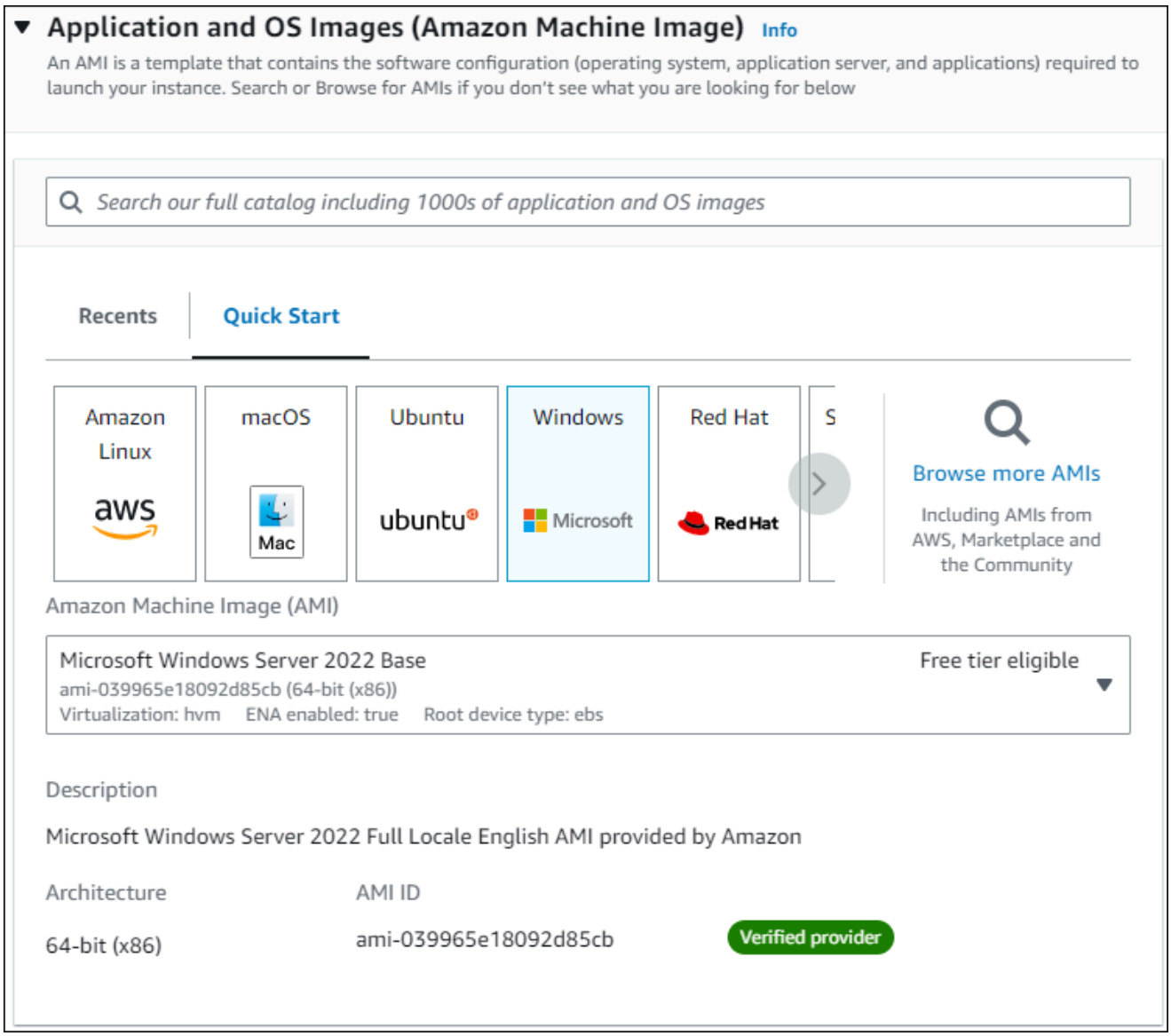


Se abre la página Lanzar una instancia.

4. Elija los siguientes ajustes en la página Lanzar una instancia.

   a. En Name and tags (Nombre y etiquetas), en Name (Nombre), introduzca **`ec2-database-connect`**.

   b. En Imágenes de aplicaciones y sistema operativo (Amazon Machine Image), elija Windows y, a continuación, elija Microsoft Windows Server 2022 Base. Mantenga los valores predeterminados para las demás opciones.



c. En Instance type (Tipo de instancia), elija t2.micro.

d. En Key pair (login) [Par de claves (inicio)], elija Key pair name (Nombre de par de claves) para utilizar un par de claves existente. Para crear un nuevo par de claves para la instancia de Amazon EC2, que se muestra a continuación, elija Create new key pair (Crear nuevo par de claves) y, a continuación, utilice la ventana Create key pair (Crear un par de claves).

   Para obtener más información sobre la creación de un par de claves, consulte Create a key pair (Cree un par de claves) en la Guía del usuario de instancias de Windows de Amazon EC2.

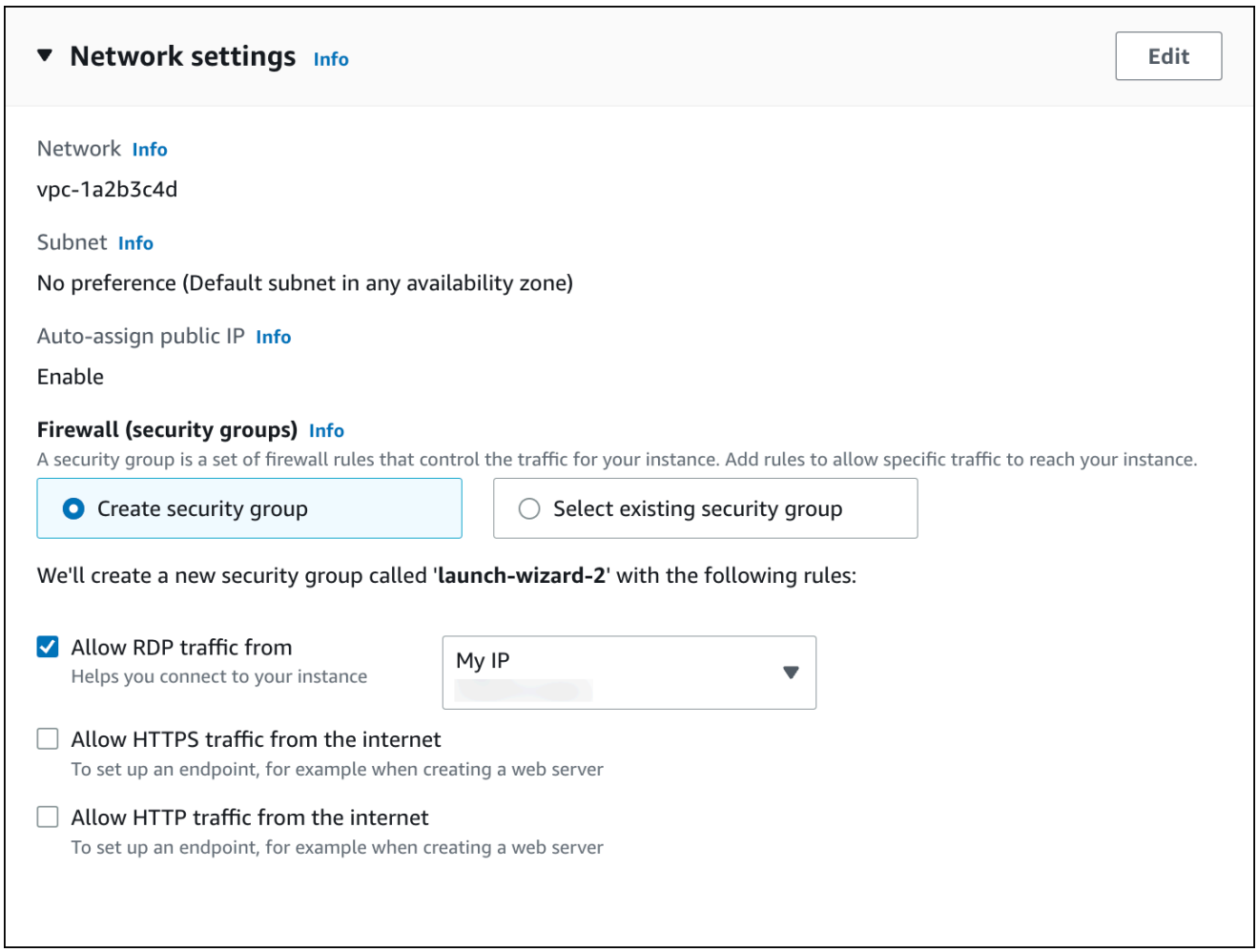
e. Para Firewall (grupos de seguridad), en Configuración de red, elija Permitir el tráfico RDP desde para conectarse a la instancia de EC2.

Puede elegir Mi IP si la dirección IP que se muestra es correcta para las conexiones RDP. De lo contrario, puede determinar la dirección IP que usará para conectarse a las instancias de EC2 en su VPC mediante RDP. Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, asegúrese de identificar el rango de direcciones IP que utilizan los equipos cliente.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso RDP, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante RDP. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante RDP.

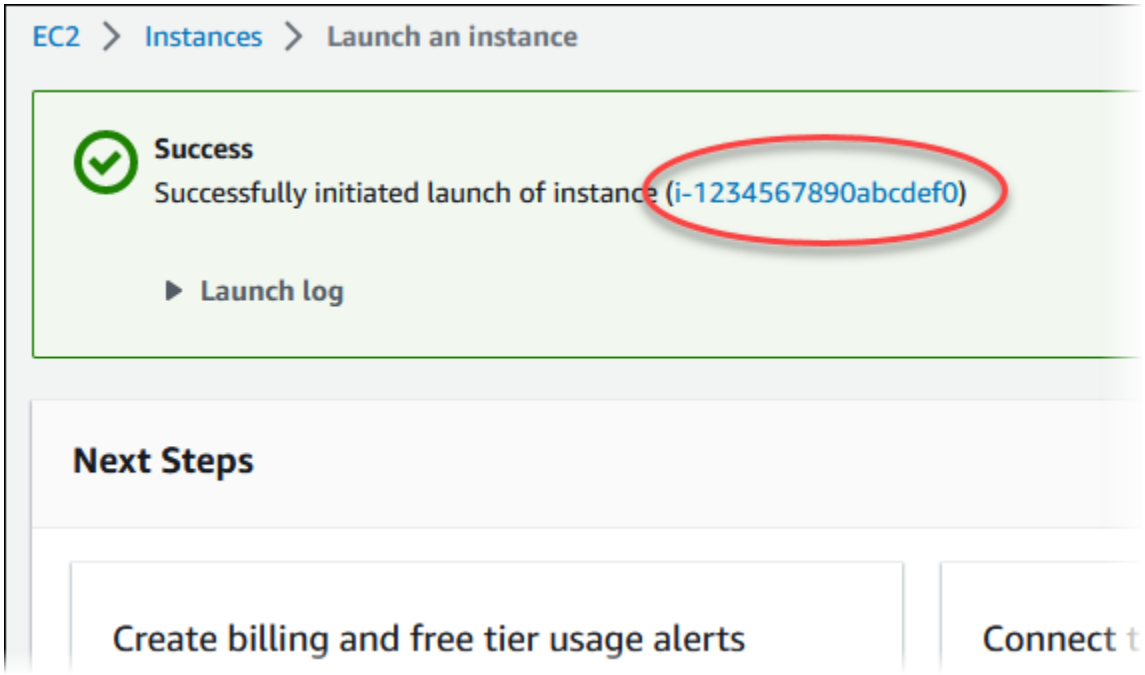
La siguiente imagen muestra un ejemplo de la sección Configuraciones de red.



f. Mantenga los valores predeterminados del resto de las secciones.

g. Revise un resumen de la configuración de su instancia de EC2 en el panel Resumen; cuando haya terminado, elija Lanzar instancia.

5. En la página Launch Status, que se muestra a continuación, anote el identificador de la nueva instancia de EC2, por ejemplo, `i-1234567890abcdef0`.



6. Elija el identificador de instancia de EC2 para abrir la lista de instancias de EC2.
7. Espere hasta que el Estado de la instancia de su instancia de EC2 tenga el estado En ejecución antes de continuar.

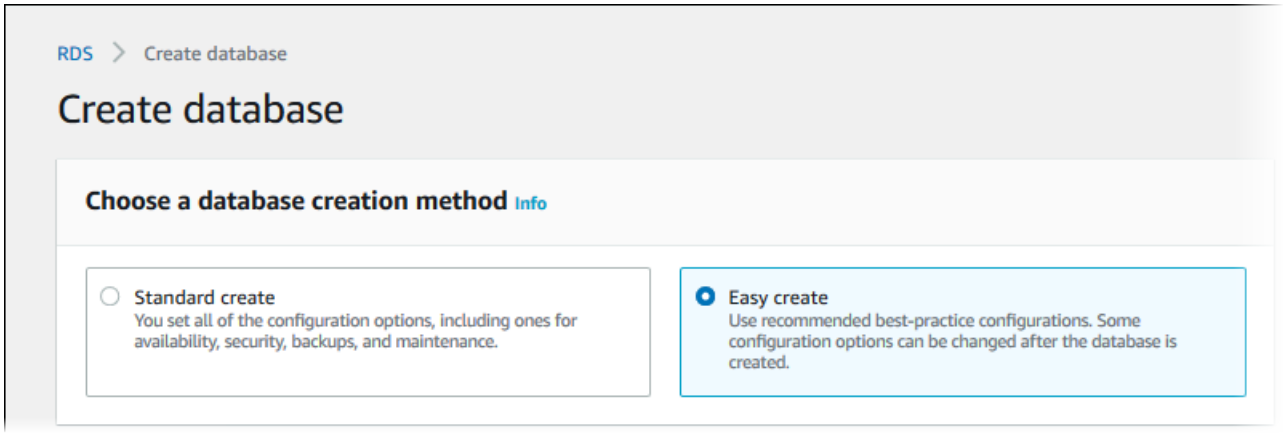
Creación de una instancia de base de datos de SQL Server

El componente básico de Amazon RDS es la instancia de base de datos. Este es el entorno en el que ejecuta las bases de datos SQL Server.

En este ejemplo, se utiliza Creación sencilla para crear una instancia de base de datos que ejecute el motor de base de datos de SQL Server con una clase de instancia de base de datos db.t2.micro.

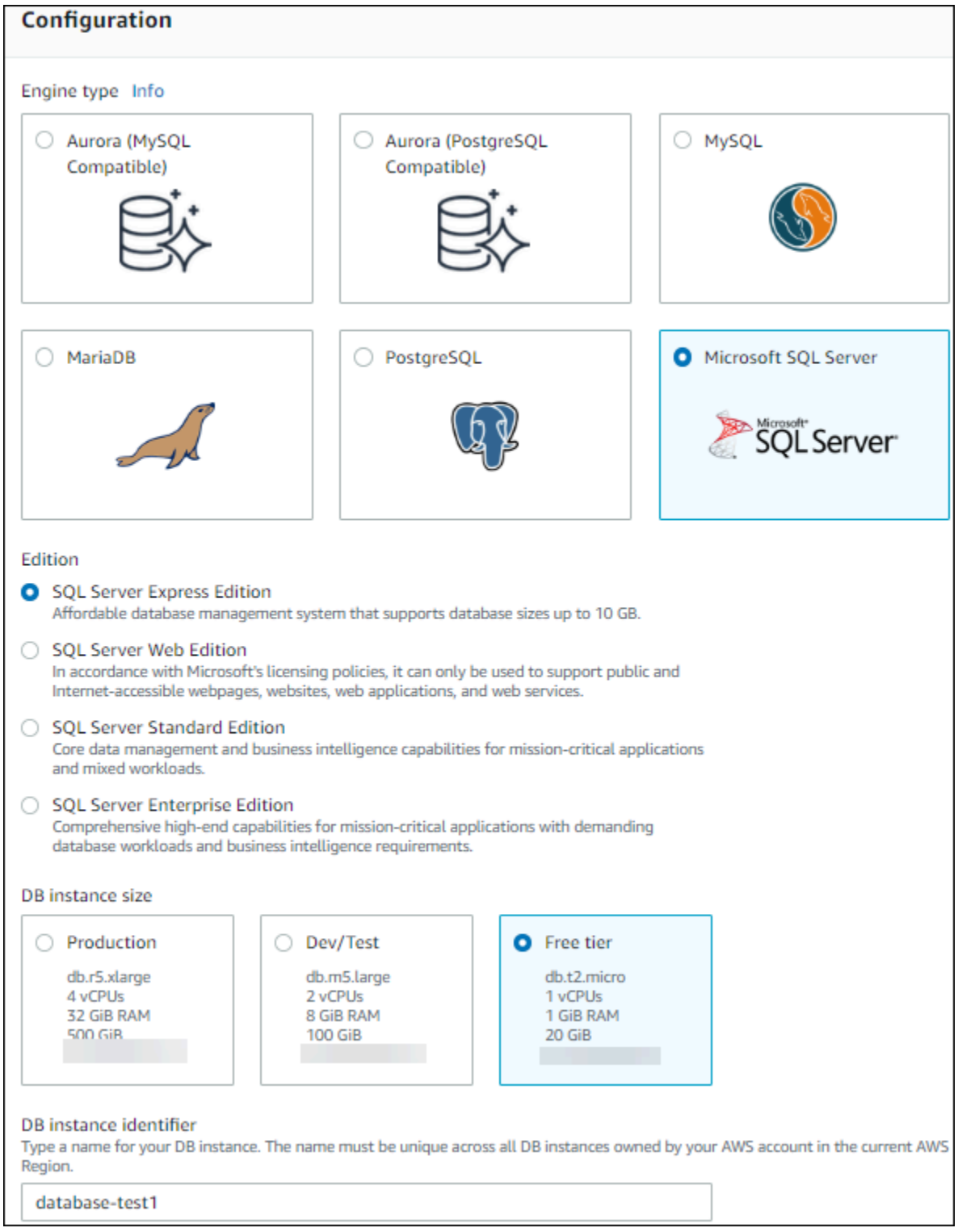
Para crear una instancia de base de datos de Microsoft SQL Server con Easy create

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Seleccione Create database (Crear base de datos) y asegúrese de que la opción Easy Create (Creación sencilla) esté seleccionada.



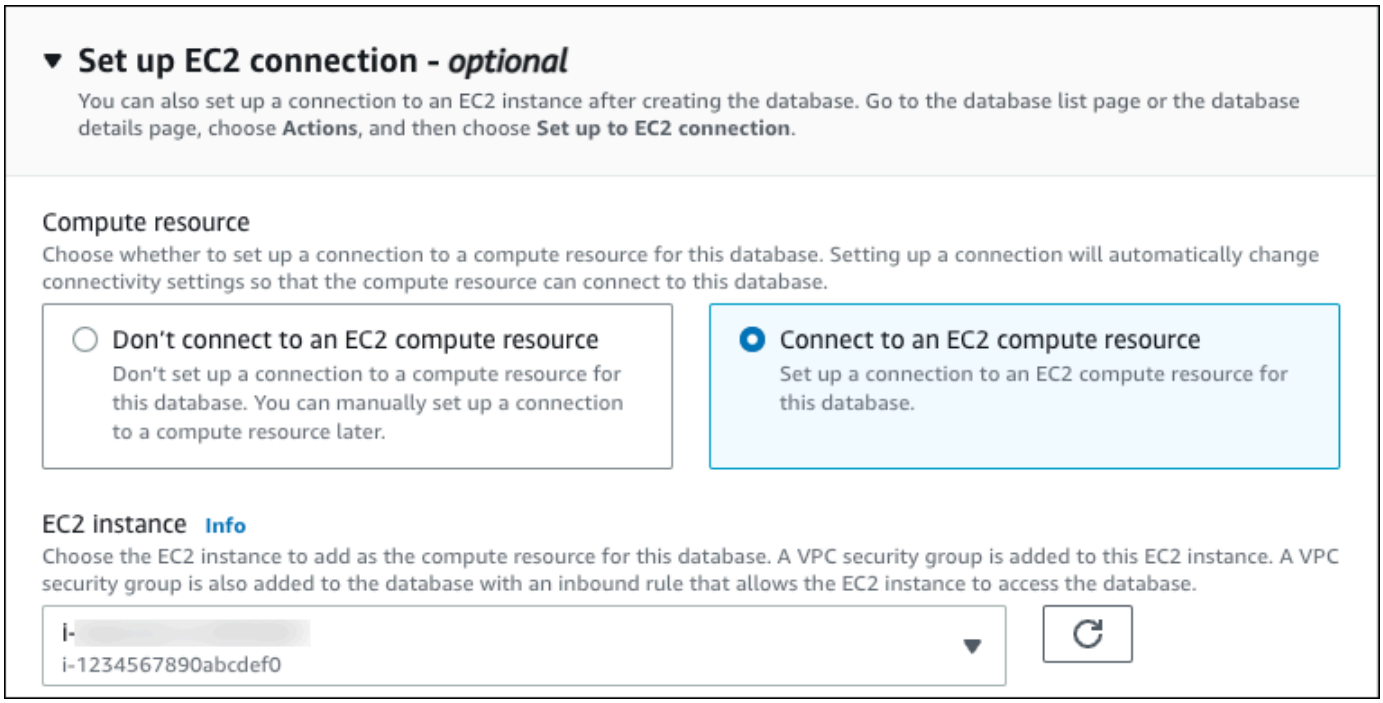
5. En Configuration (Configuración), elija Microsoft SQL Server.
6. En Edición, elija SQL Server Express Edition.
7. En DB instance size (Tamaño de la instancia de la base de datos), seleccione Free tier (Capa gratuita). El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.
8. En DB instance identifier (Identificador de instancia de base de datos), ingrese **`database-test1`**.

   La página Create database (Crear base de datos) debe ser similar a la siguiente imagen. Para las cuentas del plan gratuito, aparece Nivel gratuito. Para las cuentas de planes de pago, aparece Entorno de pruebas.



9. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro o deje el nombre predeterminado.
10. Para configurar una conexión con la instancia de EC2 que creó anteriormente, abra Configurar conexión a EC2 - (opcional).

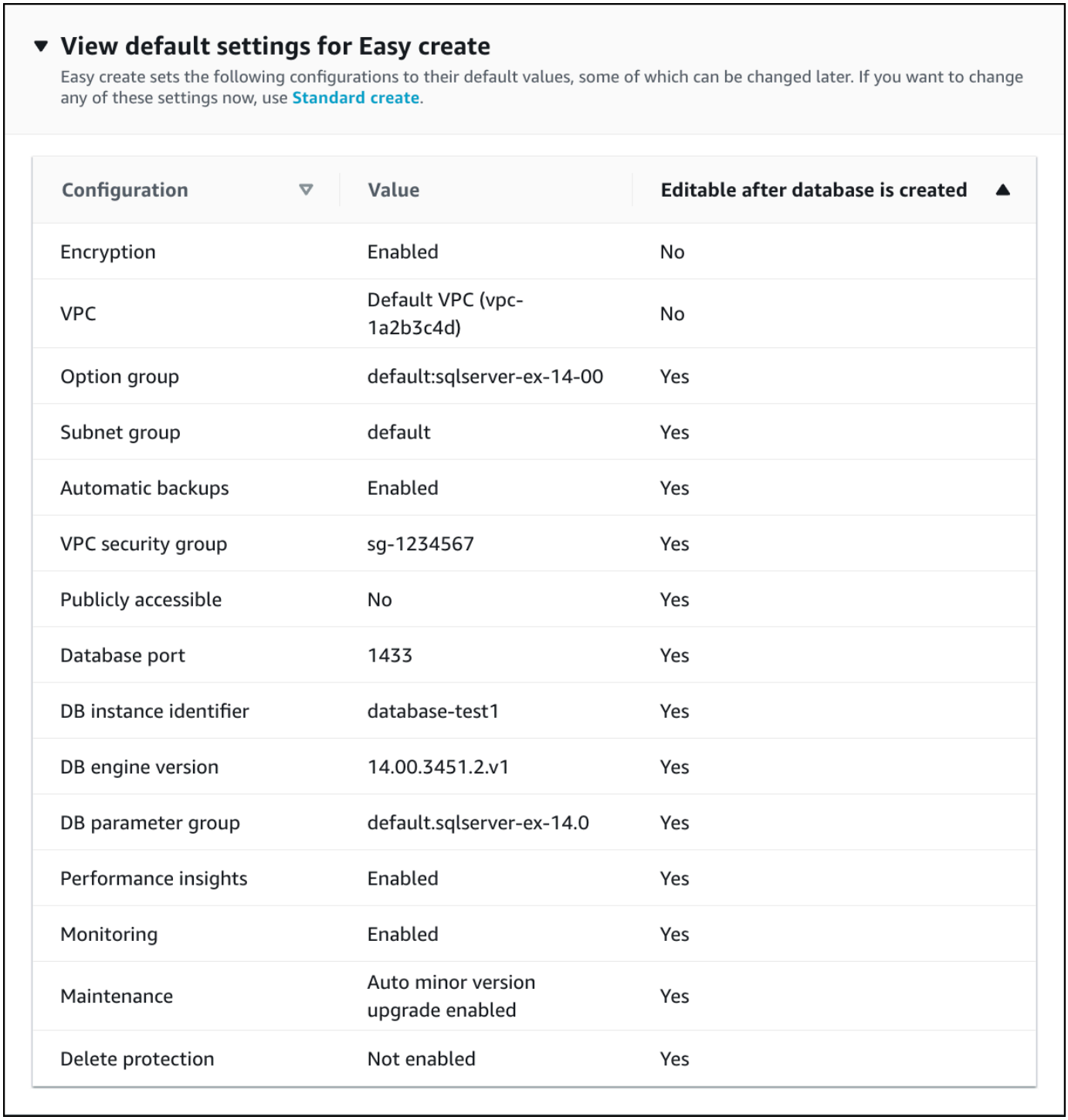
Seleccione Conectarse a un recurso informático de EC2. Elija la instancia de EC2 que ha creado anteriormente.



11. A fin de utilizar una contraseña maestra generada automáticamente para la instancia de base de datos, seleccione la casilla Auto generate a password (Generar automáticamente una contraseña).

    Para introducir la contraseña maestra, desactive la casilla Auto generate a password (Generar una contraseña automáticamente) y luego introduzca la misma contraseña en Master password (Contraseña maestra) y Confirm password (Confirmar contraseña).

12. Abra la opción Ver la configuración predeterminada de la creación sencilla.



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:sqlserver-ex-14-00	Yes
Subnet group	default	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-1234567	Yes
Publicly accessible	No	Yes
Database port	1433	Yes
DB instance identifier	database-test1	Yes
DB engine version	14.00.3451.2.v1	Yes
DB parameter group	default.sqlserver-ex-14.0	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Puede examinar la configuración predeterminada utilizada con Easy create (Creación sencilla). La columna Editable después de crear la base de datos muestra las opciones que puede cambiar después de crear la base de datos.

- Si una configuración tiene No en esa columna y desea una configuración diferente, puede usar Creación estándar para crear la instancia de base de datos.

- Si una configuración tiene Sí en esa columna y desea una configuración diferente, puede utilizar Creación estándar para crear la instancia de base de datos o modificar la instancia de base de datos después de crearla para cambiar la configuración.

13. Elija Creación de base de datos.

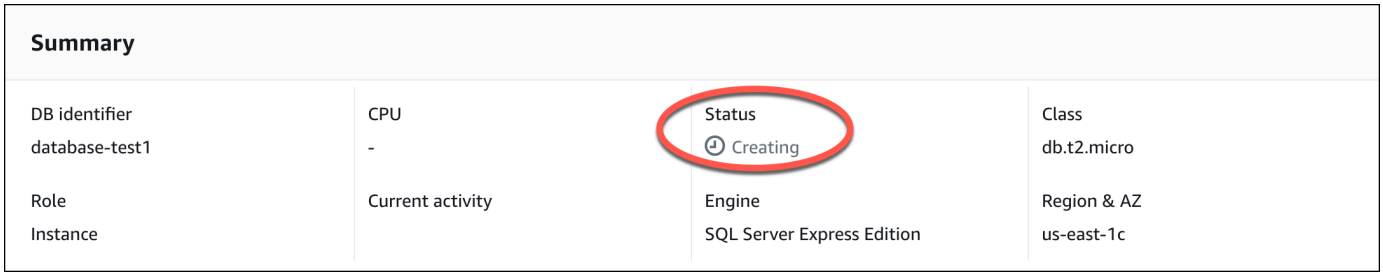
    Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales).

    Puede utilizar la contraseña y el nombre de usuario que aparecen para conectarse a la instancia de base de datos como el usuario maestro.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla.
    > Si tiene que cambiar la contraseña de usuario maestro después de que la instancia de base de datos esté disponible, puede modificar la instancia de base de datos para ello. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

14. En la lista Bases de datos, seleccione el nombre de la nueva instancia de base de datos de SQL Server para ver sus detalles.

    La instancia de base de datos tiene el estado Creando hasta que está lista para usarse.



    Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de la base de datos. Dependiendo de la clase de instancia de la base de datos y de la cantidad de almacenamiento, es posible que la nueva instancia tarde hasta 20 minutos en estar disponible.

(Opcional) Crear una VPC, una instancia EC2 y una instancia de SQL Server mediante AWS CloudFormation

En lugar de utilizar la consola para crear la VPC, la instancia de EC2 y la instancia de SQL Server, puede utilizar AWS CloudFormation para aprovisionar recursos de AWS tratando la infraestructura como código. Para ayudarle a organizar sus recursos de AWS en unidades más pequeñas y fáciles de administrar, puede utilizar la funcionalidad de pila anidada de AWS CloudFormation. Para obtener más información, consulte Creación de una pila en la consola AWS CloudFormation y Uso de pilas anidadas.

> **Important**
>
> AWS CloudFormation es gratuito, pero los recursos que CloudFormation crea están activos. Se le facturan las tarifas de uso estándar por estos recursos hasta que los finalice. Para obtener más información, consulte Precios de RDS para SQL Server.

Para crear sus recursos con la consola AWS CloudFormation, siga estos pasos:

- Descargar la plantilla de CloudFormation
- Configurar los recursos mediante CloudFormation

Descargar la plantilla de CloudFormation

Una plantilla de CloudFormation es un archivo de texto con formato JSON o YAML que contiene la información de configuración de los recursos que desea crear en la pila. Esta plantilla también crea una VPC y un host bastión para usted junto con la instancia de RDS.

Para descargar el archivo de plantilla, abra el enlace SQL Server CloudFormation template.

En la página de Github, haga clic en el botón Descargar archivo sin procesar para guardar el archivo YAML de la plantilla.

Configurar los recursos mediante CloudFormation

> **Note**
>
> Antes de iniciar este proceso, asegúrese de tener un par de claves para una instancia EC2 en su Cuenta de AWS. Para obtener más información, consulte Pares de claves de Amazon EC2 e instancias Linux.

Al utilizar la plantilla de AWS CloudFormation, debe seleccionar los parámetros correctos para asegurarse de que los recursos se crean correctamente. Siga los pasos que se indican a continuación:

1. Inicie sesión en la AWS Management Console y abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Elija Crear pila.
3. En la sección Especificar la plantilla, seleccione Cargar un archivo de plantilla desde el ordenador y Siguiente.
4. En la página Especificar detalles de la pila, introduzca los siguientes parámetros:
   a. Ponga el nombre de pila en SQLServerTestStack.
   b. En Parámetros, defina las zonas de disponibilidad seleccionando tres zonas de disponibilidad.
   c. En Configuración de host bastión de Linux, en Nombre de la clave, seleccione un par de claves para iniciar sesión en su instancia de EC2.
   d. En los ajustes de Configuración de host bastión de Linux, ponga el rango de IP permitido en su dirección IP. Para conectarse a las instancias de EC2 de su VPC mediante Secure Shell (SSH), determine su dirección IP pública mediante el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección

IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

e. En Configuración general de la base de datos, ponga la Clase de instancia de base de datos en db.t3.micro.

f. Ponga el Nombre de la base de datos en **`database-test1`**.

g. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro.

h. Ponga Administrar contraseña de usuario maestro de base de datos con Secrets Manager en `false` para este tutorial.

i. En Contraseña de base de datos, ponga la contraseña que desee. Recuerde esta contraseña para poder ver los pasos adicionales del tutorial.

j. En Configuración de almacenamiento de base de datos, ponga el Tipo de almacenamiento de base de datos en gp2.

k. En la Configuración de supervisión de base de datos, ponga Habilitar RDS Performance Insights en falso.

l. Deje el resto de la configuración con los valores predeterminados. Haga clic en Siguiente para continuar.

5. En la página Configurar opciones de pila, deje todas las opciones predeterminadas. Haga clic en Siguiente para continuar.
6. En la página Revisar la pila, seleccione Enviar después de comprobar las opciones de base de datos y de host bastión de Linux.

Una vez finalizado el proceso de creación de la pila, visualice las pilas con los nombres BastionStack y RDSNS para anotar la información que necesita para conectarse a la base de datos. Para obtener más información, consulte Viewing AWS CloudFormation stack data and resources on the AWS Management Console.

Conexión a una instancia de base de datos de SQL Server

En el siguiente procedimiento, puede conectarse a su instancia de base de datos utilizando Microsoft SQL Server Management Studio (SSMS).

Para conectarse a una instancia de base de datos de RDS para SQL Server utilizando SSMS

1. Busque el punto de enlace (nombre de DNS) y el número de puerto de la instancia de base de datos.

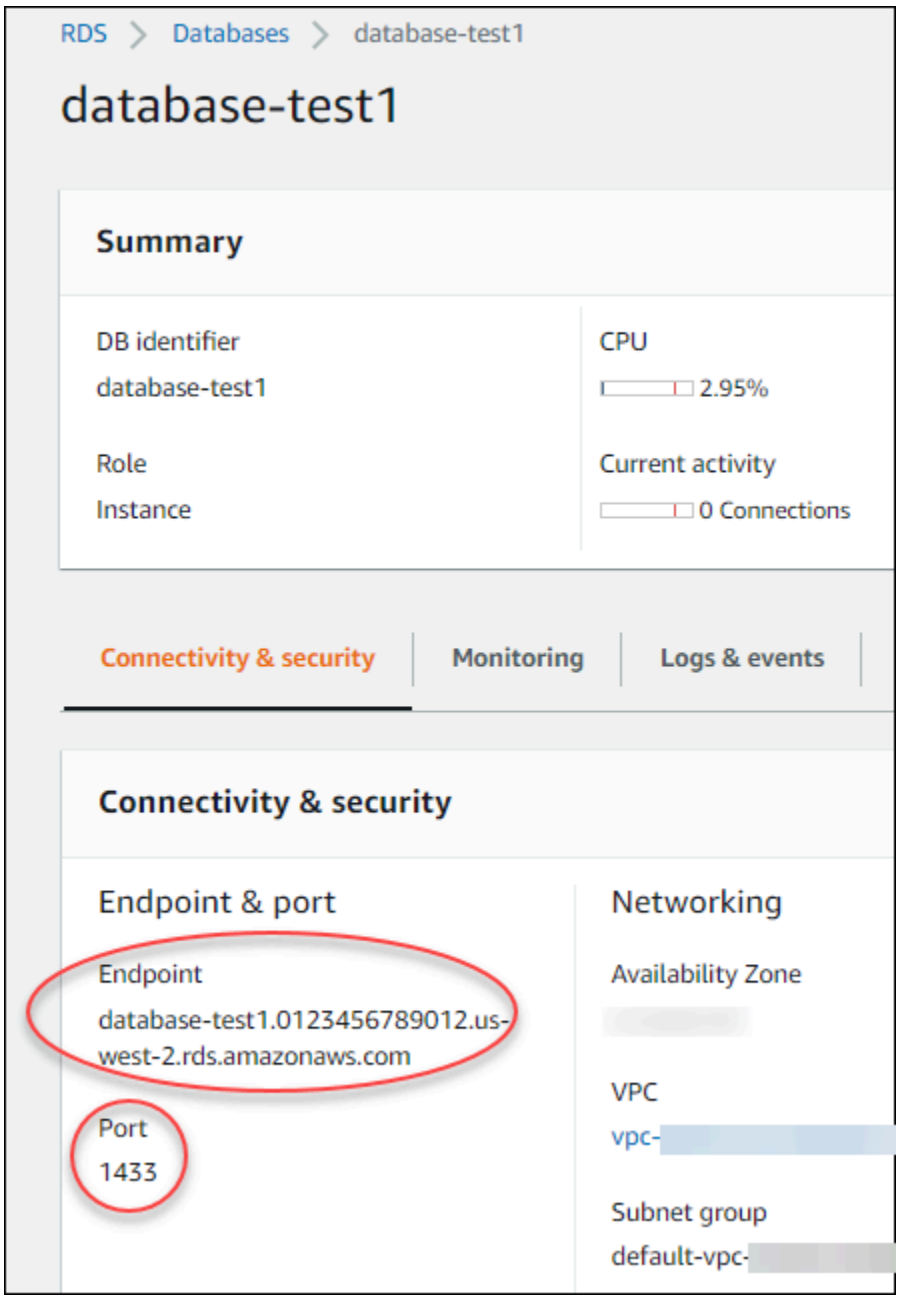
a. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

b. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS de la instancia de base de datos.

c. En el panel de navegación, elija Databases (Bases de datos).

d. Seleccione el nombre de la instancia de base de datos SQL Server para mostrar sus detalles.

e. En la pestaña Connectivity (Conectividad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



2. Conéctese a la instancia de EC2 que ha creado anteriormente siguiendo los pasos que se indican en Conexión a la instancia de Microsoft Windows en la Guía del usuario de instancias de Windows de Amazon EC2.
3. Instale el cliente de SQL Server Management Studio (SSMS) de Microsoft.

   Para descargar una versión independiente de este SSMS en su instancia de EC2, consulte Download SQL Server Management Studio (SSMS) (Descarga de SQL Server Management Studio [SSMS]) en la documentación de Microsoft.

a. Utilice el menú Inicio para abrir Internet Explorer.

b. Utilice Internet Explorer para descargar e instalar una versión independiente de SSMS. Si se le indica que el sitio no es de confianza, añádalo a la lista de sitios de confianza.

4. Inicie SQL Server Management Studio (SSMS).

   Aparecerá el cuadro de diálogo Connect to Server.

5. Proporcione la siguiente información para la instancia de base de datos de ejemplo.

   a. En Server type, elija Database Engine.

   b. En Server name (Nombre de servidor), introduzca el nombre de DNS, seguido de una coma y el número de puerto (el puerto predeterminado es 1433). Por ejemplo, el nombre del servidor debería tener el siguiente aspecto:

   ```
   database-test1.0123456789012.us-west-2.rds.amazonaws.com,1433
   ```

   c. En Authentication, elija SQL Server Authentication.

   d. En Inicio de sesión, escriba el nombre de usuario que eligió para la instancia de base de datos de ejemplo. Esto también se conoce como nombre de usuario maestro.

   e. En Password (Contraseña), escriba la contraseña que eligió anteriormente para la instancia de base de datos de ejemplo. Esto también se conoce como contraseña de usuario maestra.

6. Elija Connect.

   Luego de unos instantes, SSMS se conecta a su instancia de base de datos. Por motivos de seguridad, se recomienda utilizar conexiones cifradas. Utilice solo una conexión de SQL Server sin cifrar cuando el cliente y el servidor estén en la misma VPC y la red sea de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte ???.

Para obtener más información sobre la conexión a la instancia de base de datos de Microsoft SQL Server, consulte Conexión a la instancia de base de datos de Microsoft SQL Server.

Para obtener más información acerca de los problemas de conexión, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Exploración de una instancia de base de datos de SQL Server de ejemplo

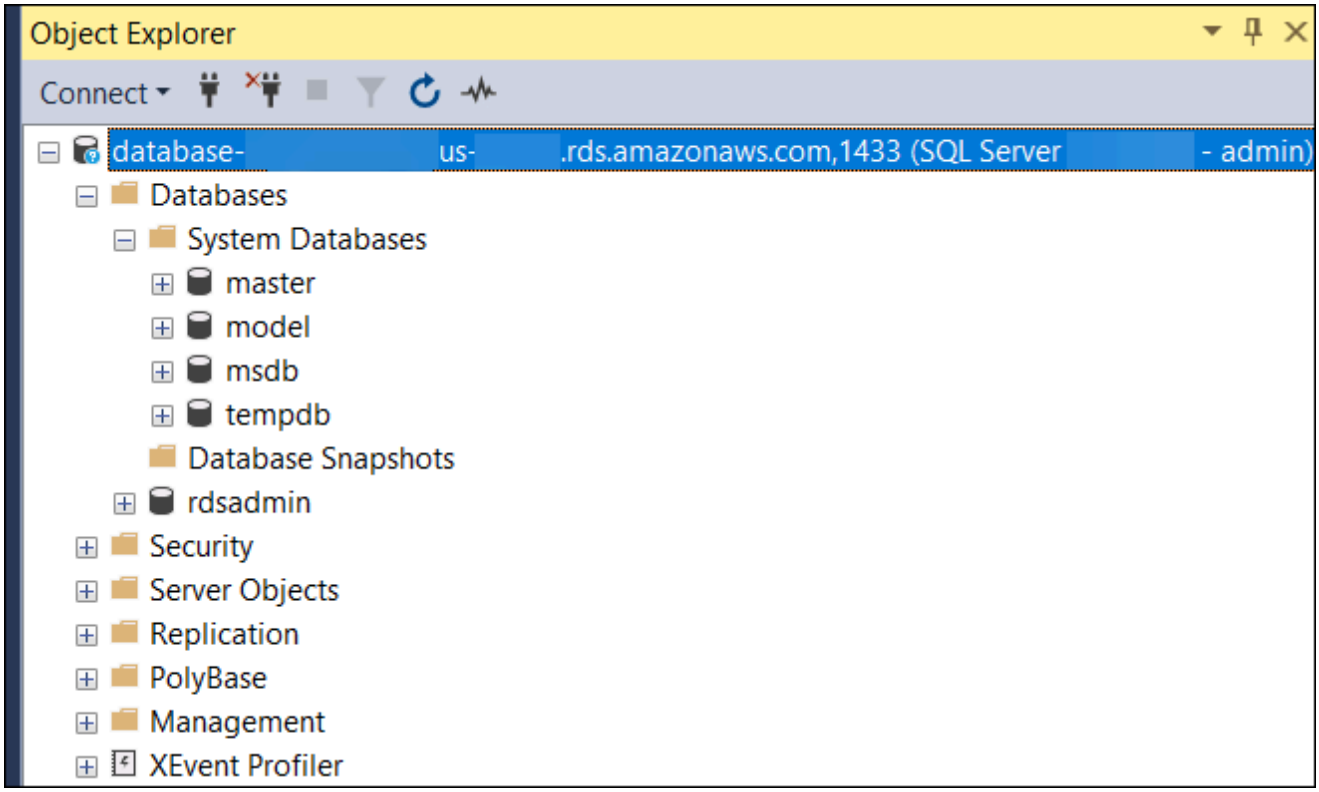
Puede explorar su instancia de base de datos de ejemplo utilizando Microsoft SQL Server Management Studio (SSMS).

Para examinar una instancia de base de datos utilizando SSMS

1. Su instancia de base de datos de SQL Server incluye bases de datos de sistema estándar integradas de SQL Server (master, model, msdb y tempdb). Para explorar las bases de datos de sistema, haga lo siguiente:

   a. En SSMS, en el menú Ver elija Explorador de objetos.

   b. Expanda la instancia de base de datos, expanda Databases (Bases de datos) y, a continuación, expanda System Databases (Bases de datos del sistema) como se muestra.



   Su instancia de base de datos de SQL Server también viene con una base de datos llamada `rdsadmin`. Amazon RDS utiliza esta base de datos para almacenar los objetos que utiliza para administrar su base de datos. La base de datos `rdsadmin` también incluye procedimientos almacenados que puede ejecutar para realizar tareas avanzadas.

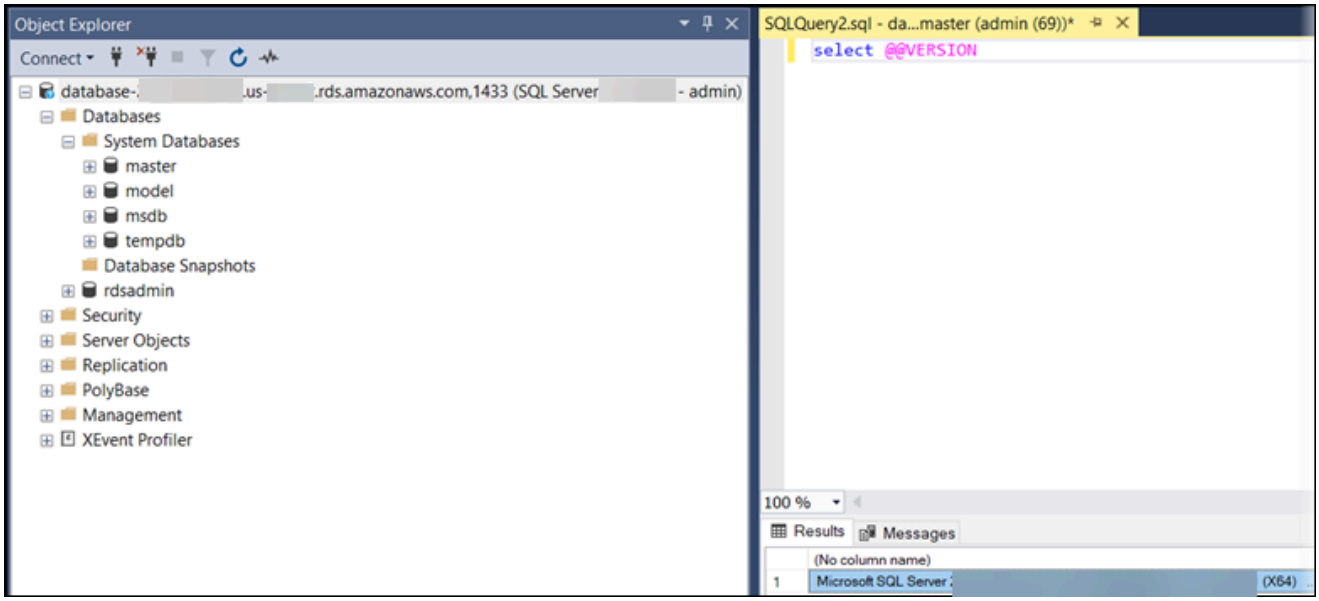
2. Comience a crear sus propias bases de datos y realizar consultas en la instancia de base de datos y bases de datos como siempre. Para ejecutar una consulta de prueba en la instancia de base de datos de ejemplo, haga lo siguiente:

   a. En SSMS, en el menú Archivo, vaya a Nuevo y, a continuación, elija Consulta con conexión actual.

   b. Escriba la siguiente consulta SQL:

   ```
   select @@VERSION
   ```

   c. Ejecute la consulta. SSMS devuelve la versión de SQL Server de su instancia de base de datos de Amazon RDS.



Eliminación de la instancia de EC2 y la instancia de base de datos

Después de conectarse y explorar la instancia de EC2 de muestra y la instancia de base de datos que creó, elimínelas para que no le sigan cobrando por ellas.

Si ha utilizado AWS CloudFormation para crear recursos, omita este paso y vaya al siguiente.

Para eliminar la instancia de EC2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).

3. Seleccione la instancia de EC2 y elija Estado de la instancia y Terminar instancia.
4. Cuando se le indique que confirme, elija Terminar.

Para obtener más información sobre la eliminación de una instancia de EC2, consulte Terminar una instancia en la Guía del usuario de instancias de Windows de Amazon EC2.

Para eliminar una instancia de base de datos sin instantánea de base de datos final

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. Desactive Crear la instantánea final y Conservar copias de seguridad automatizadas.
6. Complete la confirmación y seleccione Eliminar.

(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation

Si ha utilizado AWS CloudFormation para crear recursos, elimine la pila de CloudFormation después de conectarse a la instancia de EC2 y a la instancia de base de datos de muestra y de explorarlas; de este modo, ya no se le cobrará por ellas.

Para eliminar los recursos de CloudFormation

1. Abra la consola de AWS CloudFormation.
2. En la página Pilas de la consola de CloudFormation, seleccione la pila raíz (la pila sin el nombre VPCStack, BastionStack o RDSNS).
3. Elija Eliminar.
4. Cuando se le pida confirmación, seleccione Eliminar pila.

Para obtener información sobre cómo eliminar una pila en CloudFormation, consulte Eliminación de una pila en la consola de AWS CloudFormation, en la Guía del usuario de AWS CloudFormation.

(Opcional) Conecte la instancia de base de datos a una función de Lambda

También puede conectar la instancia de base de datos de RDS para SQL Server a un recurso de computación sin servidor de Lambda. Las funciones de Lambda permiten ejecutar código sin aprovisionar ni administrar la infraestructura. Una función de Lambda también permite responder automáticamente a las solicitudes de ejecución de código a cualquier escala, desde una docena de eventos al día hasta cientos de eventos por segundo. Para obtener más información, consulte Conexión automática de una función de Lambda y una instancia de base de datos.

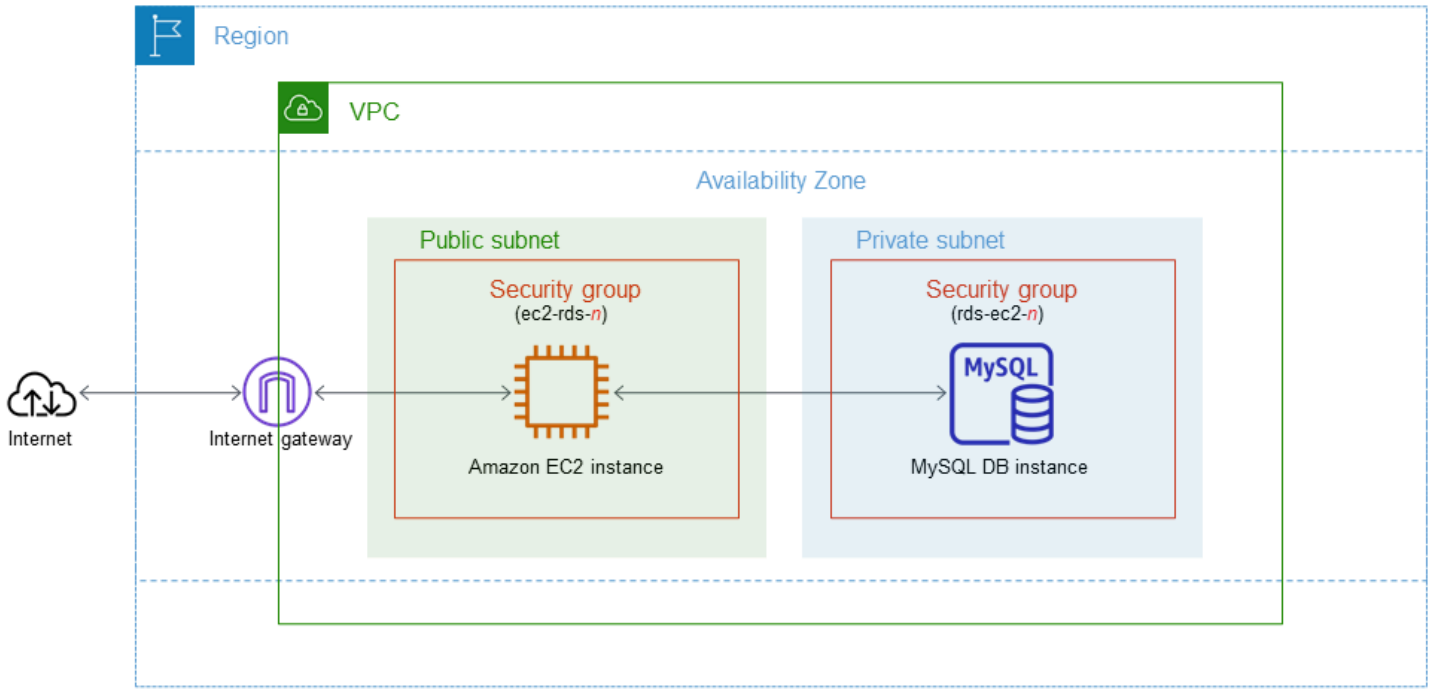
Creación de una instancia de base de datos MySQL y conexión a ella

En este tutorial, se crea una instancia de EC2 y una instancia de base de datos de RDS para MySQL. El tutorial muestra cómo acceder a la instancia de base de datos desde la instancia de EC2 mediante un cliente de MySQL estándar. Como práctica recomendada, este tutorial crea una instancia de base de datos privada en una nube privada virtual (VPC). En la mayoría de los casos, otros recursos de la misma VPC, como las instancias de EC2, pueden acceder a la instancia de base de datos, pero los recursos ajenos a la VPC no pueden acceder a ella.

Tras completar el tutorial, habrá una subred pública y una privada en cada zona de disponibilidad de la VPC. En una zona de disponibilidad, la instancia de EC2 está en la subred pública y la instancia de base de datos está en la subred privada.

> **Important**
>
> La creación de una cuenta de AWS no supone ningún costo. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de AWS que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

El siguiente diagrama muestra la configuración cuando el tutorial se completa.



Este tutorial le permite crear sus recursos mediante uno de los métodos siguientes:

1. Use la AWS Management Console: Creación de una instancia de base de datos de MySQL y Crear una instancia de EC2
2. Use AWS CloudFormation para crear la instancia de base de datos y la instancia de EC2: (Opcional) Crear una VPC, una instancia EC2 y una instancia MySQL mediante AWS CloudFormation

El primer método usa Creación sencilla para crear una instancia de base de datos MySQL privada con la AWS Management Console. Con Creación sencilla, únicamente debe especificar el tipo de motor de base de datos, el tamaño de la instancia de base de datos y el identificador de instancias de base de datos. Easy create (Creación sencilla) utiliza los ajustes predeterminados para otras opciones de configuración.

Cuando usa Creación estándar, se especifican más opciones de configuración al crear una instancia de base de datos. Estas opciones incluyen la configuración de la disponibilidad, la seguridad, las copias de seguridad y el mantenimiento. Para crear una instancia de base de datos pública, debe utilizar Creación estándar. Para obtener más información, consulta Creación de una instancia de base de datos de Amazon RDS.

Temas

- Requisitos previos
- Crear una instancia de EC2
- Creación de una instancia de base de datos de MySQL
- (Opcional) Crear una VPC, una instancia EC2 y una instancia MySQL mediante AWS CloudFormation
- Conectarse a una instancia de base de datos MySQL
- Eliminación de la instancia de EC2 y la instancia de base de datos
- (Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation
- (Opcional) Conecte la instancia de base de datos a una función de Lambda

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

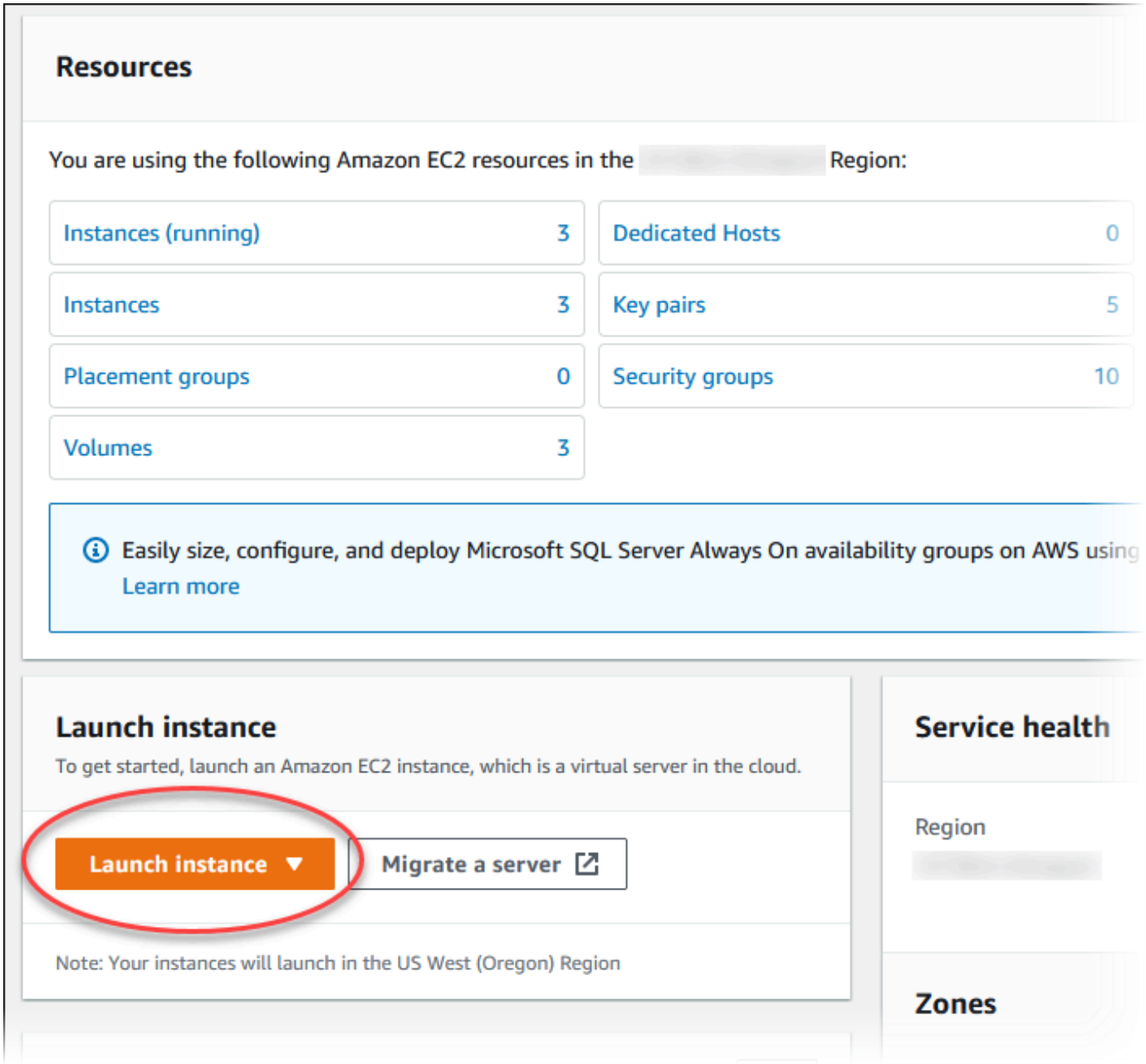
- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Crear una instancia de EC2

Cree una instancia de Amazon EC2 que utilicará para conectarse a la base de datos.

Para crear una instancia EC2;

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS en la que desea crear la instancia de EC2.
3. Elija Panel de EC2 y, a continuación, Lanzar instancia, como se muestra en la siguiente imagen.

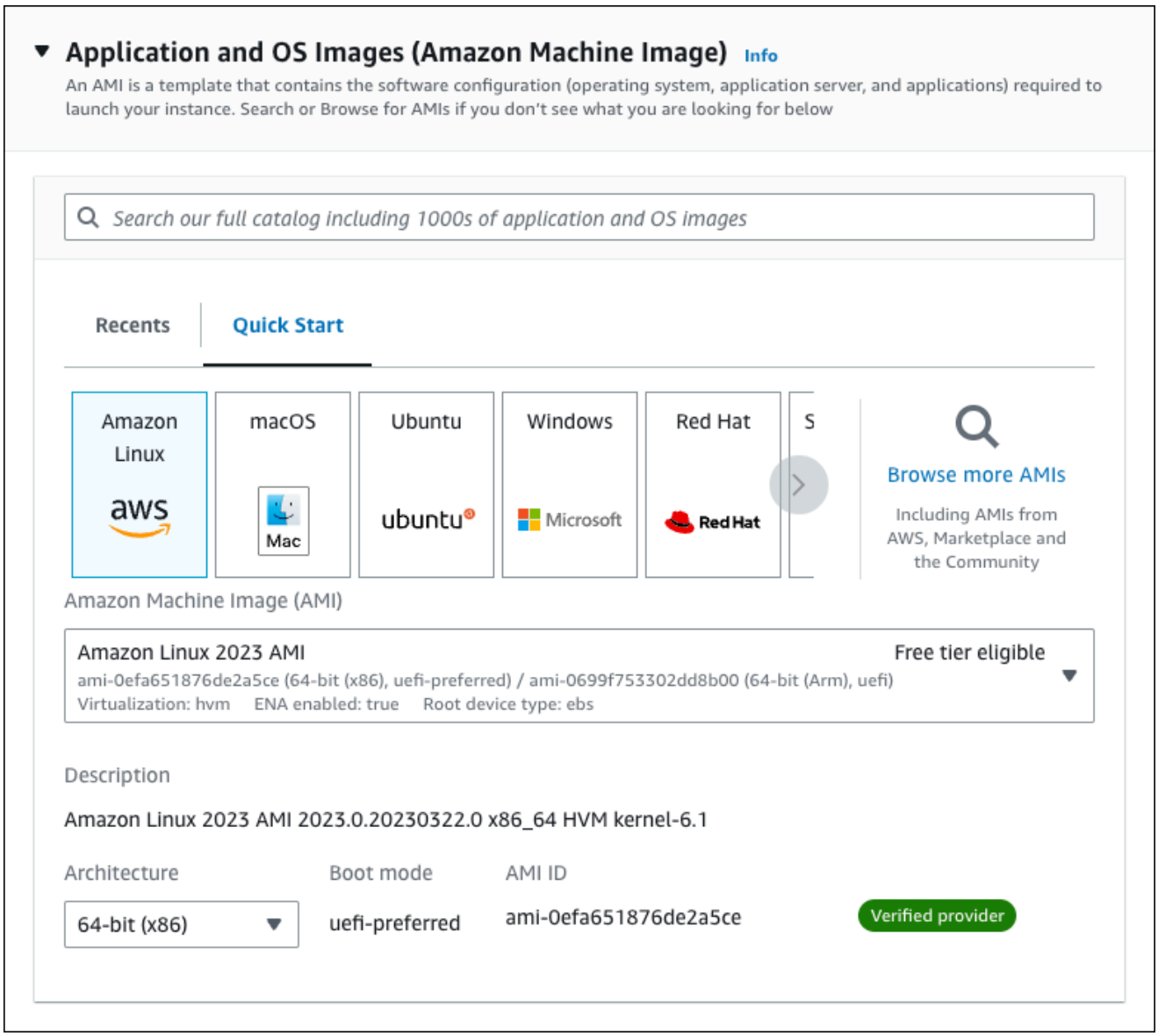


Se abre la página Lanzar una instancia.

4. Elija los siguientes ajustes en la página Lanzar una instancia.

   a. En Name and tags (Nombre y etiquetas), en Name (Nombre), introduzca **`ec2-database-connect`**.

   b. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija Amazon Linux y, a continuación, AMI de Amazon Linux 2023. Mantenga los valores predeterminados para las demás opciones.



c. En Instance type (Tipo de instancia), elija t2.micro.

d. En Key pair (login) [Par de claves (inicio)], elija Key pair name (Nombre de par de claves) para utilizar un par de claves existente. Para crear un nuevo par de claves para la instancia de Amazon EC2, que se muestra a continuación, elija Create new key pair (Crear nuevo par de claves) y, a continuación, utilice la ventana Create key pair (Crear un par de claves).

   Para obtener más información sobre la creación de un nuevo par de claves, consulte Crear un par de claves en la Guía del usuario de Amazon EC2.

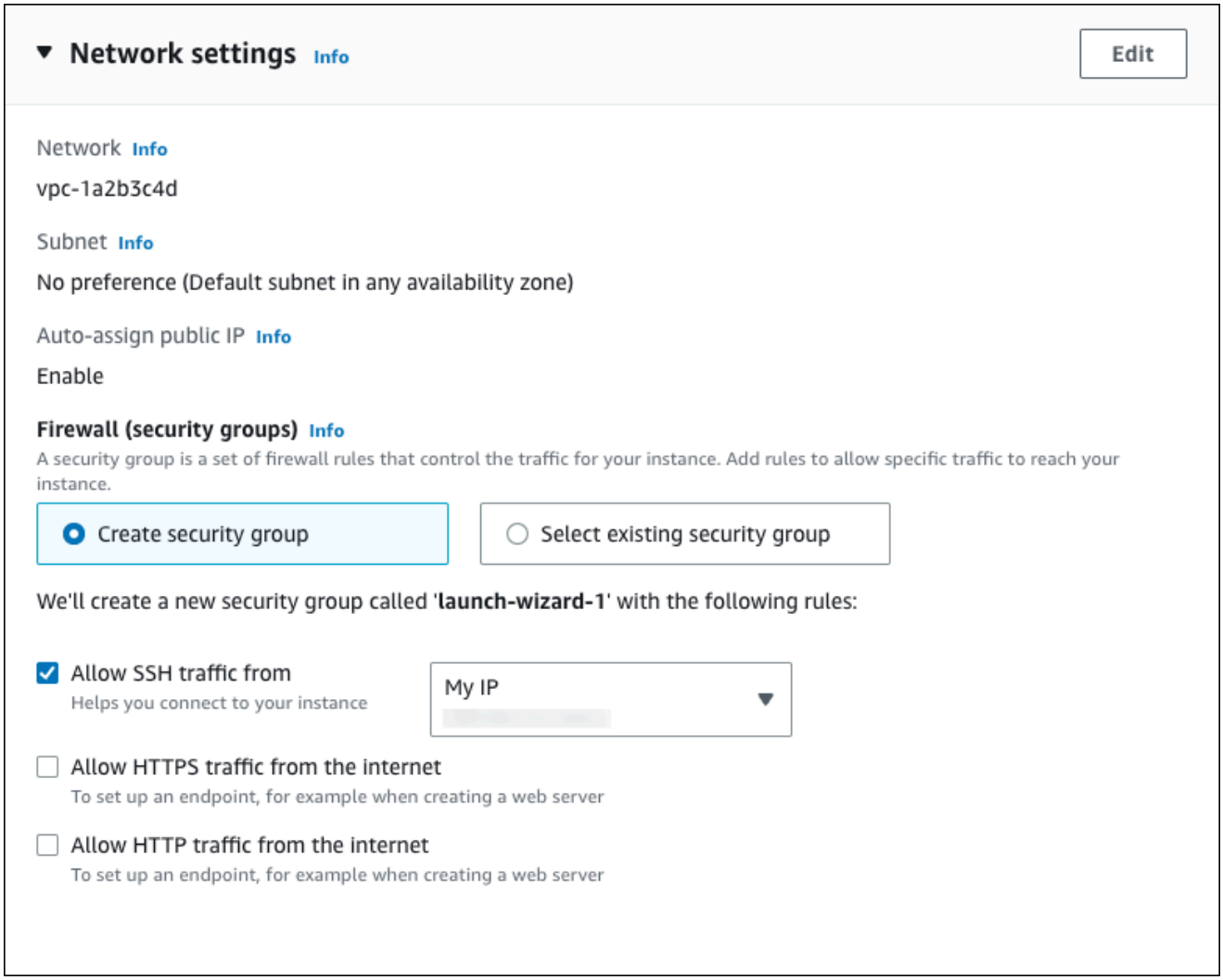
e. En Permitir tráfico de SSH en Configuraciones de red, elija el origen de las conexiones SSH a la instancia de EC2.

Puede elegir My IP (Mi IP) si la dirección IP que se muestra es correcta para las conexiones SSH. De lo contrario, puede determinar la dirección IP que usará para conectarse a las instancias de EC2 en su VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, asegúrese de identificar el rango de direcciones IP que utilizan los equipos cliente.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

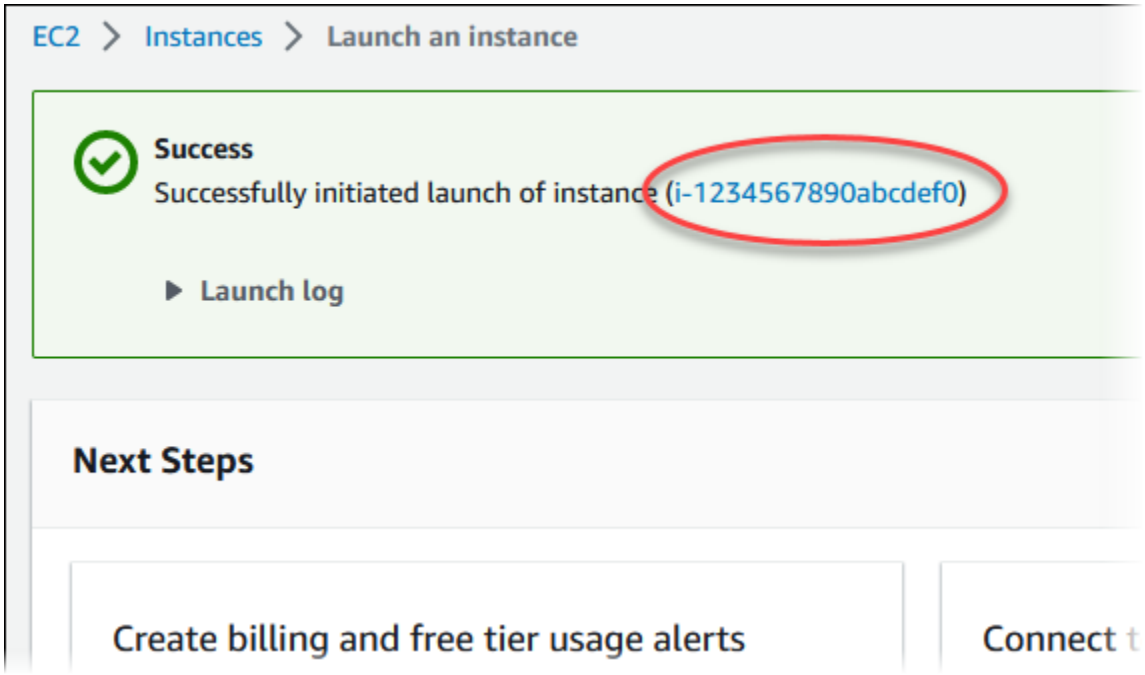
La siguiente imagen muestra un ejemplo de la sección Configuraciones de red.



f. No cambie los valores predeterminados del resto de las secciones.

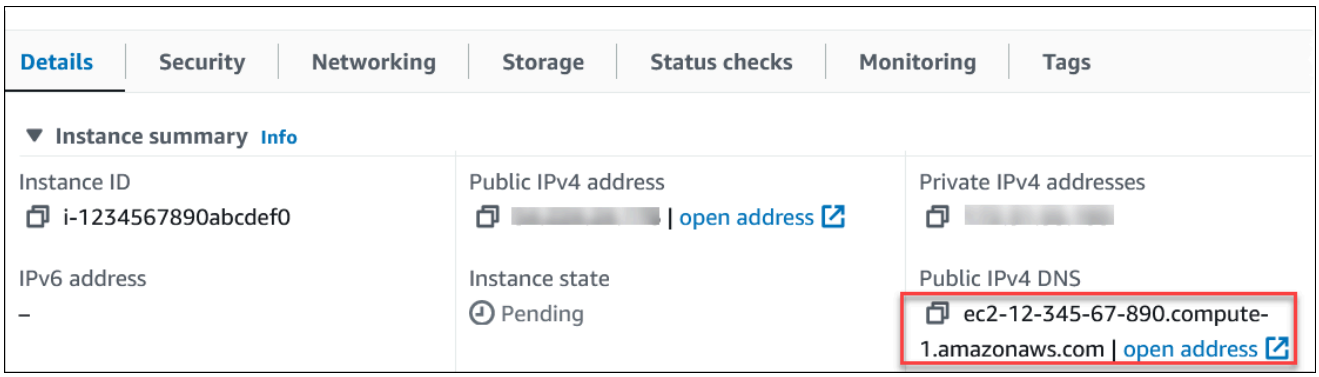
g. Revise un resumen de la configuración de su instancia de EC2 en el panel Resumen; cuando haya terminado, elija Lanzar instancia.

5. En la página Launch Status, que se muestra a continuación, anote el identificador de la nueva instancia de EC2, por ejemplo, `i-1234567890abcdef0`.

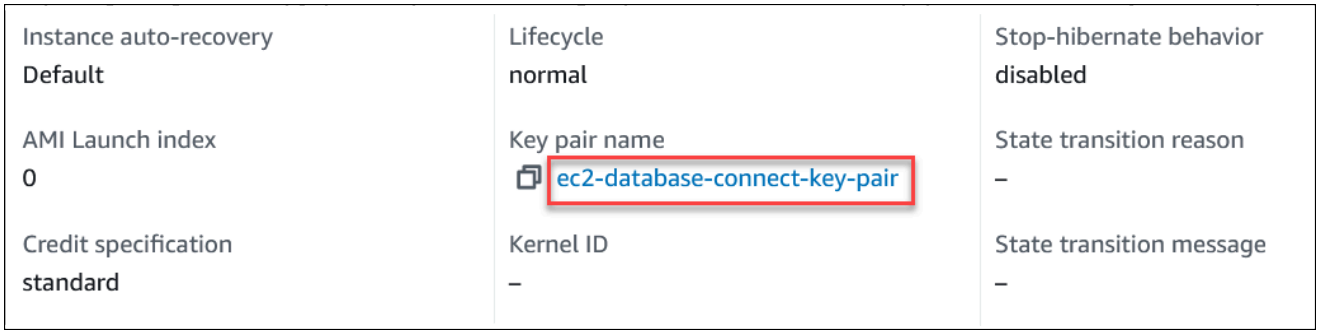


6. Elija el identificador de instancia de EC2 para abrir la lista de instancias de EC2 y, a continuación, seleccione su instancia de EC2.
7. En la pestaña Detalles, anote los siguientes valores, ya que los necesitará cuando se conecte mediante SSH:

   a. En Resumen de la instancia, anote el valor del DNS IPv4 público.



   b. En Detalles de la instancia, anote el valor de Nombre del par de claves.



8. Espere hasta que el Estado de la instancia de su instancia de EC2 tenga el estado En ejecución antes de continuar.

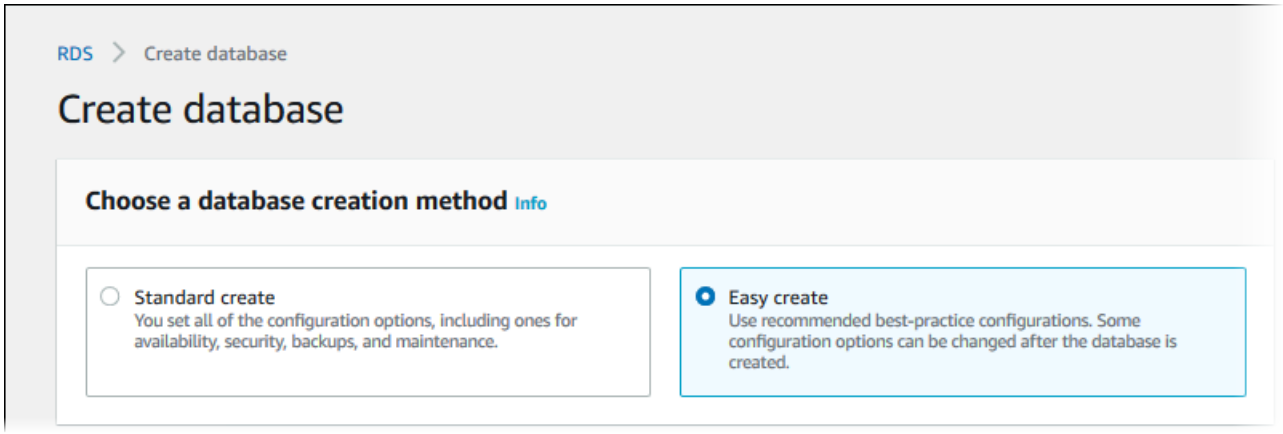
Creación de una instancia de base de datos de MySQL

El componente básico de Amazon RDS es la instancia de base de datos. Este es el entorno en el que ejecuta las bases de datos MySQL.

En este ejemplo, utilice la opción Creación sencilla para crear una instancia de base de datos que ejecuta el motor de la base de datos de MySQL con una clase de instancia de base de datos db.t3.micro.

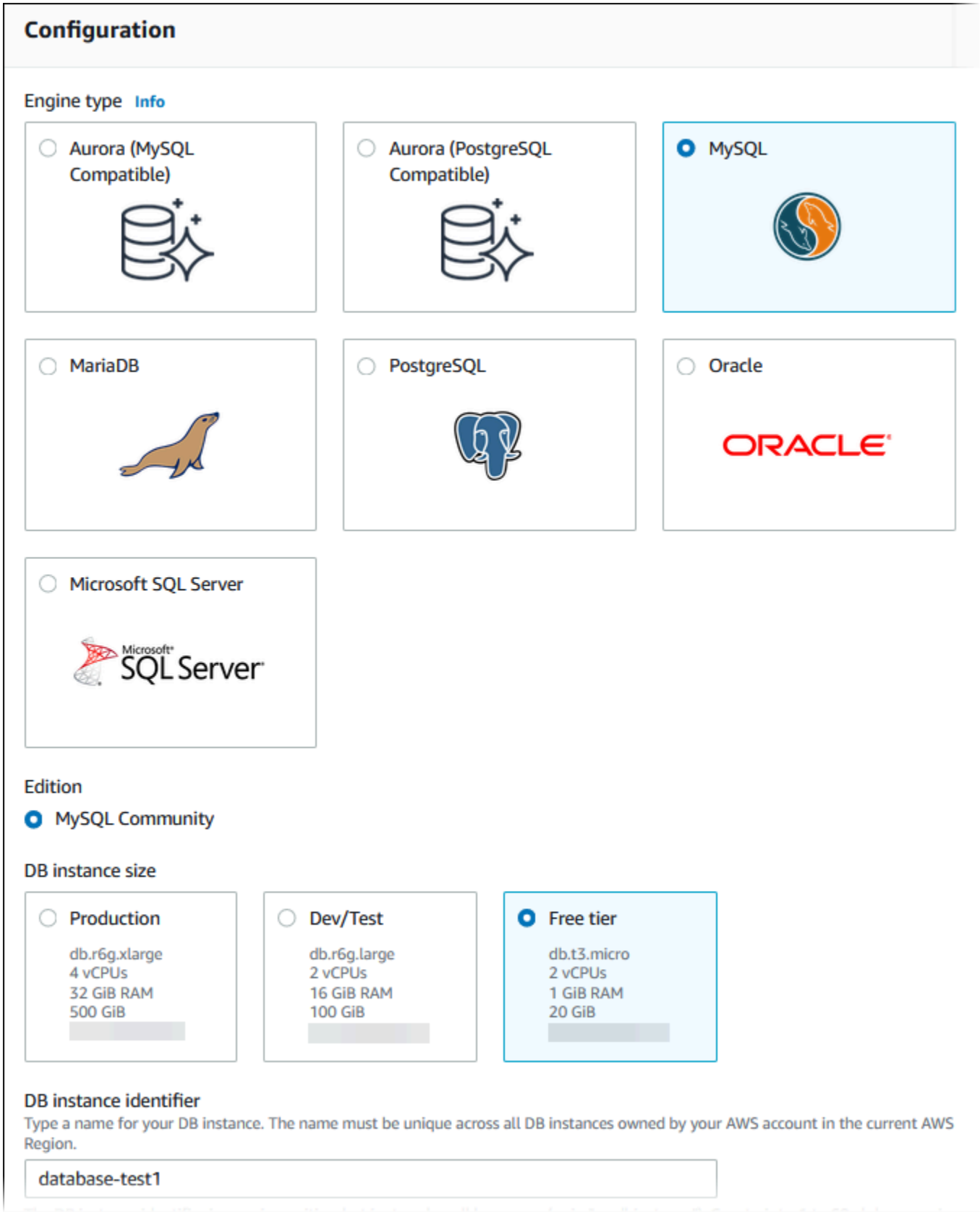
Para crear una instancia de base de datos de MySQL con la opción Easy Create (Creación sencilla)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS que utilizó anteriormente para la instancia de EC2.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Seleccione Create database (Crear base de datos) y asegúrese de que la opción Easy Create (Creación sencilla) esté seleccionada.



5. En Configuration (Configuración), seleccione MySQL.
6. En DB instance size (Tamaño de la instancia de base de datos), seleccione Free tier (Capa gratuita). El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.
7. En DB instance identifier (Identificador de instancia de base de datos), ingrese **`database-test1`**.
8. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro o deje el nombre predeterminado.

   La página Create database (Crear base de datos) debe ser similar a la siguiente imagen. Para las cuentas del plan gratuito, aparece Nivel gratuito. Para las cuentas de planes de pago, aparece Entorno de pruebas.

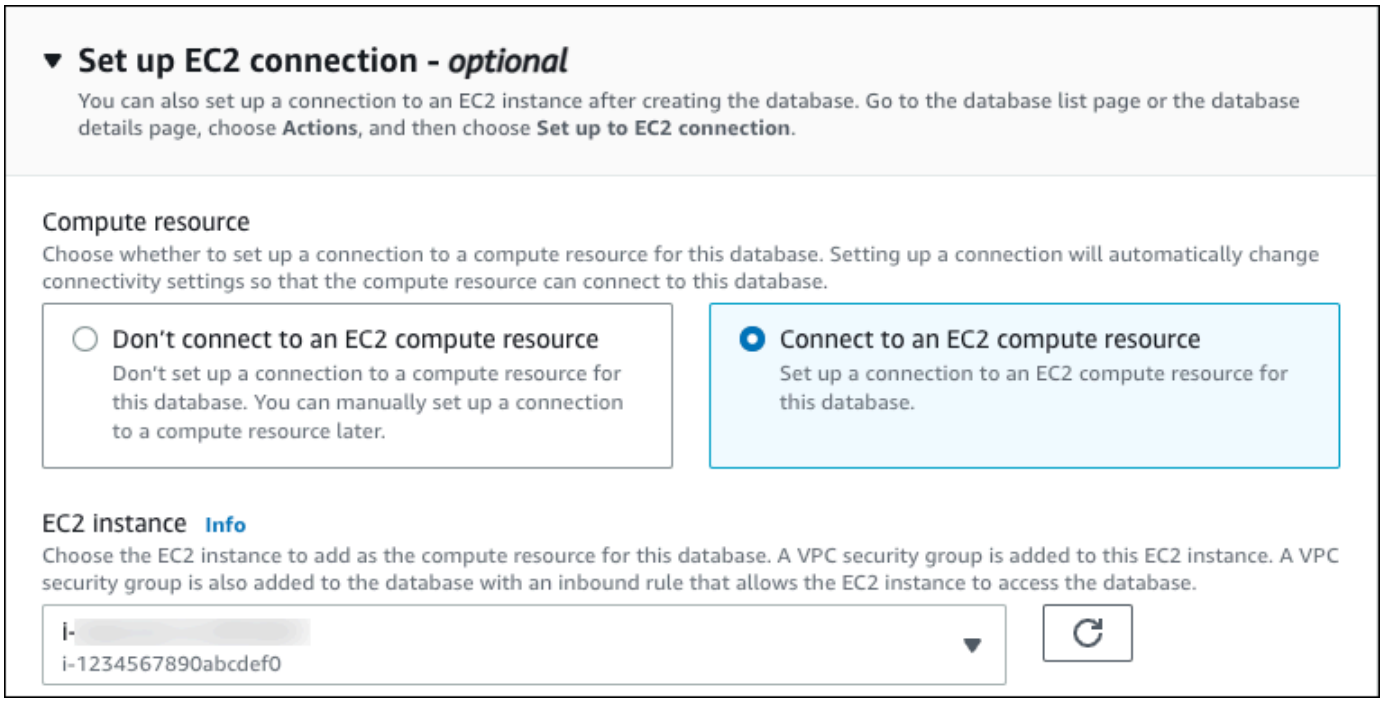

Configuration
Engine type Info
Aurora (MySQL Compatible)
Aurora (PostgreSQL Compatible)
MySQL
MariaDB
PostgreSQL
Oracle
ORACLE
Microsoft SQL Server
Microsoft SQL Server
Edition
MySQL Community
DB instance size
Production
db.r6g.xlarge
4 vCPUs
32 GiB RAM
500 GiB
Dev/Test
db.r6g.large
2 vCPUs
16 GiB RAM
100 GiB
Free tier
db.t3.micro
2 vCPUs
1 GiB RAM
20 GiB
DB instance identifier
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.
database-test1

9. Para utilizar una contraseña maestra generada automáticamente para la instancia de base de datos, seleccione Generación automática de contraseña.

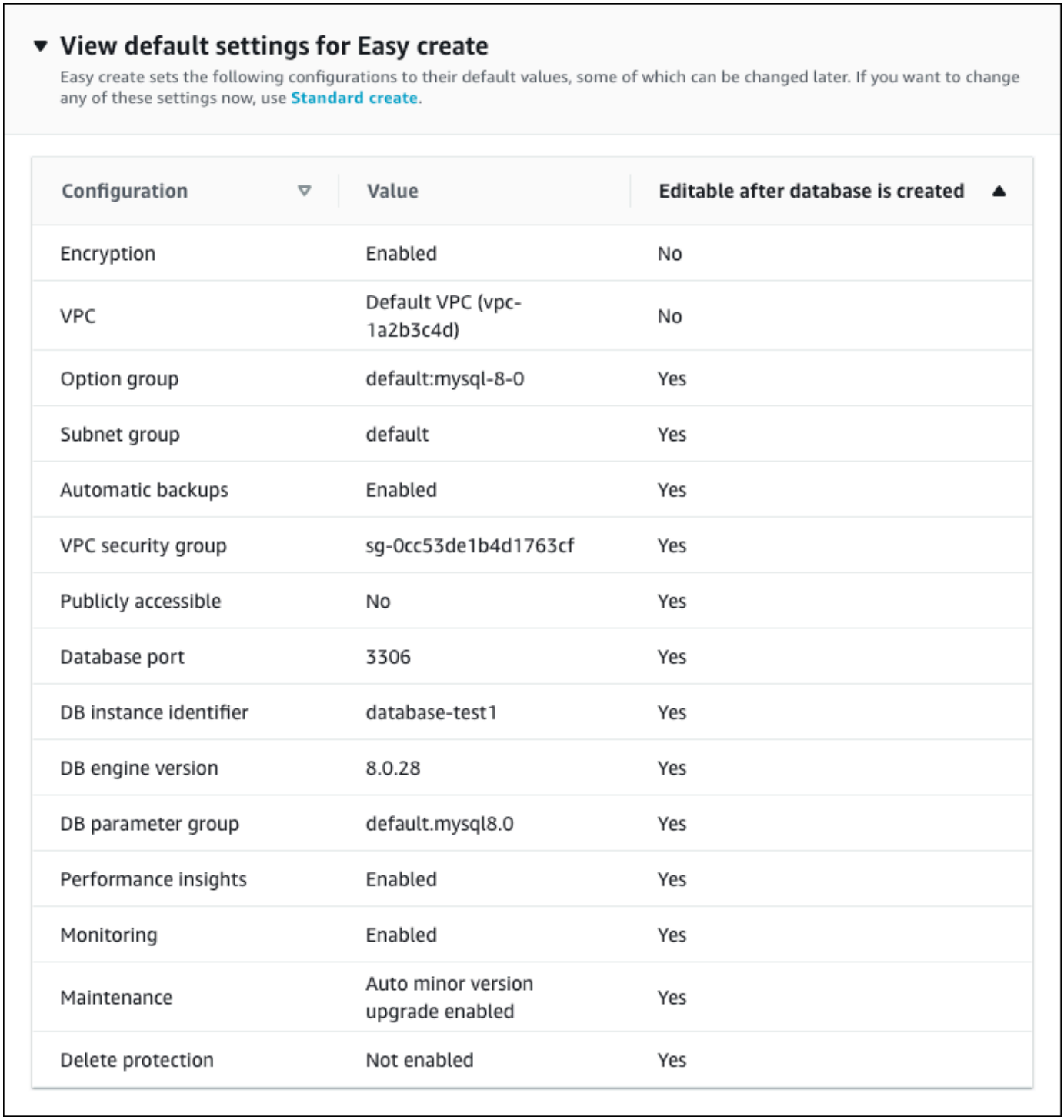
   Para introducir la contraseña maestra, asegúrese de desactivar la casilla Generación automática de contraseña y luego introduzca la misma contraseña en Contraseña maestra y Confirmar contraseña.

10. Para configurar una conexión con la instancia de EC2 que creó anteriormente, abra Configurar conexión a EC2 - (opcional).

    Seleccione Conectarse a un recurso informático de EC2. Elija la instancia de EC2 que ha creado anteriormente.



11. (Opcional) Abra la opción View default settings for Easy create (Ver configuración predeterminada para Creación sencilla).



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:mysql-8-0	Yes
Subnet group	default	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-0cc53de1b4d1763cf	Yes
Publicly accessible	No	Yes
Database port	3306	Yes
DB instance identifier	database-test1	Yes
DB engine version	8.0.28	Yes
DB parameter group	default.mysql8.0	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Puede examinar la configuración predeterminada utilizada con Easy create (Creación sencilla). La columna Editable después de crear la base de datos muestra las opciones que puede cambiar después de crear la base de datos.

- Si una configuración tiene No en esa columna y desea una configuración diferente, puede usar Creación estándar para crear la instancia de base de datos.
- Si una configuración tiene Sí en esa columna y desea una configuración diferente, puede utilizar Creación estándar para crear la instancia de base de datos o modificar la instancia de base de datos después de crearla para cambiar la configuración.

12. Elija Creación de base de datos.

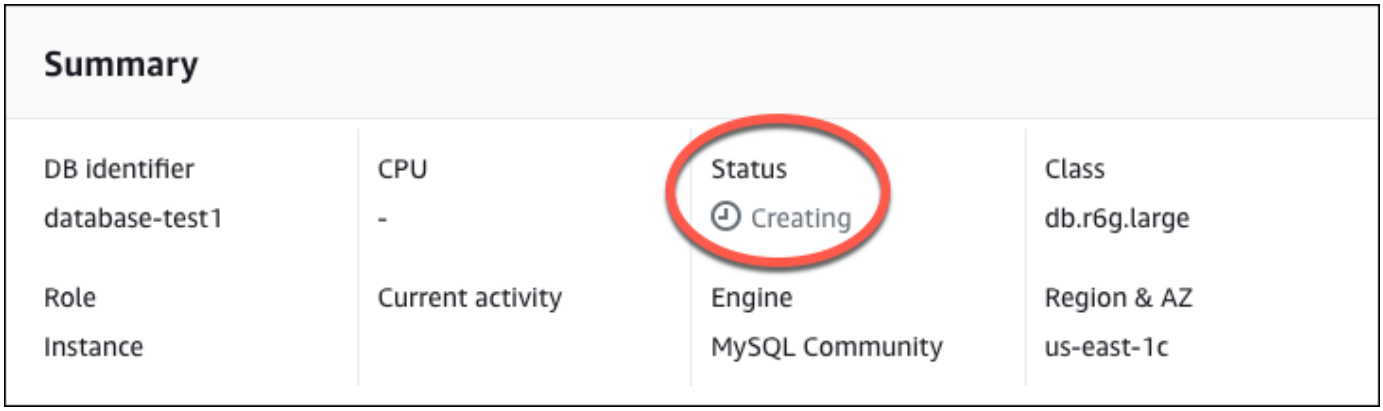
    Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales).

    Puede utilizar la contraseña y el nombre de usuario que aparecen para conectarse a la instancia de base de datos como el usuario maestro.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla.
    > Si tiene que cambiar la contraseña de usuario maestro después de que la instancia de base de datos esté disponible, puede modificar la instancia de base de datos para ello. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

13. En la lista Bases de datos, seleccione el nombre de la nueva instancia de base de datos de MySQL para ver sus detalles.

    La instancia de base de datos tiene el estado Creando hasta que está lista para usarse.



Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de la base de datos. Dependiendo de la clase de instancia de la base de datos y de la cantidad de almacenamiento, es posible que la nueva instancia tarde hasta 20 minutos en estar disponible.

(Opcional) Crear una VPC, una instancia EC2 y una instancia MySQL mediante AWS CloudFormation

En lugar de utilizar la consola para crear la VPC, la instancia de EC2 y la instancia de MySQL, puede utilizar AWS CloudFormation para aprovisionar recursos de AWS tratando la infraestructura como código. Para ayudarle a organizar sus recursos de AWS en unidades más pequeñas y fáciles de administrar, puede utilizar la funcionalidad de pila anidada de AWS CloudFormation. Para obtener más información, consulte Creación de una pila en la consola AWS CloudFormation y Uso de pilas anidadas.

> **Important**
>
> AWS CloudFormation es gratuito, pero los recursos que CloudFormation crea están activos. Se le facturan las tarifas de uso estándar por estos recursos hasta que los finalice. Para obtener más información, consulte Precios de RDS para MySQL.

Para crear sus recursos con la consola AWS CloudFormation, siga estos pasos:

- Descargar la plantilla de CloudFormation
- Configurar los recursos mediante CloudFormation

Descargar la plantilla de CloudFormation

Una plantilla de CloudFormation es un archivo de texto con formato JSON o YAML que contiene la información de configuración de los recursos que desea crear en la pila. Esta plantilla también crea una VPC y un host bastión para usted junto con la instancia de RDS.

Para descargar el archivo de plantilla, abra el enlace MySQL CloudFormation template.

En la página de Github, haga clic en el botón Descargar archivo sin procesar para guardar el archivo YAML de la plantilla.

Configurar los recursos mediante CloudFormation

> **Note**
>
> Antes de iniciar este proceso, asegúrese de tener un par de claves para una instancia EC2 en su Cuenta de AWS. Para obtener más información, consulte Pares de claves de Amazon EC2 e instancias Linux.

Al utilizar la plantilla de AWS CloudFormation, debe seleccionar los parámetros correctos para asegurarse de que los recursos se crean correctamente. Siga los pasos que se indican a continuación:

1. Inicie sesión en la AWS Management Console y abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Elija Crear pila.
3. En la sección Especificar la plantilla, seleccione Cargar un archivo de plantilla desde el ordenador y Siguiente.
4. En la página Especificar detalles de la pila, introduzca los siguientes parámetros:
   a. Ponga el nombre de pila en MySQLTestStack.
   b. En Parámetros, defina las zonas de disponibilidad seleccionando tres zonas de disponibilidad.
   c. En Configuración de host bastión de Linux, en Nombre de la clave, seleccione un par de claves para iniciar sesión en su instancia de EC2.
   d. En los ajustes de Configuración de host bastión de Linux, ponga el rango de IP permitido en su dirección IP. Para conectarse a las instancias de EC2 de su VPC mediante Secure Shell (SSH), determine su dirección IP pública mediante el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección

IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

e. En Configuración general de la base de datos, ponga la Clase de instancia de base de datos en db.t3.micro.

f. Ponga el Nombre de la base de datos en **`database-test1`**.

g. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro.

h. Ponga Administrar contraseña de usuario maestro de base de datos con Secrets Manager en `false` para este tutorial.

i. En Contraseña de base de datos, ponga la contraseña que desee. Recuerde esta contraseña para poder ver los pasos adicionales del tutorial.

j. En Configuración de almacenamiento de base de datos, ponga el Tipo de almacenamiento de base de datos en gp2.

k. En la Configuración de supervisión de base de datos, ponga Habilitar RDS Performance Insights en falso.

l. Deje el resto de la configuración con los valores predeterminados. Haga clic en Siguiente para continuar.

5. En la página Configurar opciones de pila, deje todas las opciones predeterminadas. Haga clic en Siguiente para continuar.
6. En la página Revisar la pila, seleccione Enviar después de comprobar las opciones de base de datos y de host bastión de Linux.

Una vez finalizado el proceso de creación de la pila, visualice las pilas con los nombres BastionStack y RDSNS para anotar la información que necesita para conectarse a la base de datos. Para obtener más información, consulte Viewing AWS CloudFormation stack data and resources on the AWS Management Console.

Conectarse a una instancia de base de datos MySQL

Puede usar cualquier aplicación cliente de SQL estándar para conectarse a la instancia de base de datos. En este ejemplo, se conecta a una instancia de base de datos de MySQL mediante el cliente de línea de comandos mysql.

Para conectarse a una instancia de base de datos de MySQL

1. Busque el punto de enlace (nombre de DNS) y el número de puerto de la instancia de base de datos.

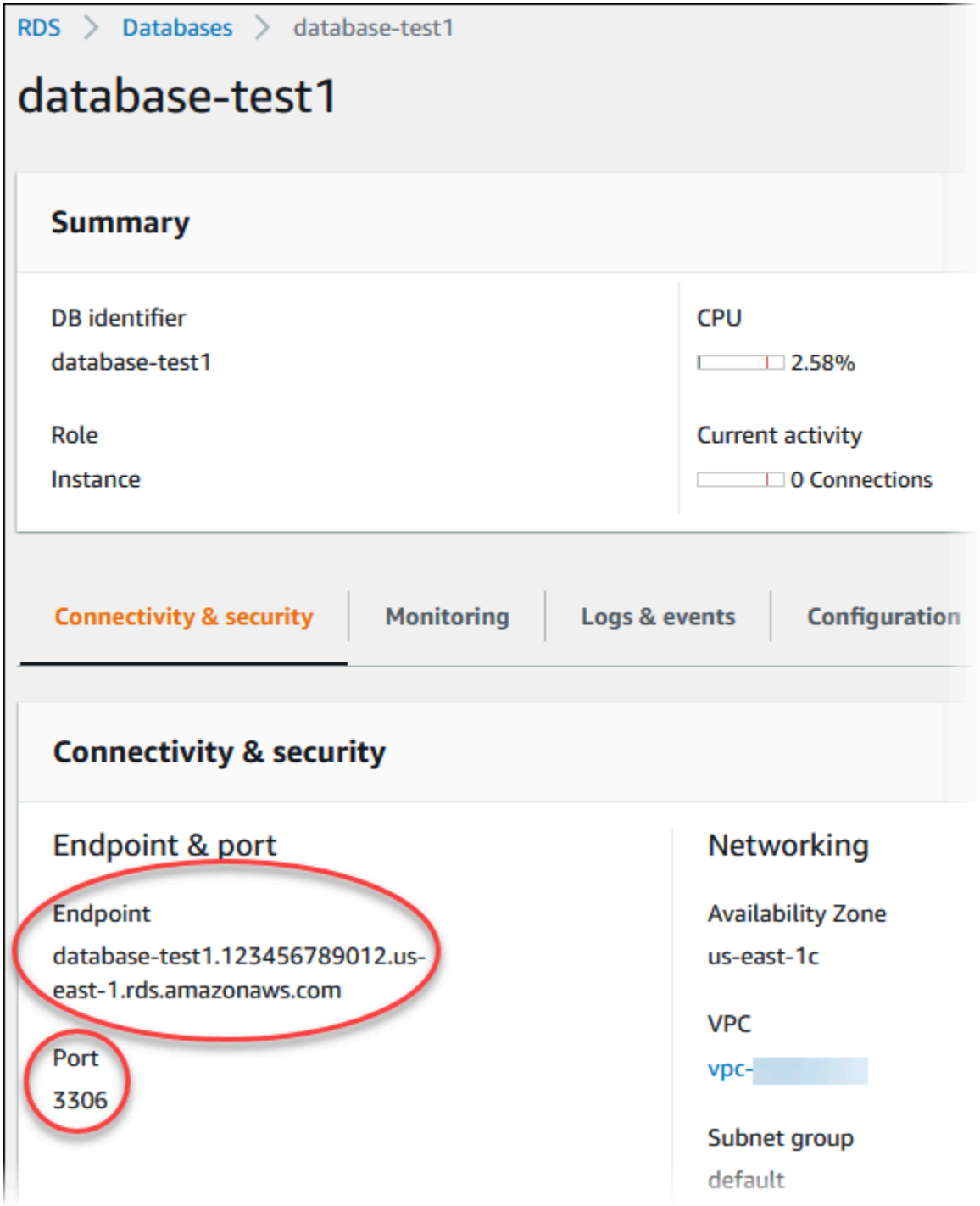
   a. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

   b. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS de la instancia de base de datos.

   c. En el panel de navegación, elija Databases (Bases de datos).

   d. Seleccione el nombre de la instancia de base de datos MySQL para mostrar sus detalles.

   e. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



2. Conéctese a la instancia de EC2 que ha creado anteriormente siguiendo los pasos que se indican en Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2.

   Le recomendamos que se conecte a la instancia de EC2 mediante SSH. Si la utilidad de cliente SSH está instalada en Windows, Linux o Mac, puede conectarse a la instancia con el siguiente formato de comando:

```
ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
```

Por ejemplo, suponga que `ec2-database-connect-key-pair.pem` está almacenado en `/dir1` en Linux y que el DNS IPv4 público de su instancia de EC2 es `ec2-12-345-678-90.compute-1.amazonaws.com`. Su comando SSH tendría el siguiente aspecto:

```
ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
user@ec2-12-345-678-90.compute-1.amazonaws.com
```

3. Obtenga las correcciones de errores y las actualizaciones de seguridad más recientes actualizando el software en su instancia de EC2. Para ello, utilice el siguiente comando.

> **Note**
>
> La opción `-y` instala las actualizaciones sin necesidad de confirmación. Para examinar las actualizaciones antes de la instalación, omita esta opción.

```
sudo dnf update -y
```

4. Para instalar el cliente de línea de comandos mysql de MariaDB en Amazon Linux 2023, ejecute el siguiente comando:

```
sudo dnf install mariadb105
```

5. Conéctese a la instancia de base de datos de MySQL. Por ejemplo, introduzca el siguiente comando. Esta acción le permite conectarse a la instancia de base de datos de MySQL mediante el cliente de MySQL.

   Sustituya el punto de conexión de la instancia de base de datos (nombre de DNS) por *`endpoint`* y sustituya el nombre de usuario maestro que utilizó por *`admin`*. Proporcione la contraseña maestra que utilizó cuando se le solicite una contraseña.

```
mysql -h endpoint -P 3306 -u admin -p
```

   Una vez especificada la contraseña del usuario, debería ver un resultado similar al siguiente.

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 3082
Server version: 8.0.28 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Para obtener más información acerca de cómo conectarse a la instancia de base de datos de MySQL, consulte Conexión a la instancia de base de datos de MySQL. Si no puede conectarse a la instancia de base de datos, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Por motivos de seguridad, se recomienda utilizar conexiones cifradas. Utilice sólo una conexión MySQL sin cifrar cuando el cliente y el servidor están en la misma VPC y la red es de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte Conexión a la instancia de base de datos de MySQL en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado).

6. Ejecutar comandos SQL.

   Por ejemplo, el siguiente comando de SQL muestra la fecha y la hora actuales:

   ```
   SELECT CURRENT_TIMESTAMP;
   ```

Eliminación de la instancia de EC2 y la instancia de base de datos

Después de conectarse y explorar la instancia de EC2 de muestra y la instancia de base de datos que creó, elimínelas para que no le sigan cobrando por ellas.

Si ha utilizado AWS CloudFormation para crear recursos, omita este paso y vaya al siguiente.

Para eliminar la instancia de EC2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).

3. Seleccione la instancia de EC2 y elija Estado de la instancia y Terminar instancia.
4. Cuando se le indique que confirme, elija Terminar.

Para obtener más información sobre la eliminación de una instancia de EC2, consulte Terminar la instancia en la Guía del usuario de Amazon EC2.

Para eliminar una instancia de base de datos sin instantánea de base de datos final

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. Desactive Crear la instantánea final y Conservar copias de seguridad automatizadas.
6. Complete la confirmación y seleccione Eliminar.

(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation

Si ha utilizado AWS CloudFormation para crear recursos, elimine la pila de CloudFormation después de conectarse a la instancia de EC2 y a la instancia de base de datos de muestra y de explorarlas; de este modo, ya no se le cobrará por ellas.

Para eliminar los recursos de CloudFormation

1. Abra la consola de AWS CloudFormation.
2. En la página Pilas de la consola de CloudFormation, seleccione la pila raíz (la pila sin el nombre VPCStack, BastionStack o RDSNS).
3. Elija Eliminar.
4. Cuando se le pida confirmación, seleccione Eliminar pila.

Para obtener información sobre cómo eliminar una pila en CloudFormation, consulte Eliminación de una pila en la consola de AWS CloudFormation, en la Guía del usuario de AWS CloudFormation.

(Opcional) Conecte la instancia de base de datos a una función de Lambda

También puede conectar la instancia de base de datos de RDS para MySQL a un recurso de computación sin servidor de Lambda. Las funciones de Lambda permiten ejecutar código sin aprovisionar ni administrar la infraestructura. Una función de Lambda también permite responder automáticamente a las solicitudes de ejecución de código a cualquier escala, desde una docena de eventos al día hasta cientos de eventos por segundo. Para obtener más información, consulte Conexión automática de una función de Lambda y una instancia de base de datos.

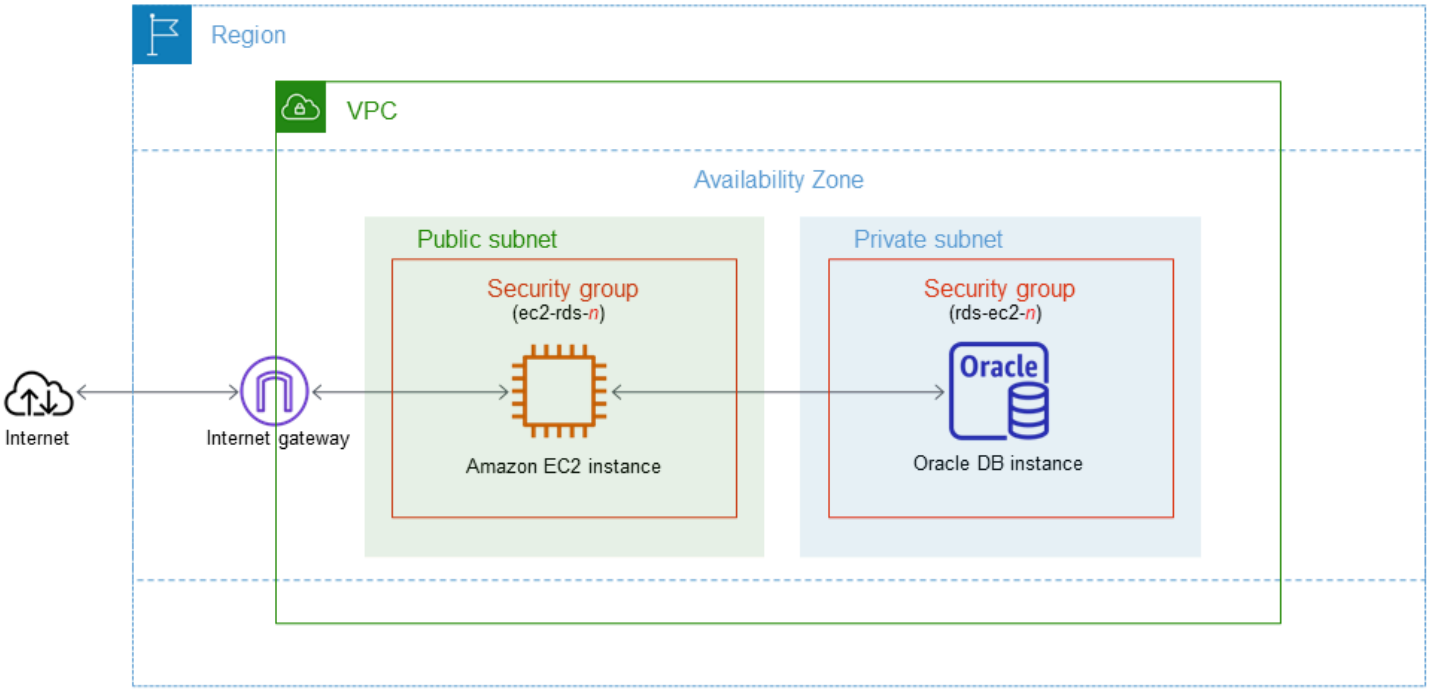
Creación y conexión a una instancia de base de datos de Oracle

En este tutorial, se crea una instancia de EC2 y una instancia de base de datos de RDS para Oracle. El tutorial muestra cómo acceder a la instancia de base de datos desde la instancia de EC2 mediante un cliente de Oracle estándar. Como práctica recomendada, este tutorial crea una instancia de base de datos privada en una nube privada virtual (VPC). En la mayoría de los casos, otros recursos de la misma VPC, como las instancias de EC2, pueden acceder a la instancia de base de datos, pero los recursos ajenos a la VPC no pueden acceder a ella.

Tras completar el tutorial, habrá una subred pública y una privada en cada zona de disponibilidad de la VPC. En una zona de disponibilidad, la instancia de EC2 está en la subred pública y la instancia de base de datos está en la subred privada.

> **Important**
>
> La creación de una cuenta de AWS no supone ningún costo. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de AWS que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

El siguiente diagrama muestra la configuración cuando el tutorial se completa.



Este tutorial le permite crear sus recursos mediante uno de los métodos siguientes:

1. Use la AWS Management Console: Paso 2: crear una instancia de base de datos de Oracle y Paso 1: crear una instancia de EC2
2. Use AWS CloudFormation para crear la instancia de base de datos y la instancia de EC2: (Opcional) Crear una VPC, una instancia EC2 y una instancia de base de datos de Oracle mediante AWS CloudFormation

El primer método utiliza Creación sencilla para crear una instancia de base de datos Oracle privada con la AWS Management Console. Con Creación sencilla, únicamente debe especificar el tipo de motor de base de datos, el tamaño de la instancia de base de datos y el identificador de instancias de base de datos. Easy create (Creación sencilla) utiliza los ajustes predeterminados para otras opciones de configuración.

Cuando usa Creación estándar, se especifican más opciones de configuración al crear una instancia de base de datos. Estas opciones incluyen la configuración de la disponibilidad, la seguridad, las copias de seguridad y el mantenimiento. Para crear una instancia de base de datos pública, debe utilizar Creación estándar. Para obtener más información, consulta Creación de una instancia de base de datos de Amazon RDS.

Temas

- Requisitos previos
- Paso 1: crear una instancia de EC2
- Paso 2: crear una instancia de base de datos de Oracle
- (Opcional) Crear una VPC, una instancia EC2 y una instancia de base de datos de Oracle mediante AWS CloudFormation
- Paso 3: conectar el cliente de SQL a una instancia de base de datos de Oracle
- Paso 4: eliminar la instancia de EC2 y la instancia de base de datos
- (Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation
- (Opcional) Conecte la instancia de base de datos a una función de Lambda

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

- Cómo crear una Cuenta de AWS

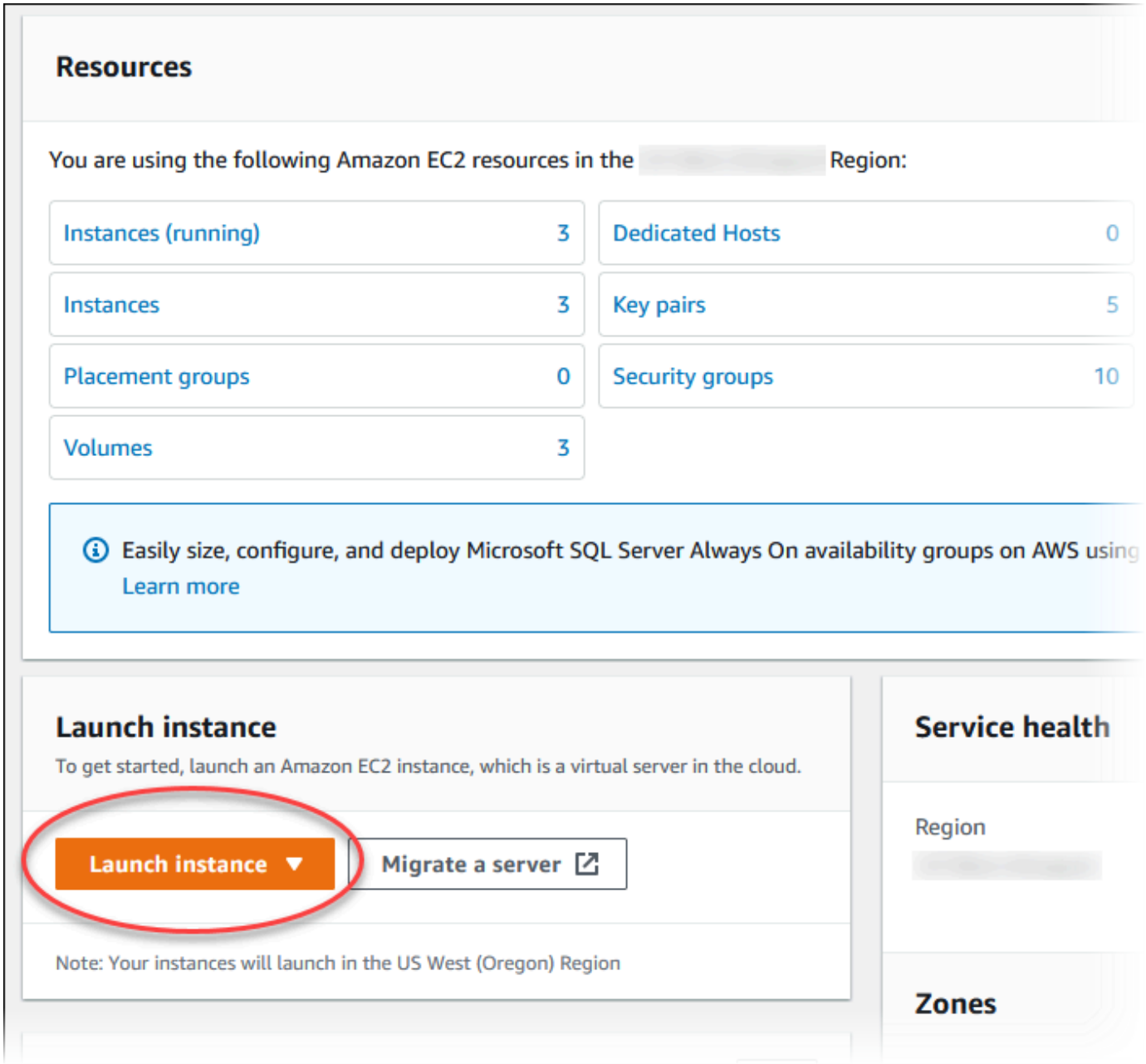
- Creación de un usuario con acceso administrativo

Paso 1: crear una instancia de EC2

Cree una instancia de Amazon EC2 que utilicará para conectarse a la base de datos.

Para crear una instancia EC2;

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS en la que desea crear la instancia de EC2.
3. Elija Panel de EC2 y, a continuación, Lanzar instancia, como se muestra en la siguiente imagen.

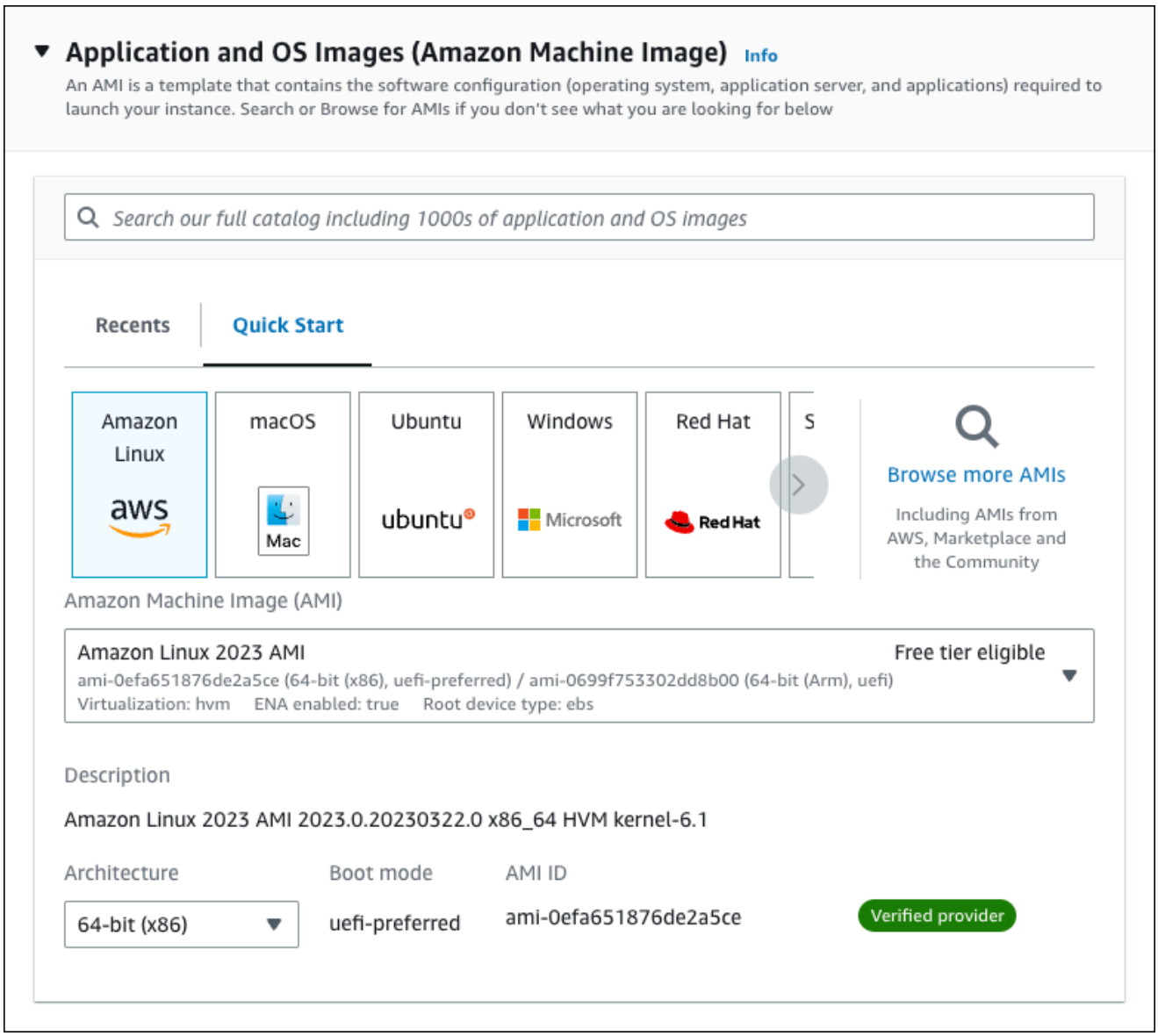


Se abre la página Lanzar una instancia.

4. Elija los siguientes ajustes en la página Lanzar una instancia.

   a. En Name and tags (Nombre y etiquetas), en Name (Nombre), introduzca **`ec2-database-connect`**.

   b. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija Amazon Linux y, a continuación, AMI de Amazon Linux 2023. Mantenga los valores predeterminados para las demás opciones.



c. En Instance type (Tipo de instancia), elija t2.micro.

d. En Key pair (login) [Par de claves (inicio)], elija Key pair name (Nombre de par de claves) para utilizar un par de claves existente. Para crear un nuevo par de claves para la instancia de Amazon EC2, que se muestra a continuación, elija Create new key pair (Crear nuevo par de claves) y, a continuación, utilice la ventana Create key pair (Crear un par de claves).

   Para obtener más información sobre la creación de un nuevo par de claves, consulte Crear un par de claves en la Guía del usuario de Amazon EC2.

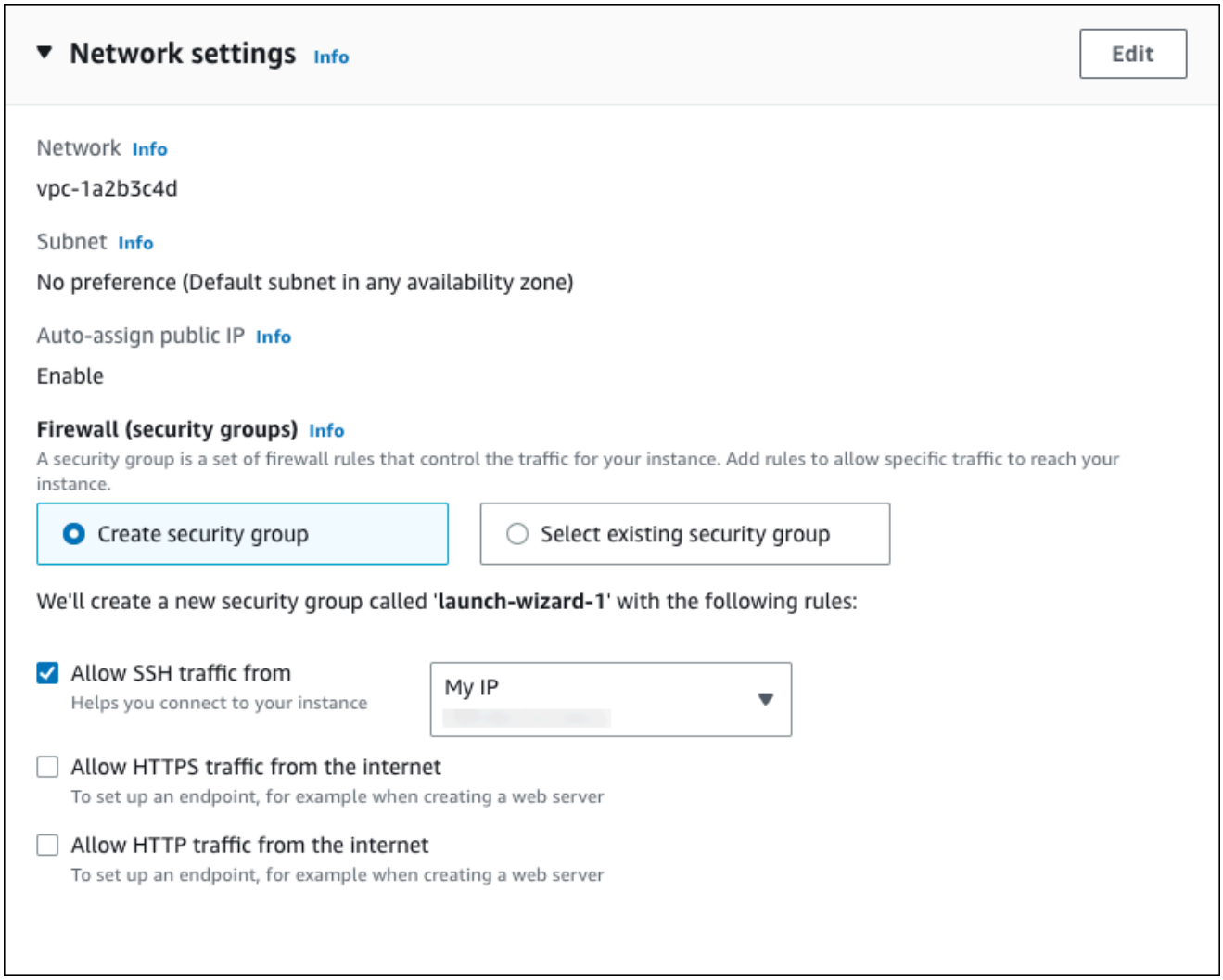
e. En Permitir tráfico de SSH en Configuraciones de red, elija el origen de las conexiones SSH a la instancia de EC2.

Puede elegir My IP (Mi IP) si la dirección IP que se muestra es correcta para las conexiones SSH. De lo contrario, puede determinar la dirección IP que usará para conectarse a las instancias de EC2 en su VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, asegúrese de identificar el rango de direcciones IP que utilizan los equipos cliente.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

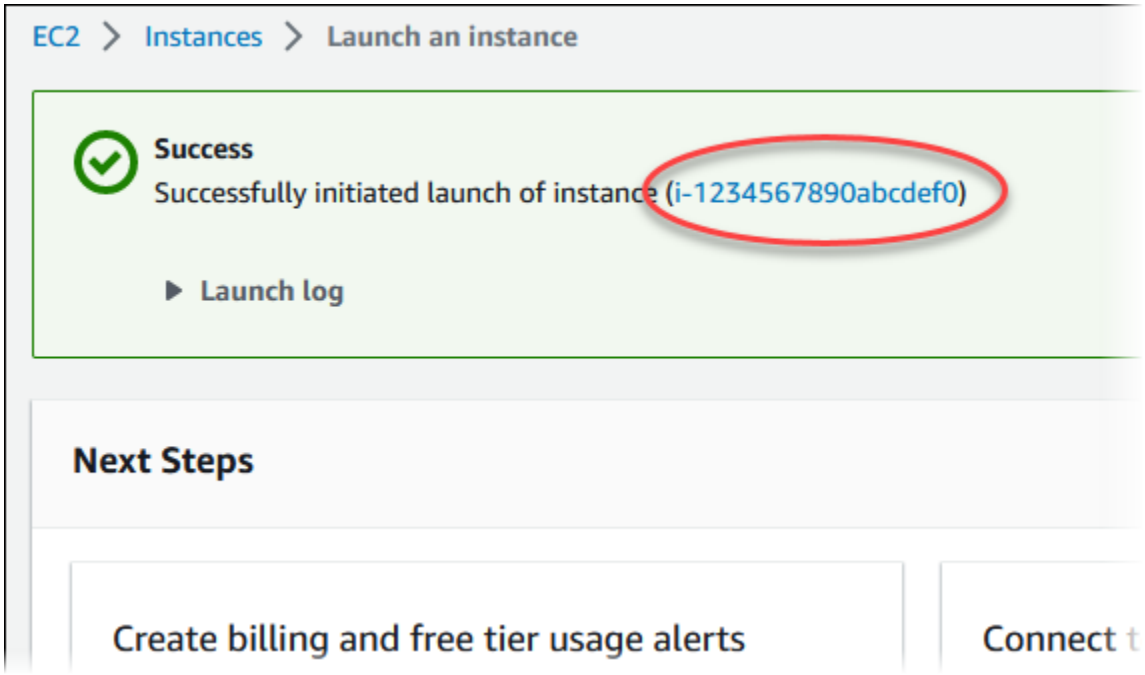
La siguiente imagen muestra un ejemplo de la sección Configuraciones de red.



f. No cambie los valores predeterminados del resto de las secciones.

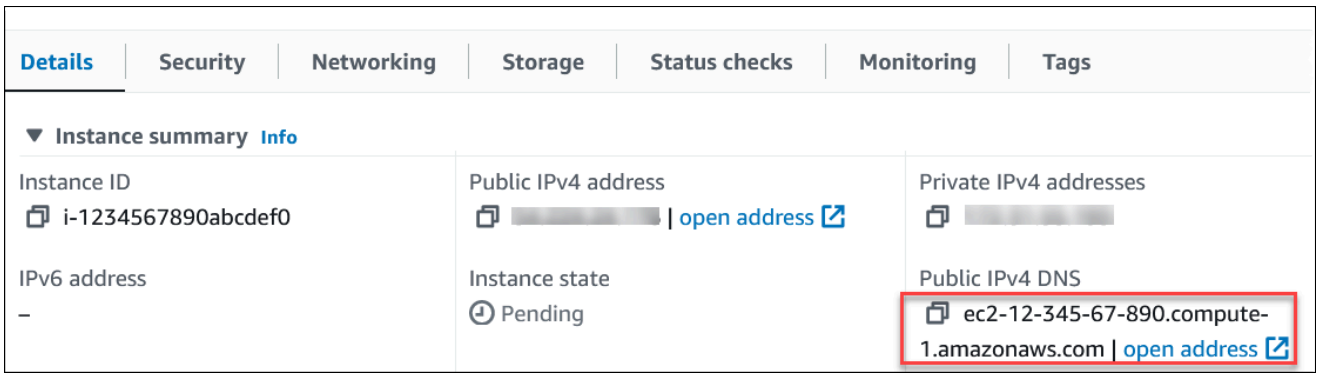
g. Revise un resumen de la configuración de su instancia de EC2 en el panel Resumen; cuando haya terminado, elija Lanzar instancia.

5. En la página Launch Status, que se muestra a continuación, anote el identificador de la nueva instancia de EC2, por ejemplo, `i-1234567890abcdef0`.

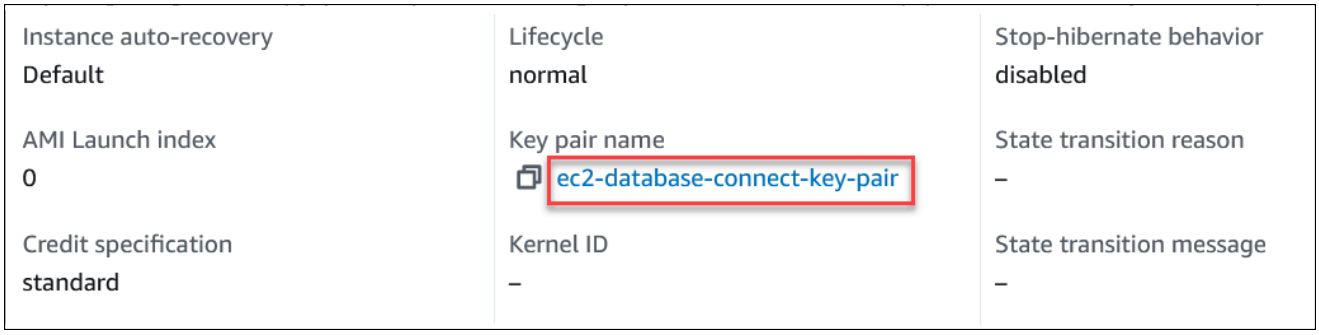


6. Elija el identificador de instancia de EC2 para abrir la lista de instancias de EC2 y, a continuación, seleccione su instancia de EC2.
7. En la pestaña Detalles, anote los siguientes valores, ya que los necesitará cuando se conecte mediante SSH:

   a. En Resumen de la instancia, anote el valor del DNS IPv4 público.



   b. En Detalles de la instancia, anote el valor de Nombre del par de claves.



8. Espere hasta que el Estado de la instancia de su instancia de EC2 tenga el estado En ejecución antes de continuar.

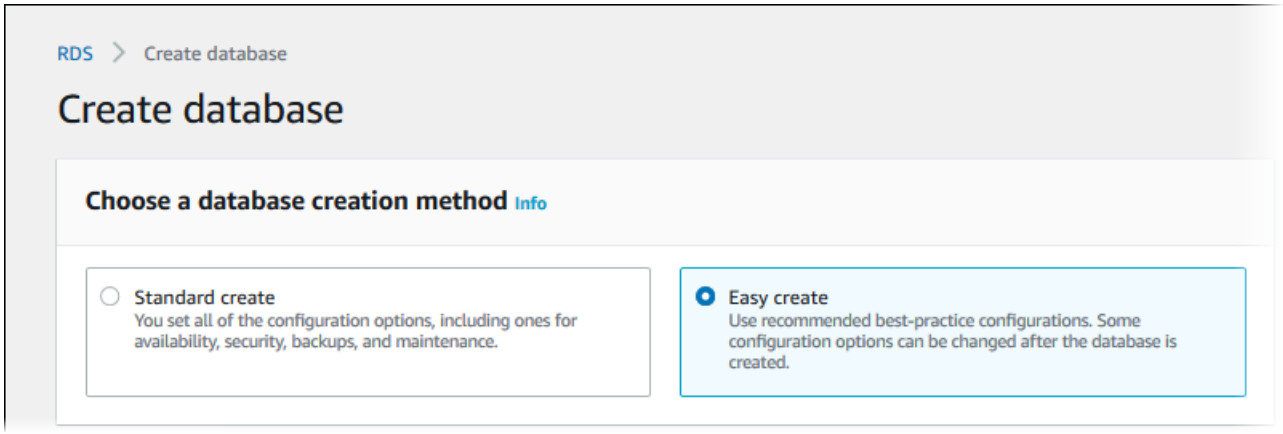
Paso 2: crear una instancia de base de datos de Oracle

El componente básico de Amazon RDS es la instancia de base de datos. Este es el entorno en el que ejecuta las bases de datos Oracle.

En este ejemplo, utilice la opción Creación sencilla para crear una instancia de base de datos que ejecuta el motor de la base de datos de Oracle con una clase de instancia de base de datos db.m5.large.

Para crear una instancia de base de datos de Oracle con Creación sencilla

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Seleccione Create database (Crear base de datos) y asegúrese de que la opción Easy Create (Creación sencilla) esté seleccionada.



5. En Configuration (Configuración), elija Oracle.
6. En DB instance size (Tamaño de la instancia de base de datos), seleccione Dev/Test (Desarrollo/Prueba).
7. En DB instance identifier (Identificador de instancia de base de datos), ingrese **`database-test1`**.
8. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro o deje el nombre predeterminado.

   La página Create database (Crear base de datos) debe ser similar a la siguiente imagen.

Configuration

Engine type Info

- Aurora (MySQL Compatible)
- Aurora (PostgreSQL Compatible)
- MySQL
- MariaDB
- PostgreSQL
- Oracle
- Microsoft SQL Server

Edition

- Oracle Enterprise Edition
  Affordable and full-featured database management system supporting up to 16 vCPUs.
- Oracle Standard Edition Two
  Affordable and full-featured database management system supporting up to 16 vCPUs. Oracle Database Standard Edition Two is a replacement for Standard Edition and Standard Edition One.

DB instance size

- Production
  db.r5.large
  2 vCPUs
  16 GiB RAM
  500 GiB
- Dev/Test
  db.m5.large
  2 vCPUs
  8 GiB RAM
  100 GiB

DB instance identifier

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-test1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Master username Info

Type a login ID for the master user of your DB instance.

admin

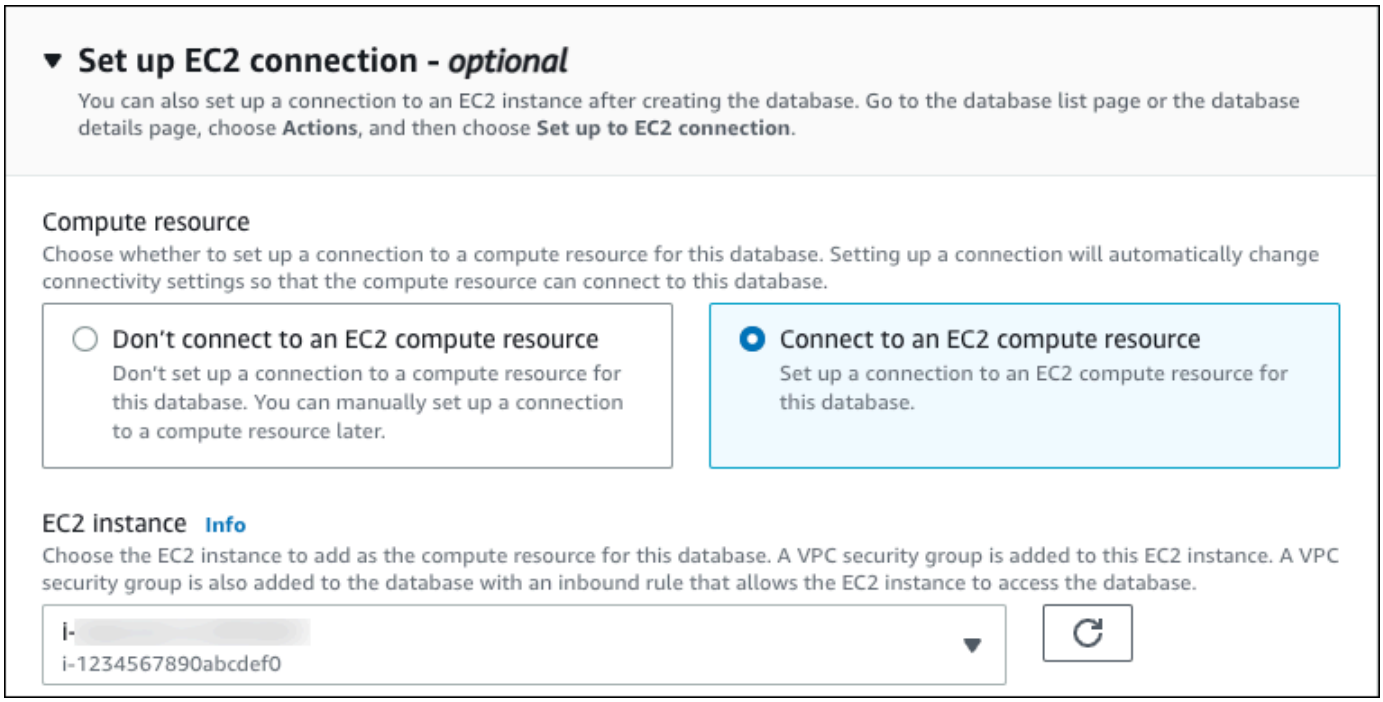
1 to 16 alphanumeric characters. First character must be a letter.

9. Para utilizar una contraseña maestra generada automáticamente para la instancia de base de datos, seleccione Generación automática de contraseña.

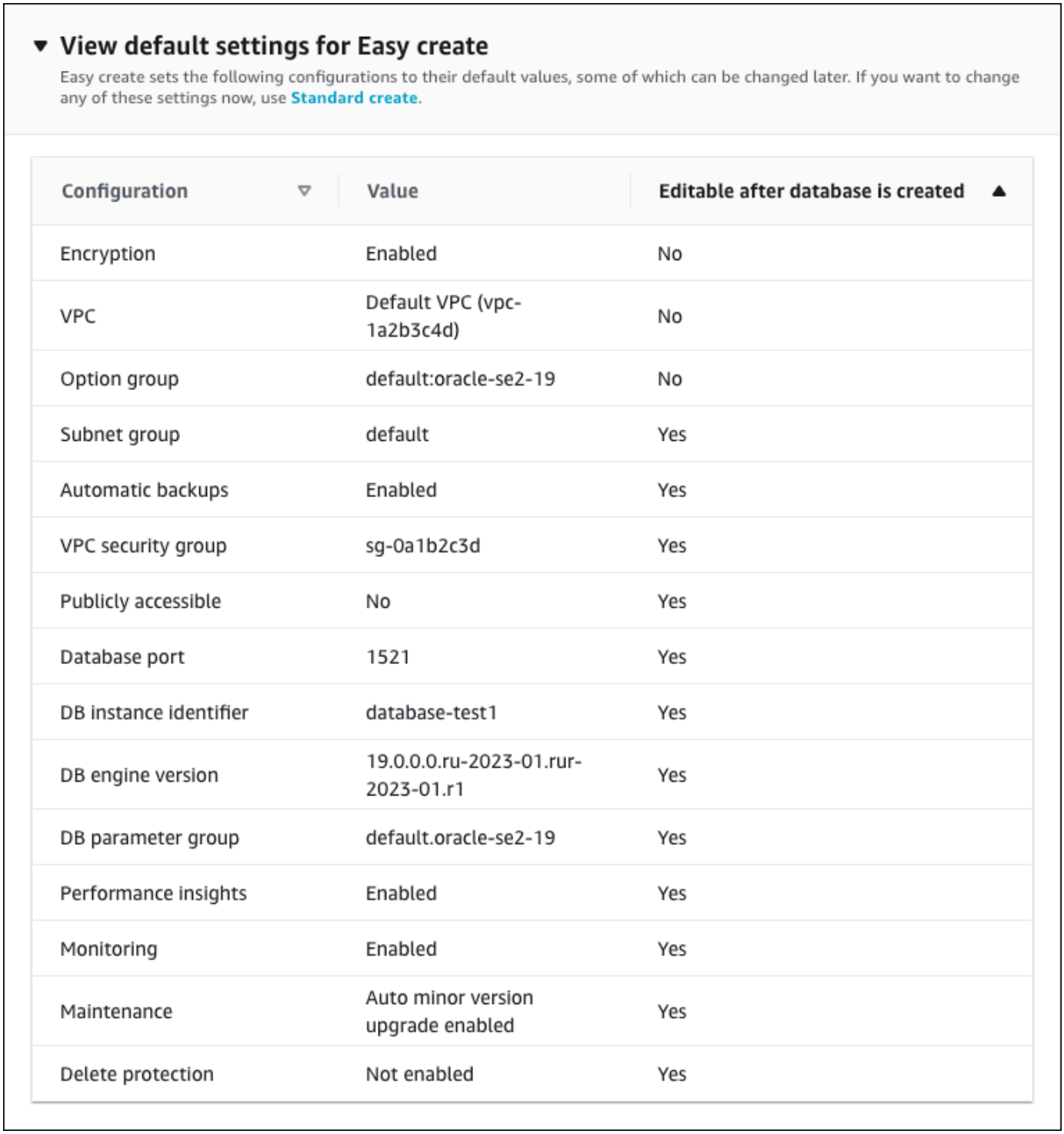
   Para introducir la contraseña maestra, asegúrese de desactivar la casilla Generación automática de contraseña y luego introduzca la misma contraseña en Contraseña maestra y Confirmar contraseña.

10. Para configurar una conexión con la instancia de EC2 que creó anteriormente, abra Configurar conexión a EC2 - (opcional).

    Seleccione Conectarse a un recurso informático de EC2. Elija la instancia de EC2 que ha creado anteriormente.



11. Abra la opción Ver la configuración predeterminada de la creación sencilla.



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:oracle-se2-19	No
Subnet group	default	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-0a1b2c3d	Yes
Publicly accessible	No	Yes
Database port	1521	Yes
DB instance identifier	database-test1	Yes
DB engine version	19.0.0.0.ru-2023-01.rur-2023-01.r1	Yes
DB parameter group	default.oracle-se2-19	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Puede examinar la configuración predeterminada utilizada con Easy create (Creación sencilla). La columna Editable después de crear la base de datos muestra las opciones que puede cambiar después de crear la base de datos.

- Si una configuración tiene No en esa columna y desea una configuración diferente, puede usar Creación estándar para crear la instancia de base de datos.
- Si una configuración tiene Sí en esa columna y desea una configuración diferente, puede utilizar Creación estándar para crear la instancia de base de datos o modificar la instancia de base de datos después de crearla para cambiar la configuración.

12. Elija Creación de base de datos.

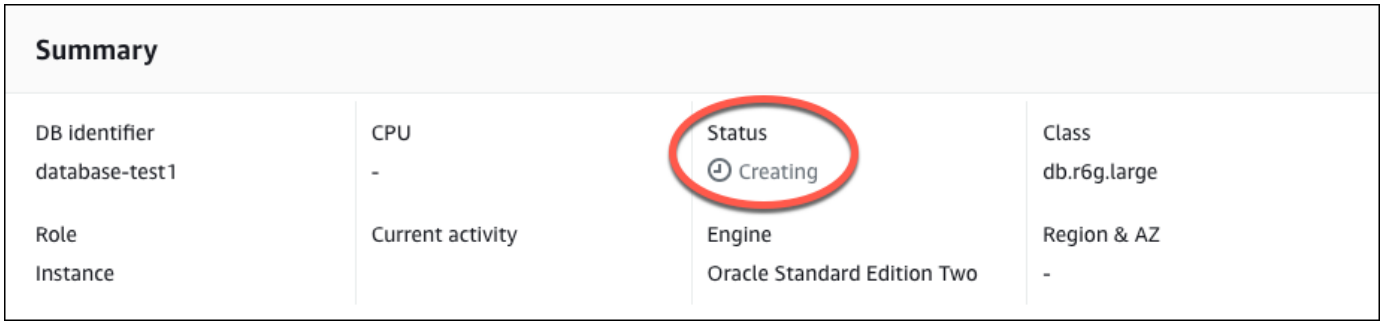
    Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales).

    Puede utilizar la contraseña y el nombre de usuario que aparecen para conectarse a la instancia de base de datos como el usuario maestro.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla.
    > Si tiene que cambiar la contraseña de usuario maestro después de que la instancia de base de datos esté disponible, puede modificar la instancia de base de datos para ello. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

13. En la lista Bases de datos, seleccione el nombre de la nueva instancia de base de datos de Oracle para ver sus detalles.

    La instancia de base de datos tiene el estado Creando hasta que está lista para usarse.



    Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de la base de datos. Dependiendo de la clase de instancia de la base de datos y de la cantidad de almacenamiento, es posible que la nueva instancia tarde hasta 20 minutos en estar disponible.

Mientras se crea la instancia de base de datos, puede ir al siguiente paso y crear una instancia de EC2.

(Opcional) Crear una VPC, una instancia EC2 y una instancia de base de datos de Oracle mediante AWS CloudFormation

En lugar de utilizar la consola para crear la VPC, la instancia de EC2 y la instancia de base de datos de Oracle, puede utilizar AWS CloudFormation para aprovisionar recursos de AWS tratando la infraestructura como código. Para ayudarle a organizar sus recursos de AWS en unidades más pequeñas y fáciles de administrar, puede utilizar la funcionalidad de pila anidada de AWS CloudFormation. Para obtener más información, consulte Creación de una pila en la consola AWS CloudFormation y Uso de pilas anidadas.

> **Important**
>
> AWS CloudFormation es gratuito, pero los recursos que CloudFormation crea están activos. Se le facturan las tarifas de uso estándar por estos recursos hasta que los finalice. Para obtener más información, consulte Precios de RDS para Oracle.

Para crear sus recursos con la consola AWS CloudFormation, siga estos pasos:

- Paso 1: Descargar la plantilla de CloudFormation
- Paso 2: Configurar los recursos mediante CloudFormation

Descargar la plantilla de CloudFormation

Una plantilla de CloudFormation es un archivo de texto con formato JSON o YAML que contiene la información de configuración de los recursos que desea crear en la pila. Esta plantilla también crea una VPC y un host bastión para usted junto con la instancia de RDS.

Para descargar el archivo de plantilla, abra el enlace Oracle CloudFormation template.

En la página de Github, haga clic en el botón Descargar archivo sin procesar para guardar el archivo YAML de la plantilla.

Configurar los recursos mediante CloudFormation

> **Note**
>
> Antes de iniciar este proceso, asegúrese de tener un par de claves para una instancia EC2 en su Cuenta de AWS. Para obtener más información, consulte Pares de claves de Amazon EC2 e instancias Linux.

Al utilizar la plantilla de AWS CloudFormation, debe seleccionar los parámetros correctos para asegurarse de que los recursos se crean correctamente. Siga los pasos que se indican a continuación:

1. Inicie sesión en la AWS Management Console y abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Elija Crear pila.
3. En la sección Especificar la plantilla, seleccione Cargar un archivo de plantilla desde el ordenador y Siguiente.
4. En la página Especificar detalles de la pila, introduzca los siguientes parámetros:
   a. Ponga el nombre de pila en OracleTestStack.
   b. En Parámetros, defina las zonas de disponibilidad seleccionando tres zonas de disponibilidad.
   c. En Configuración de host bastión de Linux, en Nombre de la clave, seleccione un par de claves para iniciar sesión en su instancia de EC2.
   d. En los ajustes de Configuración de host bastión de Linux, ponga el rango de IP permitido en su dirección IP. Para conectarse a las instancias de EC2 de su VPC mediante Secure Shell (SSH), determine su dirección IP pública mediante el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección

IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

e. En Configuración general de la base de datos, ponga la Clase de instancia de base de datos en db.t3.micro.

f. Ponga el Nombre de la base de datos en **`database-test1`**.

g. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro.

h. Ponga Administrar contraseña de usuario maestro de base de datos con Secrets Manager en `false` para este tutorial.

i. En Contraseña de base de datos, ponga la contraseña que desee. Recuerde esta contraseña para poder ver los pasos adicionales del tutorial.

j. En Configuración de almacenamiento de base de datos, ponga el Tipo de almacenamiento de base de datos en gp2.

k. En la Configuración de supervisión de base de datos, ponga Habilitar RDS Performance Insights en falso.

l. Deje el resto de la configuración con los valores predeterminados. Haga clic en Siguiente para continuar.

5. En la página Configurar opciones de pila, deje todas las opciones predeterminadas. Haga clic en Siguiente para continuar.
6. En la página Revisar la pila, seleccione Enviar después de comprobar las opciones de base de datos y de host bastión de Linux.

Una vez finalizado el proceso de creación de la pila, visualice las pilas con los nombres BastionStack y RDSNS para anotar la información que necesita para conectarse a la base de datos. Para obtener más información, consulte Viewing AWS CloudFormation stack data and resources on the AWS Management Console.

Paso 3: conectar el cliente de SQL a una instancia de base de datos de Oracle

Puede usar cualquier aplicación cliente de SQL estándar para conectarse a la instancia de base de datos. En este ejemplo, se conecta a una instancia de base de datos de Oracle mediante el cliente de línea de comandos de Oracle.

Para conectarse a una instancia de base de datos de Oracle

1. Busque el punto de enlace (nombre de DNS) y el número de puerto de la instancia de base de datos.

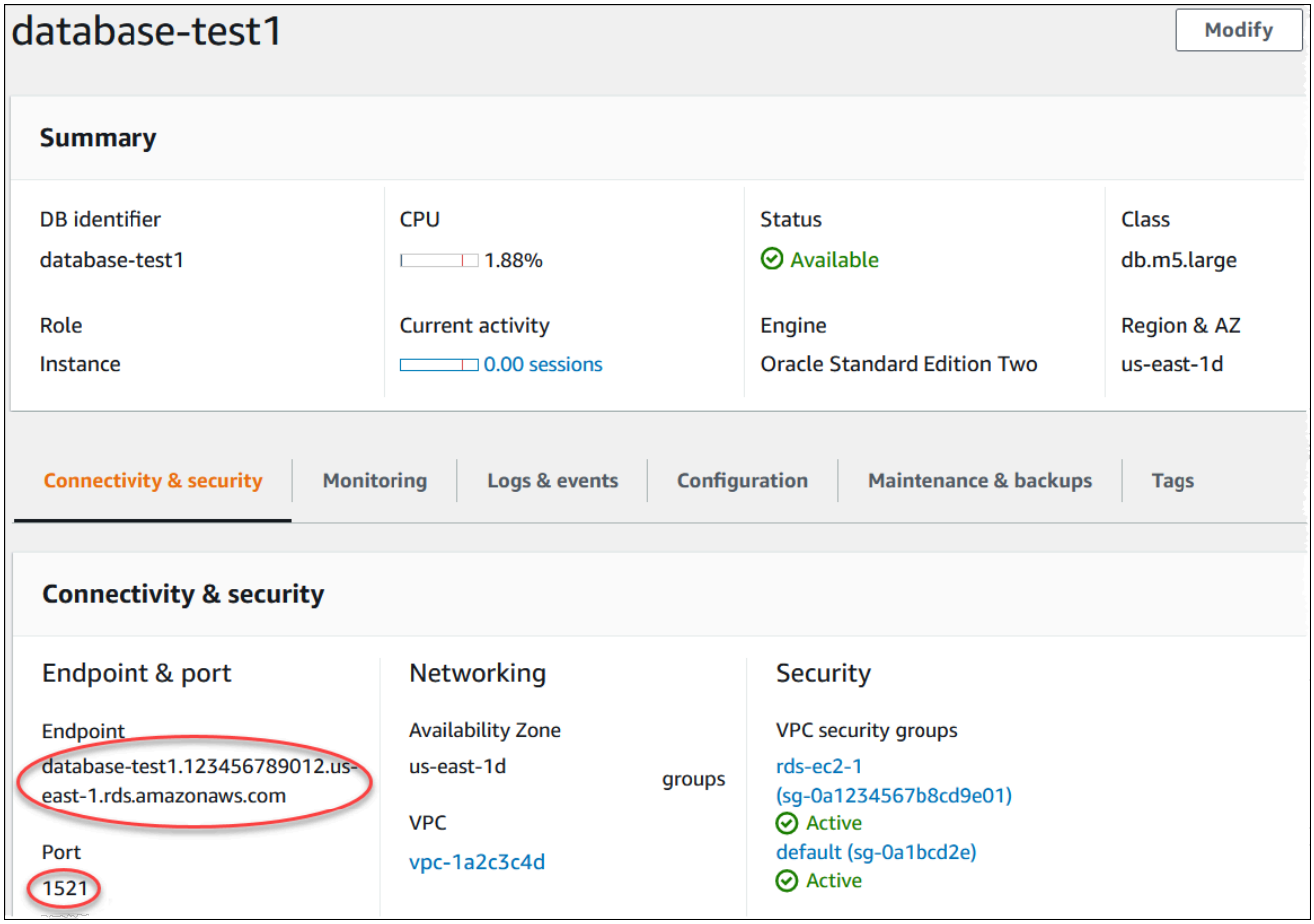
   a. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

   b. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS de la instancia de base de datos.

   c. En el panel de navegación, elija Databases (Bases de datos).

   d. Seleccione el nombre de la instancia de base de datos Oracle para mostrar sus detalles.

   e. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



2. Conéctese a la instancia de EC2 que ha creado anteriormente siguiendo los pasos que se indican en Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2.

Le recomendamos que se conecte a la instancia de EC2 mediante SSH. Si la utilidad de cliente SSH está instalada en Windows, Linux o Mac, puede conectarse a la instancia con el siguiente formato de comando:

```
ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
```

Por ejemplo, suponga que `ec2-database-connect-key-pair.pem` está almacenado en `/dir1` en Linux y que el DNS IPv4 público de su instancia de EC2 es `ec2-12-345-678-90.compute-1.amazonaws.com`. Su comando SSH tendría el siguiente aspecto:

```
ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
user@ec2-12-345-678-90.compute-1.amazonaws.com
```

3. Obtenga las correcciones de errores y las actualizaciones de seguridad más recientes actualizando el software en su instancia de EC2. Para ello, utilice el siguiente comando.

> **Note**
>
> La opción `-y` instala las actualizaciones sin necesidad de confirmación. Para examinar las actualizaciones antes de la instalación, omita esta opción.

```
sudo dnf update -y
```

4. En un navegador web, vaya a https://www.oracle.com/database/technologies/instant-client/linux-x86-64-downloads.html.
5. Para obtener la versión más reciente de la base de datos que aparece en la página web, copie los enlaces .rpm (no los enlaces .zip) del paquete básico de Instant Client y del package de SQL*Plus. Por ejemplo, los siguientes enlaces corresponden a la versión 21.9 de Oracle Database:

   - https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-instantclient-basic-21.9.0.0.0-1.el8.x86_64.rpm
   - https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-instantclient-sqlplus-21.9.0.0.0-1.el8.x86_64.rpm

6. En su sesión de SSH, ejecute el comando `wget` para descargar los archivos .rpm desde los enlaces que obtuvo en el paso anterior. En el siguiente ejemplo, se descargan los archivos.rpm de la versión 21.9 de Oracle Database:

```
wget https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-
instantclient-basic-21.9.0.0.0-1.el8.x86_64.rpm
wget https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-
instantclient-sqlplus-21.9.0.0.0-1.el8.x86_64.rpm
```

7. Ejecute el comando `dnf` para instalar los paquetes de la manera siguiente:

```
sudo dnf install oracle-instantclient-*.rpm
```

8. Inicie SQL*Plus y conéctese a la instancia de base de datos de Oracle. Por ejemplo, introduzca el siguiente comando.

   Sustituya el punto de conexión de la instancia de base de datos (nombre de DNS) por *`oracle-db-instance-endpoint`* y sustituya el nombre de usuario maestro que utilizó por *`admin`*. Cuando usa Creación sencilla para Oracle, el nombre de la base de datos es `DATABASE`. Proporcione la contraseña maestra que utilizó cuando se le solicite una contraseña.

```
sqlplus admin@oracle-db-instance-endpoint:1521/DATABASE
```

   Una vez especificada la contraseña del usuario, debería ver un resultado similar al siguiente.

```
SQL*Plus: Release 21.0.0.0.0 - Production on Wed Mar 1 16:41:28 2023
Version 21.9.0.0.0

Copyright (c) 1982, 2022, Oracle.  All rights reserved.

Enter password:
Last Successful login time: Wed Mar 01 2023 16:30:52 +00:00

Connected to:
Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production
Version 19.18.0.0.0

SQL>
```

Para obtener más información sobre la conexión a una instancia de base de datos de RDS para Oracle, consulte Conexión a una instancia de base de datos de Oracle. Si no puede conectarse a la instancia de base de datos, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Por motivos de seguridad, se recomienda utilizar conexiones cifradas. Utilice solo una conexión Oracle sin cifrar cuando el cliente y el servidor estén en la misma VPC y la red sea de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte Protección de conexiones de instancias de base de datos de Oracle.

9. Ejecutar comandos SQL.

   Por ejemplo, el siguiente comando de SQL muestra la fecha actual:

```
SELECT SYSDATE FROM DUAL;
```

Paso 4: eliminar la instancia de EC2 y la instancia de base de datos

Después de conectarse y explorar la instancia de EC2 de muestra y la instancia de base de datos que creó, elimínelas para que no le sigan cobrando por ellas.

Si ha utilizado AWS CloudFormation para crear recursos, omita este paso y vaya al siguiente.

Para eliminar la instancia de EC2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia de EC2 y elija Estado de la instancia y Terminar instancia.
4. Cuando se le indique que confirme, elija Terminar.

Para obtener más información sobre la eliminación de una instancia de EC2, consulte Terminar la instancia en la Guía del usuario de Amazon EC2.

Para eliminar una instancia de base de datos sin instantánea de base de datos final

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. Desactive Crear la instantánea final y Conservar copias de seguridad automatizadas.
6. Complete la confirmación y seleccione Eliminar.

(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation

Si ha utilizado AWS CloudFormation para crear recursos, elimine la pila de CloudFormation después de conectarse a la instancia de EC2 y a la instancia de base de datos de muestra y de explorarlas; de este modo, ya no se le cobrará por ellas.

Para eliminar los recursos de CloudFormation

1. Abra la consola de AWS CloudFormation.
2. En la página Pilas de la consola de CloudFormation, seleccione la pila raíz (la pila sin el nombre VPCStack, BastionStack o RDSNS).
3. Elija Eliminar.
4. Cuando se le pida confirmación, seleccione Eliminar pila.

Para obtener información sobre cómo eliminar una pila en CloudFormation, consulte Eliminación de una pila en la consola de AWS CloudFormation, en la Guía del usuario de AWS CloudFormation.

(Opcional) Conecte la instancia de base de datos a una función de Lambda

También puede conectar la instancia de base de datos de RDS para Oracle a un recurso de computación sin servidor de Lambda. Las funciones de Lambda permiten ejecutar código sin aprovisionar ni administrar la infraestructura. Una función de Lambda también permite responder automáticamente a las solicitudes de ejecución de código a cualquier escala, desde una docena de eventos al día hasta cientos de eventos por segundo. Para obtener más información, consulte Conexión automática de una función de Lambda y una instancia de base de datos.

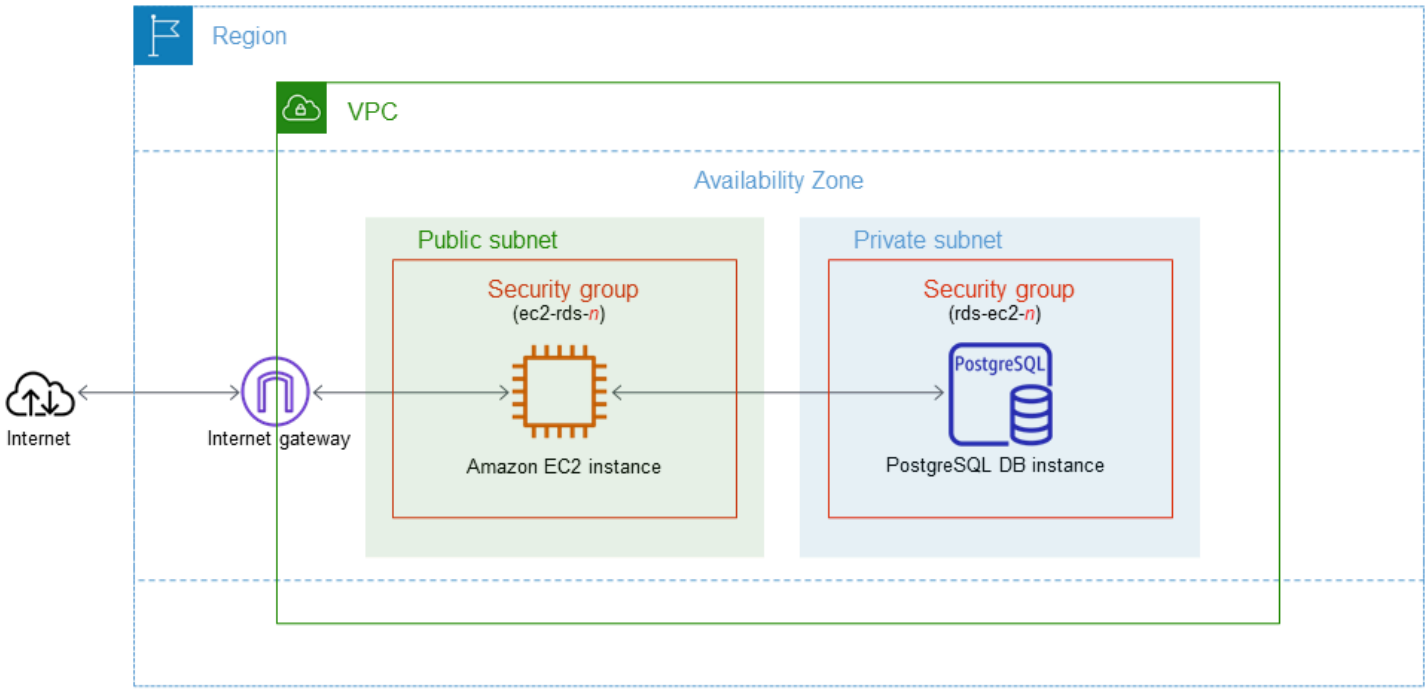
Creación de una instancia de base de datos de PostgreSQL y conexión a ella

En este tutorial, se crea una instancia de EC2 y una instancia de base de datos de RDS para PostgreSQL. El tutorial muestra cómo acceder a la instancia de base de datos desde la instancia de EC2 mediante un cliente PostgreSQL estándar. Como práctica recomendada, este tutorial crea una instancia de base de datos privada en una nube privada virtual (VPC). En la mayoría de los casos, otros recursos de la misma VPC, como las instancias de EC2, pueden acceder a la instancia de base de datos, pero los recursos ajenos a la VPC no pueden acceder a ella.

Tras completar el tutorial, habrá una subred pública y una privada en cada zona de disponibilidad de la VPC. En una zona de disponibilidad, la instancia de EC2 está en la subred pública y la instancia de base de datos está en la subred privada.

> **Important**
>
> La creación de una cuenta de AWS no supone ningún costo. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de AWS que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

El siguiente diagrama muestra la configuración cuando el tutorial se completa.



Este tutorial le permite crear sus recursos mediante uno de los métodos siguientes:

1. Use la AWS Management Console: Crear una instancia de EC2 y Creación de una instancia de base de datos de PostgreSQL
2. Use AWS CloudFormation para crear la instancia de base de datos y la instancia de EC2: (Opcional) Crear una VPC, una instancia EC2 y una instancia PostgreSQL mediante AWS CloudFormation

El primer método usa Creación sencilla para crear una instancia de base de datos PostgreSQL privada con la AWS Management Console. Con Creación sencilla, únicamente debe especificar el tipo de motor de base de datos, el tamaño de la instancia de base de datos y el identificador de instancias de base de datos. Easy create (Creación sencilla) utiliza los ajustes predeterminados para otras opciones de configuración.

Cuando usa Creación estándar, se especifican más opciones de configuración al crear una instancia de base de datos. Estas opciones incluyen la configuración de la disponibilidad, la seguridad, las copias de seguridad y el mantenimiento. Para crear una instancia de base de datos pública, debe utilizar Creación estándar. Para obtener más información, consulta Creación de una instancia de base de datos de Amazon RDS.

Temas

- Requisitos previos
- Crear una instancia de EC2
- Creación de una instancia de base de datos de PostgreSQL
- (Opcional) Crear una VPC, una instancia EC2 y una instancia PostgreSQL mediante AWS CloudFormation
- Conexión a la instancia de base de datos PostgreSQL
- Eliminación de la instancia de EC2 y la instancia de base de datos
- (Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation
- (Opcional) Conecte la instancia de base de datos a una función de Lambda

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

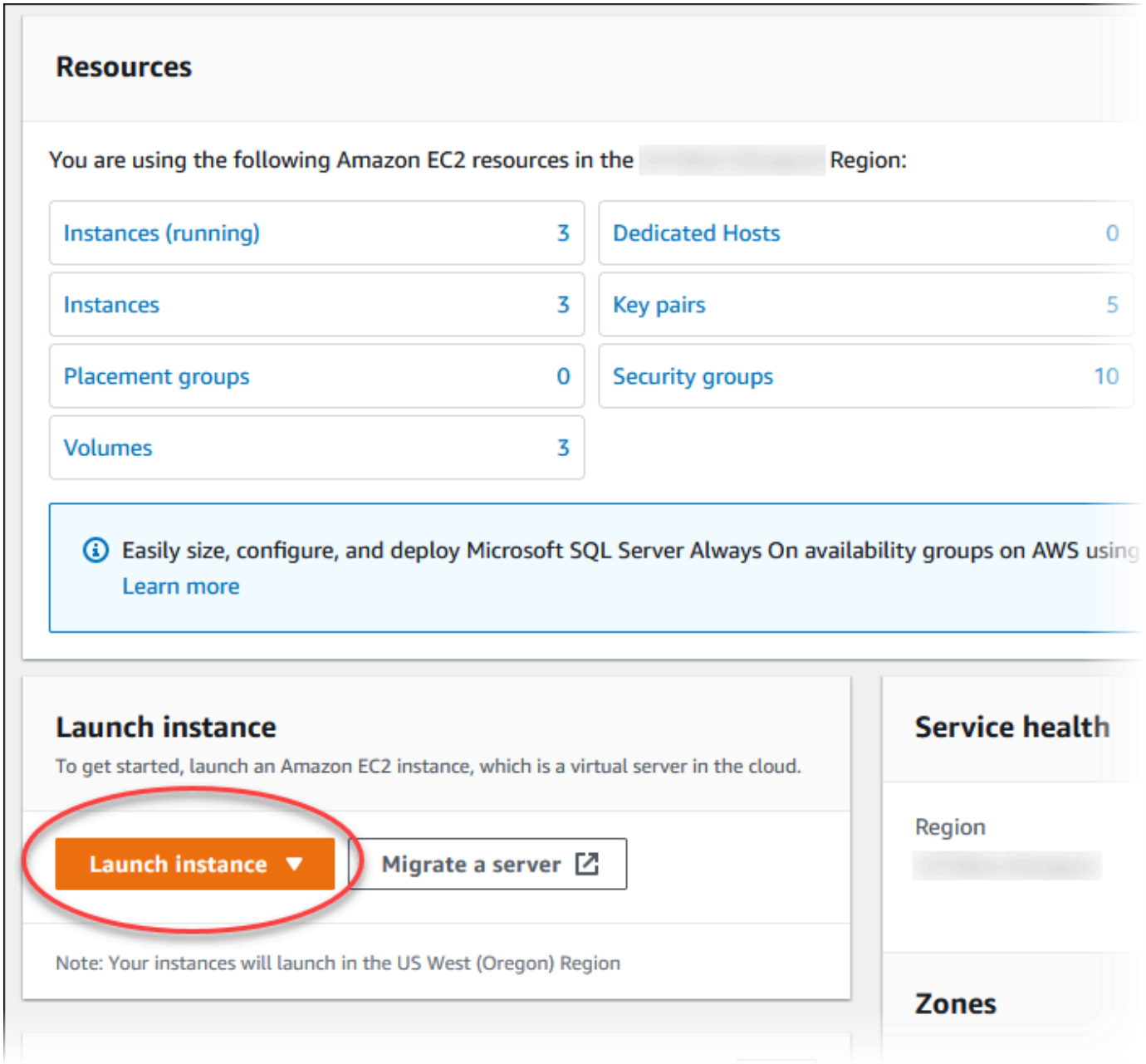
- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Crear una instancia de EC2

Cree una instancia de Amazon EC2 que utilicará para conectarse a la base de datos.

Para crear una instancia EC2;

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS en la que desea crear la instancia de EC2.
3. Elija Panel de EC2 y, a continuación, Lanzar instancia, como se muestra en la siguiente imagen.

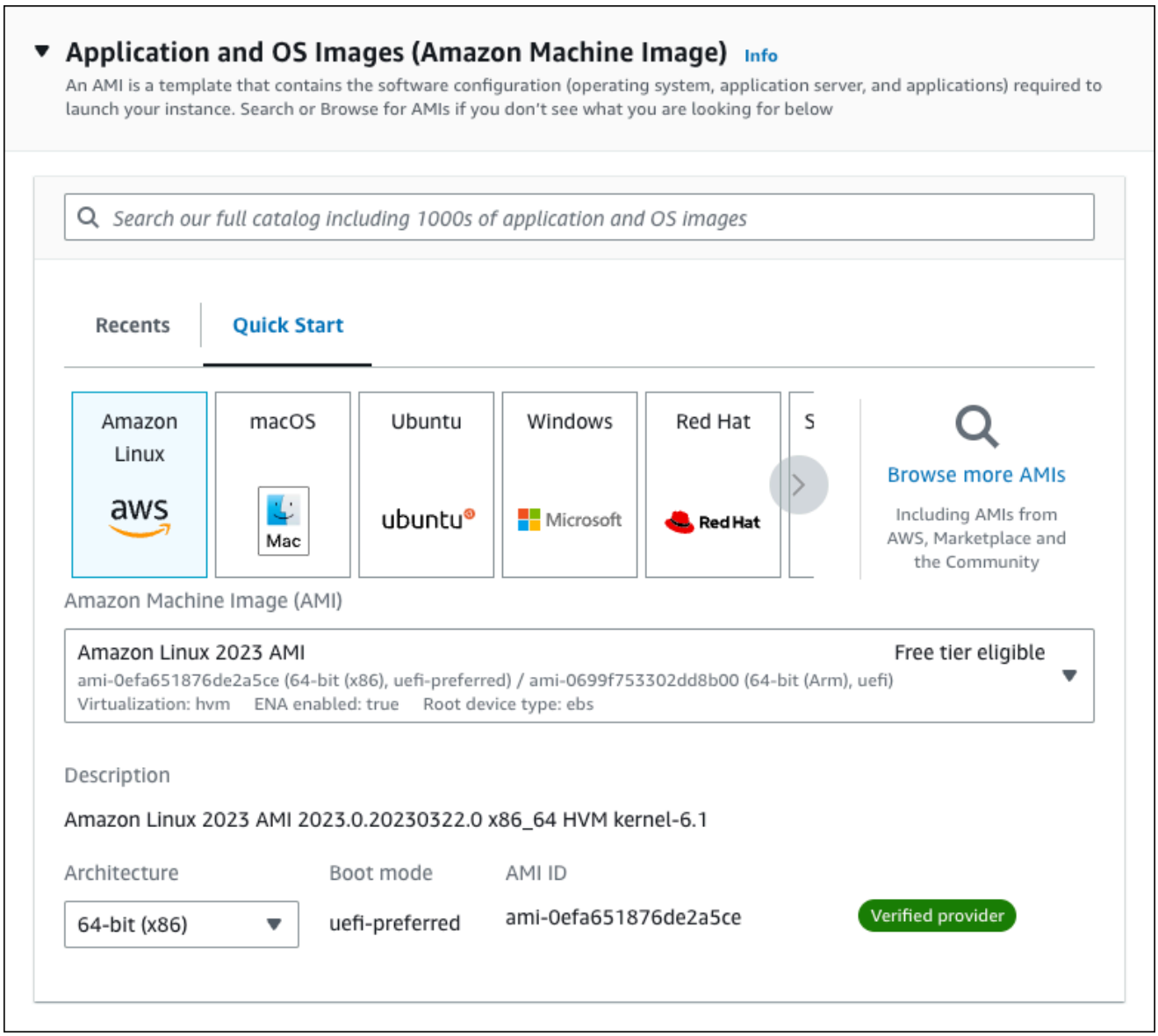


Se abre la página Lanzar una instancia.

4. Elija los siguientes ajustes en la página Lanzar una instancia.

   a. En Name and tags (Nombre y etiquetas), en Name (Nombre), introduzca **`ec2-database-connect`**.

   b. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija Amazon Linux y, a continuación, AMI de Amazon Linux 2023. Mantenga los valores predeterminados para las demás opciones.



c. En Instance type (Tipo de instancia), elija t2.micro.

d. En Key pair (login) [Par de claves (inicio)], elija Key pair name (Nombre de par de claves) para utilizar un par de claves existente. Para crear un nuevo par de claves para la instancia de Amazon EC2, que se muestra a continuación, elija Create new key pair (Crear nuevo par de claves) y, a continuación, utilice la ventana Create key pair (Crear un par de claves).

   Para obtener más información sobre la creación de un nuevo par de claves, consulte Crear un par de claves en la Guía del usuario de Amazon EC2.

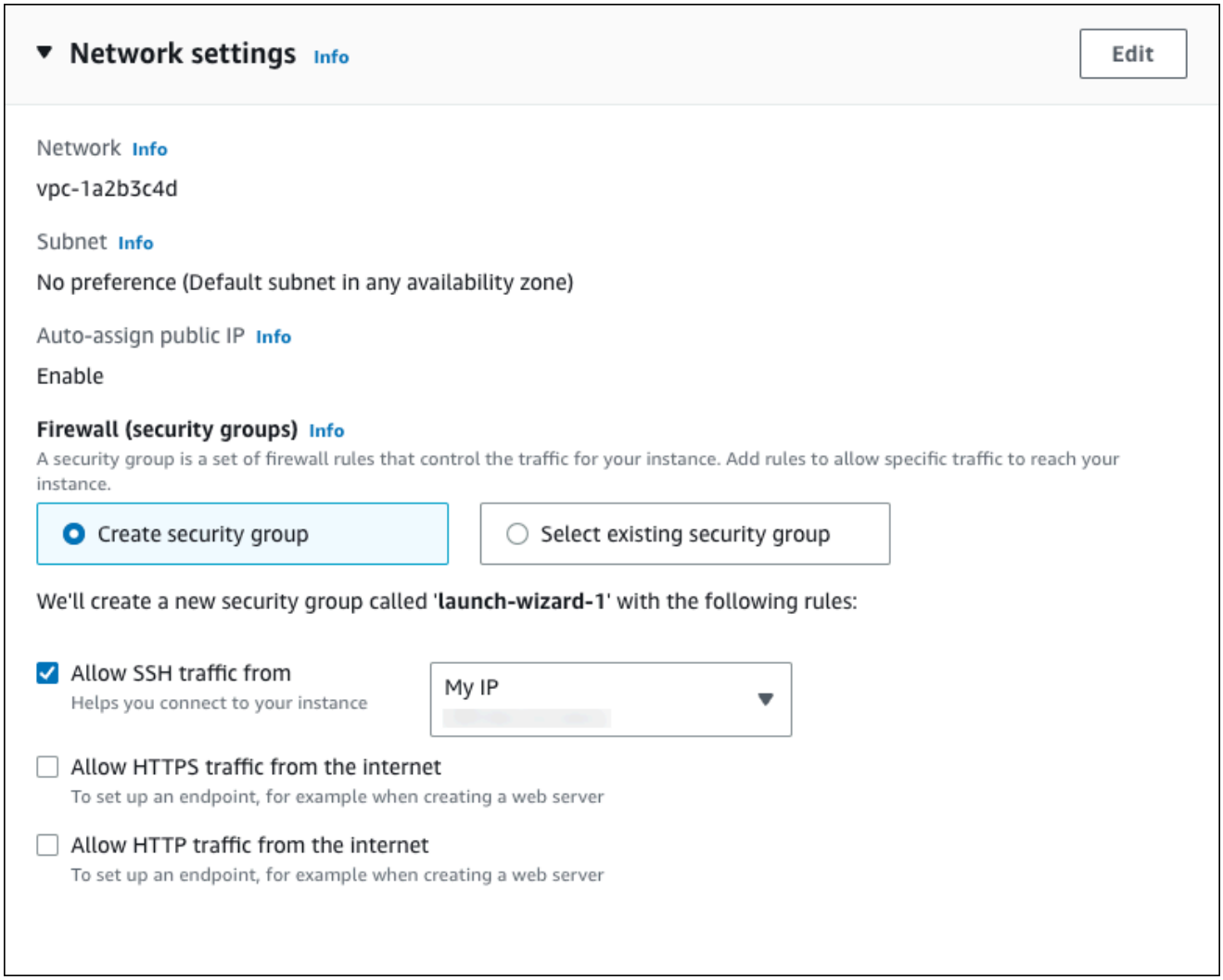
e. En Permitir tráfico de SSH en Configuraciones de red, elija el origen de las conexiones SSH a la instancia de EC2.

Puede elegir My IP (Mi IP) si la dirección IP que se muestra es correcta para las conexiones SSH. De lo contrario, puede determinar la dirección IP que usará para conectarse a las instancias de EC2 en su VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, asegúrese de identificar el rango de direcciones IP que utilizan los equipos cliente.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

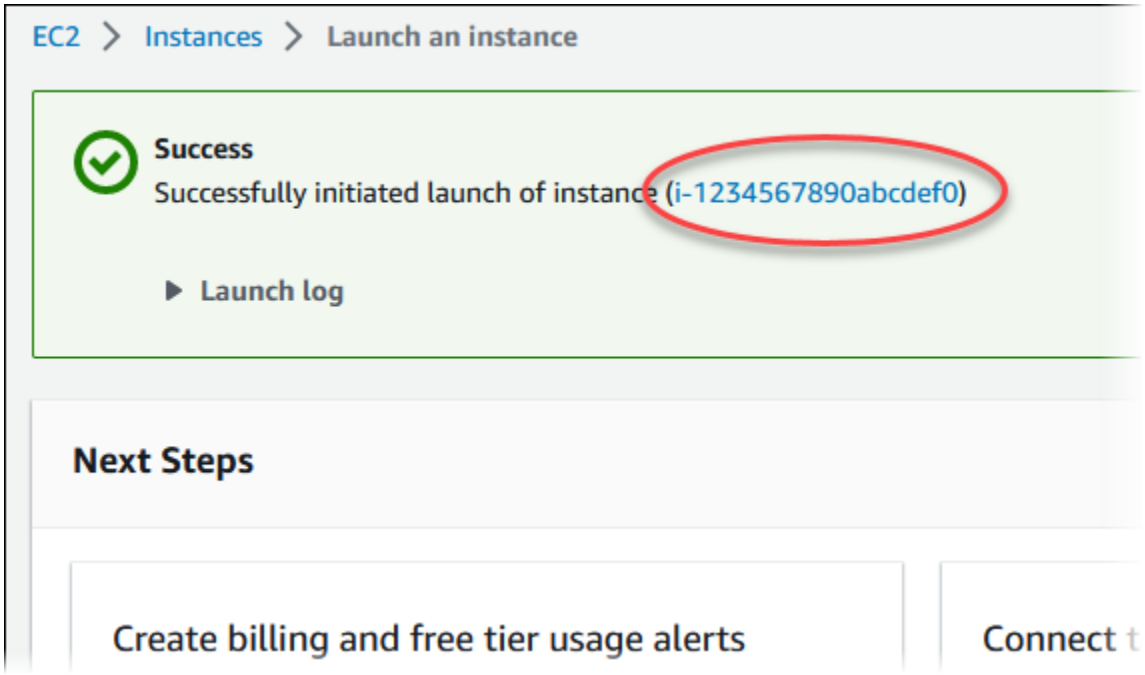
La siguiente imagen muestra un ejemplo de la sección Configuraciones de red.



f. No cambie los valores predeterminados del resto de las secciones.

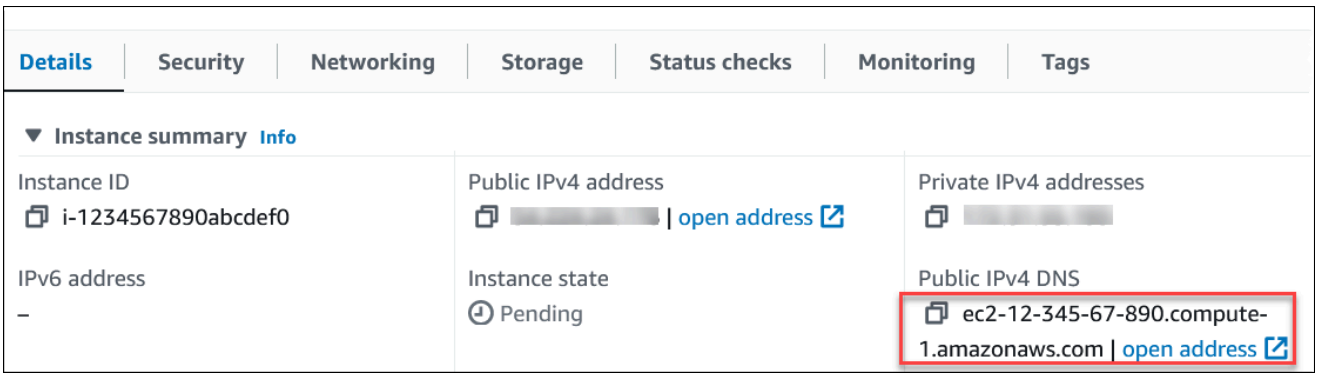
g. Revise un resumen de la configuración de su instancia de EC2 en el panel Resumen; cuando haya terminado, elija Lanzar instancia.

5. En la página Launch Status, que se muestra a continuación, anote el identificador de la nueva instancia de EC2, por ejemplo, `i-1234567890abcdef0`.

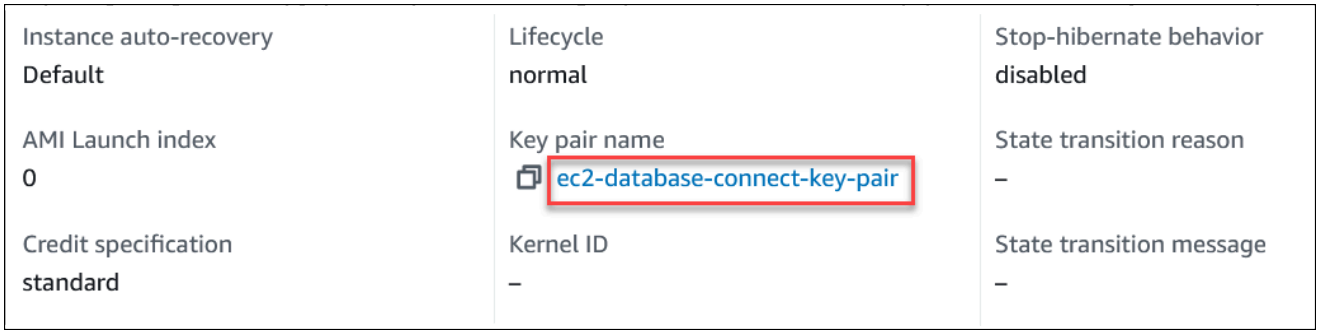


6. Elija el identificador de instancia de EC2 para abrir la lista de instancias de EC2 y, a continuación, seleccione su instancia de EC2.
7. En la pestaña Detalles, anote los siguientes valores, ya que los necesitará cuando se conecte mediante SSH:

   a. En Resumen de la instancia, anote el valor del DNS IPv4 público.



   b. En Detalles de la instancia, anote el valor de Nombre del par de claves.



8. Espere hasta que el Estado de la instancia de su instancia de EC2 tenga el estado En ejecución antes de continuar.

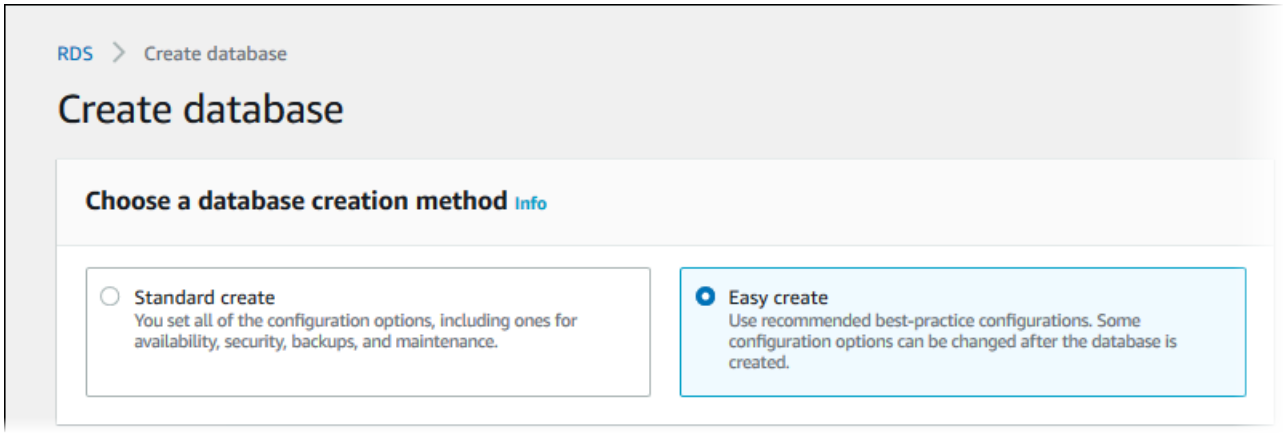
Creación de una instancia de base de datos de PostgreSQL

El componente básico de Amazon RDS es la instancia de base de datos. Este es el entorno en el que ejecuta las bases de datos PostgreSQL.

En este ejemplo, utilice la opción Creación sencilla para crear una instancia de base de datos que ejecuta el motor de la base de datos de PostgreSQL con una clase de instancia de base de datos db.t3.micro.

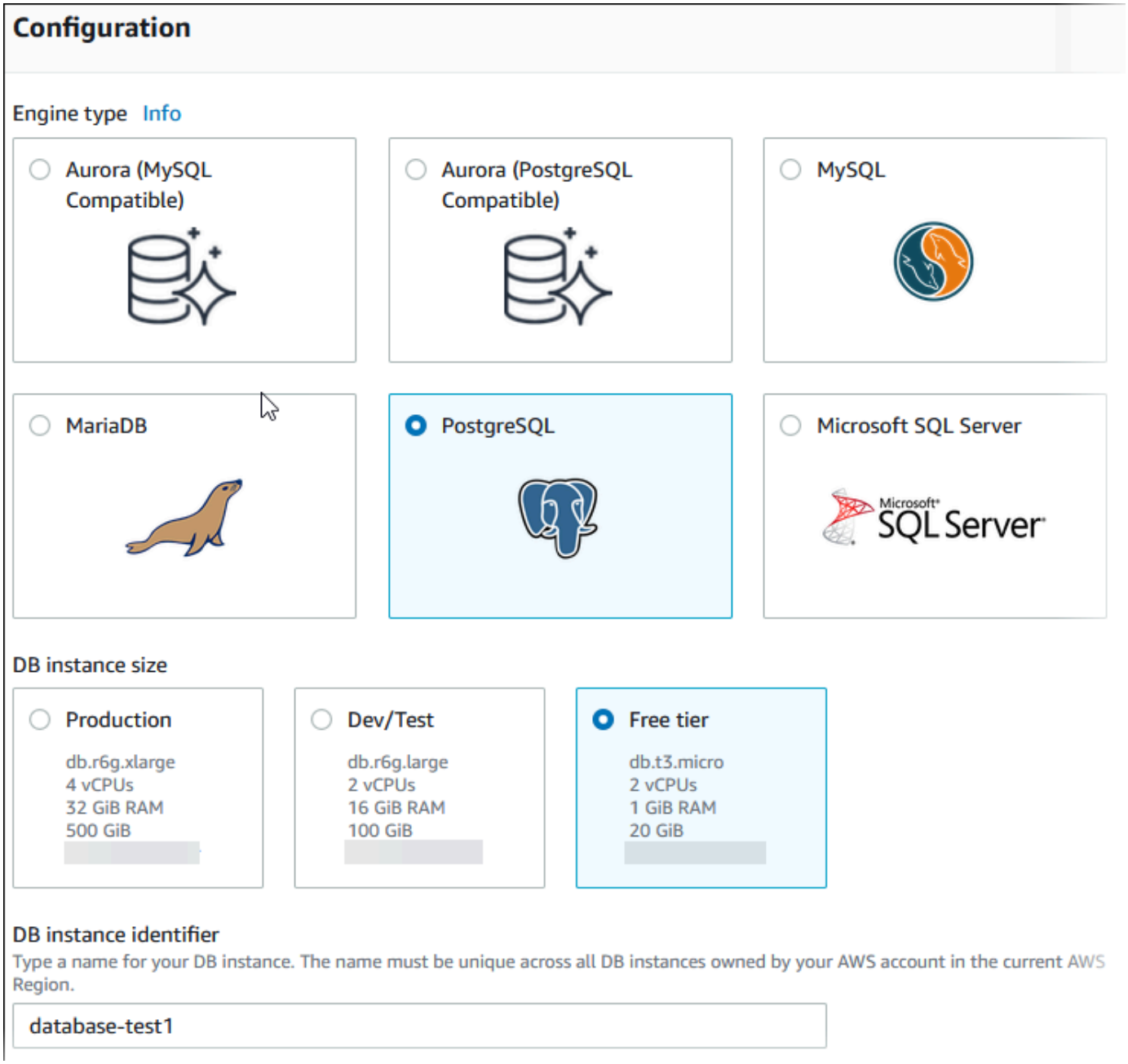
Para crear una instancia de base de datos de PostgreSQL con la opción Easy Create (Creación sencilla)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Seleccione Create database (Crear base de datos) y asegúrese de que la opción Easy Create (Creación sencilla) esté seleccionada.



5. En Configuration (Configuración), seleccione PostgreSQL.
6. En DB instance size (Tamaño de la instancia de base de datos), seleccione Free tier (Capa gratuita). El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.
7. En DB instance identifier (Identificador de instancia de base de datos), ingrese **`database-test1`**.
8. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro o deje el nombre predeterminado (**`postgres`**).

   La página Create database (Crear base de datos) debe ser similar a la siguiente imagen. Para las cuentas del plan gratuito, aparece Nivel gratuito. Para las cuentas de planes de pago, aparece Entorno de pruebas.

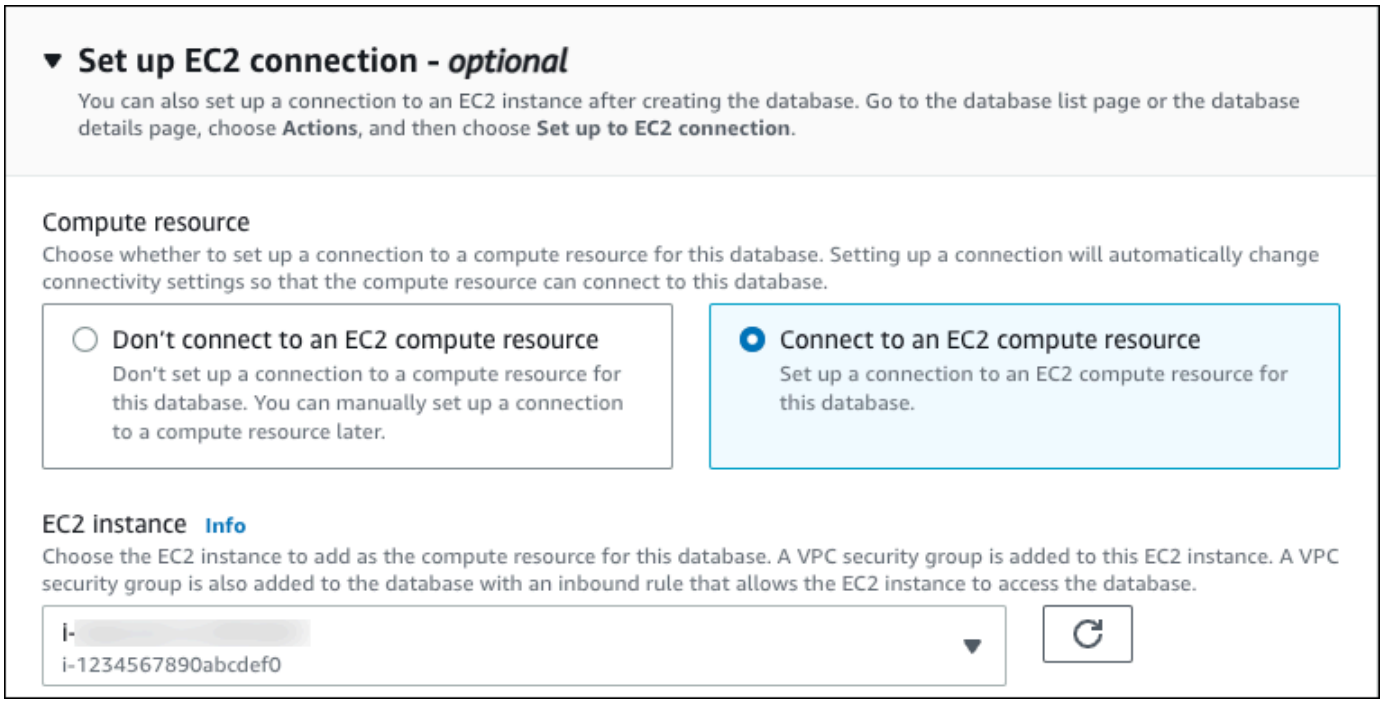


9. Para utilizar una contraseña maestra generada automáticamente para la instancia de base de datos, seleccione Generación automática de contraseña.

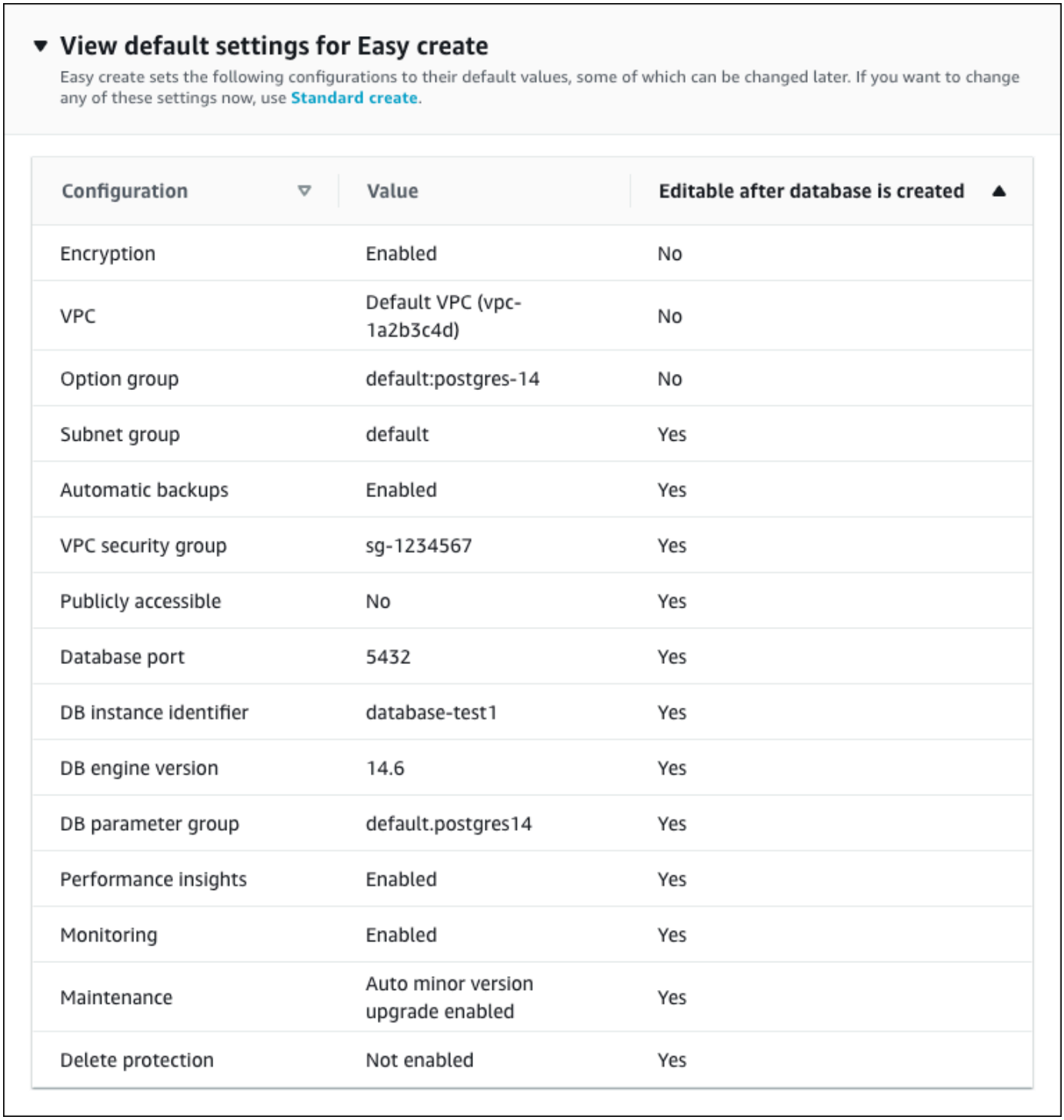
   Para introducir la contraseña maestra, asegúrese de desactivar la casilla Generación automática de contraseña y luego introduzca la misma contraseña en Contraseña maestra y Confirmar contraseña.

10. Para configurar una conexión con la instancia de EC2 que creó anteriormente, abra Configurar conexión a EC2 - (opcional).

Seleccione Conectarse a un recurso informático de EC2. Elija la instancia de EC2 que ha creado anteriormente.



11. Abra la opción Ver la configuración predeterminada de la creación sencilla.



View default settings for Easy create

Easy create sets the following configurations to their default values, some of which can be changed later. If you want to change any of these settings now, use **Standard create**.

Configuration	Value	Editable after database is created
Encryption	Enabled	No
VPC	Default VPC (vpc-1a2b3c4d)	No
Option group	default:postgres-14	No
Subnet group	default	Yes
Automatic backups	Enabled	Yes
VPC security group	sg-1234567	Yes
Publicly accessible	No	Yes
Database port	5432	Yes
DB instance identifier	database-test1	Yes
DB engine version	14.6	Yes
DB parameter group	default.postgres14	Yes
Performance insights	Enabled	Yes
Monitoring	Enabled	Yes
Maintenance	Auto minor version upgrade enabled	Yes
Delete protection	Not enabled	Yes

Puede examinar la configuración predeterminada utilizada con Easy create (Creación sencilla). La columna Editable después de crear la base de datos muestra las opciones que puede cambiar después de crear la base de datos.

- Si una configuración tiene No en esa columna y desea una configuración diferente, puede usar Creación estándar para crear la instancia de base de datos.
- Si una configuración tiene Sí en esa columna y desea una configuración diferente, puede utilizar Creación estándar para crear la instancia de base de datos o modificar la instancia de base de datos después de crearla para cambiar la configuración.

12. Elija Creación de base de datos.

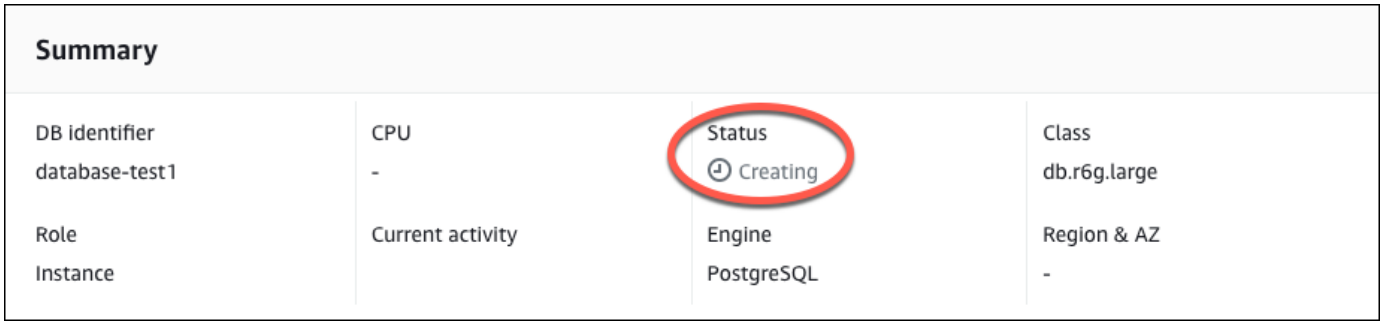
    Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales).

    Puede utilizar la contraseña y el nombre de usuario que aparecen para conectarse a la instancia de base de datos como el usuario maestro.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla.
    > Si tiene que cambiar la contraseña de usuario maestro después de que la instancia de base de datos esté disponible, puede modificar la instancia de base de datos para ello. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

13. En la lista Bases de datos, elija el nombre de la nueva instancia de base de datos de PostgreSQL para ver sus detalles.

    La instancia de base de datos tiene el estado Creando hasta que está lista para usarse.



    Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de la base de datos. Dependiendo de la clase de instancia de la base de datos y de la cantidad de almacenamiento, es posible que la nueva instancia tarde hasta 20 minutos en estar disponible.

(Opcional) Crear una VPC, una instancia EC2 y una instancia PostgreSQL mediante AWS CloudFormation

En lugar de utilizar la consola para crear la VPC, la instancia de EC2 y la instancia de PostgreSQL, puede utilizar AWS CloudFormation para aprovisionar recursos de AWS tratando la infraestructura como código. Para ayudarle a organizar sus recursos de AWS en unidades más pequeñas y fáciles de administrar, puede utilizar la funcionalidad de pila anidada de AWS CloudFormation. Para obtener más información, consulte Creación de una pila en la consola AWS CloudFormation y Uso de pilas anidadas.

> **Important**
>
> AWS CloudFormation es gratuito, pero los recursos que CloudFormation crea están activos. Se le facturan las tarifas de uso estándar por estos recursos hasta que los finalice. Para obtener más información, consulte Precios de RDS para PostgreSQL.

Para crear sus recursos con la consola AWS CloudFormation, siga estos pasos:

- Descargar la plantilla de CloudFormation
- Configurar los recursos mediante CloudFormation

Descargar la plantilla de CloudFormation

Una plantilla de CloudFormation es un archivo de texto con formato JSON o YAML que contiene la información de configuración de los recursos que desea crear en la pila. Esta plantilla también crea una VPC y un host bastión para usted junto con la instancia de RDS.

Para descargar el archivo de plantilla, abra el enlace PostgreSQL CloudFormation template.

En la página de Github, haga clic en el botón Descargar archivo sin procesar para guardar el archivo YAML de la plantilla.

Configurar los recursos mediante CloudFormation

> **Note**
>
> Antes de iniciar este proceso, asegúrese de tener un par de claves para una instancia EC2 en su Cuenta de AWS. Para obtener más información, consulte Pares de claves de Amazon EC2 e instancias Linux.

Al utilizar la plantilla de AWS CloudFormation, debe seleccionar los parámetros correctos para asegurarse de que los recursos se crean correctamente. Siga los pasos que se indican a continuación:

1. Inicie sesión en la AWS Management Console y abra la consola de AWS CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Elija Crear pila.
3. En la sección Especificar la plantilla, seleccione Cargar un archivo de plantilla desde el ordenador y Siguiente.
4. En la página Especificar detalles de la pila, introduzca los siguientes parámetros:
   a. Ponga el nombre de pila en PostgreSQLTestStack.
   b. En Parámetros, defina las zonas de disponibilidad seleccionando tres zonas de disponibilidad.
   c. En Configuración de host bastión de Linux, en Nombre de la clave, seleccione un par de claves para iniciar sesión en su instancia de EC2.
   d. En los ajustes de Configuración de host bastión de Linux, ponga el rango de IP permitido en su dirección IP. Para conectarse a las instancias de EC2 de su VPC mediante Secure Shell (SSH), determine su dirección IP pública mediante el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es 192.0.2.1/32.

> **Warning**
>
> Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias de EC2 públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección

IP específica o un intervalo de direcciones para acceder a sus instancias de EC2 mediante SSH.

e. En Configuración general de la base de datos, ponga la Clase de instancia de base de datos en db.t3.micro.

f. Ponga el Nombre de la base de datos en **`database-test1`**.

g. En Nombre de usuario maestro, introduzca un nombre para el usuario maestro.

h. Ponga Administrar contraseña de usuario maestro de base de datos con Secrets Manager en `false` para este tutorial.

i. En Contraseña de base de datos, ponga la contraseña que desee. Recuerde esta contraseña para poder ver los pasos adicionales del tutorial.

j. En Configuración de almacenamiento de base de datos, ponga el Tipo de almacenamiento de base de datos en gp2.

k. En la Configuración de supervisión de base de datos, ponga Habilitar RDS Performance Insights en falso.

l. Deje el resto de la configuración con los valores predeterminados. Haga clic en Siguiente para continuar.

5. En la página Configurar opciones de pila, deje todas las opciones predeterminadas. Haga clic en Siguiente para continuar.
6. En la página Revisar la pila, seleccione Enviar después de comprobar las opciones de base de datos y de host bastión de Linux.

Una vez finalizado el proceso de creación de la pila, visualice las pilas con los nombres BastionStack y RDSNS para anotar la información que necesita para conectarse a la base de datos. Para obtener más información, consulte Viewing AWS CloudFormation stack data and resources on the AWS Management Console.

Conexión a la instancia de base de datos PostgreSQL

Puede conectarse a la instancia de base de datos mediante pgadmin o psql. En este ejemplo, se explica cómo conectarse a una instancia de base de datos de PostgreSQL mediante el cliente de línea de comandos psql.

Para conectarse a una instancia de base de datos de PostgreSQL mediante psql

1. Busque el punto de enlace (nombre de DNS) y el número de puerto de la instancia de base de datos.

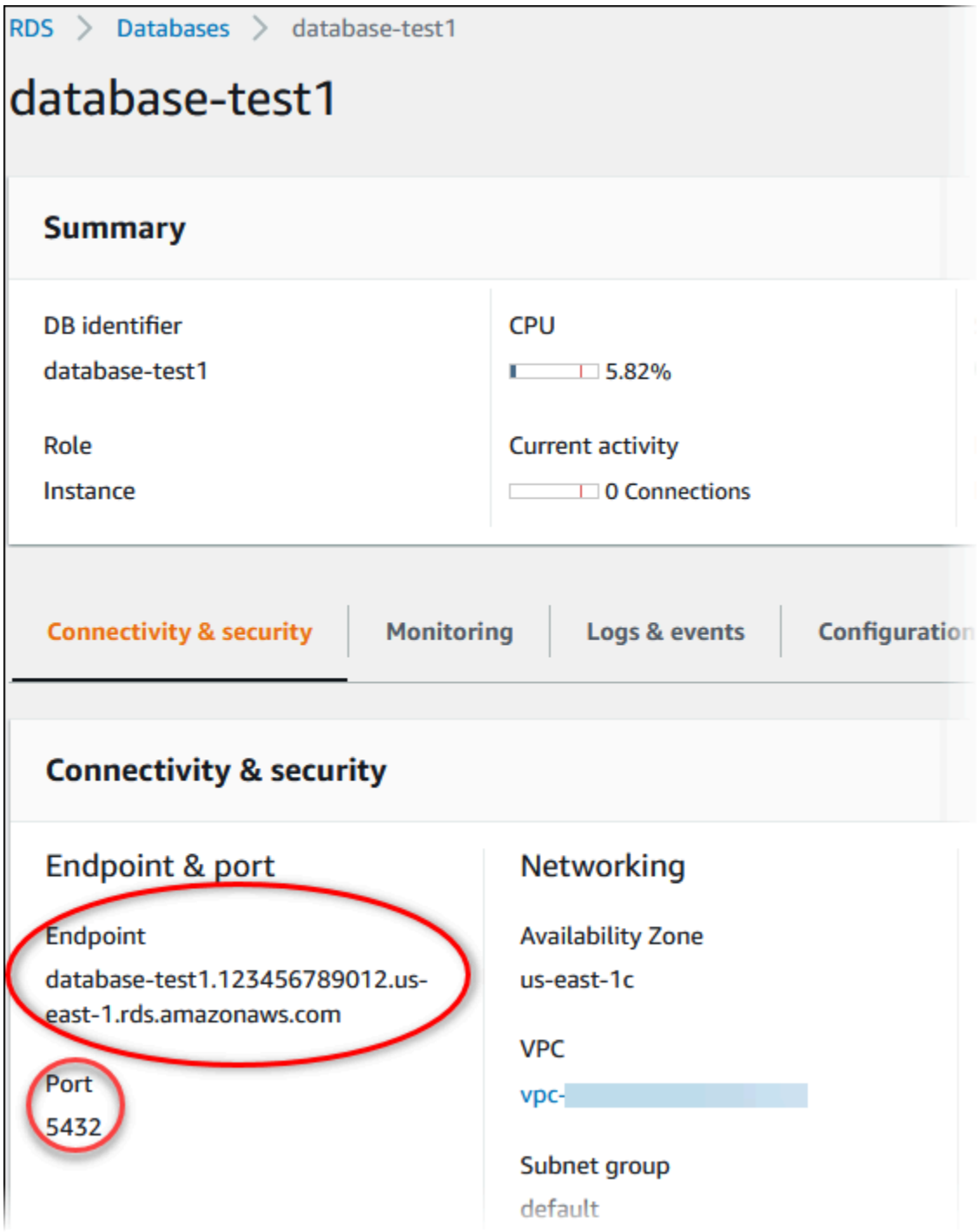
   a. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

   b. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS de la instancia de base de datos.

   c. En el panel de navegación, elija Databases (Bases de datos).

   d. Seleccione el nombre de la instancia de base de datos de PostgreSQL para mostrar sus detalles.

   e. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



2. Conéctese a la instancia de EC2 que ha creado anteriormente siguiendo los pasos que se indican en Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2.

   Le recomendamos que se conecte a la instancia de EC2 mediante SSH. Si la utilidad de cliente SSH está instalada en Windows, Linux o Mac, puede conectarse a la instancia con el siguiente formato de comando:

```
ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
```

Por ejemplo, suponga que `ec2-database-connect-key-pair.pem` está almacenado en `/dir1` en Linux y que el DNS IPv4 público de su instancia de EC2 es `ec2-12-345-678-90.compute-1.amazonaws.com`. Su comando SSH tendría el siguiente aspecto:

```
ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
user@ec2-12-345-678-90.compute-1.amazonaws.com
```

3. Obtenga las correcciones de errores y las actualizaciones de seguridad más recientes actualizando el software en su instancia de EC2. Para ello, utilice el siguiente comando.

> **Note**
>
> La opción `-y` instala las actualizaciones sin necesidad de confirmación. Para examinar las actualizaciones antes de la instalación, omita esta opción.

```
sudo dnf update -y
```

4. Para instalar el cliente de línea de comandos psql desde PostgreSQL en Amazon Linux 2023, ejecute el siguiente comando:

```
sudo dnf install postgresql15
```

5. Conéctese a la instancia de base de datos de PostgreSQL. Por ejemplo, escriba el siguiente comando en el símbolo del sistema de un equipo cliente. Esta acción le permite conectarse a la instancia de base de datos de PostgreSQL mediante el cliente psql.

   Sustituya el punto de conexión de la instancia de base de datos (nombre DNS) por *`endpoint`*, sustituya el nombre de la base de datos `--dbname` a la que quiera conectarse por *`postgres`* y sustituya el nombre de usuario maestro que utilizó por *`postgres`*. Proporcione la contraseña maestra que utilizó cuando se le solicite una contraseña.

```
psql --host=endpoint --port=5432 --dbname=postgres --username=postgres
```

Una vez especificada la contraseña del usuario, debería ver un resultado similar al siguiente:

```
psql (14.3, server 14.6)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256,
 compression: off)
Type "help" for help.

postgres=>
```

Para obtener más información acerca de cómo conectarse a la instancia de base de datos de PostgreSQL, consulte Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL. Si no puede conectarse a la instancia de base de datos, consulte Solución de problemas de conexiones a la instancia de RDS for PostgreSQL.

Por motivos de seguridad, se recomienda utilizar conexiones cifradas. Utilice solo una conexión PostgreSQL sin cifrar cuando el cliente y el servidor están en la misma VPC y la red es de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte Conectar con una instancia de base de datos PostgreSQL a través de SSL.

6. Ejecutar comandos SQL.

   Por ejemplo, el siguiente comando de SQL muestra la fecha y la hora actuales:

   ```
   SELECT CURRENT_TIMESTAMP;
   ```

Eliminación de la instancia de EC2 y la instancia de base de datos

Después de conectarse y explorar la instancia de EC2 de muestra y la instancia de base de datos que creó, elimínelas para que no le sigan cobrando por ellas.

Si ha utilizado AWS CloudFormation para crear recursos, omita este paso y vaya al siguiente.

Para eliminar la instancia de EC2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia de EC2 y elija Estado de la instancia y Terminar instancia.

4. Cuando se le indique que confirme, elija Terminar.

Para obtener más información sobre la eliminación de una instancia de EC2, consulte Terminar la instancia en la Guía del usuario de Amazon EC2.

Para eliminar una instancia de base de datos sin instantánea de base de datos final

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. Desactive Crear la instantánea final y Conservar copias de seguridad automatizadas.
6. Complete la confirmación y seleccione Eliminar.

(Opcional) Eliminar la instancia de EC2 y la instancia de base de datos creadas con CloudFormation

Si ha utilizado AWS CloudFormation para crear recursos, elimine la pila de CloudFormation después de conectarse a la instancia de EC2 y a la instancia de base de datos de muestra y de explorarlas; de este modo, ya no se le cobrará por ellas.

Para eliminar los recursos de CloudFormation

1. Abra la consola de AWS CloudFormation.
2. En la página Pilas de la consola de CloudFormation, seleccione la pila raíz (la pila sin el nombre VPCStack, BastionStack o RDSNS).
3. Elija Eliminar.
4. Cuando se le pida confirmación, seleccione Eliminar pila.

Para obtener información sobre cómo eliminar una pila en CloudFormation, consulte Eliminación de una pila en la consola de AWS CloudFormation, en la Guía del usuario de AWS CloudFormation.

(Opcional) Conecte la instancia de base de datos a una función de Lambda

También puede conectar la instancia de base de datos de RDS para PostgreSQL a un recurso de computación sin servidor de Lambda. Las funciones de Lambda permiten ejecutar código sin aprovisionar ni administrar la infraestructura. Una función de Lambda también permite responder automáticamente a las solicitudes de ejecución de código a cualquier escala, desde una docena de eventos al día hasta cientos de eventos por segundo. Para obtener más información, consulte Conexión automática de una función de Lambda y una instancia de base de datos.

Explicación: crear un servidor web y una instancia de base de datos de Amazon RDS

Este tutorial le ayuda a instalar un servidor web Apache con PHP y a crear una base de datos de MariaDB, MySQL o PostgreSQL. El servidor web se ejecuta en una instancia de Amazon EC2 mediante Amazon Linux 2023 y puede elegir entre una instancia de base de datos de MySQL o PostgreSQL. Tanto la instancia de Amazon EC2 como la instancia de base de datos se ejecutan en una nube virtual privada (VPC) basada en el servicio Amazon VPC.

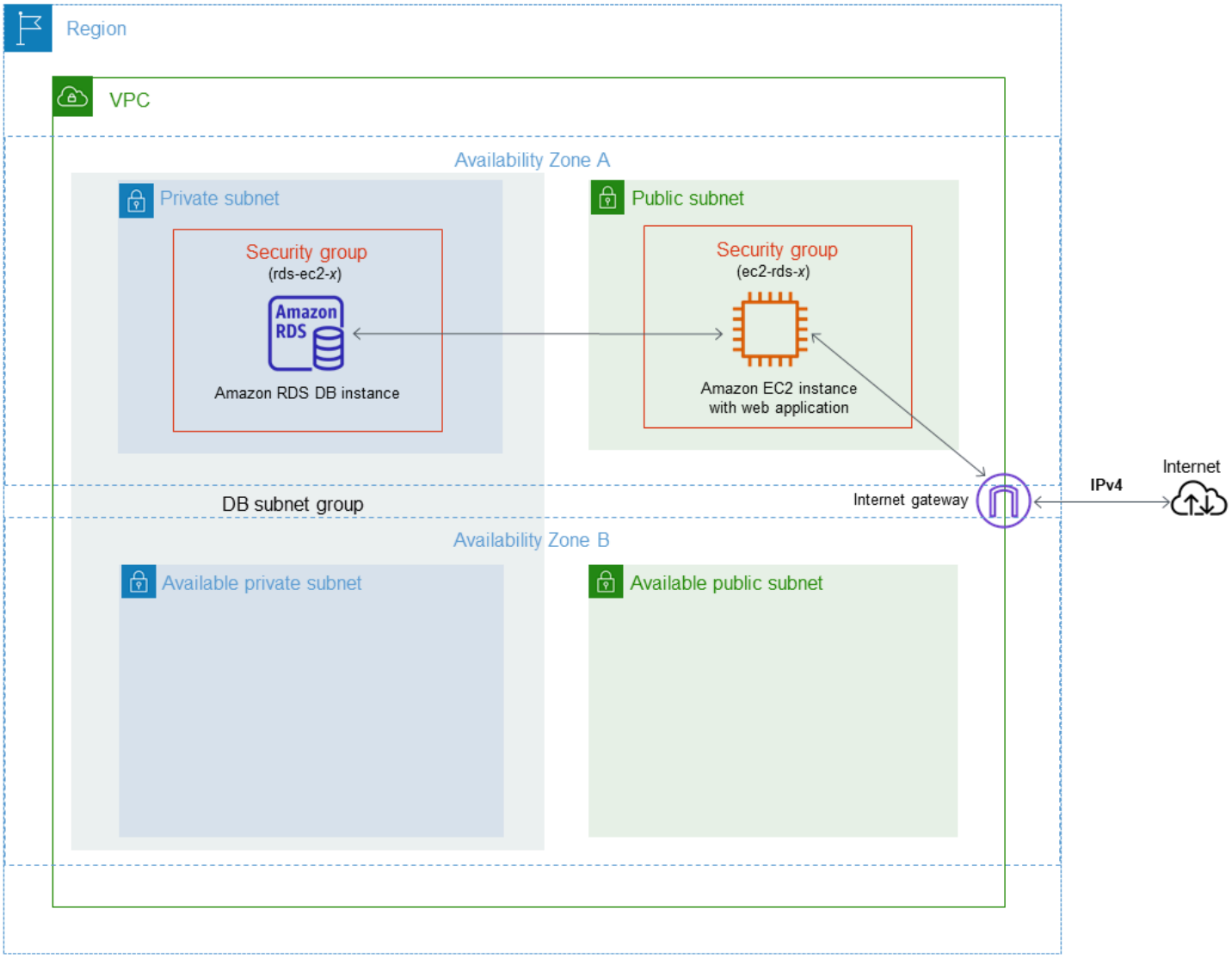
> **Important**
>
> La creación de una cuenta de AWS no supone ningún costo. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de AWS que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

> **Note**
>
> Este tutorial funciona con Amazon Linux 2023 y podría no funcionar con otras versiones de Linux.

En la siguiente explicación, cree una instancia EC2 que utilice la VPC, subredes y el grupo de seguridad predeterminados para la Cuenta de AWS. En este tutorial, se muestra cómo crear la instancia de base de datos y configurar automáticamente la conectividad con la instancia EC2 que creó. A continuación, el tutorial muestra cómo instalar el servidor web en la instancia EC2. Conecte el servidor web a su instancia de base de datos en la VPC con el punto de conexión del escritor de instancia de base de datos.

1. Lanzamiento de una instancia EC2 para conectarse con la instancia de base de datos
2. Crear una instancia de base de datos de Amazon RDS
3. Instalación de un servidor web en la instancia de EC2

El siguiente diagrama muestra la configuración cuando el tutorial se completa.



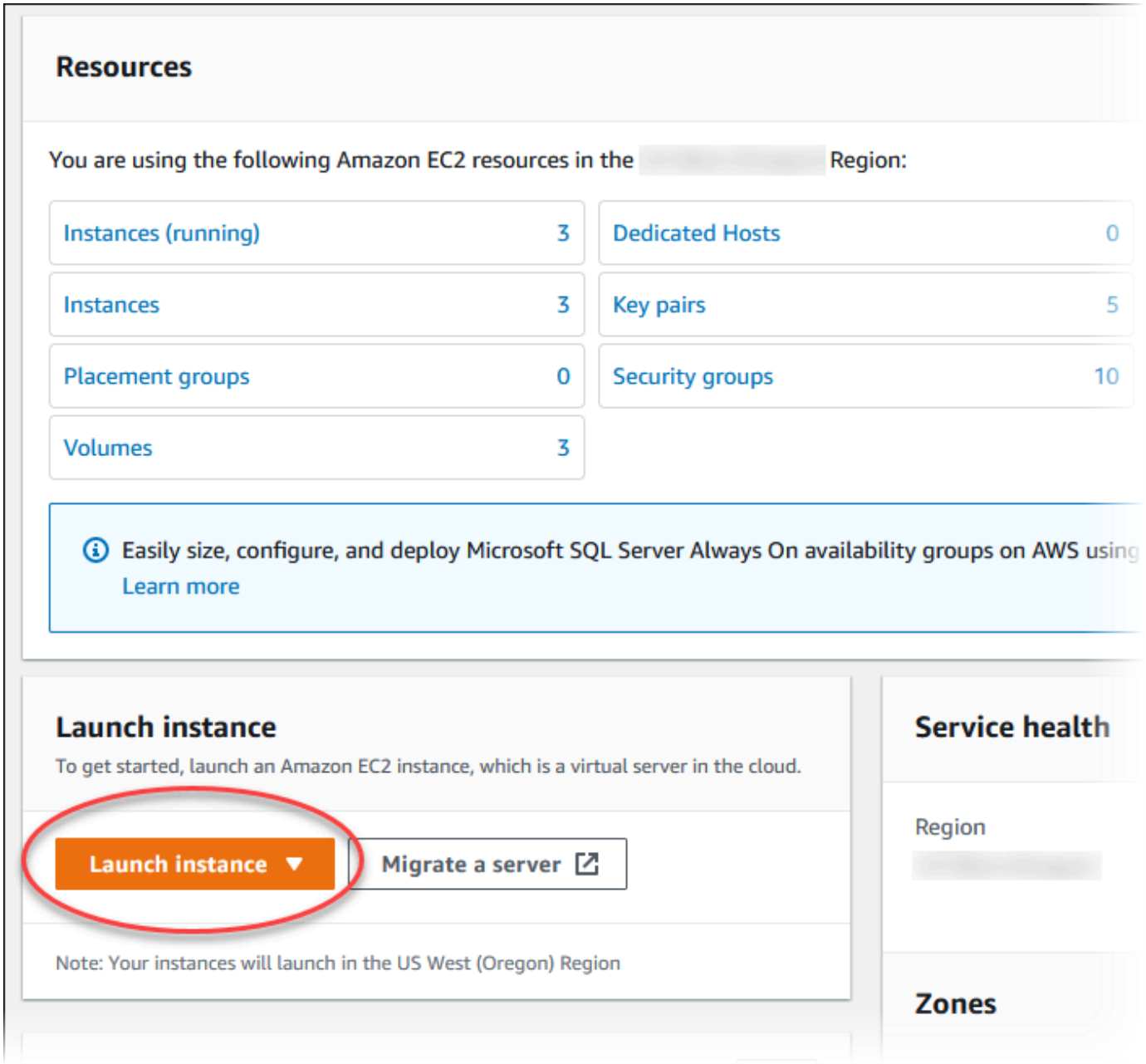
> **Note**
>
> Tras completar el tutorial, habrá una subred pública y una privada en cada zona de disponibilidad de la VPC. En este tutorial, se usa la VPC predeterminada para Cuenta de AWS que configura de forma automática la conectividad entre la instancia EC2 y la instancia de base de datos. Si prefiere configurar una nueva VPC para este escenario, complete las tareas de Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).

Lanzamiento de una instancia EC2 para conectarse con la instancia de base de datos

Cree una instancia Amazon EC2 en la subred pública de la VPC.

Para lanzar una instancia de EC2

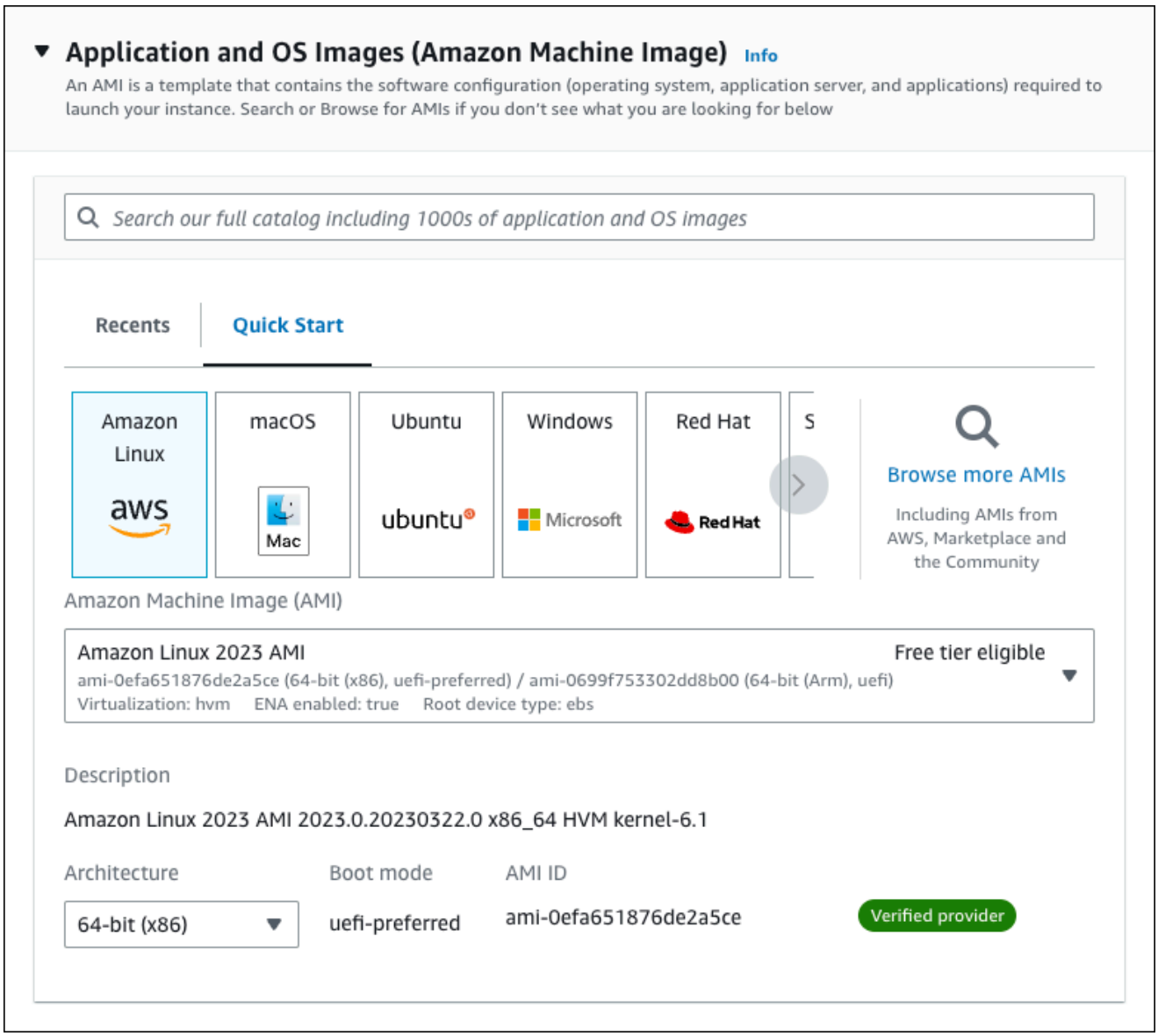
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS en la que desea crear la instancia de EC2.
3. Elija Panel de EC2 y, a continuación, Lanzar instancia, como se muestra a continuación.



4. Elija los siguientes ajustes en la página Lanzar una instancia.

   a. En Name and tags (Nombre y etiquetas), en Name (Nombre), introduzca **`tutorial-ec2-instance-web-server`**.

   b. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija Amazon Linux y, a continuación, AMI de Amazon Linux 2023. Mantenga los valores predeterminados para las demás opciones.



c. En Instance type (Tipo de instancia), elija t2.micro.

d. En Key pair (login) [Par de claves (inicio)], elija Key pair name (Nombre de par de claves) para utilizar un par de claves existente. Para crear un nuevo par de claves para la instancia de Amazon EC2, que se muestra a continuación, elija Create new key pair (Crear nuevo par de claves) y, a continuación, utilice la ventana Create key pair (Crear un par de claves).

   Para obtener más información sobre la creación de un nuevo par de claves, consulte Crear un par de claves en la Guía del usuario de Amazon EC2.

e. En Network settings (Configuración de red), defina estos valores y mantenga los ajustes predeterminados en los otros valores:

- En Allow SSH traffic from (Permitir el tráfico SSH desde), elija el origen de las conexiones SSH a la instancia de EC2.

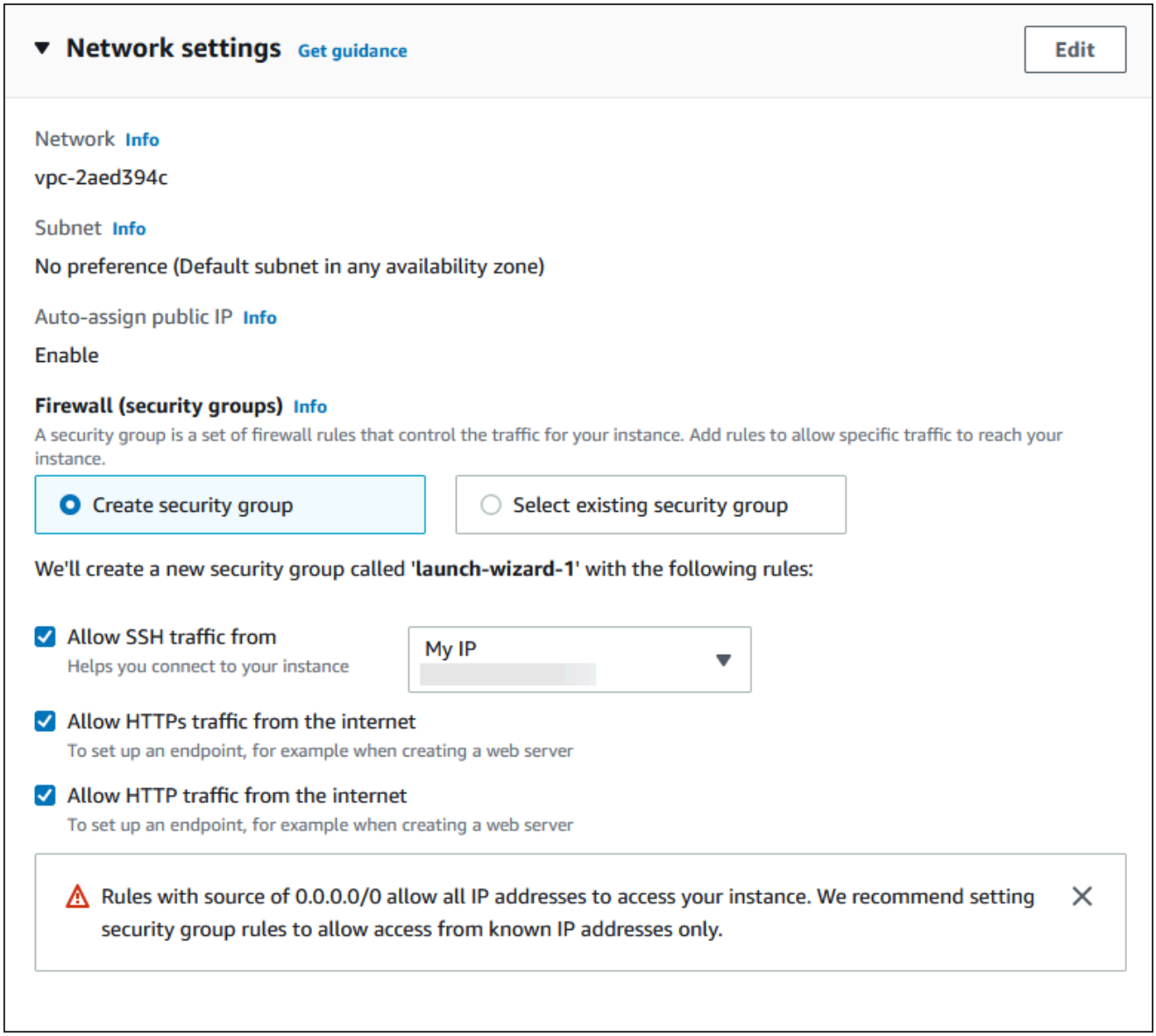
  Puede elegir My IP (Mi IP) si la dirección IP que se muestra es correcta para las conexiones SSH.

  De lo contrario, puede determinar la dirección IP que usará para conectarse a las instancias de EC2 en su VPC mediante Secure Shell (SSH). Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es `203.0.113.25/32`.

  En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, asegúrese de identificar el rango de direcciones IP que utilizan los equipos cliente.

  > **Warning**
  >
  > Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias mediante SSH.

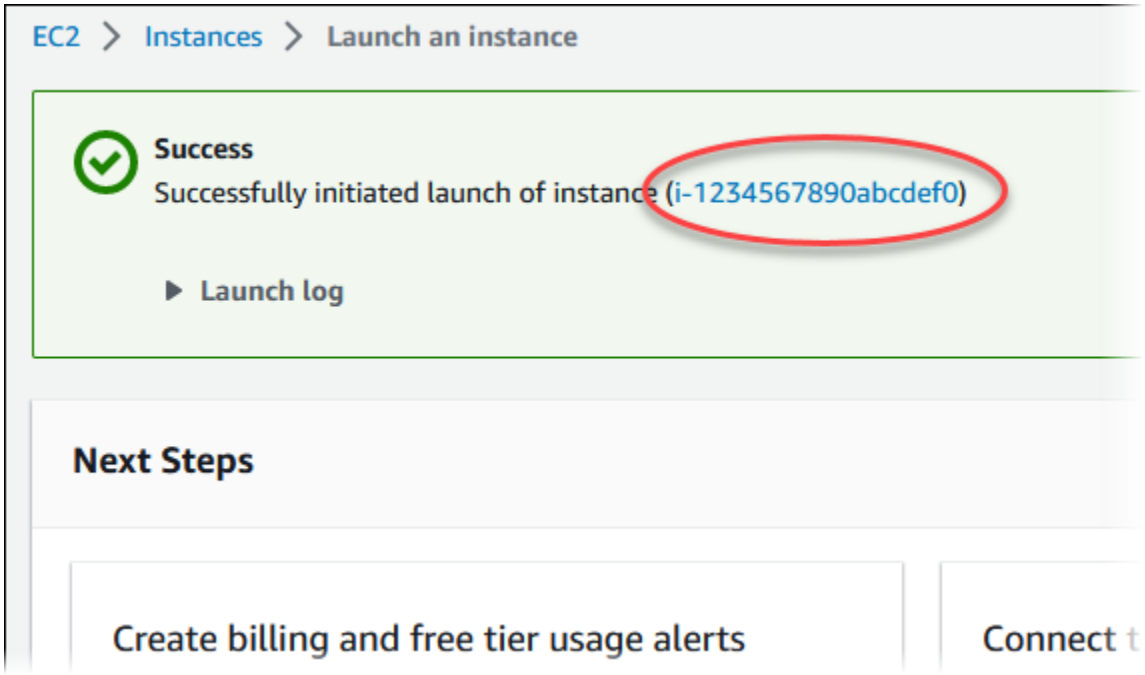
- Active Allow HTTPs traffic from the internet (Permitir el tráfico HTTP desde internet).
- Active Allow HTTPs traffic from the internet (Permitir el tráfico HTTP desde internet).



f. No cambie los valores predeterminados del resto de las secciones.

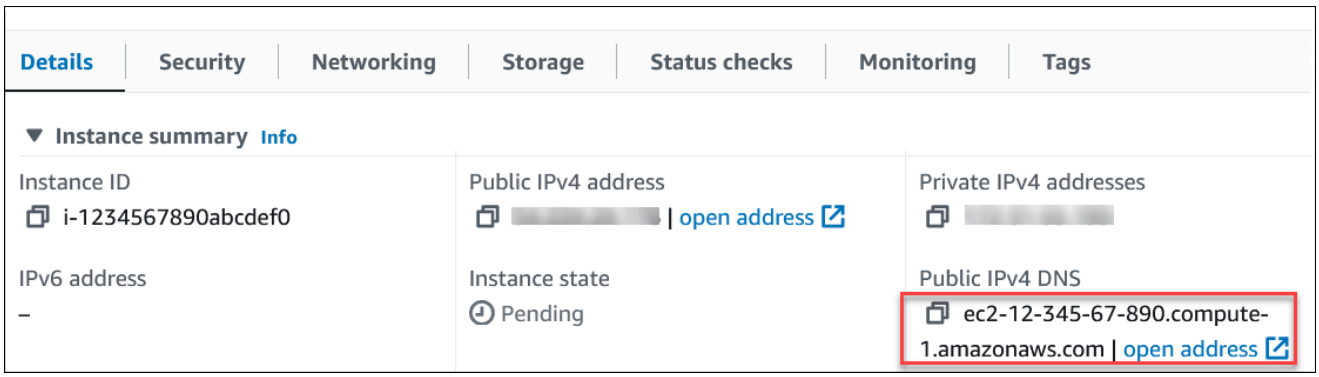
g. Revise un resumen de la configuración de su instancia en el panel Summary (Resumen); cuando haya terminado, elija Launch instance.

5. En la página Launch Status, que se muestra a continuación, anote el identificador de la nueva instancia de EC2, por ejemplo, `i-1234567890abcdef0`.

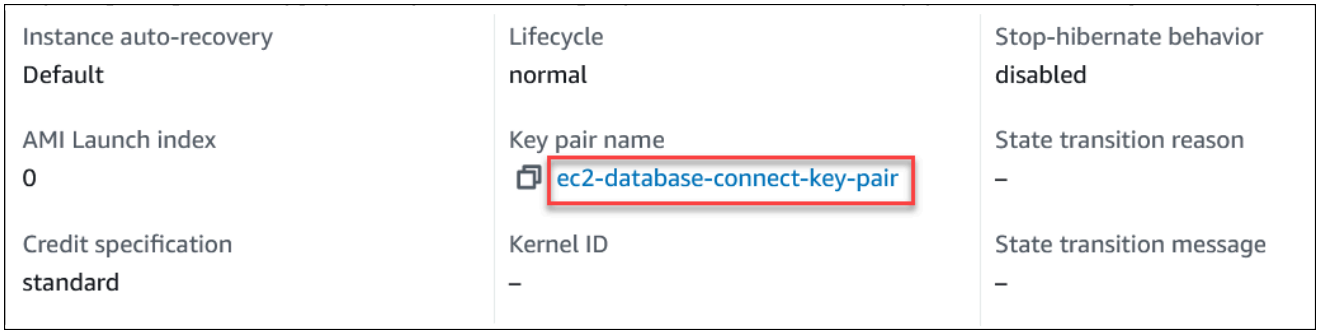


6. Elija el identificador de instancia de EC2 para abrir la lista de instancias de EC2 y, a continuación, seleccione su instancia de EC2.
7. En la pestaña Detalles, anote los siguientes valores, ya que los necesitará cuando se conecte mediante SSH:

   a. En Resumen de la instancia, anote el valor del DNS IPv4 público.



   b. En Detalles de la instancia, anote el valor de Nombre del par de claves.



8. Espere a que Instance Status (Estado de la instancia) se muestre como Running (En ejecución) antes de continuar.
9. Complete la Crear una instancia de base de datos de Amazon RDS.

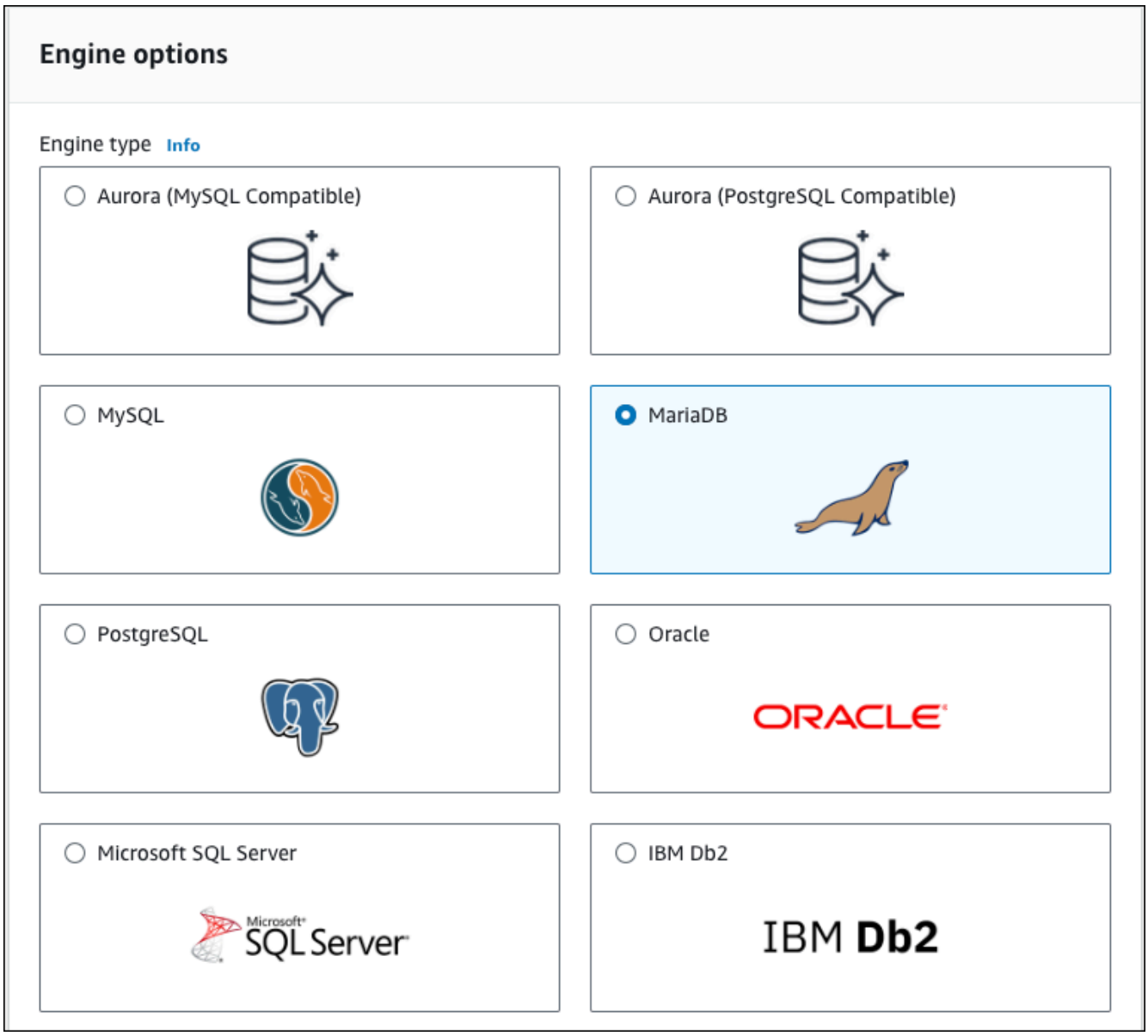
Crear una instancia de base de datos de Amazon RDS

Cree una instancia de base de datos de RDS para MariaDB, RDS para MySQL o RDS para PostgreSQL que conserve los datos utilizados por una aplicación web.

RDS for MariaDB

Para crear una instancia de MariaDB

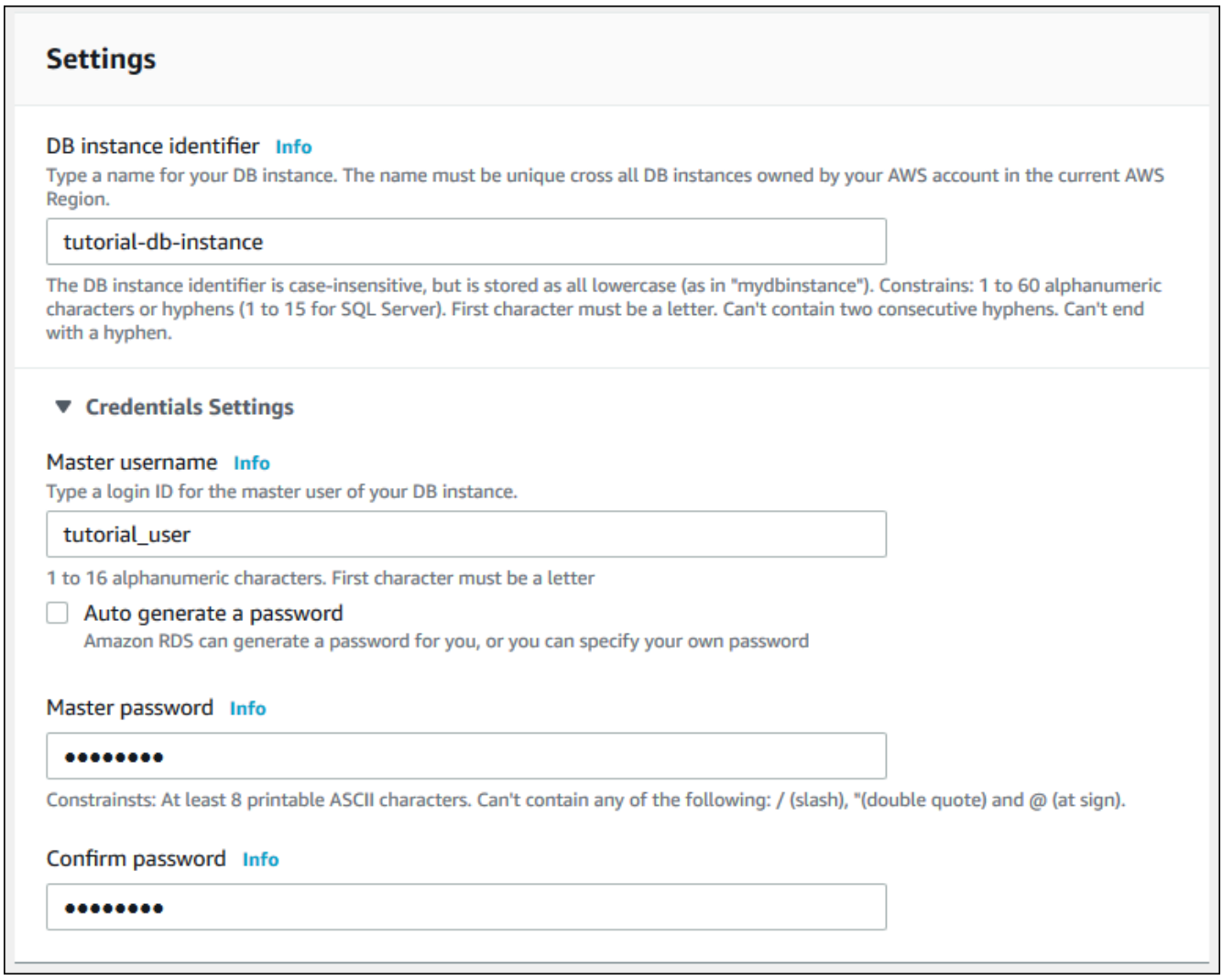
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la AWS Management Console, marque la Región de AWS. Debería ser la misma que en la que creó su instancia de EC2.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija Create database (Creación de base de datos).
5. En la página Crear base de datos, elija Creación estándar.
6. En Opciones del motor, elija MariaDB.



7. Para Plantillas, elija Nivel gratuito o Entorno de pruebas. El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.

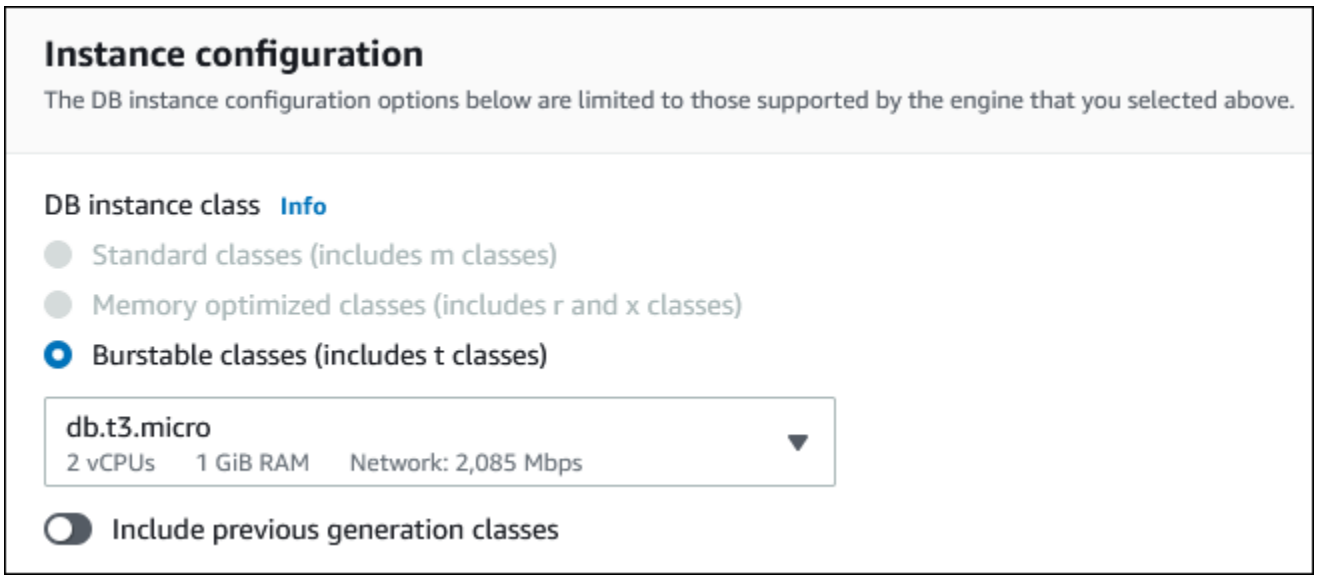


8. En la sección Availability and durability (Disponibilidad y durabilidad), mantenga los valores predeterminados.
9. En la sección Settings (Configuración), establezca los siguientes valores:
   - DB Instance Identifier (Identificador de instancias de bases de datos): **`tutorial-db-instance`**.
   - Master username (Nombre de usuario maestro): escriba **`tutorial_user`**.
   - Auto generate a password (Generar una contraseña de forma automática): deje la opción desactivada.
   - Master password (Contraseña maestra): escriba una contraseña.
   - Confirm password (Confirmar contraseña):– vuelva a introducir la contraseña.



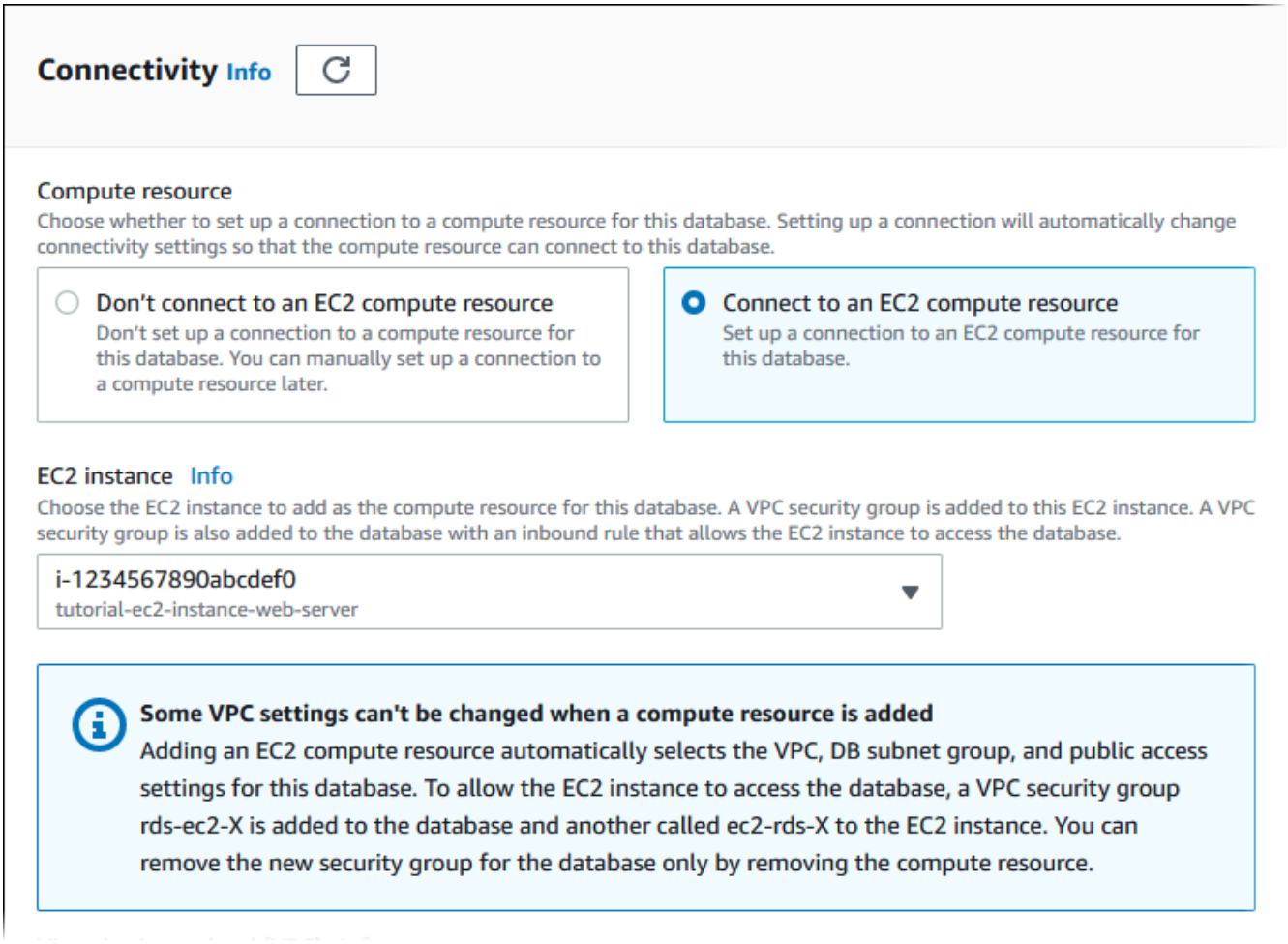
10. En la sección Instance configuration (Configuración de instancia), establezca estos valores:

    - Clases por ráfagas (incluye clases t)
    - db.t3.micro



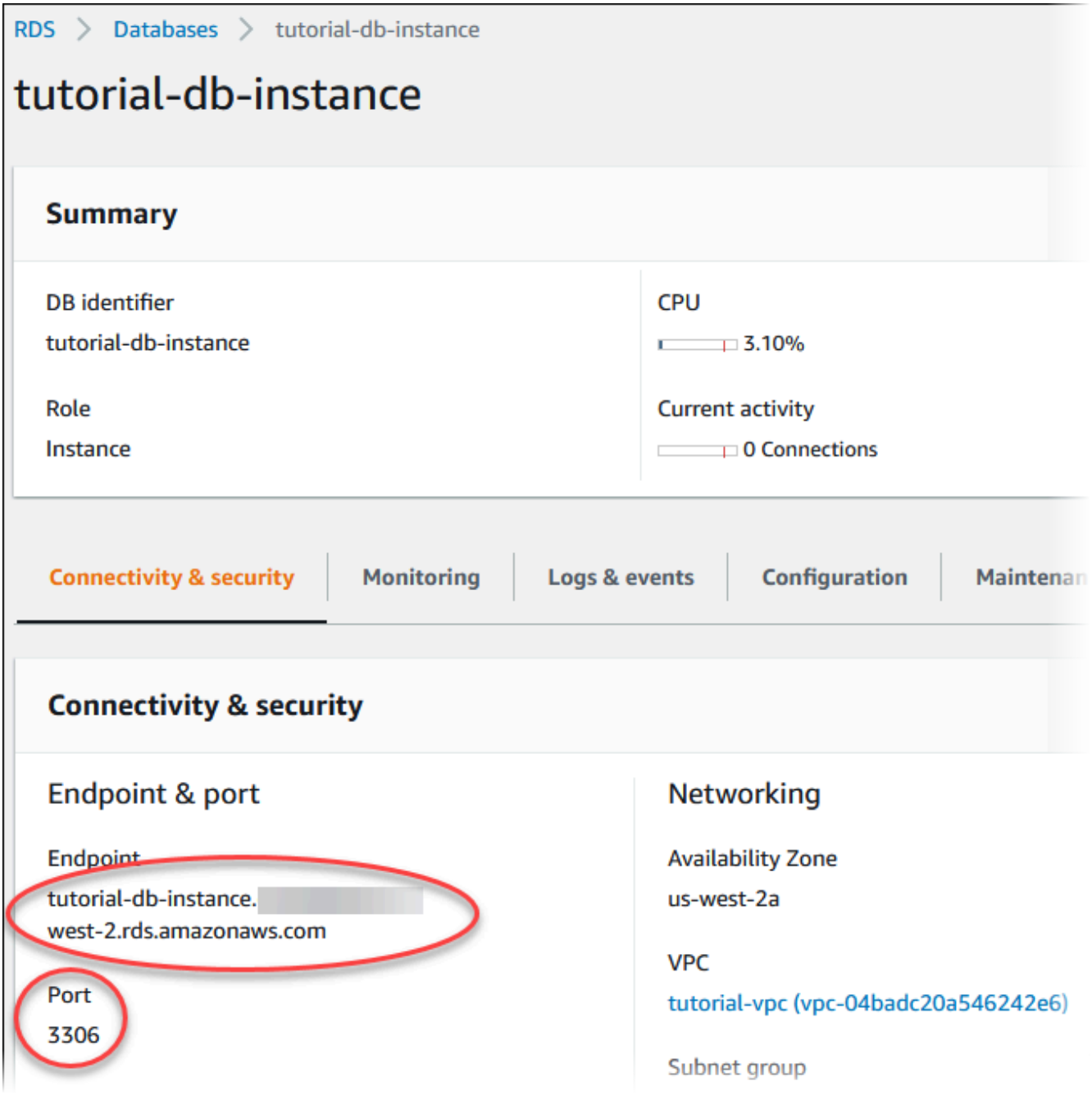
11. En la sección Storage (Almacenamiento), mantenga la configuración predeterminada.
12. En la sección Connectivity (Conectividad), defina estos valores y mantenga los demás con sus valores predeterminados:

    - En Compute resource (Recurso informático), elija Connect to an EC2 compute resource (Conectar a un recurso informático de EC2).
    - En EC2 instance (Instancia EC2), elija la instancia de EC2 que creó anteriormente, como tutorial-ec2-instance-web-server.



13. En la sección Autenticación de base de datos, asegúrese de que la Autenticación con contraseña está seleccionada.
14. Abra la sección Additional configuration (Configuración adicional) e introduzca **`sample`** para Initial database name (Nombre de la base de datos inicial) Mantenga la configuración predeterminada para el resto de las opciones.
15. Para crear una instancia de MariaDB, elija Crear base de datos.

    Su nueva instancia de base de datos aparece en la lista Databases (Bases de datos) con el estado Creating (Creándose).
16. Espere a que el Status (Estado) de su nueva instancia de base de datos se muestre como Available (Disponible). A continuación, seleccione el nombre de la instancia de base de datos para mostrar sus detalles.
17. En la sección Connectivity & security (Conectividad y seguridad) vea el Endpoint (Punto de enlace) y el Port (Puerto) de la instancia de base de datos.



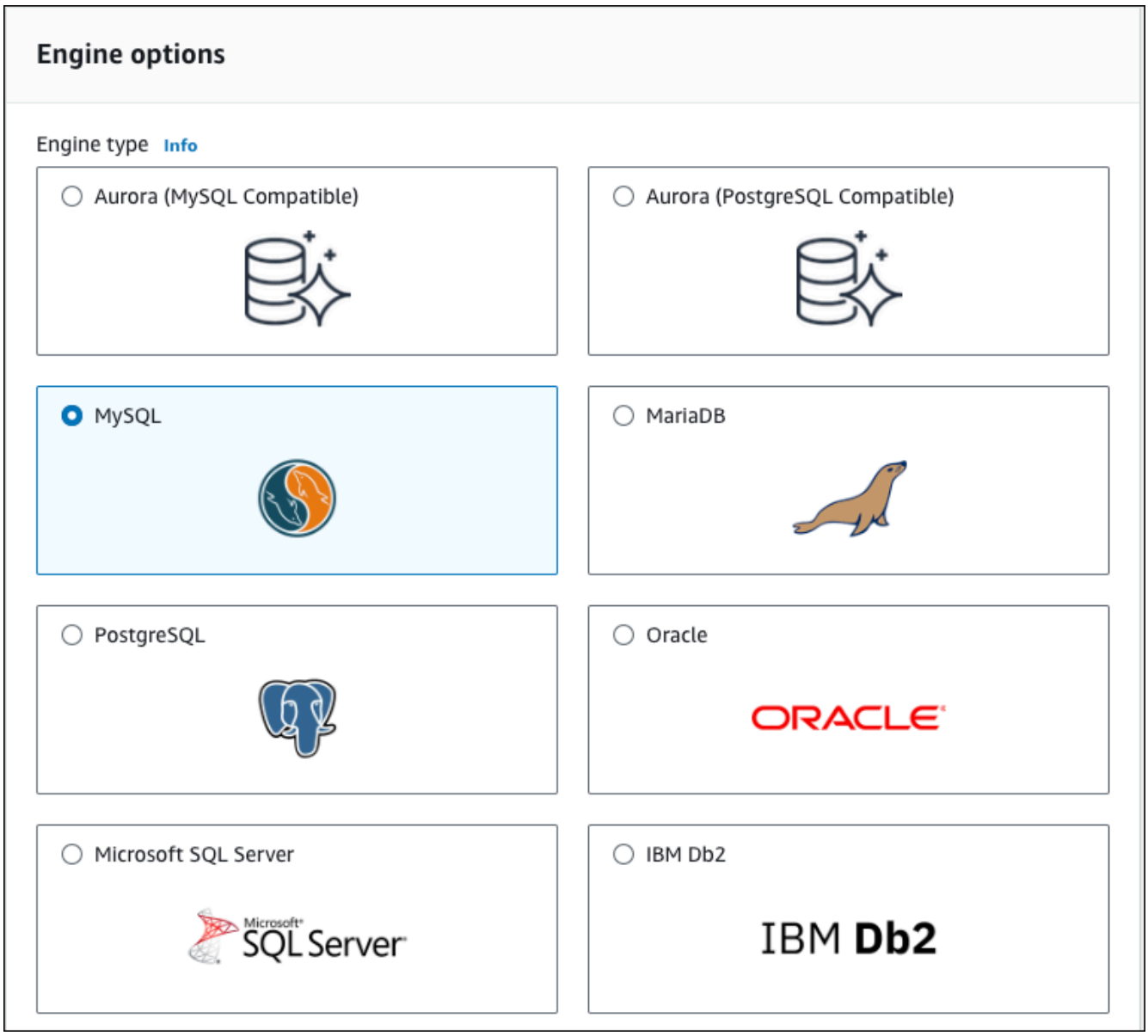
Anote el punto de enlace y el puerto de la instancia de base de datos. Utiliza esta información para conectar su servidor web a la instancia de base de datos.

18. complet Instalación de un servidor web en la instancia de EC2.

RDS for MySQL

Para crear una instancia de base de datos MySQL

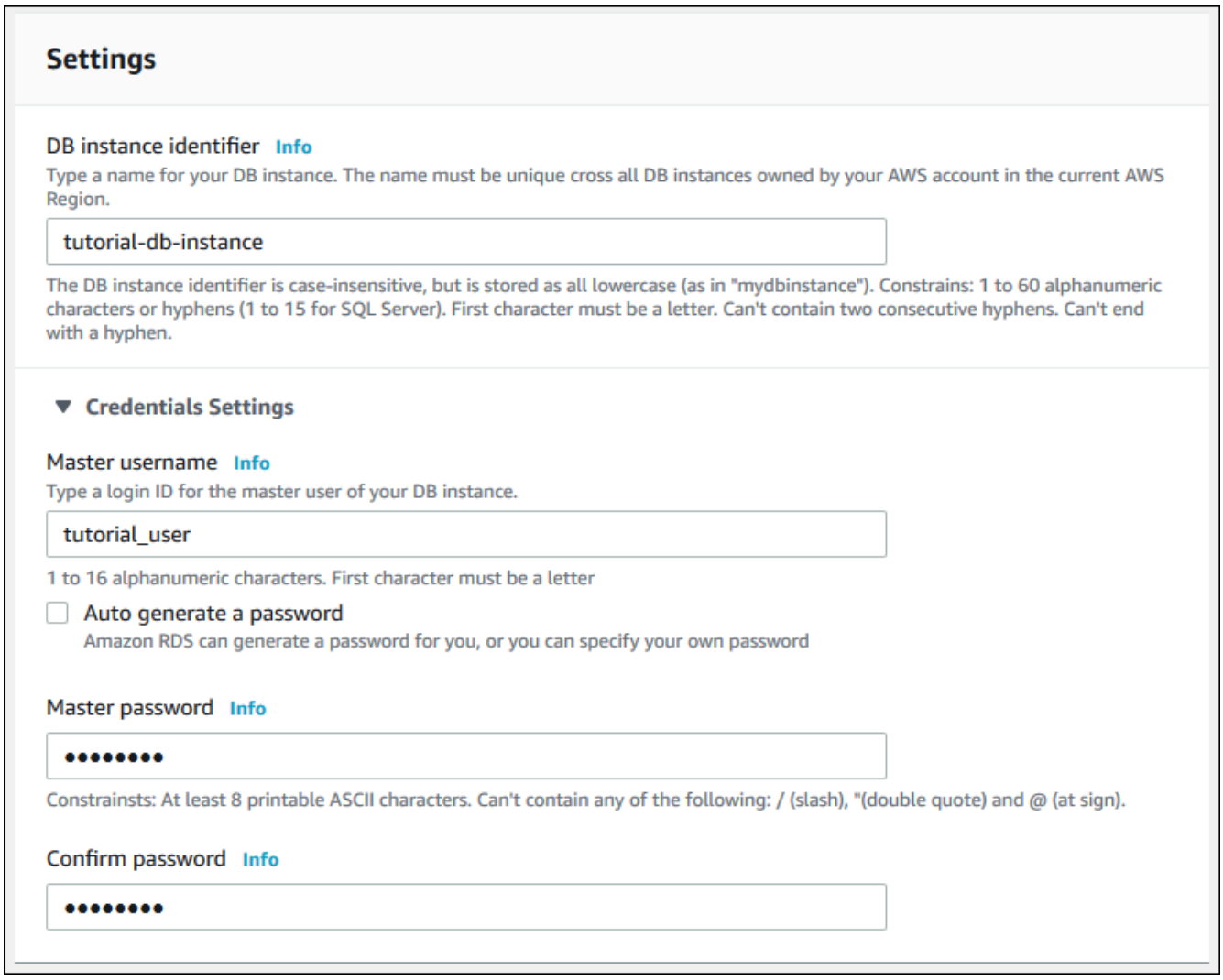
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la AWS Management Console, marque la Región de AWS. Debería ser la misma que en la que creó su instancia de EC2.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija Create database (Creación de base de datos).
5. En la página Crear base de datos, elija Creación estándar.
6. En Opciones del motor, elija MySQL.



7. Para Plantillas, elija Nivel gratuito o Entorno de pruebas. El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.

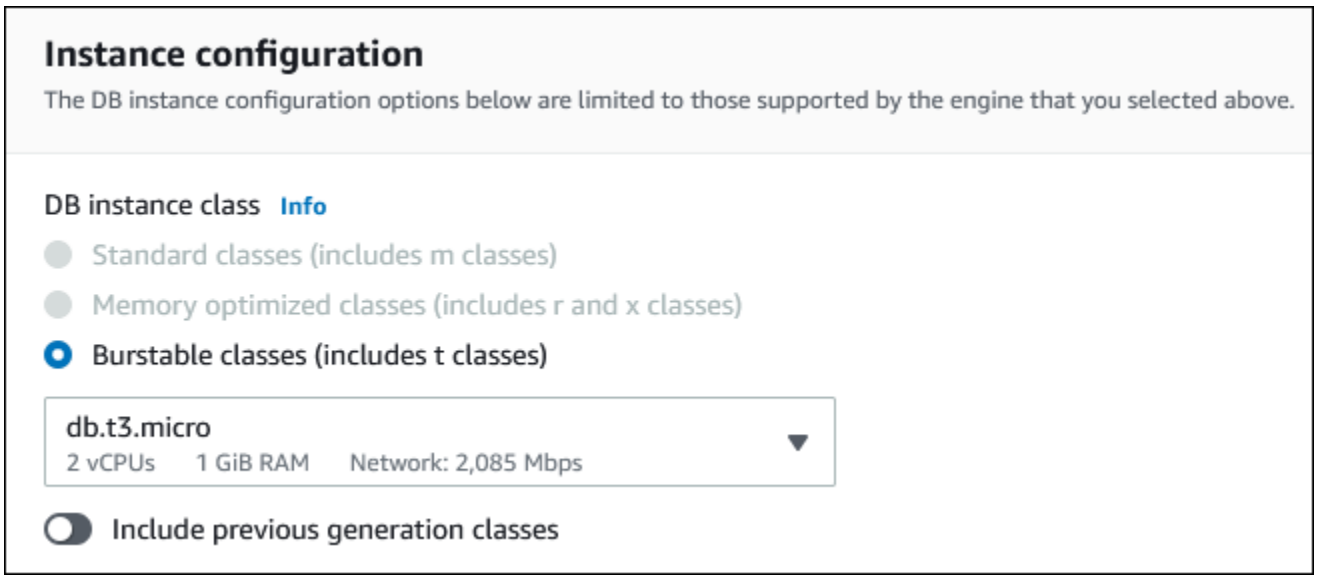


8. En la sección Availability and durability (Disponibilidad y durabilidad), mantenga los valores predeterminados.
9. En la sección Settings (Configuración), establezca los siguientes valores:
   - DB Instance Identifier (Identificador de instancias de bases de datos): **`tutorial-db-instance`**.
   - Master username (Nombre de usuario maestro): escriba **`tutorial_user`**.
   - Auto generate a password (Generar una contraseña de forma automática): deje la opción desactivada.
   - Master password (Contraseña maestra): escriba una contraseña.
   - Confirm password (Confirmar contraseña):– vuelva a introducir la contraseña.



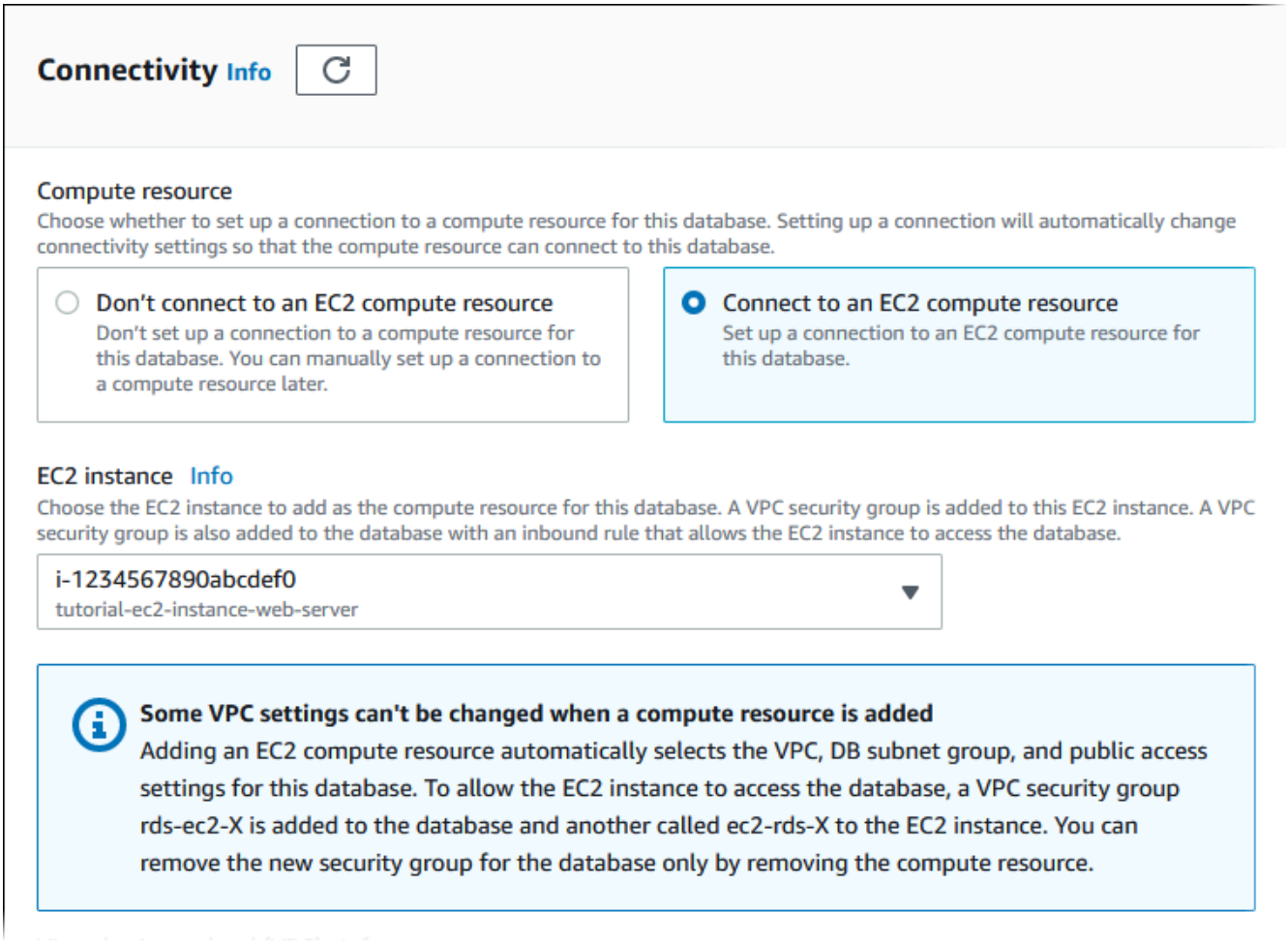
10. En la sección Instance configuration (Configuración de instancia), establezca estos valores:

    - Clases por ráfagas (incluye clases t)
    - db.t3.micro



11. En la sección Storage (Almacenamiento), mantenga la configuración predeterminada.
12. En la sección Connectivity (Conectividad), defina estos valores y mantenga los demás con sus valores predeterminados:

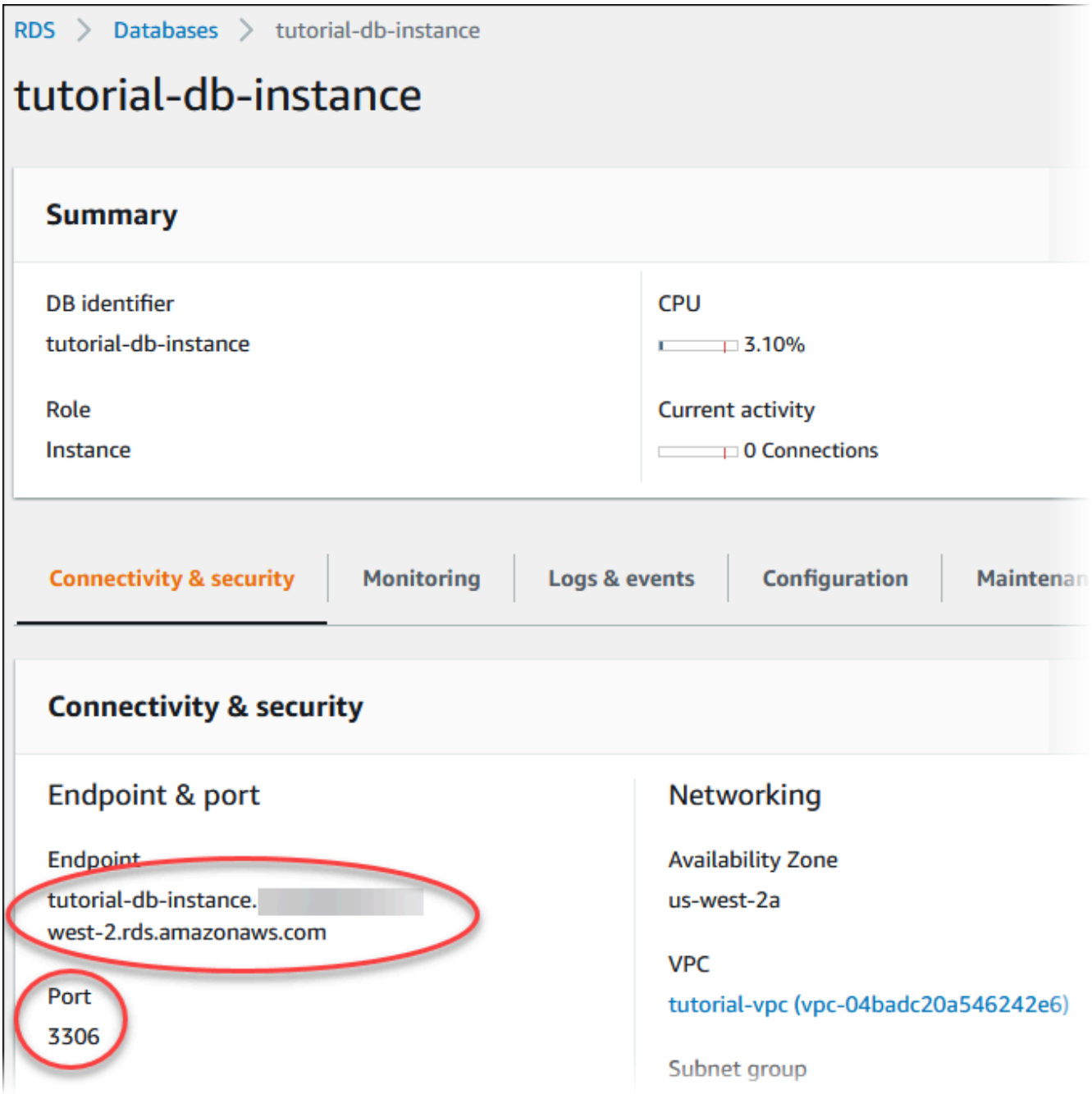
    - En Compute resource (Recurso informático), elija Connect to an EC2 compute resource (Conectar a un recurso informático de EC2).
    - En EC2 instance (Instancia EC2), elija la instancia de EC2 que creó anteriormente, como tutorial-ec2-instance-web-server.



13. En la sección Autenticación de base de datos, asegúrese de que la Autenticación con contraseña está seleccionada.
14. Abra la sección Additional configuration (Configuración adicional) e introduzca **`sample`** para Initial database name (Nombre de la base de datos inicial) Mantenga la configuración predeterminada para el resto de las opciones.
15. Para crear una instancia de base de datos MySQL, elija Create database (Crear base de datos).

    Su nueva instancia de base de datos aparece en la lista Databases (Bases de datos) con el estado Creating (Creándose).
16. Espere a que el Status (Estado) de su nueva instancia de base de datos se muestre como Available (Disponible). A continuación, seleccione el nombre de la instancia de base de datos para mostrar sus detalles.

17. En la sección Connectivity & security (Conectividad y seguridad) vea el Endpoint (Punto de enlace) y el Port (Puerto) de la instancia de base de datos.



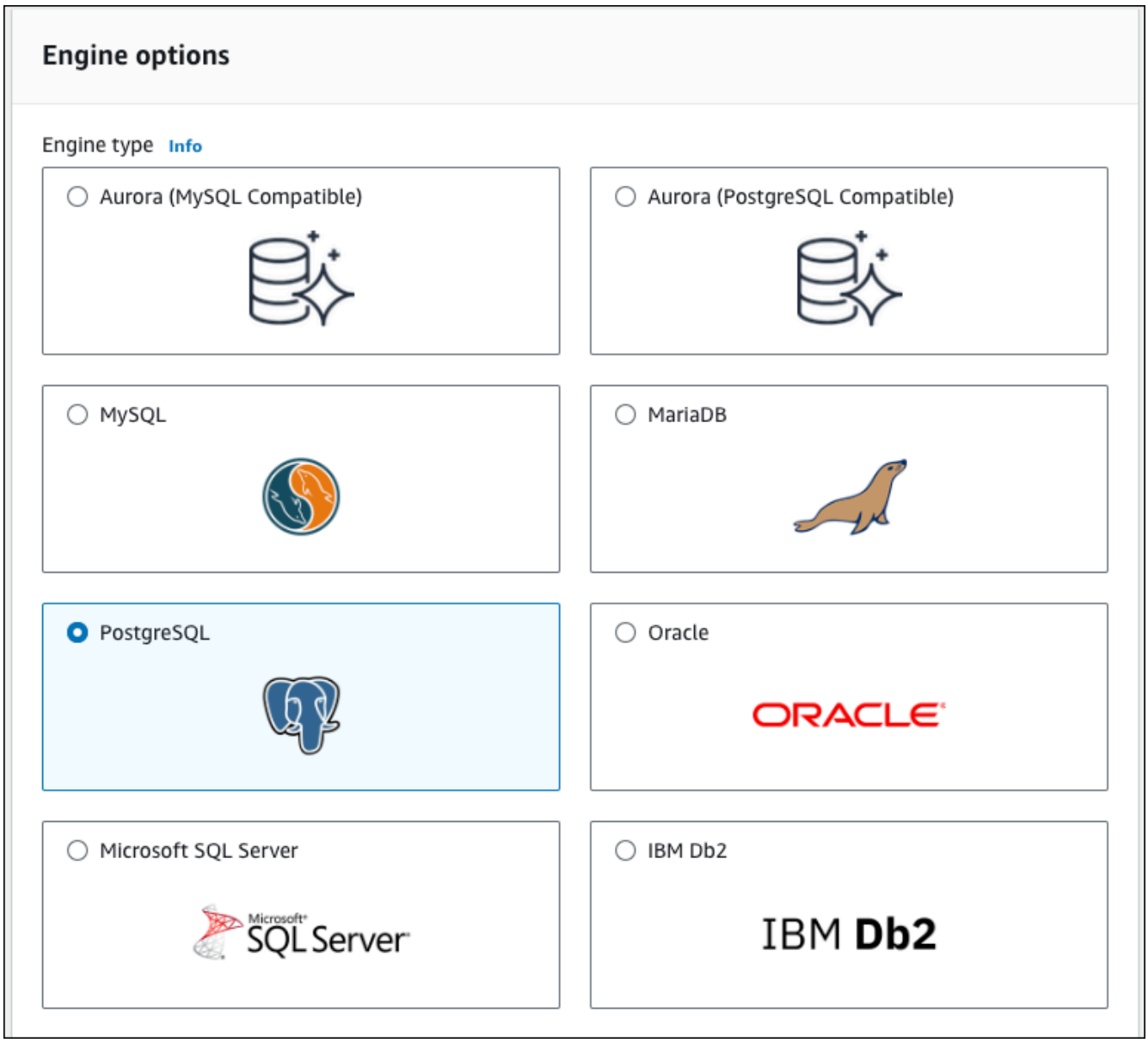
Anote el punto de enlace y el puerto de la instancia de base de datos. Utiliza esta información para conectar su servidor web a la instancia de base de datos.

18. complet Instalación de un servidor web en la instancia de EC2.

RDS for PostgreSQL

Para crear una instancia de base de datos de PostgreSQL

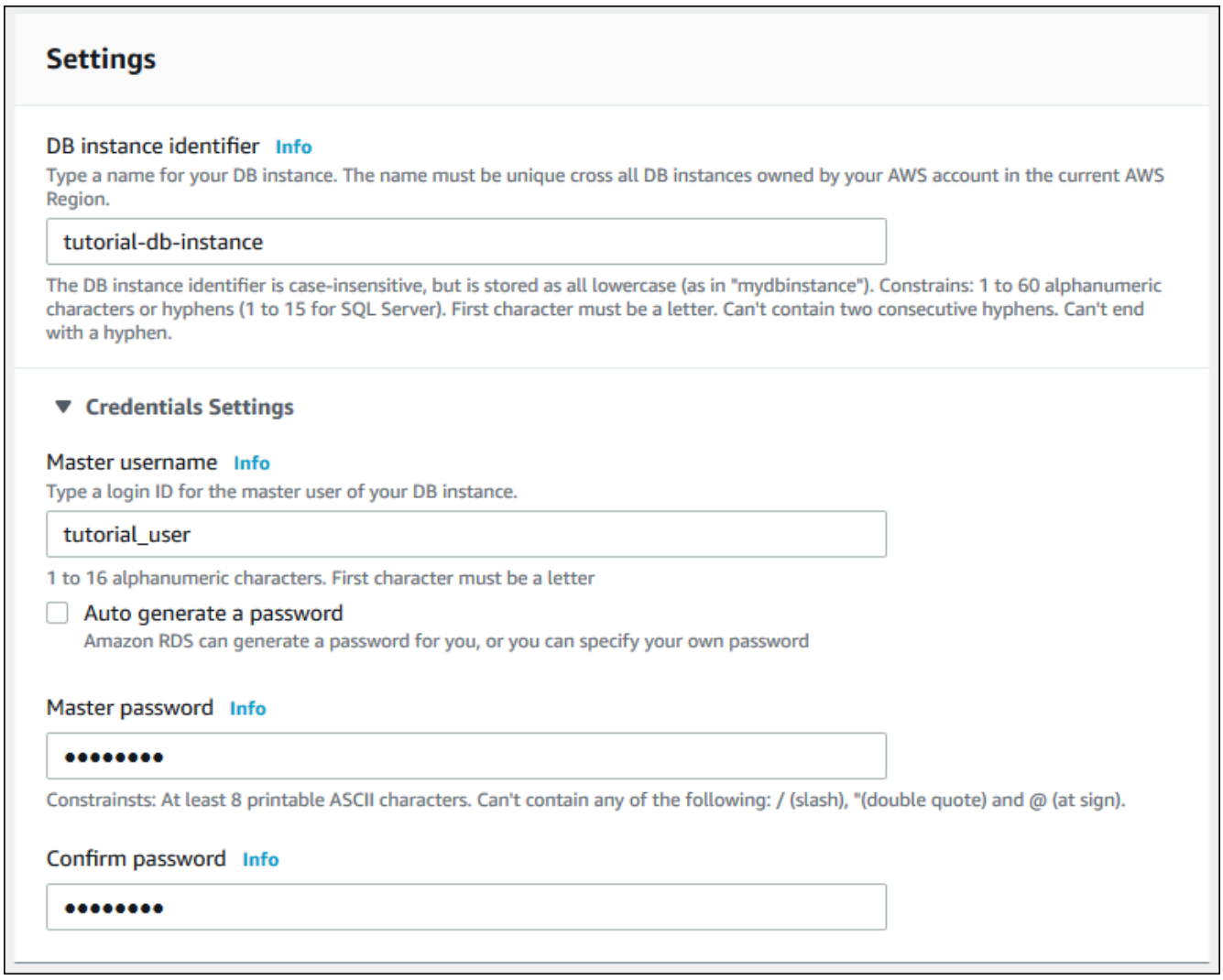
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la AWS Management Console, marque la Región de AWS. Debería ser la misma que en la que creó su instancia de EC2.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija Create database (Creación de base de datos).
5. En la página Crear base de datos, elija Creación estándar.
6. En Opciones del motor, elija PostgreSQL.



7. Para Plantillas, elija Nivel gratuito o Entorno de pruebas. El Nivel gratuito aparece en las cuentas de planes gratuitos. El Entorno de pruebas aparece para las cuentas de planes de pago.

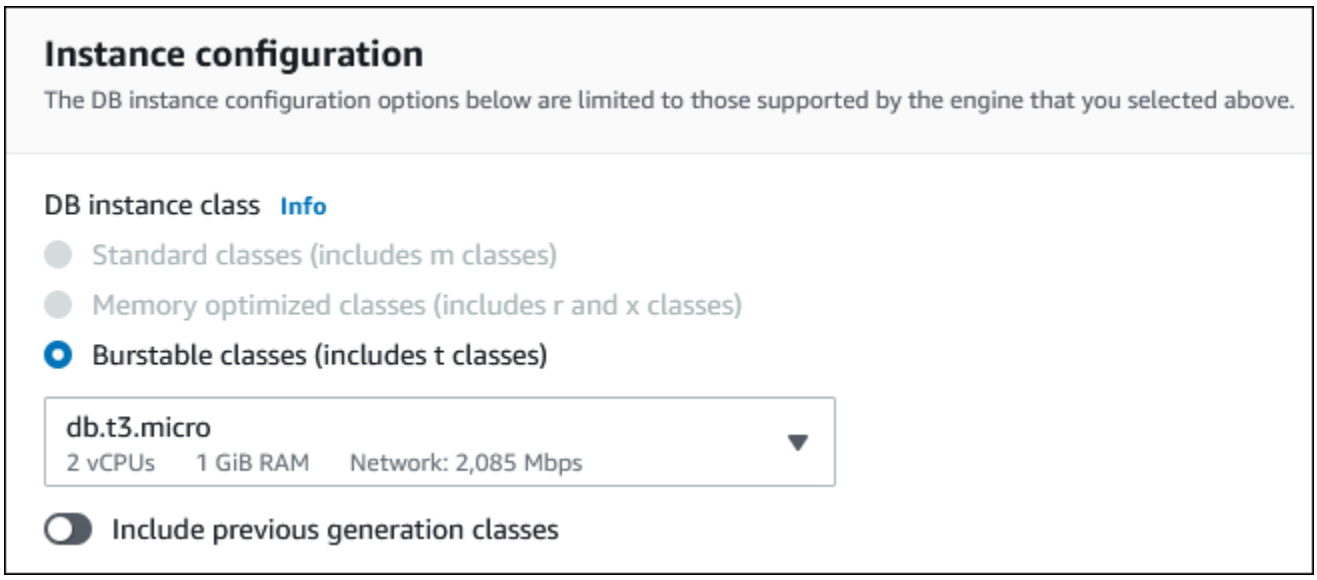


8. En la sección Availability and durability (Disponibilidad y durabilidad), mantenga los valores predeterminados.
9. En la sección Settings (Configuración), establezca los siguientes valores:
   - DB Instance Identifier (Identificador de instancias de bases de datos): **`tutorial-db-instance`**.
   - Master username (Nombre de usuario maestro): escriba **`tutorial_user`**.
   - Auto generate a password (Generar una contraseña de forma automática): deje la opción desactivada.
   - Master password (Contraseña maestra): escriba una contraseña.
   - Confirm password (Confirmar contraseña):– vuelva a introducir la contraseña.



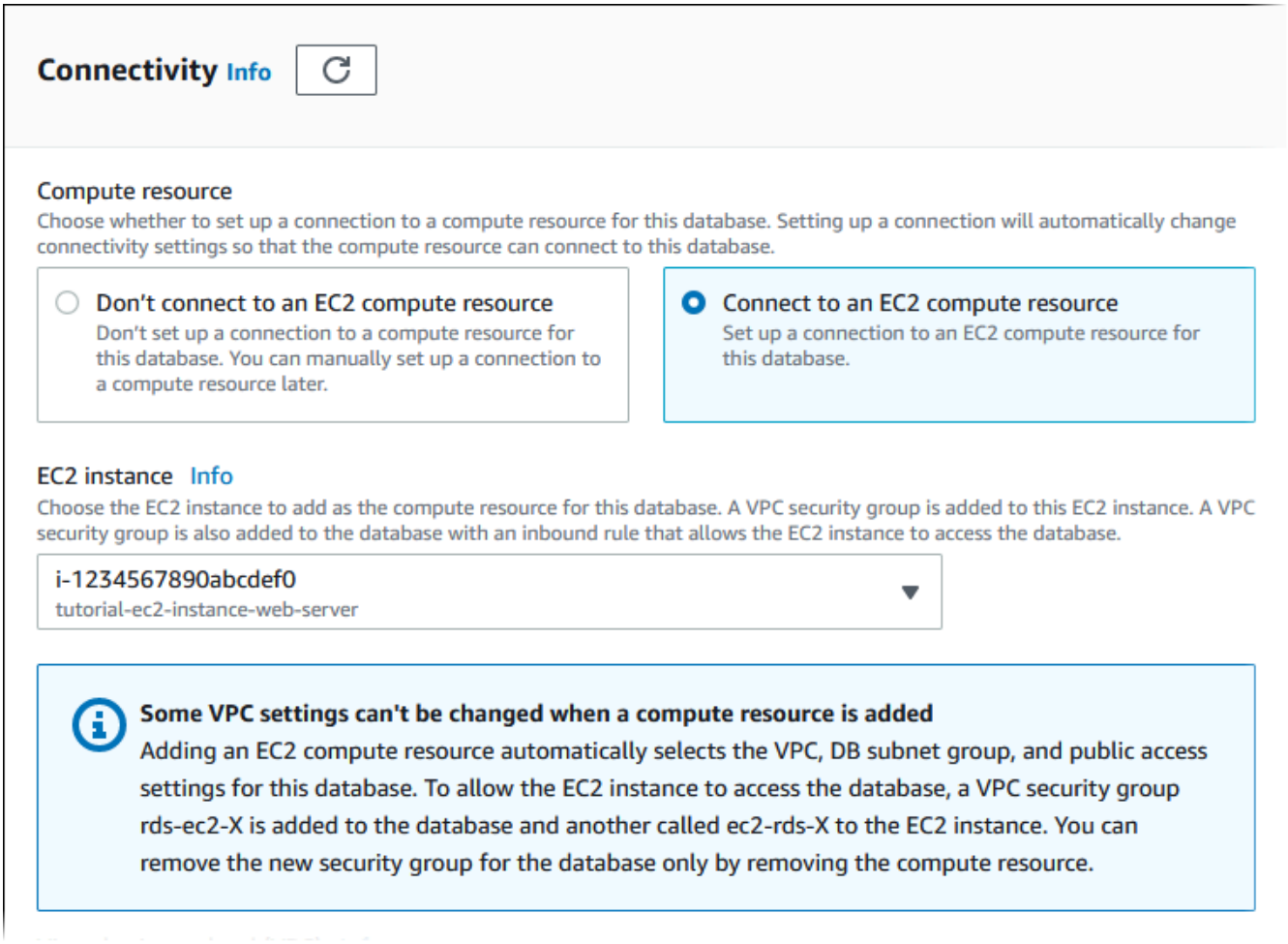
10. En la sección Instance configuration (Configuración de instancia), establezca estos valores:

    - Clases por ráfagas (incluye clases t)
    - db.t3.micro



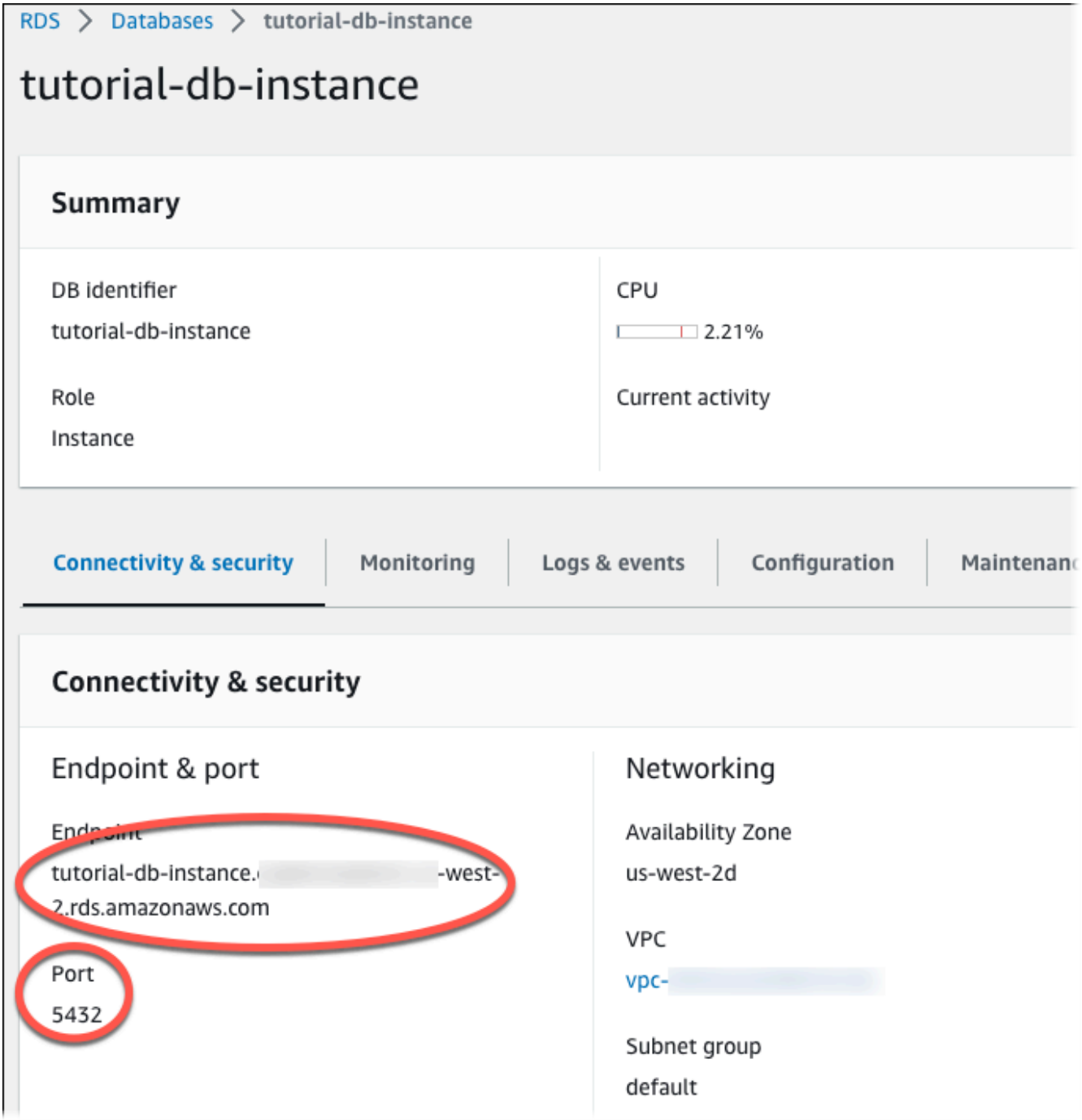
11. En la sección Storage (Almacenamiento), mantenga la configuración predeterminada.
12. En la sección Connectivity (Conectividad), defina estos valores y mantenga los demás con sus valores predeterminados:

    - En Compute resource (Recurso informático), elija Connect to an EC2 compute resource (Conectar a un recurso informático de EC2).
    - En EC2 instance (Instancia EC2), elija la instancia de EC2 que creó anteriormente, como tutorial-ec2-instance-web-server.



13. En la sección Autenticación de base de datos, asegúrese de que la Autenticación con contraseña está seleccionada.
14. Abra la sección Additional configuration (Configuración adicional) e introduzca **`sample`** para Initial database name (Nombre de la base de datos inicial) Mantenga la configuración predeterminada para el resto de las opciones.
15. Para crear una instancia de base de datos de PostgreSQL, elija Crear base de datos.

    Su nueva instancia de base de datos aparece en la lista Databases (Bases de datos) con el estado Creating (Creándose).
16. Espere a que el Status (Estado) de su nueva instancia de base de datos se muestre como Available (Disponible). A continuación, seleccione el nombre de la instancia de base de datos para mostrar sus detalles.
17. En la sección Connectivity & security (Conectividad y seguridad) vea el Endpoint (Punto de enlace) y el Port (Puerto) de la instancia de base de datos.



Anote el punto de enlace y el puerto de la instancia de base de datos. Utiliza esta información para conectar su servidor web a la instancia de base de datos.

18. complet Instalación de un servidor web en la instancia de EC2.

Instalación de un servidor web en la instancia de EC2

Instale un servidor web en una instancia de EC2 que creó en Lanzamiento de una instancia EC2 para conectarse con la instancia de base de datos. El servidor web se conecta a la instancia de base de datos de Amazon RDS que creó en Crear una instancia de base de datos de Amazon RDS.

Instalación de un servidor web Apache con PHP y MariaDB

Conéctese a su instancia de EC2 e instale el servidor web.

Para conectarse a la instancia de EC2 e instalar el servidor web Apache con PHP

1. Conéctese a la instancia de EC2 que ha creado anteriormente siguiendo los pasos que se indican en Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2.

   Le recomendamos que se conecte a la instancia de EC2 mediante SSH. Si la utilidad de cliente SSH está instalada en Windows, Linux o Mac, puede conectarse a la instancia con el siguiente formato de comando:

   ```
   ssh -i location_of_pem_file ec2-user@ec2-instance-public-dns-name
   ```

   Por ejemplo, suponga que `ec2-database-connect-key-pair.pem` está almacenado en `/dir1` en Linux y que el DNS IPv4 público de su instancia de EC2 es `ec2-12-345-678-90.compute-1.amazonaws.com`. Su comando SSH tendría el siguiente aspecto:

   ```
   ssh -i /dir1/ec2-database-connect-key-pair.pem ec2-
   user@ec2-12-345-678-90.compute-1.amazonaws.com
   ```

2. Obtenga las correcciones de errores y las actualizaciones de seguridad más recientes actualizando el software en su instancia de EC2. Para ello, utilice el siguiente comando.

   > **Note**
   >
   > La opción `-y` instala las actualizaciones sin necesidad de confirmación. Para examinar las actualizaciones antes de la instalación, omita esta opción.

   ```
   sudo dnf update -y
   ```

3. Una vez completadas las actualizaciones, instale el servidor web Apache, PHP y el software de MariaDB o PostgreSQL con los siguientes comandos. Este comando instala varios paquetes de software y dependencias relacionadas al mismo tiempo.

   MariaDB & MySQL

   ```
   sudo dnf install -y httpd php php-mysqli mariadb105
   ```

   PostgreSQL

   ```
   sudo dnf install -y httpd php php-pgsql postgresql15
   ```

   Si recibe un error, probablemente la instancia no se ha iniciado con una AMI de Amazon Linux 2023. Es posible que esté usando la AMI Amazon Linux 2 en su lugar. Puede ver la versión de Amazon Linux usando el comando siguiente:

   ```
   cat /etc/system-release
   ```

   Para obtener más información, consulte Actualización del software de instancia.

4. Inicie el servidor web mediante el comando que se muestra a continuación.

   ```
   sudo systemctl start httpd
   ```

   Puede probar que el servidor web esté correctamente instalado e iniciado. Para ello, escriba el nombre público del Sistema de nombres de dominio (DNS) de su instancia de EC2 en la barra de direcciones de un navegador web, por ejemplo: `http://ec2-42-8-168-21.us-west-1.compute.amazonaws.com`. Si el servidor web se está ejecutando, se mostrará la página de prueba de Apache.

   Si no ve la página de prueba de Apache, compruebe las reglas de entrada para el grupo de seguridad de VPC que creó en Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4). Asegúrese de que las reglas de entrada incluyan una que permita el acceso HTTP (puerto 80) a la dirección IP que utiliza para conectarse al servidor web.

> **Note**
>
> La página de prueba de Apache aparece únicamente cuando el directorio raíz de documentos está vac, `/var/www/html`. Después de añadir contenido al directorio raíz de documentos, el contenido aparece en la dirección DNS pública de la instancia de EC2. Antes de este punto, aparece en la página de prueba de Apache.

5. Configure el servidor web para que se inicie en cada arranque del sistema con el comando `systemctl`.

```
sudo systemctl enable httpd
```

Para permitir a `ec2-user` administrar archivos en el directorio raíz predeterminado del servidor web Apache, modifique los propietarios y los permisos del directorio `/var/www`. Existen muchas formas de realizar esta tarea. En este tutorial se añade el usuario `ec2-user` al grupo `apache`, se otorga al grupo `apache` la propiedad del directorio `/var/www` y se asignan permisos de escritura al grupo.

Para configurar los permisos de archivo para el servidor web Apache

1. Agregue el usuario `ec2-user` al grupo `apache`.

```
sudo usermod -a -G apache ec2-user
```

2. Cierre la sesión para actualizar los permisos e incluir el nuevo grupo `apache`.

```
exit
```

3. Inicie sesión nuevamente y compruebe que existe el grupo `apache` mediante el comando `groups`.

```
groups
```

   El resultado tiene un aspecto similar al siguiente:

```
ec2-user adm wheel apache systemd-journal
```

4. Cambie la propiedad de grupo del directorio `/var/www` y su contenido al grupo `apache`.

```
sudo chown -R ec2-user:apache /var/www
```

5. Cambie los permisos del directorio `/var/www` y sus subdirectorios para añadir permisos de escritura de grupo y establecer el ID de grupo en los subdirectorios que se creen en el futuro.

```
sudo chmod 2775 /var/www
find /var/www -type d -exec sudo chmod 2775 {} \;
```

6. Cambie recursivamente los permisos de los archivos del directorio `/var/www` y sus subdirectorios para añadir permisos de escritura de grupo.

```
find /var/www -type f -exec sudo chmod 0664 {} \;
```

Ahora `ec2-user` (y cualquier miembro futuro del grupo de `apache`) puede añadir, eliminar y editar archivos en la raíz de documentos de Apache. Esto le permite añadir contenido, como un sitio web estático o una aplicación PHP.

> **Note**
>
> Un servidor web que ejecuta el protocolo HTTP no proporciona seguridad de transporte de los datos que envía o recibe. Cuando se conecta a un servidor HTTP utilizando un navegador web, la mayor parte de la información es visible a cualquier acceso no autorizado en la ruta de la red. Esta información incluye las URL que visita, el contenido de las páginas web que recibe y el contenido (incluidas las contraseñas) de cualquier formulario HTML.
> La práctica recomendada para proteger el servidor web es instalar soporte para HTTPS (HTTP seguro). Este protocolo protege los datos con el cifrado SSL/TLS. Para obtener más información, consulte Tutorial: Configurar SSL/TLS con la AMI de Amazon Linux en la Guía del usuario deAmazon EC2.

Conecte el servidor web Apache con la instancia de base de datos.

A continuación, agregue contenido al servidor web Apache que se conecta a su instancia de base de datos de Amazon RDS.

Para agregar contenido al servidor web Apache que se conecta a su instancia de base de datos

1. Mientras está conectado a la instancia de EC2, cambie el directorio a `/var/www` y cree un subdirectorio nuevo denominado `inc`.

```
cd /var/www
mkdir inc
cd inc
```

2. Cree un archivo en el directorio `inc`, denominado `dbinfo.inc` y, a continuación, edite el archivo mediante nano (o a cualquier otro editor de su elección).

```
>dbinfo.inc
nano dbinfo.inc
```

3. Añada el siguiente contenido al archivo `dbinfo.inc`. Aquí, *`db_instance_endpoint`* es su punto de conexión de instancia de base de datos, sin el puerto, para su instancia de base de datos.

> **Note**
>
> Recomendamos colocar la información del nombre de usuario y la contraseña en una carpeta que no forme parte de la raíz del documento del servidor web. Al hacerlo, se reduce la posibilidad de que se exponga la información de seguridad.
> Asegúrese de cambiar la `master password` a una contraseña adecuada en su aplicación.

```
<?php

define('DB_SERVER', 'db_instance_endpoint');
define('DB_USERNAME', 'tutorial_user');
define('DB_PASSWORD', 'master password');
define('DB_DATABASE', 'sample');
?>
```

4. Guarde y cierre el archivo `dbinfo.inc`. Si utiliza nano, guarde y cierre el archivo con Ctrl+S y Ctrl+X.

5. Cambie el directorio a `/var/www/html`.

```
cd /var/www/html
```

6. Cree un archivo en el directorio `html`, denominado `SamplePage.php` y, a continuación, edite el archivo mediante nano (o a cualquier otro editor de su elección).

```
>SamplePage.php
nano SamplePage.php
```

7. Añada el siguiente contenido al archivo `SamplePage.php`:

   MariaDB & MySQL

```
<?php include "../inc/dbinfo.inc"; ?>
<html>
<body>
<h1>Sample page</h1>
<?php

  /* Connect to MySQL and select the database. */
  $connection = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD);

  if (mysqli_connect_errno()) echo "Failed to connect to MySQL: " .
 mysqli_connect_error();

  $database = mysqli_select_db($connection, DB_DATABASE);

  /* Ensure that the EMPLOYEES table exists. */
  VerifyEmployeesTable($connection, DB_DATABASE);

  /* If input fields are populated, add a row to the EMPLOYEES table. */
  $employee_name = htmlentities($_POST['NAME']);
  $employee_address = htmlentities($_POST['ADDRESS']);

  if (strlen($employee_name) || strlen($employee_address)) {
    AddEmployee($connection, $employee_name, $employee_address);
  }
?>

<!-- Input form -->
<form action="<?PHP echo $_SERVER['SCRIPT_NAME'] ?>" method="POST">
  <table border="0">
    <tr>
```

```
      <td>NAME</td>
      <td>ADDRESS</td>
    </tr>
    <tr>
      <td>
        <input type="text" name="NAME" maxlength="45" size="30" />
      </td>
      <td>
        <input type="text" name="ADDRESS" maxlength="90" size="60" />
      </td>
      <td>
        <input type="submit" value="Add Data" />
      </td>
    </tr>
  </table>
</form>

<!-- Display table data. -->
<table border="1" cellpadding="2" cellspacing="2">
  <tr>
    <td>ID</td>
    <td>NAME</td>
    <td>ADDRESS</td>
  </tr>

<?php

$result = mysqli_query($connection, "SELECT * FROM EMPLOYEES");

while($query_data = mysqli_fetch_row($result)) {
  echo "<tr>";
  echo "<td>",$query_data[0], "</td>",
       "<td>",$query_data[1], "</td>",
       "<td>",$query_data[2], "</td>";
  echo "</tr>";
}
?>

</table>

<!-- Clean up. -->
<?php

  mysqli_free_result($result);
```

```
  mysqli_close($connection);

?>

</body>
</html>


<?php

/* Add an employee to the table. */
function AddEmployee($connection, $name, $address) {
   $n = mysqli_real_escape_string($connection, $name);
   $a = mysqli_real_escape_string($connection, $address);

   $query = "INSERT INTO EMPLOYEES (NAME, ADDRESS) VALUES ('$n', '$a');";

   if(!mysqli_query($connection, $query)) echo("<p>Error adding employee data.</
p>");
}

/* Check whether the table exists and, if not, create it. */
function VerifyEmployeesTable($connection, $dbName) {
  if(!TableExists("EMPLOYEES", $connection, $dbName))
  {
     $query = "CREATE TABLE EMPLOYEES (
         ID int(11) UNSIGNED AUTO_INCREMENT PRIMARY KEY,
         NAME VARCHAR(45),
         ADDRESS VARCHAR(90)
       )";

     if(!mysqli_query($connection, $query)) echo("<p>Error creating table.</
p>");
  }
}

/* Check for the existence of a table. */
function TableExists($tableName, $connection, $dbName) {
  $t = mysqli_real_escape_string($connection, $tableName);
  $d = mysqli_real_escape_string($connection, $dbName);

  $checktable = mysqli_query($connection,
      "SELECT TABLE_NAME FROM information_schema.TABLES WHERE TABLE_NAME = '$t'
 AND TABLE_SCHEMA = '$d'");
```

```
  if(mysqli_num_rows($checktable) > 0) return true;

  return false;
}
?>
```

PostgreSQL

```
<?php include "../inc/dbinfo.inc"; ?>

<html>
<body>
<h1>Sample page</h1>
<?php

/* Connect to PostgreSQL and select the database. */
$constring = "host=" . DB_SERVER . " dbname=" . DB_DATABASE . " user=" .
 DB_USERNAME . " password=" . DB_PASSWORD ;
$connection = pg_connect($constring);

if (!$connection){
 echo "Failed to connect to PostgreSQL";
 exit;
}

/* Ensure that the EMPLOYEES table exists. */
VerifyEmployeesTable($connection, DB_DATABASE);

/* If input fields are populated, add a row to the EMPLOYEES table. */
$employee_name = htmlentities($_POST['NAME']);
$employee_address = htmlentities($_POST['ADDRESS']);

if (strlen($employee_name) || strlen($employee_address)) {
  AddEmployee($connection, $employee_name, $employee_address);
}

?>

<!-- Input form -->
<form action="<?PHP echo $_SERVER['SCRIPT_NAME'] ?>" method="POST">
  <table border="0">
```

```
    <tr>
      <td>NAME</td>
      <td>ADDRESS</td>
    </tr>
    <tr>
      <td>
    <input type="text" name="NAME" maxlength="45" size="30" />
      </td>
      <td>
    <input type="text" name="ADDRESS" maxlength="90" size="60" />
      </td>
      <td>
    <input type="submit" value="Add Data" />
      </td>
    </tr>
  </table>
</form>
<!-- Display table data. -->
<table border="1" cellpadding="2" cellspacing="2">
  <tr>
    <td>ID</td>
    <td>NAME</td>
    <td>ADDRESS</td>
  </tr>

<?php

$result = pg_query($connection, "SELECT * FROM EMPLOYEES");

while($query_data = pg_fetch_row($result)) {
  echo "<tr>";
  echo "<td>",$query_data[0], "</td>",
       "<td>",$query_data[1], "</td>",
       "<td>",$query_data[2], "</td>";
  echo "</tr>";
}
?>
</table>

<!-- Clean up. -->
<?php

  pg_free_result($result);
  pg_close($connection);
```

```
?>
</body>
</html>


<?php

/* Add an employee to the table. */
function AddEmployee($connection, $name, $address) {
   $n = pg_escape_string($name);
   $a = pg_escape_string($address);
   echo "Forming Query";
   $query = "INSERT INTO EMPLOYEES (NAME, ADDRESS) VALUES ('$n', '$a');";

   if(!pg_query($connection, $query)) echo("<p>Error adding employee data.</
p>");
}

/* Check whether the table exists and, if not, create it. */
function VerifyEmployeesTable($connection, $dbName) {
  if(!TableExists("EMPLOYEES", $connection, $dbName))
  {
     $query = "CREATE TABLE EMPLOYEES (
         ID serial PRIMARY KEY,
         NAME VARCHAR(45),
         ADDRESS VARCHAR(90)
       )";

     if(!pg_query($connection, $query)) echo("<p>Error creating table.</p>");
  }
}
/* Check for the existence of a table. */
function TableExists($tableName, $connection, $dbName) {
  $t = strtolower(pg_escape_string($tableName)); //table name is case sensitive
  $d = pg_escape_string($dbName); //schema is 'public' instead of 'sample' db
 name so not using that

  $query = "SELECT TABLE_NAME FROM information_schema.TABLES WHERE TABLE_NAME =
 '$t';";
  $checktable = pg_query($connection, $query);

  if (pg_num_rows($checktable) >0) return true;
  return false;
```

```
}
?>
```

8. Guarde y cierre el archivo `SamplePage.php`.
9. Compruebe que el servidor web se conecta correctamente a su instancia de base de datos abriendo un navegador web y navegando a `http://`*`EC2 instance endpoint`*`/SamplePage.php`, por ejemplo: `http://ec2-12-345-67-890.us-west-2.compute.amazonaws.com/SamplePage.php`.

Puede utilizar `SamplePage.php` para agregar datos a su instancia de base de datos. Los datos que añada se mostrarán en la página. Para verificar que los datos se insertaron en la tabla, puede instalar el cliente MySQL en la instancia de Amazon EC2. A continuación, se conectará a la instancia de base de datos y ejecutará una consulta en la tabla.

Para obtener información acerca de la instalación del cliente MySQL y la conexión a la instancia de base de datos, consulte Conexión a la instancia de base de datos de MySQL.

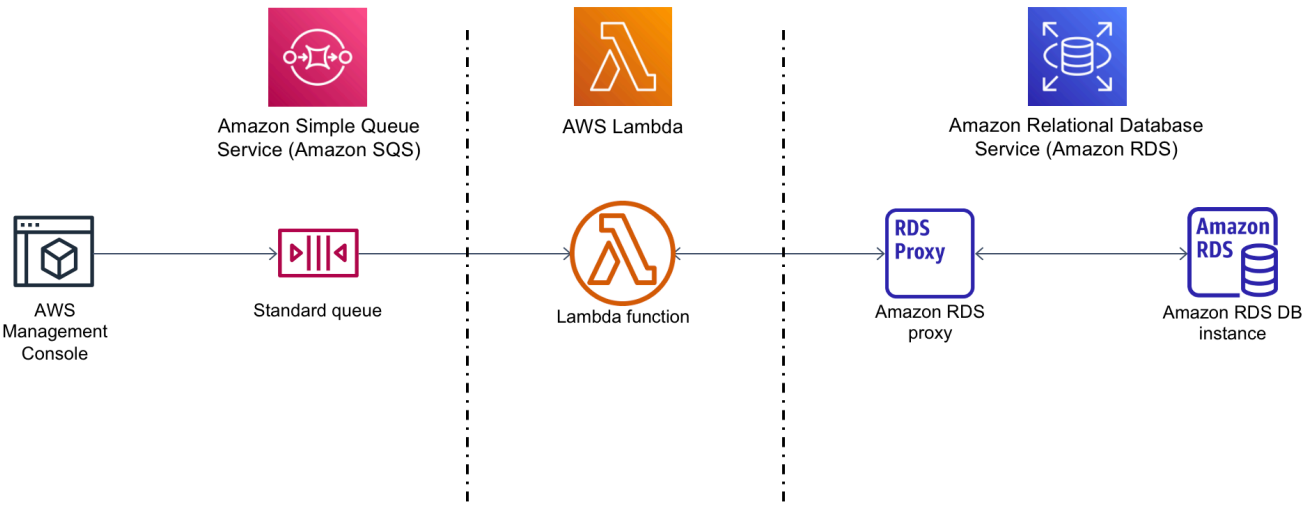
Para asegurarse de que su instancia de base de datos es lo más seguro posible, compruebe que los orígenes fuera de la VPC no se pueden conectar a su instancia de base de datos.

Una vez que haya terminado de probar su servidor web y su base de datos, debe eliminar la instancia de base de datos y la instancia Amazon EC2.

- Para eliminar una instancia de base de datos, siga las instrucciones que se indican en Eliminación de una instancia de base de datos. No es necesario crear una instantánea final.
- Para finalizar una instancia Amazon EC2, siga las instrucciones de Terminar su instancia en la Guía del usuario de Amazon EC2.

Tutorial: Uso de una función de Lambda para obtener acceso a la base de datos de Amazon RDS

En este tutorial, utilizará una función de Lambda para escribir datos en una base de datos de Amazon Relational Database Service (Amazon RDS) a través de RDS Proxy. La función de Lambda lee registros de una cola de Amazon Simple Queue Service (Amazon SQS) y escribe un elemento nuevo en una tabla de la base de datos siempre que se agrega un mensaje. En este ejemplo, utiliza la AWS Management Console para agregar mensajes a la cola de forma manual. En el siguiente diagrama, se muestran los recursos de AWS que utiliza para completar el tutorial.



Con Amazon RDS, puede ejecutar una base de datos relacional administrada en la nube mediante productos de bases de datos habituales como Microsoft SQL Server, MariaDB, MySQL, Oracle Database y PostgreSQL. Al utilizar Lambda para acceder a su base de datos, puede leer y escribir datos en respuesta a eventos, como el registro de un nuevo cliente en su sitio web. Su función, instancia de base de datos y proxy también se escalan automáticamente para hacer frente a los períodos de alta demanda.

Para completar este tutorial, lleve a cabo las siguientes tareas:

1. Inicie una instancia de base de datos de RDS para MySQL y un proxy en la VPC predeterminada de su Cuenta de AWS.

2. Cree y pruebe una función de Lambda que cree una tabla nueva en la base de datos y escriba datos en ella.
3. Cree una cola de Amazon SQS y configúrela para que invoque la función de Lambda cada vez que se agregue un mensaje nuevo.
4. Para probar la configuración completa, agregue mensajes a la cola mediante la AWS Management Console y supervise los resultados con los Registros de CloudWatch.

Al completar estos pasos, aprenderá lo siguiente:

- Cómo usar Amazon RDS para crear una instancia de base de datos y un proxy, y conectar una función de Lambda al proxy.
- Cómo utilizar Lambda para llevar a cabo operaciones de creación y lectura en una base de datos de Amazon RDS.
- Cómo utilizar Amazon SQS para invocar una función de Lambda.

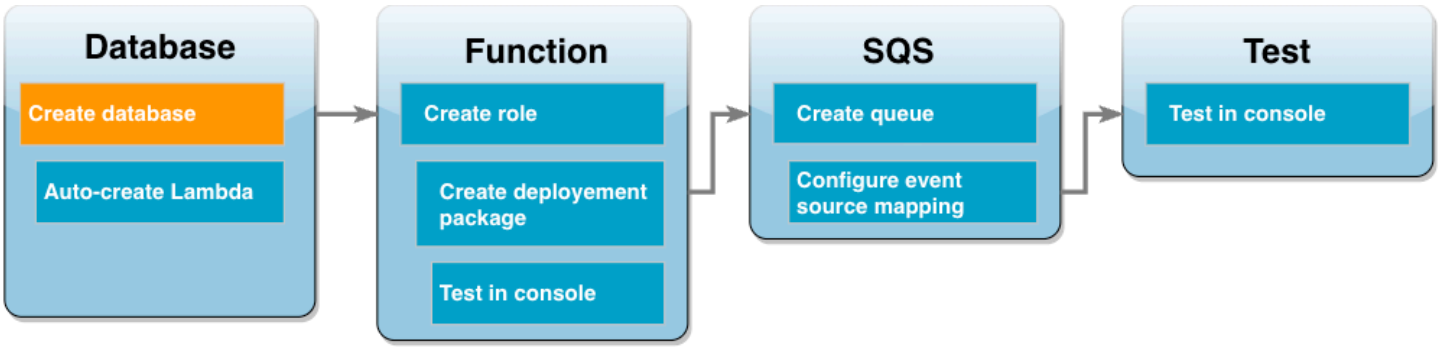
Puede completar esta tarea mediante la AWS Management Console o la AWS Command Line Interface (AWS CLI).

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Creación de una instancia de base de datos de Amazon RDS



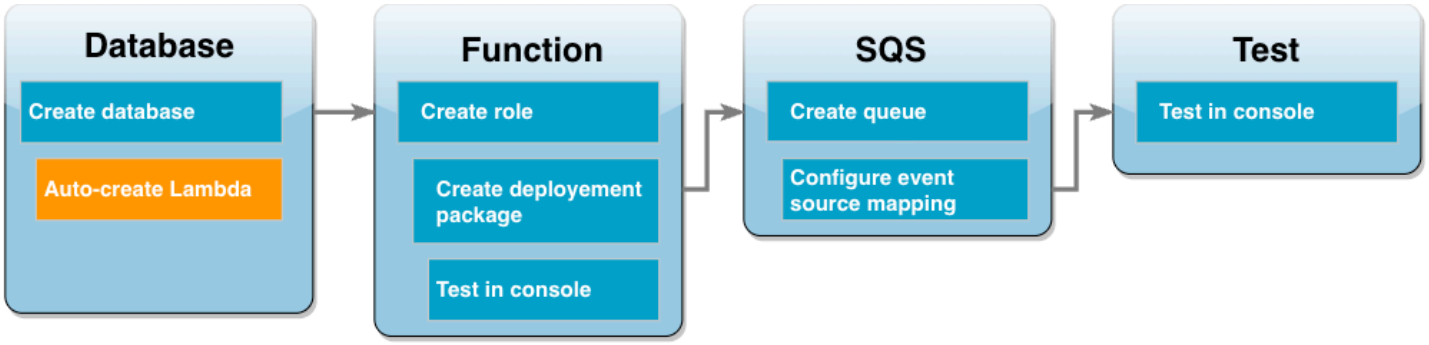
Una instancia de base de datos de Amazon RDS es un entorno de base de datos aislado que se ejecuta en la Nube de AWS. Una instancia puede contener una o más bases de datos creadas por el usuario. A menos que especifique lo contrario, Amazon RDS crea nuevas instancias de bases de datos en la VPC predeterminada incluida en la Cuenta de AWS. Para obtener más información sobre Amazon VPC, consulte la Guía del usuario de Amazon Virtual Private Cloud.

En este tutorial, creará una nueva instancia en su VPC predeterminada de la Cuenta de AWS y creará una base de datos llamada `ExampleDB` en esa instancia. Puede crear su instancia de base de datos y la base de datos mediante la AWS Management Console o la AWS CLI.

Para crear una instancia de base de datos

1. Abra la consola de Amazon RDS y elija Crear base de datos.
2. Deje seleccionada la opción Creación estándar y, a continuación, en Opciones del motor, elija MySQL.
3. En Plantillas, elija Nivel gratuito o Entorno de pruebas. El Nivel gratuito aparece para las cuentas de nivel gratuito. El Entorno de pruebas aparece para las cuentas de planes de pago.
4. En Configuración, en Identificador de instancia de base de datos, ingrese **`MySQLForLambda`**.
5. Para establecer su nombre de usuario y contraseña, haga lo siguiente:
   a. En Configuración de credenciales, deje Nombre de usuario maestro establecido en `admin`.
   b. En Contraseña maestra, introduzca y confirme una contraseña para acceder a la base de datos.
6. Para especificar el nombre de la base de datos, haga lo siguiente:
   - Deje todas las opciones predeterminadas restantes seleccionadas y desplácese hacia abajo hasta la sección Configuración adicional.
   - Amplíe esta sección e introduzca **`ExampleDB`** como Nombre de base de datos inicial.
7. Deje todas las opciones predeterminadas restantes seleccionadas y elija Crear base de datos.

Creación de una función de Lambda y un proxy



Puede utilizar la consola de RDS para crear una función de Lambda y un proxy en la misma VPC que la base de datos.

> **Note**
>
> Solo puede crear estos recursos asociados cuando la base de datos haya terminado de crearse y esté en estado Disponible.

Para crear una función y un proxy asociados

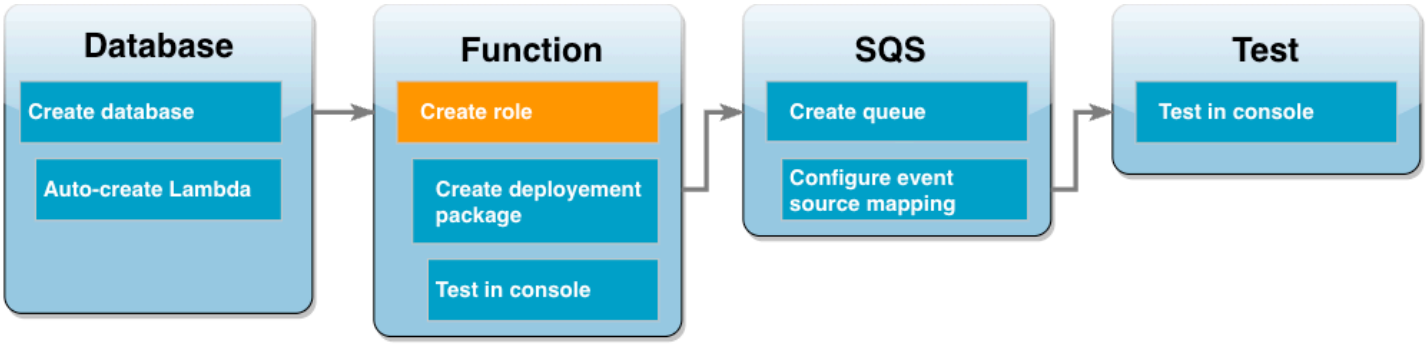
1. Desde la página Bases de datos, compruebe si su base de datos está en estado Disponible. Si es así, continúe con el siguiente paso. De no ser así, espere a que la base de datos esté disponible.
2. Seleccione la base de datos y elija Configurar la conexión de Lambda en Acciones.
3. En la página Configurar la conexión de Lambda, elija Crear nueva función.

   Configure el Nombre de la nueva función de Lambda a **`LambdaFunctionWithRDS`**.
4. En la sección RDS Proxy, seleccione la opción Conectarse mediante RDS Proxy. Además, elija Crear un nuevo proxy.

   - En Credenciales de la base de datos, elija Nombre de usuario y contraseña de la base de datos.
   - En Nombre de usuario, especifique `admin`.
   - En Contraseña, escriba la contraseña que ha creado para la instancia de base de datos.
5. Seleccione Configurar para completar la creación de la función de Lambda y el proxy.

El asistente completa la configuración y proporciona un enlace a la consola de Lambda para que revise la nueva función. Tenga en cuenta el punto de conexión del proxy antes de cambiar a la consola de Lambda.

Crear un rol de ejecución de función



Antes de crear la función de Lambda, debe crear un rol de ejecución para conceder a la función los permisos necesarios. Para este tutorial, Lambda necesita permiso para administrar la conexión de red a la VPC que contiene la instancia de base de datos y para sondear los mensajes de una cola de Amazon SQS.

Para dar a la función de Lambda los permisos que necesita, se utilizan políticas administradas por IAM en este tutorial. Se trata de políticas que conceden permisos para muchos casos de uso comunes y están disponibles en la Cuenta de AWS. Para obtener más información sobre el uso de políticas administradas, consulte Prácticas recomendadas relativas a políticas.

Para crear el rol de ejecución de Lambda

1. Abra la página Roles de la consola de IAM y elija Crear rol.
2. En Tipo de entidad de confianza, elija Servicio de AWS, y en Caso de uso, elija Lambda.
3. Elija Siguiente.
4. Agregue las políticas administradas por IAM de la siguiente manera:
    a. En el cuadro de búsqueda de políticas, busque **`AWSLambdaSQSQueueExecutionRole`**.
    b. En la lista de resultados, seleccione la casilla de verificación junto al rol y, a continuación, elija Borrar filtros.
    c. En el cuadro de búsqueda de políticas, busque **`AWSLambdaVPCAccessExecutionRole`**.
    d. En la lista de resultados, seleccione la casilla de verificación junto al rol y, a continuación, elija Siguiente.

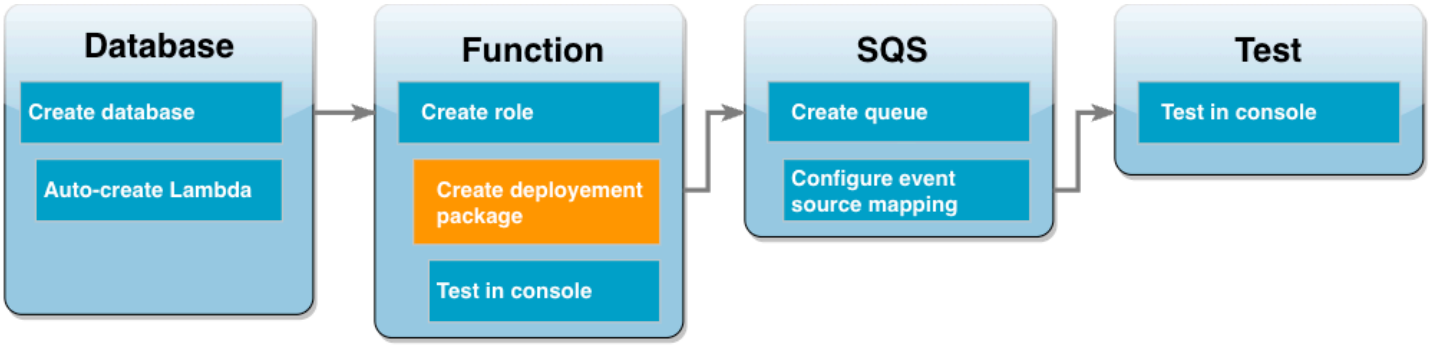
5. En Nombre del rol, ingrese **`lambda-vpc-sqs-role`** y, a continuación, elija Crear rol.

Más adelante en el tutorial, necesitará el nombre de recurso de Amazon (ARN) del rol de ejecución que acaba de crear.

Para encontrar el ARN del rol de ejecución

1. Abra la página Roles de la consola de IAM y elija su rol (`lambda-vpc-sqs-role`).
2. Copie el ARN que se muestra en la sección Resumen.

Creación del paquete de despliegue de Lambda



En el siguiente ejemplo de código Python, se utiliza el paquete PyMySQL para abrir una conexión a la base de datos. La primera vez que invoca su función, también crea una nueva tabla llamada `Customer`. La tabla utiliza el siguiente esquema, en el que `CustID` es la clave principal:

```
Customer(CustID, Name)
```

La función también utiliza PyMySQL para agregar registros a esta tabla. La función agrega registros mediante los ID de cliente y los nombres especificados en los mensajes que agregará a la cola de Amazon SQS.

El código crea la conexión a la base de datos fuera de la función del controlador. La creación de la conexión en el código de inicialización permite volver a utilizar la conexión mediante invocaciones posteriores de la función y mejora el rendimiento. En una aplicación de producción, también puede utilizar la simultaneidad aprovisionada para inicializar el número solicitado de conexiones a la base de datos. Estas conexiones están disponibles en cuanto se invoca la función.

```
import sys
import logging
```

```
import pymysql
import json
import os

# rds settings
user_name = os.environ['USER_NAME']
password = os.environ['PASSWORD']
rds_proxy_host = os.environ['RDS_PROXY_HOST']
db_name = os.environ['DB_NAME']

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# create the database connection outside of the handler to allow connections to be
# re-used by subsequent function invocations.
try:
        conn = pymysql.connect(host=rds_proxy_host, user=user_name, passwd=password,
 db=db_name, connect_timeout=5)
except pymysql.MySQLError as e:
    logger.error("ERROR: Unexpected error: Could not connect to MySQL instance.")
    logger.error(e)
    sys.exit(1)

logger.info("SUCCESS: Connection to RDS for MySQL instance succeeded")

def lambda_handler(event, context):
    """
    This function creates a new RDS database table and writes records to it
    """
    message = event['Records'][0]['body']
    data = json.loads(message)
    CustID = data['CustID']
    Name = data['Name']

    item_count = 0
    sql_string = f"insert into Customer (CustID, Name) values(%s, %s)"

    with conn.cursor() as cur:
        cur.execute("create table if not exists Customer ( CustID  int NOT NULL, Name
 varchar(255) NOT NULL, PRIMARY KEY (CustID))")
        cur.execute(sql_string, (CustID, Name))
        conn.commit()
        cur.execute("select * from Customer")
        logger.info("The following items have been added to the database:")
```

```
        for row in cur:
            item_count += 1
            logger.info(row)
    conn.commit()

    return "Added %d items to RDS for MySQL table" %(item_count)
```

> **Note**
>
> En este ejemplo, las credenciales de acceso a la base de datos se almacenan como variables de entorno. En las aplicaciones de producción, se recomienda utilizar AWS Secrets Manager como una opción más segura. Tenga en cuenta que si la función de Lambda está en una VPC, debe crear un punto de conexión de VPC para conectarse a Secrets Manager. Para obtener más información, consulte How to connect to AWS Secrets Manager service within a Virtual Private Cloud.

Para incluir la dependencia PyMySQL en el código de la función, cree un paquete de despliegue .zip. Los siguientes comandos funcionan en Linux, macOS o Unix:

Para crear un paquete de paquete de despliegue .zip

1. Guarde el código de ejemplo como un archivo denominado `lambda_function.py`.
2. En el mismo directorio en el que creó el archivo `lambda_function.py`, cree un nuevo directorio llamado `package` e instale la biblioteca de PyMySQL.

   ```
   mkdir package
   pip install --target package pymysql
   ```

3. Cree un archivo zip que contenga el código de la aplicación y la biblioteca de PyMySQL. En Linux o macOS, ejecute los siguientes comandos de la CLI. En Windows, utilice la herramienta de compresión que prefiera para crear el archivo `lambda_function.zip`. El archivo de código de origen `lambda_function.py` y las carpetas que contienen las dependencias deben estar instalados en la raíz del archivo .zip.

   ```
   cd package
   zip -r ../lambda_function.zip .
   cd ..
   ```

```
zip lambda_function.zip lambda_function.py
```

También puede crear su paquete de despliegue mediante un entorno virtual de Python. Consulte Implementación de funciones Python Lambda con archivos .zip.

Actualización de la función de Lambda

Con el paquete .zip que acaba de crear, ahora puede actualizar una función de Lambda mediante la consola de Lambda. Para permitir que la función acceda a la base de datos, también debe configurar las variables de entorno con las credenciales de acceso.

Para actualizar la función de Lambda

1. Abra la página Funciones de la consola de Lambda y elija su función `LambdaFunctionWithRDS`.
2. En la pestaña Configuración de tiempo de ejecución, seleccione Editar para cambiar el Tiempo de ejecución de la función a Python 3.10.
3. Cambie el Controlador a `lambda_function.lambda_handler`.
4. En la pestaña Código, elija Cargar desde y, a continuación, archivo .zip.
5. Seleccione el archivo `lambda_function.zip` que creó en la fase anterior y elija Guardar.

Ahora, configure la función con el rol de ejecución que creó anteriormente. Esto concede a la función los permisos que necesita para acceder a la instancia de base de datos y sondear una cola de Amazon SQS.

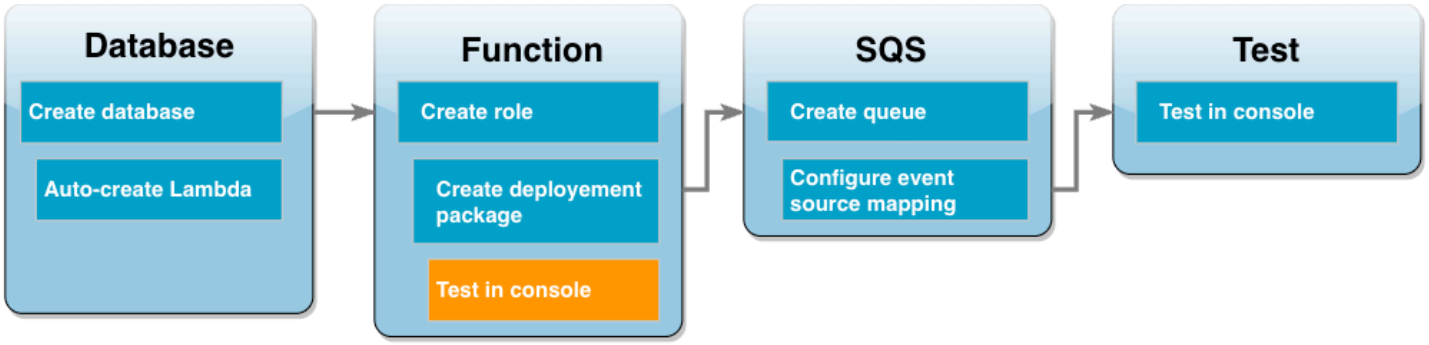
Para configura el rol de ejecución de la función

1. En la página Funciones de la consola de Lambda, seleccione la pestaña Configuración y, a continuación, elija Permisos.
2. En Rol de ejecución, elija Editar.
3. En Rol existente, elija su rol de ejecución (`lambda-vpc-sqs-role`).
4. Seleccione Save.

Para configurar las variables de entorno de la función

1. En la página Funciones de la consola de Lambda, seleccione la pestaña Configuración y luego elija Variables de entorno.
2. Seleccione Editar.
3. Para agregar las credenciales de acceso a la base de datos, haga lo siguiente:
   a. Elija Agregar variable de entorno y, luego, para Clave, ingrese **`USER_NAME`**. A continuación, para Valor, ingrese **`admin`**.
   b. Elija Agregar variable de entorno y, luego, para Clave, ingrese **`DB_NAME`**. A continuación, para Valor, ingrese **`ExampleDB`**.
   c. Elija Agregar variable de entorno y, luego, para Clave, ingrese **`PASSWORD`**. A continuación, para Valor, ingrese la contraseña que eligió al crear la base de datos.
   d. Elija Agregar variable de entorno y, luego, para Clave, ingrese **`RDS_PROXY_HOST`**. A continuación, para Valor, ingrese el punto de conexión de RDS Proxy del que tomo nota antes.
   e. Seleccione Save.

Prueba de la función de Lambda en la consola



Puede seguir utilizando la consola de Lambda para probar la función. En la fase final del tutorial, debe crear un evento de prueba que imita los datos que recibirá la función cuando la invoque con Amazon SQS. El evento de prueba contiene un objeto JSON que especifica un ID y un nombre de cliente para agregarlos a la tabla `Customer` que crea la función.

Para probar la función de Lambda

1. Abra la página Funciones de la consola de Lambda y elija su función.

2. Elija la sección Prueba.
3. Elija Crear un nuevo evento y escriba **myTestEvent** como nombre del evento.
4. Copie el siguiente código en Evento JSON y seleccione Guardar.

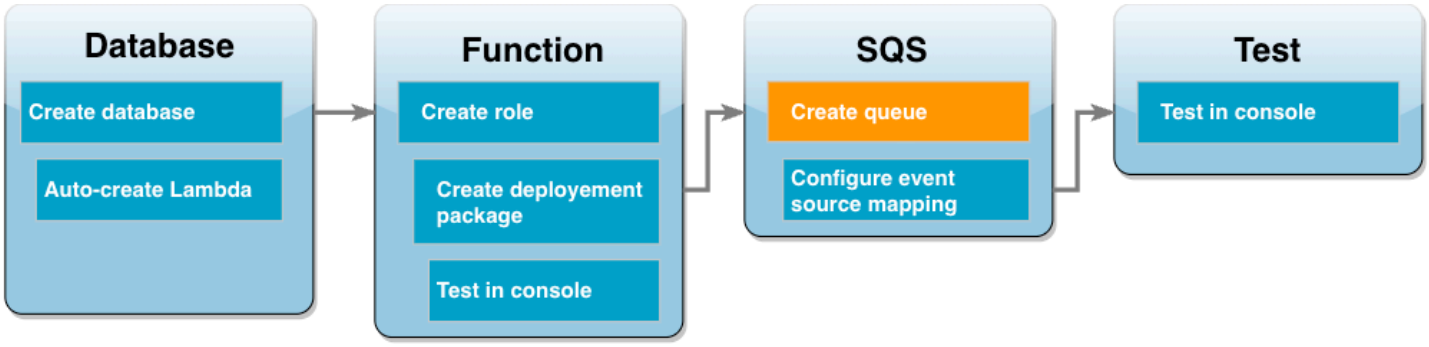
```
{
  "Records": [
    {
      "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
      "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
      "body": "{\n     \"CustID\": 1021,\n     \"Name\": \"Martha Rivera\"\n}",
      "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOLO23YVJ4VO",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
      },
      "messageAttributes": {},
      "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
      "eventSource": "aws:sqs",
      "eventSourceARN": "arn:aws:sqs:us-west-2:123456789012:my-queue",
      "awsRegion": "us-west-2"
    }
  ]
}
```

5. Seleccione Probar.

En la pestaña Resultados de ejecución, debería ver resultados similares a los siguientes que se muestran en los Registros de funciones:

```
[INFO] 2023-02-14T19:31:35.149Z bdd06682-00c7-4d6f-9abb-89f4bbb4a27f The following
 items have been added to the database:
[INFO] 2023-02-14T19:31:35.149Z bdd06682-00c7-4d6f-9abb-89f4bbb4a27f (1021, 'Martha
 Rivera')
```

Cree una cola de Amazon SQS.

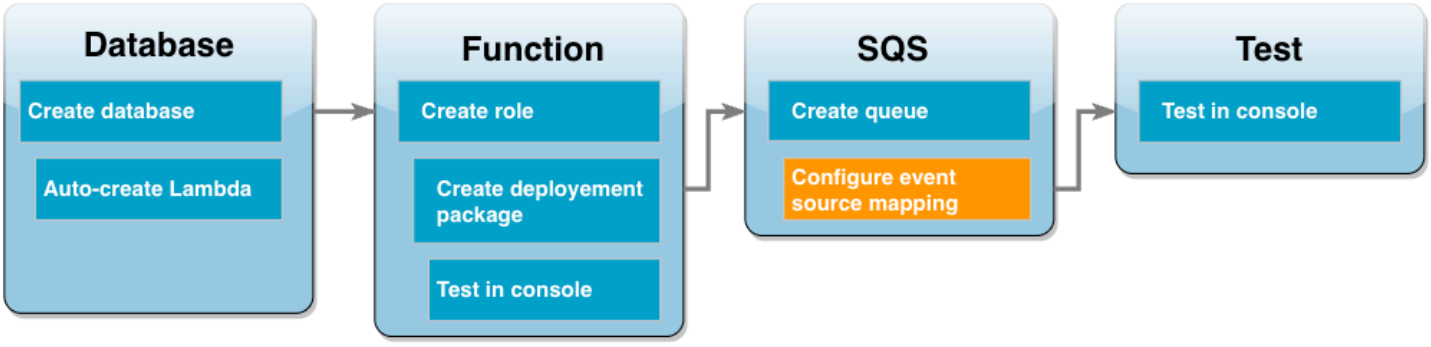


Ha probado correctamente la integración de la función de Lambda y la instancia de base de datos de Amazon RDS. Ahora, cree la cola de Amazon SQS que utilizará para invocar la función de Lambda en la fase final del tutorial.

Para crear la cola de Amazon SQS (consola)

1. Abra la página Colas de la consola de Amazon SQS y seleccione Crear cola.
2. Deje Tipo como Estándar e ingrese **`LambdaRDSQueue`** como nombre de la cola.
3. Deje todas las opciones predeterminadas seleccionadas y seleccione Crear cola.

Creación de una asignación de orígenes de eventos para invocar la función de Lambda



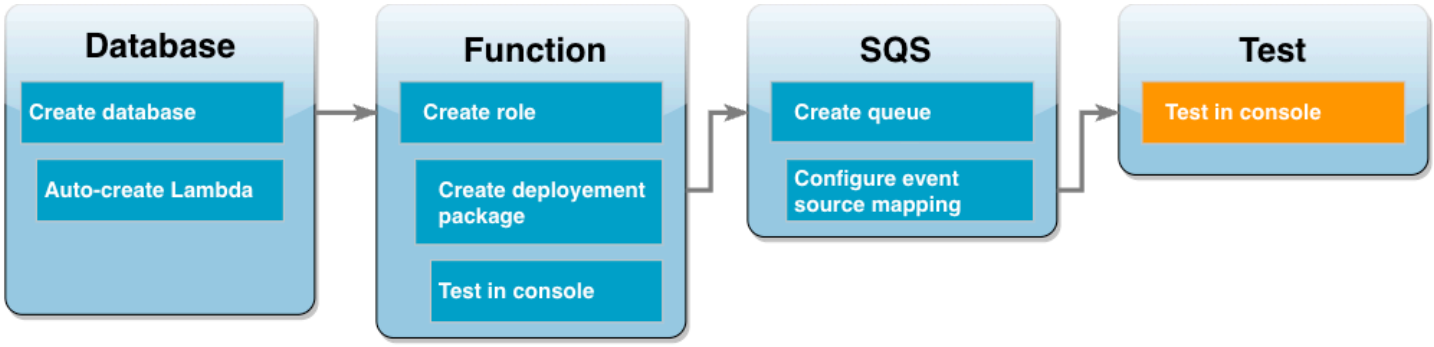
Una asignación de orígenes de eventos es un recurso de Lambda que lee elementos de un flujo o una cola e invoca una función de Lambda. Al configurar una asignación de orígenes de eventos, puede especificar un tamaño de lote para que los registros de su flujo o cola se agrupen en una sola carga. En este ejemplo, ha establecido el tamaño del lote en 1 para que la función de Lambda se invoque cada vez que envíe un mensaje a la cola. Puede configurar la asignación de orígenes de eventos mediante la AWS CLI o la consola de Lambda.

Para crear una asignación de orígenes de eventos (consola)

1. Abra la página Funciones de la consola de Lambda y seleccione su función (`LambdaFunctionWithRDS`).
2. En la sección Información general de la función, elija Agregar desencadenador.
3. Para el origen, seleccione Amazon SQS y, a continuación, seleccione el nombre de la cola (`LambdaRDSQueue`).
4. En Tamaño del lote, ingrese **1**.
5. Deje todas las demás opciones configuradas en los valores predeterminados y seleccione Agregar.

Ya lo tiene todo listo para probar la configuración completa. Para ello, agregue un mensaje a su cola de Amazon SQS.

Prueba y supervisión de la configuración



Para probar la configuración completa, agregue mensajes a la cola de Amazon SQS mediante la consola. A continuación, utilice Registros de CloudWatch para confirmar que la función de Lambda esté escribiendo registros en la base de datos según lo previsto.

Para probar y supervisar la configuración

1. Abra la página Colas de la consola de Amazon SQS y seleccione su cola (`LambdaRDSQueue`).
2. Elija Enviar y recibir mensajes y pegue el siguiente JSON en el Cuerpo del mensaje de la sección Enviar mensaje.

```
{
    "CustID": 1054,
    "Name": "Richard Roe"
```

```
}
```

3. Elija Enviar mensaje.

   Al enviar el mensaje a la cola, Lambda invocará la función a través de la asignación de orígenes de eventos. Para confirmar que Lambda haya invocado su función según lo previsto, utilice Registros de CloudWatch para comprobar que la función haya escrito el ID y el nombre del cliente en la tabla de la base de datos.

4. Abra la página Grupos de registro de la consola de CloudWatch y seleccione el grupo de registro para su función (`/aws/lambda/LambdaFunctionWithRDS`).

5. En la sección Flujos de registro, elija el flujo de registro más reciente.

   La tabla debe contener dos registros de clientes, uno de cada invocación de la función. En el flujo de registro, debería ver mensajes similares al siguiente:

```
[INFO] 2023-02-14T19:06:43.873Z 45368126-3eee-47f7-88ca-3086ae6d3a77 The following
 items have been added to the database:
[INFO] 2023-02-14T19:06:43.873Z 45368126-3eee-47f7-88ca-3086ae6d3a77 (1021, 'Martha
 Rivera')
[INFO] 2023-02-14T19:06:43.873Z 45368126-3eee-47f7-88ca-3086ae6d3a77 (1054,
 'Richard Roe')
```

Limpiar los recursos de

A menos que desee conservar los recursos que creó para este tutorial, puede eliminarlos ahora. Si elimina los recursos de AWS que ya no utiliza, evitará gastos innecesarios en su cuenta de AWS.

Cómo eliminar la función de Lambda

1. Abra la página de Funciones en la consola de Lambda.
2. Seleccione la función que ha creado.
3. Elija Actions (Acciones), Delete (Eliminar).
4. Elija Eliminar.

Cómo eliminar el rol de ejecución

1. Abra la página Roles en la consola de IAM.

2. Seleccione el rol de ejecución que creó.
3. Elija Delete role (Eliminar rol).
4. Elija Sí, eliminar.

Para eliminar la instancia de base de datos MySQL

1. Abra la página Databases (Bases de datos) de la consola de Amazon RDS.
2. Seleccione la base de datos que ha creado.
3. Elija Acciones, Eliminar.
4. Borre el cuadro de verificación Create final snapshot (Crear instantánea final).
5. Escriba **`delete me`** en el cuadro de texto.
6. Elija Eliminar.

Para eliminar la cola de Amazon SQS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SQS en https://console.aws.amazon.com/sqs/.
2. Seleccione la cola que ha creado.
3. Elija Eliminar.
4. Escriba **`delete`** en el cuadro de texto.
5. Elija Eliminar.

Tutoriales de Amazon RDS y código de muestra

La documentación de AWS incluye varios tutoriales que lo guiarán a través de los casos de uso comunes de Amazon RDS. Muchos de estos tutoriales muestran cómo utilizar Amazon RDS con otros servicios de AWS. Además, puede acceder al código de muestra en GitHub.

> **Note**
>
> Puede encontrar más tutoriales en el Blog de AWS Database. Para obtener información acerca de la capacitación, consulte AWS Training and Certification.

Temas

- Tutoriales en esta guía
- Tutoriales en otras AWS guías
- Portal de contenido de laboratorios y talleres de AWS para Amazon RDS PostgreSQL
- Portal de contenido de laboratorios y talleres de AWS para Amazon RDS MySQL
- Tutoriales y código de muestra en GitHub
- Cómo utilizar este servicio con un AWS SDK

Tutoriales en esta guía

En los siguientes tutoriales aprenderá a realizar tareas comunes con Amazon RDS:

- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4)

  Aprenda a incluir una instancia de BD en una nube privada virtual (VPC) basada en el servicio Amazon VPC. En este caso, la VPC comparte datos con un servidor web que se ejecuta en una instancia de Amazon EC2 en la misma VPC.
- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (modo de pila doble)

  Aprenda a incluir una instancia de BD en una nube privada virtual (VPC) basada en el servicio Amazon VPC. En este caso, la VPC comparte datos con una instancia de Amazon EC2 en la misma VPC. En este tutorial, creará la VPC para este escenario que funciona con una base de datos que se ejecuta en modo de pila doble.

- Explicación: crear un servidor web y una instancia de base de datos de Amazon RDS

  Obtenga información sobre cómo instalar un servidor web Apache con PHP y crear una base de datos MySQL. El servidor web se ejecuta en una instancia Amazon EC2 mediante Amazon Linux y la base de datos de MySQL es una instancia de base de datos de MySQL. Tanto la instancia de Amazon EC2 y el clúster de instancia se ejecutan en una Amazon VPC.

- Tutorial: restauración de una instancia de base de datos de Amazon RDS a partir de una instantánea de base de datos

  Obtenga información sobre cómo restaurar una instancia de base de datos a partir de una instantánea de base de datos.

- Tutorial: Uso de una función de Lambda para obtener acceso a la base de datos de Amazon RDS

  Obtenga información sobre cómo crear una función de Lambda para obtener acceso a la base de datos a través de un proxy, crear una tabla, agregar algunos registros y recuperar los registros de la tabla. También aprenderá a invocar la función Lambda y verificar los resultados de la consulta.

- Tutorial: especificar qué instancias de base de datos se deben detener mediante etiquetas

  Obtenga información sobre el uso de etiquetas para especificar qué instancias de base de datos se deben detener.

- Tutorial: Registrar el estado de una instancia de base de datos con Amazon EventBridge

  Obtenga información para registrar un cambio de estado de instancia de base de datos mediante Amazon EventBridge y AWS Lambda.

- Tutorial: creación de una alarma de Amazon CloudWatch para el retardo de réplica del clúster de base de datos multi-AZ para Amazon RDS

  Aprenda a crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando el retraso de réplica de un clúster de base de datos Multi-AZ supere un límite. Una alarma vigila una métrica de `ReplicaLag` durante el periodo especificado. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Amazon EC2 Auto Scaling.

Tutoriales en otras AWS guías

Los siguientes tutoriales de otras guías de AWS muestran cómo realizar tareas comunes con Amazon RDS:

- Tutorial: Rotación de un secreto para una base de datos de AWS en la guía del usuario de AWS Secrets Manager

  Aprenda a crear un secreto para una AWS base de datos y configurar el secreto a fin de rotar según una programación. Puede activar una rotación manualmente y después confirmar que la nueva versión del secreto continúa proporcionando acceso.

- Tutoriales y ejemplos en la guía para desarrolladores de AWS Elastic Beanstalk

  Obtenga información para implementar aplicaciones que utilizan bases de datos de Amazon RDS con AWS Elastic Beanstalk.

- Uso de datos de una base de datos de Amazon RDS para crear un origen de datos de Amazon ML en la Amazon Machine Learning Developer Guide

  Obtenga información sobre cómo crear un objeto de origen de datos de Amazon Machine Learning (Amazon ML) a partir de datos almacenados en una instancia de base de datos MySQL.

- Habilitar manualmente el acceso a una instancia de Amazon RDS en una VPC en la Guía del usuario de Amazon QuickSight

  Obtenga información sobre cómo habilitar el acceso de QuickSight a una instancia de base de datos de Amazon RDS en una VPC.

Portal de contenido de laboratorios y talleres de AWS para Amazon RDS PostgreSQL

La siguiente colección de talleres y otros contenidos prácticos le ayudan a conocer las características y capacidades de Amazon RDS PostgreSQL:

- Creación de una instancia de base de datos

  Aprenda a crear la instancia de base de datos.

- Supervisión del rendimiento con las herramientas de RDS

  Aprenda a utilizar las herramientas de AWS y SQL (Cloudwatch, Monitorización mejorada, Slow Query Logs, Información sobre rendimiento, PostgreSQL Catalog Views) para comprender los problemas de rendimiento e identificar formas de mejorar el rendimiento de su base de datos.

Portal de contenido de laboratorios y talleres de AWS para Amazon RDS MySQL

La siguiente colección de talleres y otros contenidos prácticos le ayudan a conocer las características y capacidades de Amazon RDS MySQL:

- Creación de una instancia de base de datos

  Aprenda a crear la instancia de base de datos.

- Uso de Información sobre rendimiento

  Aprenda a supervisar y ajustar su instancia de base de datos mediante Información sobre rendimiento.

Tutoriales y código de muestra en GitHub

En los siguientes tutoriales y en el código de muestra, aprenderá a realizar tareas comunes con Amazon RDS:

- Creación del rastreador de elementos de Amazon Relational Database Service

  Aprenda a crear una aplicación que realice un seguimiento e informe sobre los elementos de trabajo. Esta aplicación utiliza Amazon RDS, Amazon Simple Email Service, Elastic Beanstalk y SDK for Java 2.x.

Cómo utilizar este servicio con un AWS SDK

Los kits de desarrollo de software (SDK) de AWS se encuentran disponibles en muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK para C++	Ejemplos de código de AWS SDK para C++
AWS CLI	Ejemplos de código de la AWS CLI

Documentación de SDK	Ejemplos de código
AWS SDK para Go	Ejemplos de código de la AWS SDK para Go
AWS SDK para Java	Ejemplos de código de la AWS SDK para Java
AWS SDK para JavaScript	Ejemplos de código de la AWS SDK para JavaScript
AWS SDK para Kotlin	Ejemplos de código de la AWS SDK para Kotlin
AWS SDK para .NET	Ejemplos de código de la AWS SDK para .NET
AWS SDK para PHP	Ejemplos de código de la AWS SDK para PHP
Herramientas de AWS para PowerShell	Ejemplos de código de la Herramientas de AWS para PowerShell
AWS SDK para Python (Boto3)	Ejemplos de código de la AWS SDK para Python (Boto3)
AWS SDK para Ruby	Ejemplos de código de la AWS SDK para Ruby
AWS SDK para Rust	Ejemplos de código de la AWS SDK para Rust
AWS SDK para SAP ABAP	Ejemplos de código de la AWS SDK para SAP ABAP
AWS SDK para Swift	Ejemplos de código de la AWS SDK para Swift

Para obtener ejemplos específicos de este servicio, consulte Ejemplos de código de Amazon RDS con SDK de AWS.

> **Ejemplo de disponibilidad**
>
> ¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Prácticas recomendadas para Amazon RDS

Descubra las prácticas recomendadas para trabajar con Amazon RDS. A medida que se identifiquen nuevas prácticas recomendadas, se actualizará esta sección.

Temas

- Directrices operativas básicas de Amazon RDS
- Recomendaciones de RAM de las instancias de base de datos
- Mantenimiento de versiones actualizadas del motor de base de datos
- Controladores de bases de datos de AWS
- Uso del monitoreo mejorado para identificar los problemas del sistema operativo
- Uso de métricas para identificar los problemas de rendimiento
- Ajuste de consultas
- Prácticas recomendadas para trabajar con MySQL
- Prácticas recomendadas para trabajar con MariaDB
- Prácticas recomendadas para trabajar con Oracle
- Prácticas recomendadas para trabajar con PostgreSQL
- Prácticas recomendadas para trabajar con SQL Server
- Trabajo con los grupos de parámetros de base de datos
- Prácticas recomendadas para automatizar la creación de instancias de base de datos
- Vídeo de nuevas características de Amazon RDS

> **Note**
>
> Para ver recomendaciones frecuentes para Amazon RDS, consulte Recomendaciones para Amazon RDS.

Directrices operativas básicas de Amazon RDS

A continuación se detallan las directrices operativas básicas que se deben seguir al trabajar con Amazon RDS. El Acuerdo de nivel de servicios de Amazon RDS requiere que se sigan estas directrices:

- Utilice métricas para supervisar la memoria, la CPU, el retraso de las réplicas y el uso de almacenamiento. Puede configurar Amazon CloudWatch para que le notifique cuando cambien los patrones de uso o cuando su implementación se acerque a los límites de capacidad. De esta forma, puede mantener el rendimiento y la disponibilidad del sistema.
- Escale la instancia de base de datos cuando se esté acercando a los límites de la capacidad de almacenamiento. Debe tener búfer de almacenamiento y de memoria para asumir incrementos imprevistos de la demanda de las aplicaciones.
- Habilite las copias de seguridad automáticas y configure la ventana de copia de seguridad para que se produzca durante el momento diario en el que más bajen las IOPS de escritura. Es entonces cuando una copia de seguridad es menos perjudicial para el uso de la base de datos.
- Si la carga de trabajo de la base de datos requiere más E/S de la aprovisionada, la recuperación tras una conmutación por error o tras un error de la base de datos será lenta. Para incrementar la capacidad de E/S de una instancia de base de datos, lleve a cabo una de las acciones siguientes o todas ellas:
  - Migre a una clase de instancia de base de datos distinta con una alta capacidad de E/S.
  - Convierta desde el almacenamiento magnético al almacenamiento de uso general o de IOPS provisionadas en función del incremento que necesite. Para obtener información acerca de los tipos de almacenamiento disponibles, consulte Tipos de almacenamiento de Amazon RDS.

    Si convierte a almacenamiento de IOPS provisionadas, asegúrese de que también usa una clase de instancia de base de datos que se haya optimizado para las IOPS provisionadas. Para obtener información acerca de las IOPS provisionadas, consulte Almacenamiento de SSD de IOPS aprovisionadas.
  - Si ya está usando almacenamiento de IOPS provisionadas, aprovisione capacidad de rendimiento adicional.
- Si la aplicación cliente almacena en caché los datos del Servicio de nombres de dominio (DNS) de las instancias de base de datos, defina un valor de tiempo de vida (TTL) de menos de 30 segundos. La dirección IP subyacente de una instancia de base de datos puede cambiar después de producirse una conmutación por error. Por lo tanto, almacenar en caché los datos de DNS durante un tiempo prolongado puede provocar errores de conexión. Es posible que tu aplicación intente conectarse a una dirección IP que ya no esté en servicio.
- Pruebe la conmutación por error de la instancia de base de datos para comprender cuánto tiempo tarda el proceso en su caso de uso particular. Pruebe también la conmutación por error para asegurarse de que la aplicación que accede a su instancia de base de datos puede conectarse automáticamente a la nueva instancia de base de datos después de la conmutación por error.

Recomendaciones de RAM de las instancias de base de datos

Una práctica recomendada de rendimiento de Amazon RDS consiste en asignar suficiente RAM para que el conjunto de trabajo resida casi por completo en la memoria. El conjunto de trabajo son los datos e índices que se usan con frecuencia en su instancia. Cuanto más use la instancia de base de datos, más crecerá el conjunto de trabajo.

Para saber si el conjunto de trabajo está en la memoria casi en su totalidad, compruebe la métrica ReadIOPS (usando Amazon CloudWatch) mientras la instancia de base de datos está sometida a carga. El valor de ReadIOPS debe ser pequeño y estable. En algunos casos, escalar verticalmente la clase de instancia de base de datos a una clase con más RAM da como resultado una disminución brusca de ReadIOPS. En estos casos, el conjunto de trabajo no estaba casi completamente en la memoria. Siga escalando hasta que ReadIOPS no se reduzca bruscamente después de una operación de escalado o hasta que ReadIOPS se reduzca muy poco. Para obtener más información acerca de la monitorización de las métricas de las instancias de base de datos, consulte Consulta de métricas en la consola de Amazon RDS.

Mantenimiento de versiones actualizadas del motor de base de datos

Actualice con regularidad la versión de motor de base de datos para mantener la seguridad, el rendimiento y el cumplimiento. Amazon RDS publica nuevas versiones principales y secundarias que incluyen revisiones de seguridad, mejoras de rendimiento y características nuevas. Ejecutar un motor de base de datos obsoleto puede exponer las cargas de trabajo a vulnerabilidades conocidas, problemas de compatibilidad y una asistencia reducida por parte de AWS y los proveedores de bases de datos.

Para minimizar las interrupciones, tenga en cuenta lo siguiente cuando planifique las actualizaciones:

- Realice pruebas en un entorno provisional: valide la nueva versión en la carga de trabajo antes de actualizar las bases de datos de producción.
- Utilice las actualizaciones administradas por Amazon RDS: habilite las actualizaciones automáticas de versiones secundarias para facilitar la aplicación de revisiones.
- Programe las actualizaciones de las versiones principales: consulte las notas de la versión, compruebe la compatibilidad de las aplicaciones y planifique un periodo de actualización controlado.

Las actualizaciones periódicas ayudan a garantizar que la base de datos permanezca segura, optimizada y alineada con las prácticas recomendadas de AWS.

Controladores de bases de datos de AWS

Recomendamos el conjunto de controladores de AWS para la conectividad de las aplicaciones. Los controladores se han diseñado para permitir tiempos de transición y conmutación por error más rápidos y autenticarse con AWS Secrets Manager, AWS Identity and Access Management (IAM) e identidad federada. Los controladores de AWS se basan en la supervisión del estado de la instancia de base de datos y en el conocimiento de la topología de la instancia para determinar quién es el nuevo escritor. Este enfoque reduce los tiempos de transición y conmutación por error a segundos de un solo dígito, en comparación con las decenas de segundos de los controladores de código abierto.

A medida que se introducen nuevas características de servicio, el objetivo del conjunto de controladores de AWS es contar con soporte integrado para estas características de servicio.

Para obtener más información, consulte Conexión a instancias de base de datos con los controladores de AWS.

Uso del monitoreo mejorado para identificar los problemas del sistema operativo

Cuando el monitoreo mejorado está habilitado, Amazon RDS proporciona métricas en tiempo real para el sistema operativo (SO) en el que se ejecuta la instancia de base de datos. Puede ver las métricas de su instancia de base de datos mediante la consola. También puede consumir la salida JSON de monitoreo mejorado en Amazon CloudWatch Logs en un sistema de monitoreo de su elección. Para obtener más información acerca de la monitorización mejorada, consult Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Uso de métricas para identificar los problemas de rendimiento

Para identificar los problemas de desempeño causados por la falta de recursos y otros cuellos de botella frecuentes, puede monitorizar las métricas disponibles para la instancia de base de datos de Amazon RDS.

Visualización de métricas de rendimiento

Debe monitorizar las métricas de desempeño con frecuencia para ver los valores medios, máximos y mínimos de diversos intervalos de tiempo. De este modo podrá identificar cuándo se degrada el rendimiento. También puede definir alarmas de Amazon CloudWatch para umbrales de métricas concretos si desea recibir alertas cuando se alcancen.

Para solucionar los problemas de rendimiento, es importante conocer el rendimiento de referencia del sistema. Al configurar una instancia de base de datos y ejecutarla con una carga de trabajo típica, capture los valores promedio, máximo y mínimo de todas las métricas de rendimiento. Hágalo en diferentes intervalos (por ejemplo, una hora, 24 horas, una semana o dos semanas). Esto puede darle una idea de lo que es normal. Ayuda a obtener comparaciones para las horas con picos y valles de funcionamiento. Puede usar esta información para saber cuándo cae el desempeño por debajo de los niveles estándar.

Si utiliza clústeres de base de datos Multi-AZ, supervise la diferencia de tiempo entre la última transacción en la instancia de base de datos del escritor y la última transacción aplicada en una instancia de base de datos del lector. Esta diferencia se llama retraso de réplicas. Para obtener más información, consulte Retraso de réplica y clústeres de base de datos Multi-AZ.

Puede ver las métricas combinadas de Información de rendimiento y CloudWatch en el panel de Información de rendimiento y monitorizar su instancia de base de datos. Para utilizar esta vista de monitorización, es necesario activar Información de rendimiento para la instancia de base de datos. Para obtener más información sobre la monitorización, consulte Visualización de las métricas combinadas en la consola de Amazon RDS.

Puede crear un informe de análisis de rendimiento para un período de tiempo específico y ver la información identificada y las recomendaciones para resolver los problemas. Para obtener más información, consulte Creación de un informe de análisis de rendimiento en Información de rendimiento.

Para ver las métricas de desempeño

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y seleccione una instancia de base de datos.
3. Elija Monitoring (Monitorización).

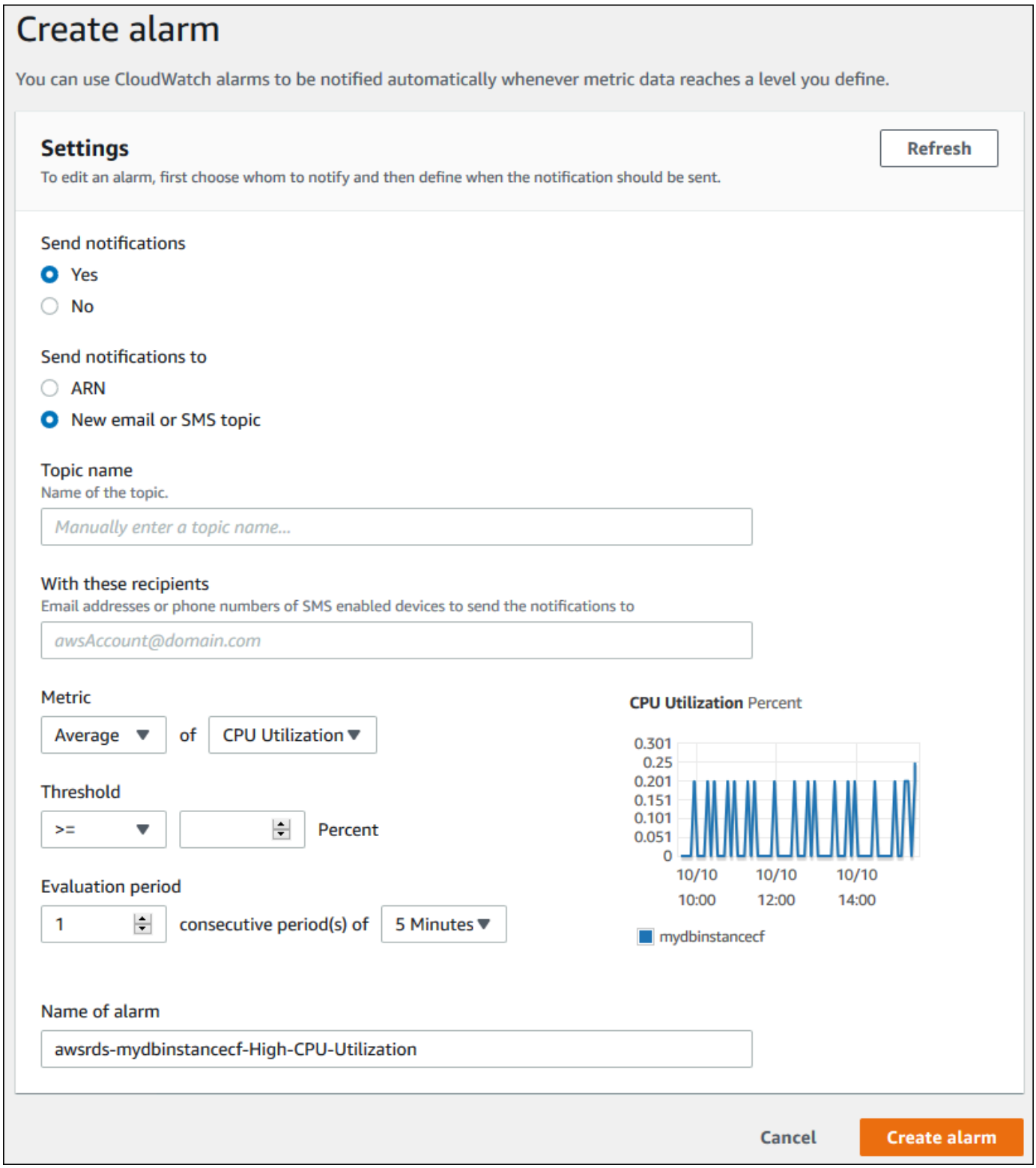
El panel proporciona las métricas de rendimiento. Las métricas muestran de forma predeterminada la información de las últimas tres horas.

4. Use los botones numerados de la esquina superior derecha para recorrer las métricas adicionales o ajustar la configuración para ver más métricas.
5. Seleccione una métrica de rendimiento para ajustar el intervalo de tiempo con el fin de ver los datos de un día distinto del actual. Puede cambiar los valores Statistic, Time Range y Period para ajustar la información mostrada. Por ejemplo, puede que desee ver los valores máximos de una métrica para cada día de las dos últimas semanas. Si es así, establezca Statistic (Estadísticas) en Maximum (Máximo), Máximo (Intervalo de tiempo) en Last 2 Weeks (Últimas 2 semanas) y Period (Período) en Day (Día).

También puede ver las métricas de rendimiento usando la interfaz de línea de comandos (CLI) o la API. Para obtener más información, consulte Consulta de métricas en la consola de Amazon RDS.

Para definir una alarma de CloudWatch

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y seleccione una instancia de base de datos.
3. Seleccione Logs & events (Registros y eventos).
4. En la sección CloudWatch alarms (Alarmas de CloudWatch), elija Create alarm (Crear alarma).



5. En Send notifications (Enviar notificaciones), elija Yes (Sí) y en Send notifications to (Enviar notificaciones a), elija New email or SMS topic (Nuevo correo electrónico o tema de SMS).

6. En Topic name (Nombre de tema), escriba un nombre para la notificación y en With these recipients (Con estos destinatarios), escriba una lista separada por comas de direcciones de correo electrónico y números de teléfono.
7. En Metric (Métrica), seleccione la estadística de alarmas y métrica que definir.
8. Para Threshold (Umbral), especifique si la métrica debe ser mayor que, menor que o igual que el umbral y especifique el valor del umbral.
9. Para Evaluation period (Período de evaluación), elija el periodo de evaluación de la alarma. Para consecutive period(s) of (períodos consecutivos de), elija el período durante el que desea que el umbral se deba haber alcanzado para disparar la alarma.
10. En Name of alarm (Nombre de la alarma), escriba un nombre para la alarma.
11. Elija Create Alarm.

La alarma aparece en la sección CloudWatch alarms (Alarmas de CloudWatch).

Evaluación de las métricas de rendimiento

Una instancia de base de datos tiene varias categorías de métricas diferentes, y la forma de determinar los valores aceptables depende de la métrica.

CPU

- Utilización de la CPU: porcentaje de la capacidad de procesamiento del equipo que está en uso.

Memoria

- Memoria que se puede liberar: cuánta RAM está disponible en la instancia de base de datos en bytes. La línea roja de las métricas de la pestaña de monitorización está marcada en el 75 % para las métricas de CPU, memoria y almacenamiento. Si el consumo de memoria de instancia supera con frecuencia esta línea, significa que debe verificar la carga de trabajo o actualizar la instancia.
- Uso del espacio de intercambio: cuánto espacio de intercambio usa la instancia de base de datos en bytes.

Espacio en disco

- Espacio de almacenamiento disponible: cuánto espacio en disco no usa actualmente la instancia de base de datos en megabytes.

Operaciones de entrada y salida

- IOPS de lectura, IOPS de escritura: número medio de operaciones de lectura o escritura en disco por segundo.
- Latencia de lectura, latencia de escritura: tiempo medio de una operación de lectura o escritura en milisegundos.
- Rendimiento de lectura, rendimiento de escritura: número medio de megabytes leídos o escritos en el disco por segundo.
- Profundidad de la cola: número de operaciones de E/S que están esperando para la lectura o escritura en el disco.

Tráfico de red

- Rendimiento de recepción de la red, rendimiento de transmisión de la red – La velocidad del tráfico de red de entrada y salida de la instancia de base de datos en bytes por segundo.

Conexiones a base de datos

- Conexiones a base de datos: número de sesiones cliente que están conectadas a la instancia de base de datos.

Para obtener descripciones individuales más detalladas de cada métrica de rendimiento disponible, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.

En general, los valores aceptables para las métricas de desempeño dependen del aspecto de la referencia y de lo que hace la aplicación. Investigue las variaciones coherentes o de las tendencias con respecto a la referencia. La siguiente sección ofrece algunas sugerencias sobre tipos concretos de métricas:

- High CPU or RAM consumption (Alto consumo de CPU o RAM): unos valores elevados de consumo de CPU o RAM pueden ser adecuados. Por ejemplo, pueden ser si se ajustan a los objetivos de su aplicación (de rendimiento o simultaneidad, por ejemplo) y son los esperados.
- Consumo de espacio en disco: investigue el consumo de espacio en el disco si el espacio utilizado está por sistema alrededor o por encima del 85 % del espacio total disponible en el disco. Compruebe si es posible eliminar datos de la instancia o archivar los datos en un sistema diferente para liberar espacio.

- Tráfico de red: para el tráfico de red, hable con el administrador de su sistema para saber cuál es el rendimiento esperado para la red de su dominio y para su conexión a Internet. Investigue el tráfico de red si el rendimiento es por sistema inferior al esperado.
- Conexiones a bases de datos: valore la posibilidad de restringir las conexiones a las bases de datos si ve que hay un alto número de conexiones de usuarios junto con una reducción en el rendimiento y el tiempo de respuesta de la instancia. El mejor número de conexiones de usuarios para su instancia de base de datos variará en función de la clase de instancia y de la complejidad de las operaciones que se estén llevando a cabo. Para determinar el número de conexiones a bases de datos, asocie la instancia de base de datos con un grupo de parámetros. En este grupo, defina el parámetro User Connections (Conexiones de usuario) en un valor distinto de 0 (ilimitado). Puede utilizar un grupo de parámetros existente o crear uno nuevo. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
- Métricas de IOPS: los valores esperados para las métricas de IOPS dependen de la especificación del disco y la configuración del servidor, así que debe usar su referencia para conocer los valores típicos. Investigue si los valores son por sistema diferentes de los de la referencia. Para un desempeño óptimo de IOPS, asegúrese de que el conjunto de trabajo típico se ajuste a la memoria para minimizar las operaciones de lectura y escritura.

Para los problemas con las métricas de rendimiento, un primer paso para mejorar el rendimiento es ajustar las consultas más utilizadas y más costosas. Ajústelas para ver si hacerlo reduce la presión sobre los recursos del sistema. Para obtener más información, consulte Ajuste de consultas.

Si sus consultas están ajustadas y el problema persiste, considere la posibilidad de actualizar su Clases de instancia de base de datos de de Amazon RDS. Puede actualizarla a una con más cantidad del recurso (CPU, RAM, espacio en disco, ancho de banda de red, capacidad de E/S) relacionado con el problema.

Ajuste de consultas

Una de las formas más eficaces de mejorar el desempeño de la instancia de base de datos es ajustar las consultas más utilizadas y que más recursos consumen. Aquí, se ajustan para que sean menos costosos de ejecutar. Para obtener información sobre cómo mejorar las consultas, utilice los siguientes recursos:

- MySQL – Consulte Optimización de sentencias SELECT en la documentación de MySQL. También puede ir a MySQL Performance Tuning and Optimization Resources para ver otros recursos relacionados con el ajuste de las consultas.

- Oracle – Consulte la Guía de ajuste SQL de base de datos en la documentación de Oracle Database.
- SQL Server – Consulte Análisis de una consulta en la documentación de Microsoft. También puede usar las vistas de administración de datos (DMV) relacionadas con la ejecución, los índices y las operaciones de E/S que se describen en la documentación de System Dynamic Management Views en la documentación de Microsoft para solucionar los problemas de las consultas de SQL Server.

  Un aspecto habitual del ajuste de consultas es la creación de índices eficaces. Para obtener mejoras potenciales en el índice de la instancia de base de datos, consulte el Asesor de ajuste del motor de base de datos en la documentación de Microsoft. Para obtener información sobre el uso del Asesor de Ajustes en RDS for SQL Server, consulte Análisis de la carga de trabajo de una base de datos de una instancia de base de datos de Amazon RDS for SQL Server con el Asistente para la optimización del motor de base de datos.
- PostgreSQL – Vaya a Using EXPLAIN en la documentación de PostgreSQL para ver cómo se analiza un plan de consulta. Puede utilizar esta información para modificar una consulta o las tablas subyacentes con el fin de mejorar el desempeño de las consultas.

  Para obtener información sobre cómo especificar uniones en las consultas para un mejor desempaño, consulte Controlling the Planner with Explicit JOIN Clauses.
- MariaDB – Consulte optimizaciones de consultas en la documentación de MariaDB.

Prácticas recomendadas para trabajar con MySQL

Tanto el tamaño de las tablas como el número de tablas de una base de datos MySQL pueden afectar al rendimiento.

Tamaño de las tablas

Normalmente, las restricciones del sistema operativo relativas al tamaño de los archivos determinan el tamaño máximo efectivo de las tablas para las bases de datos MySQL. Por tanto, los límites generalmente no están determinados por restricciones internas de MySQL.

En una instancia de base de datos de MySQL, evite que las tablas de la base de datos crezcan demasiado. Aunque el límite de almacenamiento general es de 64 TiB, los límites de almacenamiento aprovisionado restringen el tamaño máximo de un archivo de tabla de MySQL a 16 TiB. Divida las tablas grandes para que los tamaños de archivo estén claramente por debajo del

límite de 16 TiB. Este método también puede mejorar el desempeño y el tiempo de recuperación. Para obtener más información, consulte Límites de tamaño de archivo de MySQL en Amazon RDS.

Las tablas muy grandes (de más de 100 GB de tamaño) pueden afectar negativamente al rendimiento tanto de las lecturas como de las escrituras (incluidas las instrucciones de lenguaje de manipulación de datos o DML y especialmente las instrucciones lenguaje de definición de datos o DDL). Que haya índices en tablas grandes puede aumentar considerablemente el desempeño de SELECT, pero también puede deteriorar el rendimiento de las instrucciones DML. Las instrucciones DDL, como `ALTER TABLE`, pueden ser considerablemente más lentas con las tablas grandes, pues con esas operaciones es posible que en algunos casos se reconstruya completamente una tabla. Con estas instrucciones DDL es posible que las tablas se bloqueen durante la duración de la operación.

La cantidad de memoria que requiere MySQL para lecturas y escrituras depende de las tablas que se impliquen en las operaciones. Es una práctica recomendada tener al menos suficiente RAM para mantener los índices de las tablas que se utilicen activamente. Para determinar cuáles son las diez tablas e índices más grandes de una base de datos, utilice la siguiente consulta:

```
select table_schema, TABLE_NAME, dat, idx from
(SELECT table_schema, TABLE_NAME,
       ( data_length ) / 1024 / 1024 as dat,
       ( index_length ) / 1024 / 1024 as idx
FROM information_schema.TABLES
order by 3 desc ) a
order by 3 desc
limit 10;
```

Número de tablas

El sistema de archivos subyacente puede tener un límite en cuanto al número de archivos que representan tablas. Sin embargo, MySQL no tiene límite en el número de tablas. A parte de esto, el número total de tablas que haya en el motor de almacenamiento de InnoDB de MySQL puede contribuir al deterioro del rendimiento, independientemente del tamaño que tengan esas tablas. Para limitar el efecto del sistema operativo, puede distribuir las tablas entre varias bases de datos en la misma instancia de base de datos MySQL. Si lo hace, se podría limitar el número de archivos que hay en un directorio, pero no se resolverá el problema general.

Si hay deterioro del rendimiento debido a un número de tablas grande (más de 10 000), es a causa de que MySQL está trabajando con archivos de almacenamiento, que incluye abrirlos y cerrarlos.

Para atender esta cuestión, puede aumentar el tamaño de los parámetros `table_open_cache` y `table_definition_cache`. Sin embargo, aumentar los valores de esos parámetros podría aumentar considerablemente la cantidad de memoria que usa MySQL e incluso podría agotar toda la memoria disponible. Para obtener más información, consulte How MySQL Opens and Closes Tables, en la documentación de MySQL.

Además, que haya demasiadas tablas puede afectar considerablemente el tiempo de inicio de MySQL. Es posible que afecte la posibilidad de que haya un apagado y un reinicio perfectos, así como una recuperación ante bloqueos, especialmente en versiones anteriores a MySQL 8.0.

Recomendamos tener menos de 10 000 tablas en total distribuidas entre todas las bases de datos de una instancia de base de datos. Para un caso de uso con un número de tablas grande en una base de datos MySQL, consulte One Million Tables in MySQL 8.0 (1 millón de tablas en MySQL 8.0).

Motor de almacenamiento

Las características de restauración a un momento dado y restauración de instantáneas de Amazon RDS para MySQL requieren un motor de almacenamiento que pueda recuperarse en caso de bloqueo. Estas características solo son compatibles para el motor de almacenamiento InnoDB. Aunque MySQL admite varios motores de almacenamiento con diversas capacidades, no todos están optimizados para la recuperación en caso de bloqueo y la durabilidad de los datos. Por ejemplo, el motor de almacenamiento de MyISAM no admite la recuperación fiable tras bloqueo y podría impedir que la restauración a un momento dado o la restauración de instantáneas funcionen según lo previsto. Esto podría traducirse en datos perdidos o dañados cuando MySQL se reinicia después de un bloqueo.

InnoDB es el motor de almacenamiento recomendado y admitido para las instancias de base de datos de MySQL en Amazon RDS. Las instancias de base de datos de InnoDB también se pueden migrar a Aurora, mientras que las instancias de MyISAM no se pueden migrar. Sin embargo, MyISAM funciona mejor que InnoDB si se requiere una capacidad intensiva de búsqueda de texto completo. Si a pesar de ello quiere usar MyISAM con Amazon RDS, seguir los pasos que se describen en Copias de seguridad automatizadas con motores de almacenamiento de MySQL no compatibles puede resultar útil en algunas situaciones para la funcionalidad de restauración de instantáneas.

Si desea convertir tablas de MyISAM en tablas de InnoDB, puede utilizar el proceso que se describe en Converting Tables from MyISAM to InnoDB, en la documentación de MySQL. MyISAM e InnoDB tienen diferentes fortalezas y debilidades, por lo que debe evaluar a fondo el impacto de este cambio en sus aplicaciones antes de realizarlo.

Además, no se admite el motor de almacenamiento federado para Amazon RDS for MySQL.

Prácticas recomendadas para trabajar con MariaDB

Tanto el tamaño de las tablas como el número de tablas de una base de datos de MariaDB pueden afectar al rendimiento.

Tamaño de las tablas

Normalmente, las restricciones del sistema operativo relativas al tamaño de los archivos determinan el tamaño máximo efectivo de las tablas para las bases de datos de MariaDB. Por tanto, los límites generalmente no están determinados por restricciones internas de MariaDB.

En una instancia de base de datos de MariaDB, evite que las tablas de la base de datos aumenten demasiado de tamaño. Aunque el límite de almacenamiento general es 64 TiB, debido a los límites de almacenamiento aprovisionado el tamaño máximo de un archivo de tabla de MariaDB se restringe a 16 TiB. Divida las tablas grandes para que los tamaños de archivo estén claramente por debajo del límite de 16 TiB. Este método también puede mejorar el desempeño y el tiempo de recuperación.

Las tablas muy grandes (de más de 100 GB de tamaño) pueden afectar negativamente al rendimiento tanto de las lecturas como de las escrituras (incluidas las instrucciones de lenguaje de manipulación de datos o DML y especialmente las instrucciones lenguaje de definición de datos o DDL). Que haya índices en tablas grandes puede aumentar considerablemente el desempeño de SELECT, pero también puede deteriorar el rendimiento de las instrucciones DML. Las instrucciones DDL, como `ALTER TABLE`, pueden ser considerablemente más lentas con las tablas grandes, pues con esas operaciones es posible que en algunos casos se reconstruya completamente una tabla. Con estas instrucciones DDL es posible que las tablas se bloqueen durante la duración de la operación.

La cantidad de memoria que requiere MariaDB para lecturas y escrituras depende de las tablas que se impliquen en las operaciones. Es una práctica recomendada tener al menos suficiente RAM para mantener los índices de las tablas que se utilicen activamente. Para determinar cuáles son las diez tablas e índices más grandes de una base de datos, utilice la siguiente consulta:

```
select table_schema, TABLE_NAME, dat, idx from
(SELECT table_schema, TABLE_NAME,
       ( data_length ) / 1024 / 1024 as dat,
       ( index_length ) / 1024 / 1024 as idx
FROM information_schema.TABLES
order by 3 desc ) a
```

```
order by 3 desc
limit 10;
```

Número de tablas

El sistema de archivos subyacente puede tener un límite en cuanto al número de archivos que representan tablas. Sin embargo, MariaDB no tiene límite en el número de tablas. A parte de esto, el número total de tablas que haya en el motor de almacenamiento de InnoDB de MariaDB puede contribuir al deterioro del rendimiento, independientemente del tamaño que tengan esas tablas. Para limitar el efecto del sistema operativo, puede distribuir las tablas entre varias bases de datos en la misma instancia de base de datos de MariaDB. Si lo hace, se podría limitar el número de archivos que hay en un directorio, pero no se resuelve el problema general.

Si hay deterioro del rendimiento debido a un número de tablas grande (más de 10 000), es a causa de que MariaDB está trabajando con archivos de almacenamiento. Este trabajo incluye que MariaDB abra y cierre archivos de almacenamiento. Para atender esta cuestión, puede aumentar el tamaño de los parámetros `table_open_cache` y `table_definition_cache`. Sin embargo, aumentar los valores de esos parámetros podría aumentar considerablemente la cantidad de memoria que usa MariaDB. Incluso podría usar toda la memoria disponible. Para obtener más información, consulte Optimizing table_open_cache, en la documentación de MariaDB.

Además, que haya demasiadas tablas puede afectar considerablemente el tiempo de inicio de MariaDB. Es posible que afecte la posibilidad de que haya un apagado y un reinicio perfectos, así como una recuperación ante bloqueos. Recomendamos tener menos de 10 000 tablas en total distribuidas entre todas las bases de datos de una instancia de base de datos.

Motor de almacenamiento

Las características de restauración a un momento dado y restauración de instantáneas de Amazon RDS for MariaDB requieren un motor de almacenamiento que pueda recuperarse en caso de bloqueo. Aunque MariaDB admite varios motores de almacenamiento con diversas capacidades, no todos están optimizados para la recuperación en caso de bloqueo y la durabilidad de los datos. Por ejemplo, aunque Aria es un sustituto a prueba de bloqueos para MyISAM, también podría impedir que la restauración a un momento dado o la restauración de instantáneas funcionen según lo previsto. Esto podría traducirse en datos perdidos o dañados cuando MariaDB se reinicia después de un bloqueo. InnoDB es el motor de almacenamiento recomendado y admitido para las instancias de base de datos de MariaDB en Amazon RDS. Si a pesar de ello quiere usar Aria con Amazon RDS, seguir los pasos que se describen en Copias de seguridad automatizadas con motores de

almacenamiento de MariaDB no compatibles puede resultar útil en algunas situaciones para la funcionalidad de restauración de instantáneas.

Si desea convertir tablas de MyISAM en tablas de InnoDB, puede utilizar el proceso que se describe en Converting Tables from MyISAM to InnoDB en la documentación de MariaDB. MyISAM e InnoDB tienen diferentes fortalezas y debilidades, por lo que debe evaluar a fondo el impacto de este cambio en sus aplicaciones antes de realizarlo.

Prácticas recomendadas para trabajar con Oracle

Para obtener información sobre las prácticas recomendadas para trabajar con Amazon RDS for Oracle, consulte Prácticas recomendadas para ejecutar Oracle Database en Amazon Web Services.

Un taller virtual de AWS de 2020 incluyó una presentación sobre la ejecución de bases de datos de Oracle de producción en Amazon RDS. Puede ver aquí un vídeo de la presentación.

Prácticas recomendadas para trabajar con PostgreSQL

De las dos áreas importantes en las que puede mejorar el rendimiento con RDS para PostgreSQL, una es la carga de datos en una instancia de base de datos. Otra es cuando se utiliza la característica autovacuum de PostgreSQL. Las siguientes secciones tratan algunas de las prácticas recomendadas para esas áreas.

Para obtener información sobre cómo Amazon RDS implementa otras tareas comunes de DBA de PostgreSQL, consulte Tareas comunes de los administradores de base de datos (DBA) para Amazon RDS para PostgreSQL.

Carga de datos en una instancia de base de datos de PostgreSQL

Cuando se cargan datos en una instancia de base de datos de Amazon RDS para PostgreSQL, se debe modificar la configuración de la instancia de base de datos y los valores del grupo de parámetros de base de datos. Configúrelos para permitir la importación más eficiente de datos a su instancia de base de datos.

Modifique la configuración de su instancia de base de datos como se indica a continuación:

- Deshabilite las copias de seguridad de la instancia de base de datos (defina backup_retention como 0)
- Desactive Multi-AZ

Modifique el grupo de parámetros de base de datos para incluir la siguiente configuración. Asimismo, pruebe la configuración de los parámetros para encontrar los ajustes más eficientes para su instancia de base de datos.

- Aumente el valor del parámetro `maintenance_work_mem`. Para obtener más información acerca de los parámetros de consumo de recursos de PostgreSQL, consulte la documentación de PostgreSQL.
- Aumente el valor de los parámetros `max_wal_size` u `checkpoint_timeout` para reducir el número de escrituras en el registro de escritura anticipada (WAL).
- Desactive el parámetro `synchronous_commit`.
- Deshabilite el parámetro autovacuum de PostgreSQL.
- Asegúrese de que ninguna de las tablas que está importando esté sin registrar. Los datos almacenados en tablas sin registrar pueden perderse durante una conmutación por error. Para obtener más información, consulte el apartado de CREACIÓN DE TABLA SIN REGISTRAR.

Use los comandos `pg_dump -Fc` (comprimido) o `pg_restore -j` (paralelo) con estos ajustes.

Una vez finalizada la operación de carga, devuelva la instancia de base de datos y los parámetros de base de datos a su configuración normal.

Trabajo con la característica autovacuum de PostgreSQL

La característica autovacuum de las bases de datos de PostgreSQL es una función cuyo uso se recomienda para mantener la instancia de base de datos de PostgreSQL en buen estado. Autovacuum automatiza la ejecución de los comandos VACUUM y ANALYZE. El uso de autovacuum es requerido por PostgreSQL, no impuesto por Amazon RDS, y es esencial para un buen desempeño. La característica está habilitada de manera predeterminada para todas las nuevas instancias de base de datos de Amazon RDS para PostgreSQL, y los parámetros de configuración relacionados se definen correctamente de forma predeterminada.

El administrador de la base de datos debe conocer y entender esta operación de mantenimiento. Para obtener la documentación de PostgreSQL sobre autovacuum, consulte The Autovacuum Daemon.

Autovacuum no es una operación que no consuma recursos, pero funciona en segundo plano y deja a las operaciones del usuario toda la capacidad posible. Cuando está habilitado, autovacuum busca las tablas en las que se ha insertado, actualizado o eliminado un número elevado de tuplas. También

protege contra la pérdida de los datos muy antiguos debida al reinicio de los ID de transacciones. Para obtener más información, consulte Preventing Transaction ID Wraparound Failures.

Autovacuum no se debe entender como una operación de alto consumo que se puede reducir para mejorar el desempeño. Por el contrario, las tablas con una velocidad alta de actualizaciones y eliminaciones se deteriorarán con rapidez si no se ejecuta autovacuum.

> **Important**
>
> No ejecutar autovacuum puede llevar a una interrupción para realizar una operación de vacío mucho más intrusiva. En algunos casos, una instancia de base de datos de RDS para PostgreSQL puede dejar de estar disponible debido a un uso demasiado conservador de autovacuum. En estos casos, la base de datos de PostgreSQL se cierra para protegerse. En ese punto, Amazon RDS debe realizar un vacío completo en modo de un usuario directamente en la instancia de base de datos. Este vacío total puede provocar una interrupción de varias horas. Por ello, es recomendable no desactivar autovacuum, que está activado de manera predeterminada.

Los parámetros de autovacuum determinan cuándo y con qué intensidad funciona autovacuum. Los parámetros`autovacuum_vacuum_threshold` y `autovacuum_vacuum_scale_factor` determinan cuándo se ejecuta autovacuum. Los parámetros `autovacuum_max_workers`, `autovacuum_nap_time`, `autovacuum_cost_limit` y `autovacuum_cost_delay` determinan la intensidad con la que trabaja autovacuum. Para obtener más información acerca de autovacuum, de cuándo se ejecuta y de los parámetros que requiere, consulte Routine Vacuuming en la documentación de PostgreSQL.

La siguiente consulta muestra el número de tuplas “muertas” en una tabla denominada table1:

```
SELECT relname, n_dead_tup, last_vacuum, last_autovacuum FROM
pg_catalog.pg_stat_all_tables
WHERE n_dead_tup > 0 and relname = 'table1';
```

Los resultados de la consulta serán similares a los siguientes:

```
relname | n_dead_tup | last_vacuum | last_autovacuum
---------+------------+-------------+-----------------
 tasks   |   81430522 |             |
```

```
(1 row)
```

Video de prácticas recomendadas de Amazon RDS for PostgreSQL

La conferencia de AWS re:Invent de 2020 incluyó una presentación sobre nuevas características y prácticas recomendadas para trabajar con PostgreSQL en Amazon RDS. Puede ver aquí un vídeo de la presentación.

Prácticas recomendadas para trabajar con SQL Server

Entre las prácticas recomendadas para un despliegue Multi-AZ con una instancia de base de datos de SQL Server se incluyen las siguientes:

- Use los eventos de base de datos de Amazon RDS para monitorizar las conmutaciones por error. Por ejemplo, puede recibir una notificación en un mensaje de texto o un correo electrónico cuando se produzca una conmutación por error de una instancia de base de datos. Para obtener más información acerca de los eventos de Amazon RDS, consulte Uso de notificaciones de eventos de Amazon RDS.
- Si su aplicación almacena en caché los valores DNS, defina el tiempo de vida (TTL) en menos de 30 segundos. Definir TTL en este valor es una práctica recomendada en caso de que se produzca una conmutación por error. En una conmutación por error, la dirección IP podría cambiar y el valor en caché podría dejar de estar en servicio.
- Es recomendable que no habilite los modos siguientes porque desactivan el registro de transacciones, que es necesario para el uso de Multi-AZ:
  - Modo de recuperación simple
  - Modo sin conexión
  - Modo de solo lectura
- Pruebe para determinar cuánto tiempo se tarda en completar la conmutación por error de la instancia de base de datos. El tiempo de la conmutación por error puede variar en función del tipo de base de datos, la clase de instancia y el tipo de almacenamiento utilizado. También debe probar la capacidad de su aplicación para seguir trabajando si se produce una conmutación por error.
- Para acortar el tiempo necesario para la conmutación por error, haga lo siguiente:
  - Compruebe que tiene asignadas las IOPS provisionadas necesarias para su carga de trabajo. Los valores de E/S inadecuados pueden alargar los tiempos de conmutación por error. La recuperación de la base de datos requiere E/S.

  - Use transacciones más pequeñas. La recuperación de bases de datos se basa en las transacciones, de modo que si divide las transacciones grandes en varias transacciones más pequeñas, el tiempo de conmutación por error debería acortarse.
- Tenga en cuenta que, durante una conmutación por error, habrá latencias elevadas. Como parte del proceso de conmutación por error, Amazon RDS replica automáticamente los datos en una nueva instancia en espera. Esta replicación significa que los datos nuevos se envían a dos instancias de base de datos diferentes. Por lo tanto, puede haber latencia hasta que la instancia de base de datos en espera alcance el ritmo de la nueva instancia de base de datos principal.
- Implemente sus aplicaciones en todas las zonas de disponibilidad. Si una zona de disponibilidad deja de funcionar, las aplicaciones de las otras zonas de disponibilidad seguirán estando disponibles.

Cuando trabaje con una implementación Multi-AZ de SQL Server, recuerde que Amazon RDS crea réplicas para todas las bases de datos de SQL Server de su instancia. Si no desea que determinadas bases de datos tengan réplicas secundarias, configure una instancia de base de datos independiente que no use Multi-AZ para esas bases de datos.

Video de prácticas recomendadas de Amazon RDS for SQL Server

La conferencia de AWS re:Invent de 2019 incluyó una presentación sobre nuevas características y prácticas recomendadas para trabajar con SQL Server en Amazon RDS. Puede ver aquí un vídeo de la presentación.

Trabajo con los grupos de parámetros de base de datos

Es recomendable que pruebe los cambios de los grupos de parámetros de base de datos en una instancia de base de datos de prueba antes de aplicarlos en las instancias de base de datos de producción. Si se configuran de forma incorrecta los parámetros del motor de base de datos de un grupo de parámetros de base de datos, pueden producirse efectos adversos no deseados, como la degradación del desempeño y la inestabilidad del sistema. Tenga cuidado siempre que modifique los parámetros del motor de base de datos y cree una copia de seguridad de la instancia de base de datos antes de modificar un grupo de parámetros de base de datos.

Para obtener información acerca del procedimiento para realizar la copia de seguridad de la instancia de base de datos, consulte Copia de seguridad, restauración y exportación de datos.

Prácticas recomendadas para automatizar la creación de instancias de base de datos

Es una práctica recomendada de Amazon RDS crear una instancia de base de datos con la versión secundaria preferida del motor de base de datos. Puede utilizar la AWS CLI, la API de Amazon RDS o la AWS CloudFormation para automatizar la creación de una instancia de base de datos. Cuando utiliza estos métodos, solo puede especificar la versión principal y Amazon RDS crea automáticamente la instancia con la versión secundaria preferida. Por ejemplo, si PostgreSQL 12.5 es la versión secundaria preferida y si especifica la versión 12 con `create-db-instance`, la instancia de base de datos será la versión 12.5.

Para determinar la versión secundaria preferida, puede ejecutar el comando `describe-db-engine-versions` con la opción `--default-only` que se muestra en el siguiente ejemplo.

```
aws rds describe-db-engine-versions --default-only --engine postgres

{
    "DBEngineVersions": [
        {
            "Engine": "postgres",
            "EngineVersion": "12.5",
            "DBParameterGroupFamily": "postgres12",
            "DBEngineDescription": "PostgreSQL",
            "DBEngineVersionDescription": "PostgreSQL 12.5-R1",
            ...some output truncated...
        }
    ]
}
```

Para obtener información sobre la creación de instancias de base de datos mediante programación, consulte los siguientes recursos:

- Uso de la AWS CLI: create-db-instance
- Uso de la API de Amazon RDS–: CreateDBInstance
- Uso de AWS CloudFormation: AWS::RDS::DBInstance

Vídeo de nuevas características de Amazon RDS

La conferencia de AWS re:Invent de 2023 incluyó una presentación sobre nuevas características de Amazon RDS. Puede ver aquí un vídeo de la presentación.

Acceso mediante programación a Amazon RDS

Amazon RDS le proporciona las siguientes herramientas para administrar los recursos de Amazon RDS mediante programación.

AWS Command Line Interface (AWS CLI)

Puede crear y administrar los recursos de RDS mediante el intérprete de comandos de la línea de comandos de la AWS CLI. La AWS CLI ofrece acceso directo a las API para servicios de AWS, por ejemplo, Amazon RDS. Para obtener la sintaxis y ejemplos de los comandos de Amazon RDS, consulte rds en la Referencia de comandos de AWS CLI.

AWS CloudFormation

Con la herramienta Infraestructura como código (IaC) de AWS, puede crear plantillas que describan todos los recursos de Amazon RDS que desee, y AWS CloudFormation aprovisiona y configura esos recursos. Para obtener más información, consulte the section called “Creación de recursos con AWS CloudFormation”.

Kits de desarrollo de software (SDK) de AWS

AWS proporciona SDK para muchas tecnologías y lenguajes de programación conocidos. Podrá comenzar a llamar de forma más sencilla a los servicios de AWS desde sus aplicaciones en ese lenguaje o tecnología. Para obtener más información sobre estos SDK, consulte Tools for developing and managing applications on AWS.

API de Amazon RDS

Esta API es la interfaz de protocolo de Amazon RDS. Al utilizar esta API, debe formatear correctamente todas las solicitudes de HTTPS y añadir una firma digital válida a cada solicitud. Para obtener más información, consulte Referencia de la API de Amazon RDS.

Console-to-Code

Con esta herramienta, puede generar código para las acciones que realiza en la consola de Amazon RDS y usar ese mismo código en otras herramientas, como, por ejemplo, AWS CloudFormation. Para obtener más información, consulte the section called “Console-to-Code”.

Use Console-to-Code para generar código para las acciones de la consola de Amazon RDS.

La consola proporciona una ruta guiada para crear recursos y probar prototipos. Si desea crear los mismos recursos a escala, necesitará un código de automatización. Console-to-Code es una característica de Amazon Q Developer que puede ayudarlo a empezar a usar el código de automatización. Console-to-Code registra las acciones de la consola, incluidos los valores predeterminados y los valores de parámetros que indique. A continuación, utiliza la IA generativa para sugerir código en el lenguaje y formato que prefiera para las acciones que elija. Como el flujo de trabajo de la consola garantiza que los valores de los parámetros que especifique sean válidos juntos, el código que genere mediante el uso de Console-to-Code tiene valores de parámetros compatibles. Puede usar el código como punto de partida y luego personalizarlo para que esté listo para producción en función de su caso de uso específico.

Por ejemplo, con Console-to-Code, puede registrar la creación de una instancia de base de datos de RDS y optar por generar código en el formato JSON de AWS CloudFormation. Luego, puede copiar ese código y personalizarlo para usarlo en su plantilla AWS CloudFormation.

Actualmente, Console-to-Code puede generar infraestructura como código (IaC) en los siguientes formatos e idiomas:

- Java de CDK
- Python de CDK
- TypeScript de CDK
- JSON de CloudFormation
- YAML de CloudFormation

Para obtener más información e instrucciones sobre cómo utilizar Console-to-Code, consulte Automatización de servicios AWS con Console-to-Code de Amazon Q Developer en la Guía del usuario de Amazon Q Developer.

Configuración de una instancia de base de datos de Amazon RDS

En esta sección se muestra cómo configurar una instancia de base de datos de Amazon RDS. Antes de crear una instancia de base de datos, decida qué clase de instancia de base de datos ejecutará la instancia de base de datos. Además, decida dónde se ejecutará la instancia de base de datos seleccionando una región AWS. A continuación, cree la instancia de base de datos.

Puede configurar una instancia de base de datos con un grupo de opciones y un grupo de parámetros de base de datos.

- Un grupo de opciones especifica características, llamadas opciones, que están disponibles para una instancia de base de datos de Amazon RDS particular.
- Un grupo de parámetros de base de datos sirve de contenedor para los valores de configuración del motor que se aplican a una o varias instancias de bases de datos.

Las opciones y los parámetros disponibles dependen del motor de base de datos y de la versión del motor de base de datos. Puede especificar un grupo de opciones y un grupo de parámetros de base de datos al crear una instancia de base de datos. También puede modificar una instancia de base de datos para especificarlas.

Temas

- Creación de una instancia de base de datos de Amazon RDS
- Creación de recursos de Amazon RDS con AWS CloudFormation
- Conexión a una instancia de base de datos de Amazon RDS
- Trabajo con grupos de opciones
- Grupos de parámetros para Amazon RDS
- Creación de una caché de Amazon ElastiCache mediante el uso de ajustes de la instancia de base de datos de Amazon RDS
- Migración automática de bases de datos de EC2 a Amazon RDS mediante AWS Database Migration Service
- Tutorial: Creación de una instancia de base de datos de MySQL con un grupo de parámetros personalizados y un grupo de opciones nuevas

Creación de una instancia de base de datos de Amazon RDS

El bloque de creación básico de Amazon RDS es la instancia de base de datos, donde se crean las bases de datos. Elija las características específicas del motor de la instancia de base de datos cuando la cree. También podrá elegir la capacidad de almacenamiento, la CPU, la memoria, etc. de la instancia de AWS en la que se ejecuta el servidor de base de datos.

Temas

- Requisitos previos para las instancias de base de datos
- Creación de una instancia de base de datos
- Configuración de instancias de base de datos

Requisitos previos para las instancias de base de datos

> **Important**
>
> Antes de crear una instancia de base de datos de Amazon RDS, debe completar las tareas en Configuración del entorno para Amazon RDS.

A continuación, se describen los requisitos previos para crear una instancia de base de datos de RDS.

Temas

- Configurar la red para la instancia de base de datos
- Requisitos previos adicionales

Configurar la red para la instancia de base de datos

Puede crear una instancia de base de datos de Amazon RDS solo en una nube privada virtual (VPC) en función del servicio de Amazon VPC. Asimismo, debe estar en una Región de AWS que tenga al menos dos zonas de disponibilidad. El grupo de subred de base de datos que elija para la instancia de base de datos debe abarcar al menos dos zonas de disponibilidad. Esta configuración garantiza que pueda configurar una implementación Multi-AZ cuando cree la instancia de base de datos o pase fácilmente a una en el futuro.

Para configurar la conectividad entre su nueva instancia de base de datos y una instancia de Amazon EC2 en la misma VPC, hágalo cuando cree la instancia de base de datos. Para conectarse a su instancia de base de datos desde recursos que no sean instancias de EC2 en la misma VPC, configure las conexiones de red manualmente.

Temas

- Configurar la conectividad de red automática con una instancia de EC2
- Configurar la red manualmente

Configurar la conectividad de red automática con una instancia de EC2

Cuando cree una instancia de base de datos de RDS, puede utilizar la AWS Management Console para configurar la conectividad entre una instancia de EC2 y la nueva instancia de base de datos. Al hacerlo, RDS configura automáticamente los ajustes de red y VPC. La instancia de base de datos se crea en la misma VPC que la instancia EC2 para que la instancia EC2 pueda acceder a la instancia de base de datos.

Estos son los requisitos para conectar una instancia EC2 a la instancia de base de datos:

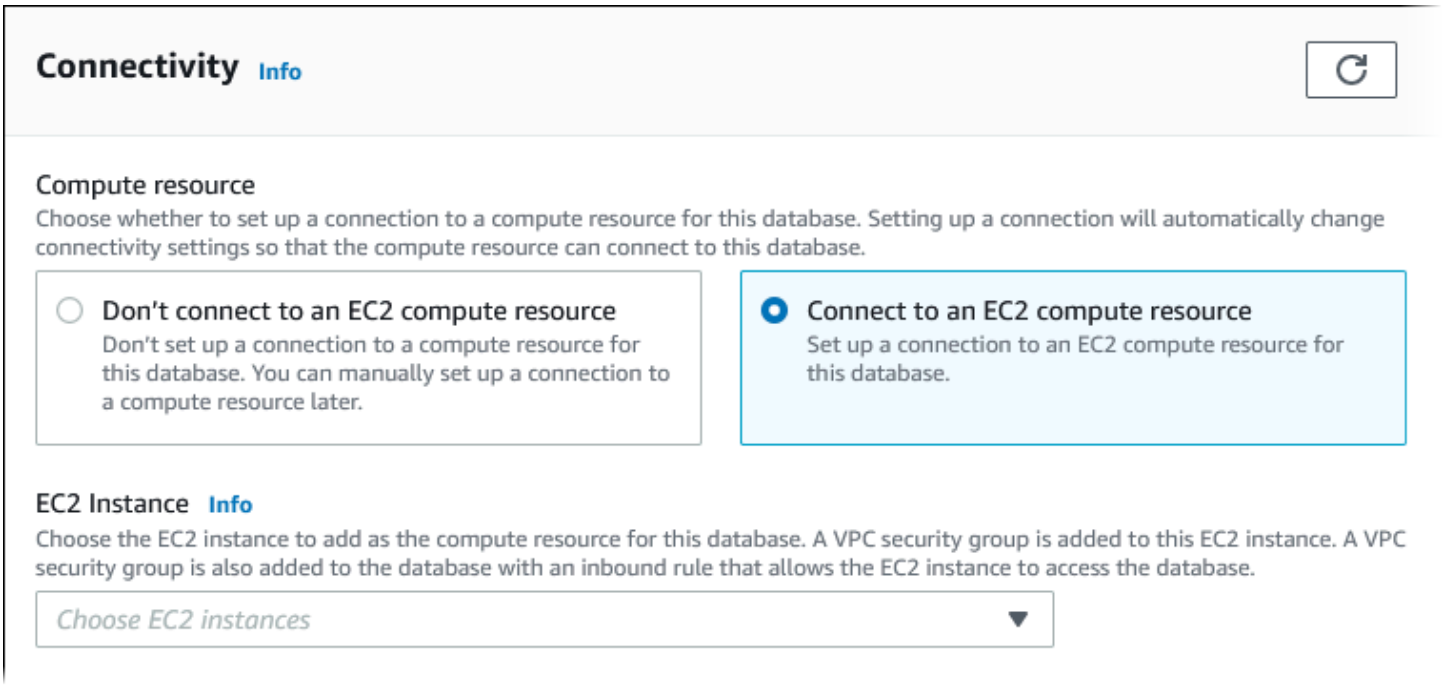
- La instancia EC2 debe existir en la Región de AWS antes de crear la instancia de base de datos.

  Si no existen instancias EC2 en la Región de AWS, la consola proporciona un enlace para crear una.
- El usuario que crea la instancia de base de datos debe tener permisos para realizar las siguientes operaciones:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSubnet`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`

- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Esta opción permite crear una instancia de base de datos privada. La instancia de base de datos usa un grupo de subredes de base de datos con solo subredes privadas para restringir el acceso a los recursos dentro de la VPC.

Para conectar una instancia EC2 a la instancia de base de datos, seleccione Connect to an EC2 compute resource (Conectarse a un recurso de computación de EC2) en la sección Connectivity (Conectividad) de la página Create database (Crear base de datos).



Cuando elige Connect to an EC2 compute resource (Conectarse a un recurso de computación de EC2), RDS establece las siguientes opciones automáticamente. No puede cambiar esta configuración a menos que decida no configurar la conectividad con una instancia de EC2 seleccionando Don't connect to an EC2 compute resource (No conectarse a un recurso de computación de EC2).

Opción de la consola	Configuración automática
Tipo de red	

Opción de la consola	Configuración automática
	RDS establece el tipo de red en IPv4. Actualmente, el modo de pila doble no se admite cuando se configura una conexión entre una instancia EC2 y la instancia de base de datos.
Virtual Private Cloud (VPC) (Nube virtual privada)	RDS establece la VPC en la asociada a la instancia de EC2.

Opción de la consola	Configuración automática
Grupo de subredes de base de datos	RDS necesita un grupo de subredes de base de datos con una subred privada en la misma zona de disponibilidad que la instancia de EC2. Si existe un grupo de subredes de base de datos que cumpla este requisito, RDS utiliza el grupo de subredes de base de datos existente. De forma predeterminada, esta opción está configurada en Automatic setup (Configuración automática). Si selecciona Automatic setup (Configuración automática) y no hay ningún grupo de subredes de base de datos que cumpla este requisito, se produce lo siguiente. RDS usa tres subredes privadas disponibles en tres zonas de disponibilidad, donde una de las zonas de disponibilidad es la misma que la instancia de EC2. Si una subred privada no está disponible en una zona de disponibilidad, RDS crea una subred privada en la zona de disponibilidad. Luego RDS crea el grupo de subredes de base de datos. Cuando hay una subred privada disponible, RDS usa la tabla de enrutamiento asociada a ella y añade cualquier subred que cree a esta tabla de enrutamiento. Cuando no hay ninguna subred privada disponible, RDS crea una tabla de enrutamiento sin acceso a la puerta de enlace de Internet y añade las subredes que crea a la tabla de enrutamiento. RDS también permite utilizar los grupos de subredes de base de datos existentes. Seleccione Choose existing (Elegir existente) si desea utilizar un grupo de subredes de base de datos existente de su elección.

Opción de la consola	Configuración automática
Acceso público	RDS elige No para que no se pueda acceder a la instancia de base de datos de forma pública. Por motivos de seguridad, se recomienda mantener la base de datos privada y asegurarse de que no se pueda acceder a ella desde Internet.
Grupo de seguridad de VPC (firewall)	RDS crea un nuevo grupo de seguridad que se asocia a la instancia de base de datos. El grupo de seguridad se denomina `rds-ec2-`*n*, donde *n* es un número. Este grupo de seguridad incluye una regla de entrada con el grupo de seguridad de VPC de EC2 (firewall) como origen. Este grupo de seguridad que está asociado a la instancia de base de datos permite que la instancia EC2 acceda a la instancia de base de datos. RDS crea un nuevo grupo de seguridad que se asocia a la instancia EC2. El grupo de seguridad se denomina `ec2-rds-`*n*, donde *n* es un número. Este grupo de seguridad incluye una regla de salida con el grupo de seguridad de VPC de la instancia de base de datos como origen. Este grupo de seguridad permite que la instancia de EC2 envíe tráfico a la instancia de base de datos. Para agregar otro grupo de seguridad nuevo, elija Create new (Crear nuevo) y escriba el nombre del nuevo grupo de seguridad . Para añadir grupos de seguridad existentes, elija Choose existing (Elegir existentes) y seleccione los grupos de seguridad que desea añadir.

Opción de la consola	Configuración automática
Zona de disponibilidad	Cuando elige Single DB instance (Instancia de base de datos individual) en Availability & durability (Disponibilidad y durabilidad) (implementación Single-AZ), RDS elige la zona de disponibilidad de la instancia de EC2. Cuando se elige Multi-AZ DB instance (Instancia de base de datos Multi-AZ) en Availability & durability (Disponibilidad y durabilidad) (implementación de instancia de base de datos Multi-AZ), RDS elige la zona de disponibilidad de la instancia EC2 para una instancia de base de datos en la implementación. RDS elige aleatoriamente una zona de disponibilidad diferente para la otra instancia de base de datos. La instancia de base de datos principal o la réplica en espera se crean en la misma zona de disponibilidad que la instancia de EC2. Cuando elige Multi-AZ DB instance (Instancia de base de datos Multi-AZ), existe la posibilidad de incurrir en costos entre zonas de disponibilidad si la instancia de base de datos y la instancia de EC2 están en zonas de disponibilidad diferentes.

Para obtener más información sobre estas opciones, consulte Configuración de instancias de base de datos.

Si cambia esta configuración después de crear la instancia de base de datos, los cambios pueden afectar a la conexión entre la instancia EC2 y la instancia de base de datos.

Configurar la red manualmente

Para conectarse a su instancia de base de datos desde recursos que no sean instancias de EC2 en la misma VPC, configure las conexiones de red manualmente. Si utiliza la AWS Management Console para crear una instancia de base de datos, puede hacer que Amazon RDS cree automáticamente una VPC. O puede usar una VPC ya existente o crear una nueva VPC para su instancia de base de datos. Con cualquier enfoque, su VPC requiere al menos una subred en cada una de al menos dos zonas de disponibilidad para su uso con una instancia de base de datos de RDS.

De forma predeterminada, Amazon RDS crea automáticamente la instancia de base de datos en una zona de disponibilidad. Para elegir una zona de disponibilidad específica, debe cambiar la opción Availability & durability(Disponibilidad y durabilidad) a Single DB instance (Instancia de base de datos individual). Hacerlo habilita una opción de Availability Zone (Zona de disponibilidad) que le permite elegir entre las zonas de disponibilidad de la VPC. Sin embargo, si elige una implementación Multi-AZ, RDS elige la zona de disponibilidad de la instancia de base de datos principal o de escritura automáticamente y la opción Availability Zone (Zona de disponibilidad) no aparece.

En algunos casos, es posible que no tenga una VPC predeterminada o no haya creado una VPC. En estos casos, puede hacer que Amazon RDS cree automáticamente una VPC cuando se cree una instancia de base de datos usando la consola. De lo contrario, realice lo siguiente:

- Cree una VPC que tenga como mínimo una subred en al menos dos de las zonas de disponibilidad de la Región de AWS en la que desea implementar su instancia de base de datos. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC y Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).
- Especifique un grupo de seguridad de VPC que autorice las conexiones con su instancia de base de datos de . Para obtener más información, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad y Control de acceso con grupos de seguridad.
- Especifique un grupo de subredes de base de datos de RDS que defina al menos dos subredes de la VPC que pueda usar la instancia de base de datos. Para obtener más información, consulte Uso de los grupos de subredes de base de datos.

Si desea conectarse a un recurso que no esté en la misma VPC que la instancia de base de datos, consulte los escenarios adecuados en Escenarios de acceso a una instancia de base de datos en una VPC.

Requisitos previos adicionales

Antes de crear la instancia de base de datos Multi-AZ, tenga en cuenta los siguientes requisitos previos adicionales:

- Si está conectando a AWS utilizando credenciales de AWS Identity and Access Management (IAM), su cuenta de AWS debe tener determinadas políticas de IAM. Estas otorgan los permisos necesarios para realizar operaciones de Amazon RDS. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.

Para usas IAM para acceder a la consola de RDS, inicie sesión en la AWS Management Console con sus credenciales de usuario de IAM. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

- Para adaptar los parámetros de configuración para su instancia de base de datos, especifique un grupo de parámetros de base de datos con la configuración de parámetros requerida. Para obtener información acerca de cómo crear o modificar un grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.

> **Important**
>
> Si utiliza el modelo BYOL para Amazon RDS para Db2, antes de crear una instancia de base de datos, primero debe crear un grupo de parámetros personalizado que contenga su IBM Site ID y su IBM Customer ID. Para obtener más información, consulte Traiga su propia licencia para Db2.

- Determine el número de puerto de TCP/IP que quiera especificar para la instancia de base de datos. Los firewalls de algunas compañías bloquean las conexiones a estos puertos predeterminados para las instancias de base de datos de RDS. Si el firewall de su empresa bloquea el puerto predeterminado, elija otro puerto para la instancia de base de datos. Los puertos predeterminados para los motores de bases de datos de Amazon RDS son:

RDS para Db2	RDS para MariaDB	RDS para MySQL	RDS para Oracle	RDS para PostgreSQL	RDS para SQL Server
50000	3306	3306	1521	5432	1433

Para RDS para SQL Server, los puertos siguientes están reservados y no se pueden usar al crear una instancia de base de datos: `1234`, `1434`, `3260`, `3343`, `3389`, `47001`, y `49152-49156`.

Creación de una instancia de base de datos

Puede crear una instancia de base de datos de Amazon RDS utilizando la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> En el caso de RDS para Db2, le recomendamos que configure los elementos necesarios para el modelo de licencia antes de crear una instancia de base de datos de RDS para Db2. Para obtener más información, consulte Opciones de licencias de Amazon RDS para Db2.

Consola

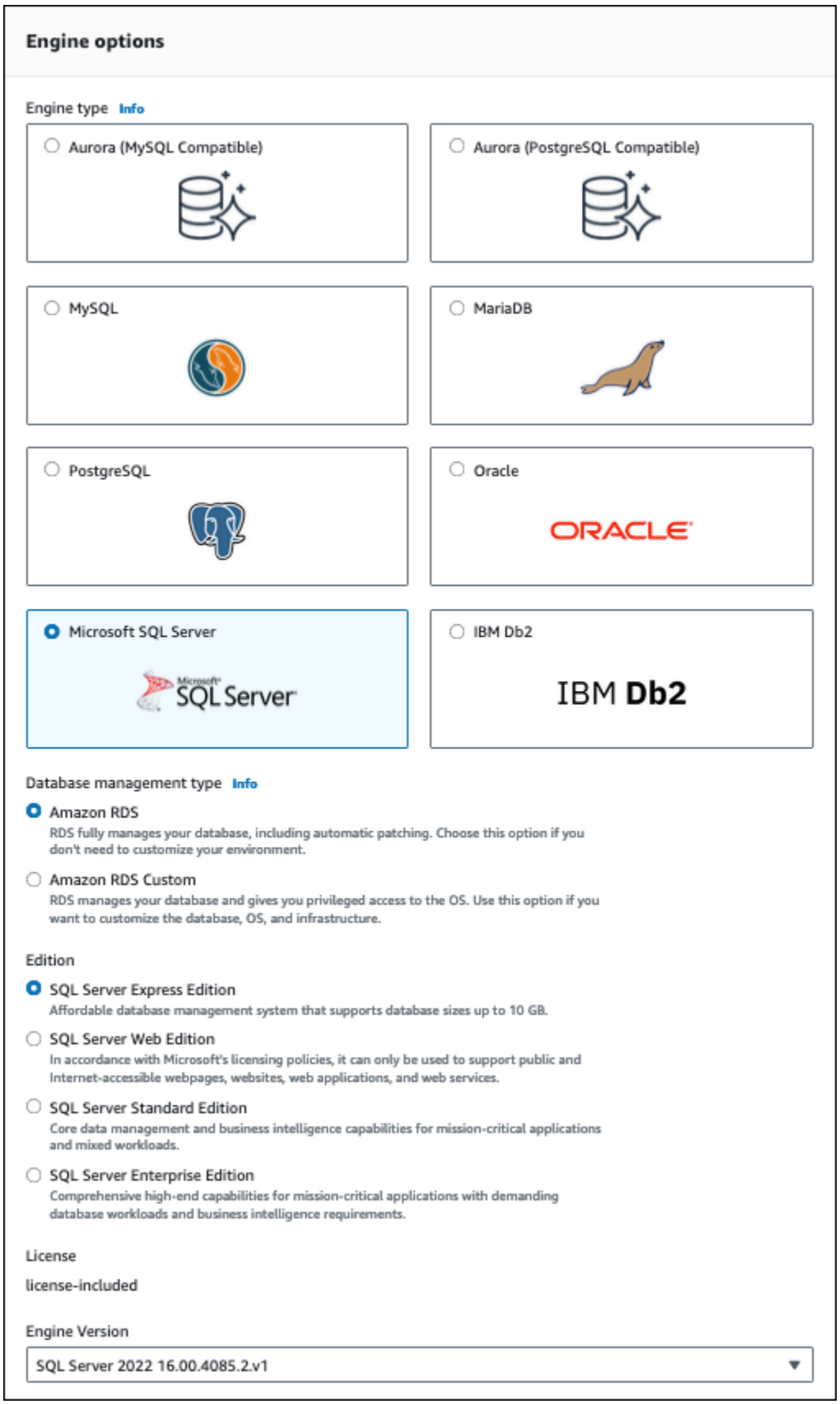
Puede crear una instancia de base de datos mediante la AWS Management Console con Easy Create (Creación sencilla) habilitada o deshabilitada. Con Easy create (Creación sencilla) habilitada, únicamente debe especificar el tipo de motor de base de datos, el tamaño de la instancia de base de datos y el identificador de instancias de bases de datos. Easy create (Creación sencilla) utiliza la configuración predeterminada para otras opciones de configuración. Con Easy create (Creación sencilla) deshabilitada, se especifican más opciones de configuración al crear una base de datos, incluidas las de disponibilidad, seguridad, copias de seguridad y mantenimiento.

> **Note**
>
> En el siguiente procedimiento, está habilitada la Standard Create (Creación estándar) y no está habilitada la Easy Create (Creación sencilla). Este procedimiento utiliza Microsoft SQL Server como ejemplo.
> Para ver ejemplos que utilizan la Easy Create (Creación sencilla) para guiarle a través de la creación y conexión a instancias de base de datos de ejemplo para cada motor, consulte Introducción a Amazon RDS.

Para crear una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Elija Crear base de datos y luego elija Creación estándar.
5. En Tipo de motor, elija IBM Db2, MariaDB, Microsoft SQL Server, MySQL, Oracle o PostgreSQL.

   Aquí se muestra Microsoft SQL Server.


Engine options
Engine type Info
Aurora (MySQL Compatible)
Aurora (PostgreSQL Compatible)
MySQL
MariaDB
PostgreSQL
Oracle
ORACLE
Microsoft SQL Server
Microsoft SQL Server
IBM Db2
IBM Db2
Database management type Info
Amazon RDS
RDS fully manages your database, including automatic patching. Choose this option if you don't need to customize your environment.
Amazon RDS Custom
RDS manages your database and gives you privileged access to the OS. Use this option if you want to customize the database, OS, and infrastructure.
Edition
SQL Server Express Edition
Affordable database management system that supports database sizes up to 10 GB.
SQL Server Web Edition
In accordance with Microsoft's licensing policies, it can only be used to support public and Internet-accessible webpages, websites, web applications, and web services.
SQL Server Standard Edition
Core data management and business intelligence capabilities for mission-critical applications and mixed workloads.
SQL Server Enterprise Edition
Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.
License
license-included
Engine Version
SQL Server 2022 16.00.4085.2.v1

6. En Tipo de administración de base de datos, si utiliza Oracle o SQL Server, elija Amazon RDS o Amazon RDS Custom.

   Aquí se muestra Amazon RDS. Para obtener más información sobre RDS Custom, consulte Amazon RDS Custom.

7. En Edición, si utiliza Oracle o SQL Server, elija la edición del motor de base de datos que desea utilizar.

   MySQL solo tiene una opción para la edición; MariaDB y PostgreSQL no tienen ninguna.

8. En Versión (Versión), elija la versión del motor.

9. En Templates (Plantillas), elija la plantilla que coincida con su caso de uso. Si elige Production (Producción), las siguientes opciones aparecen preseleccionadas más adelante:

   - Opción de conmutación por error Multi-AZ
   - Opción de almacenamiento Provisioned IOPS SSD (io1) (SSD de IOPS aprovisionadas [io1])
   - Opción Enable deletion protection (Habilitar la protección contra la eliminación)

   Es recomendable usar estas características para cualquier entorno de producción.

   > **Note**
   >
   > Las elecciones de plantilla varían en función de la edición.

10. En la sección Settings (Configuración), abra Credential Settings (Configuración de credenciales). A continuación, proceda del modo siguiente:

    a. (Opcional) Cambie el valor Master username (Nombre de usuario maestro).

    b. Elija cualquiera de las siguientes opciones de administración de credenciales:

       - Administrado en AWS Secrets Manager

         En Seleccionar la clave de cifrado, elija una clave de KMS que cree Secrets Manager o una clave que haya creado usted.

         > **Note**
         >
         > Recomendamos AWS Secrets Manager como la técnica más segura para administrar las credenciales. Se aplican cargos adicionales. Para obtener más

información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.

- Autoadministrado

  Para especificar una contraseña, desactive la casilla de verificación Generar una contraseña de forma automática si está seleccionada. Ingrese la misma contraseña en Contraseña principal y elija Confirmar contraseña principal.

11. (Opcional) Configure una conexión a un recurso de computación para esta instancia de base de datos.

    Puede configurar la conectividad entre una instancia de Amazon EC2 y la nueva instancia de base de datos durante la creación de la instancia de base de datos. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2.

12. En la sección Conectividad del Grupo de seguridad de VPC (firewall), si selecciona Crear nuevo, se crea un grupo de seguridad de VPC con una regla de entrada que permite que la dirección IP del equipo local acceda a la base de datos.

13. En el resto de secciones, especifique los ajustes de configuración de la instancia de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.

14. Elija Create database (Crear base de datos).

    Si decide utilizar una contraseña generada automáticamente, el botón View credential details (Ver detalles de credenciales) aparece en la página Databases (Bases de datos).

    Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales).

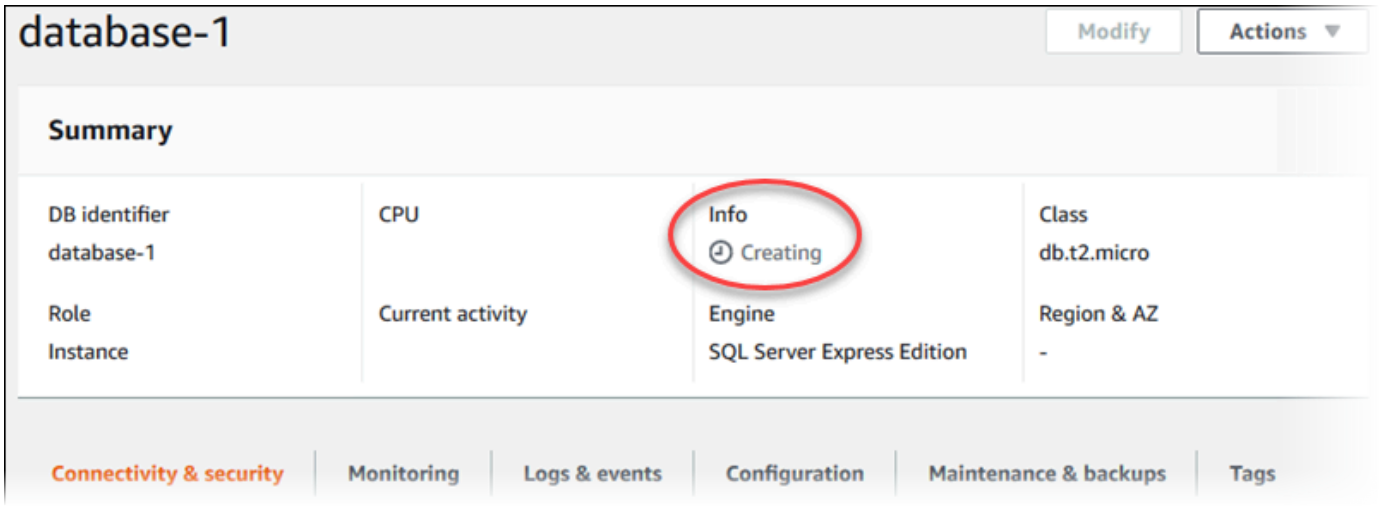
    Para conectarse a la instancia de base de datos como usuario maestro, utilice el nombre de usuario y la contraseña que aparecen.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla. Si tiene que cambiar la contraseña de usuario maestro después de que la instancia de base de datos esté disponible, modifique la instancia de base de datos para ello. Para obtener más información acerca de la modificación de una

instancia de base de datos de , consulte Modificación de una instancia de base de datos de Amazon RDS.

15. En Databases (Bases de datos), seleccione el nombre de la nueva instancia de base de datos.

    Los detalles de la nueva instancia de base de datos aparecen en la consola de RDS. La instancia de base de datos tiene el estado Creating (Creándose) hasta que la instancia de base de datos se cree y esté lista para su uso. Cuando el estado cambie a Available (Disponible), podrá conectarse a la instancia de base de datos. En función de la clase de instancia de base de datos y del almacenamiento asignado, es posible que la nueva instancia tarde varios minutos en estar disponible.



AWS CLI

> **Note**
>
> Si desea utilizar una licencia de Db2 mediante AWS Marketplace, primero debe suscribirse a AWS Marketplace y registrarse en IBM mediante la AWS Management Console. Para obtener más información, consulte Suscripción a listados de Db2 Marketplace y registro con IBM.

Para crear una instancia de base de datos con la AWS CLI, llame al comando create-db-instance con los siguientes parámetros:

- `--db-instance-identifier`

- `--db-instance-class`
- `--vpc-security-group-ids`
- `--db-subnet-group`
- `--engine`
- `--master-username`
- `--master-user-password` o `--manage-master-user-password`
- `--allocated-storage`
- `--backup-retention-period`

Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

En este ejemplo se utiliza Microsoft SQL Server.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --engine sqlserver-se \
    --db-instance-identifier mymsftsqlserver \
    --allocated-storage 250 \
    --db-instance-class db.t3.large \
    --vpc-security-group-ids mysecuritygroup \
    --db-subnet-group mydbsubnetgroup \
    --master-username masterawsuser \
    --manage-master-user-password \
    --backup-retention-period 3
```

Para Windows:

```
aws rds create-db-instance ^
    --engine sqlserver-se ^
    --db-instance-identifier mydbinstance ^
    --allocated-storage 250 ^
    --db-instance-class db.t3.large ^
    --vpc-security-group-ids mysecuritygroup ^
    --db-subnet-group mydbsubnetgroup ^
    --master-username masterawsuser ^
```

```
    --manage-master-user-password ^
    --backup-retention-period 3
```

El resultado de este comando debería ser similar al siguiente.

```
DBINSTANCE  mydbinstance  db.t3.large  sqlserver-se  250  sa  creating  3  ****  n
 10.50.2789
SECGROUP  default  active
PARAMGRP  default.sqlserver-se-14  in-sync
```

API de RDS

> **Note**
>
> Si desea utilizar una licencia de Db2 mediante AWS Marketplace, primero debe suscribirse a AWS Marketplace y registrarse en IBM mediante la AWS Management Console. Para obtener más información, consulte Suscripción a listados de Db2 Marketplace y registro con IBM.

Para crear una instancia de base de datos con la API de Amazon RDS, llame a la operación CreateDBInstance.

Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

Configuración de instancias de base de datos

La siguiente tabla contiene detalles de los ajustes que puede elegir al crear una instancia de base de datos. La tabla también muestra los motores de base de datos para los que se admite cada configuración.

Puede crear una instancia de base de datos de MySQL mediante la consola, el comando de la CLI create-db-instance o la operación CreateDBInstance de la API de RDS.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Allocated storage (Almacenamiento asignado)	La cantidad de almacenamiento que se debe asignar a la instancia de base de datos (en gibibytes). En algunos casos, asignar a la instancia de base de datos una cantidad de almacenamiento mayor que el tamaño de la base de datos puede mejorar el desempeño de E/S.
	
	Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.
		Opción de la CLI:
		
		`--allocated-storage`
		
		Parámetro de la API:
		
		`AllocatedStorage`
			Todos

Architecture settings (Configuración de arquitectura)	Si elige Usar arquitectura multitenencia, RDS para Oracle crea una base de datos de contenedores (CDB). Si no elige esta opción, RDS for Oracle crea una CDB que no es de CDB. Una no CDB utiliza la arquitectura de base de datos tradicional de Oracle. Una CDB puede contener bases de datos conectables (PDB), a diferencia de una no CDB. Oracle Database 21c utiliza únicamente la arquitectura CDB. Oracle Database 19c puede utilizar la arquitectura CDB o no CDB. Las versiones anteriores a Oracle Database 19c utilizan únicamente arquitecturas no CDB.	Opción de la CLI: `--engine oracle-ee-cdb` (Oracle multitenencia) `--engine oracle-se2-cdb` (Oracle multitenencia) `--engine oracle-ee` (tradicional) `--engine oracle-se2` (tradicional) Parámetro de la API: `Engine`	Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	Para obtener más información, consulte Descripción general de las CDB de RDS para Oracle.		

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
Configuración de arquitectura	Estos ajustes solo son válidos si elige la Arquitectura multitenencia de Oracle en Configuración de arquitectura. Elija cualquiera de las siguientes opciones adicionales: • Con la Configuración de varios inquilinos, la instancia de CDB de RDS para Oracle puede contener de 1 a 30 bases de datos de inquilinos, según la edición de la base de datos y las licencias de opciones requeridas. En el contexto de una base de datos de Oracle, una base de datos de inquilinos es una PDB. No se admiten las PDB de aplicaciones ni las PDB proxy. La instancia de base de datos se crea con 1 base de datos inicial de inquilinos. Elija los valores para Nombre de la base de datos de inquilinos, Nombre de usuario principal de la base de datos de inquilinos, Contraseña principal de la base de datos de inquilinos y Conjunto de caracteres de base de datos de inquilinos. La configuración de varios inquilinos es permanente. Por lo tanto, no se puede convertir de nuevo una CDB con la configuración de varios inquilino	Opción de la CLI: `--multi-tenant` (configuración de varios inquilinos) `--no-multi-tenant` (configuración de un solo inquilino) Parámetro de la API: `MultiTenant`	Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	s en una CDB de un solo inquilino. La actualización de versión mínima compatible (RU) para la configuración de varios inquilinos es 19.0.0.0.ru-2022-01.rur-2022.r1. **Note** La configuración de Amazon RDS se denomina “de varios inquilinos”, en lugar de “multitenencia”, ya que es una capacidad de la plataforma RDS, no solo del motor de base de datos de Oracle. De manera similar, el término “inquilino” de RDS se refiere a cualquier inquilino en una configuración de RDS, no solo a las PDB de Oracle. En la documentación de RDS, el término “de varios inquilinos de Oracle” sin guion se refiere exclusivamente a la arquitectura CDB de la base de datos de Oracle, que es compatible tanto con las implementaciones en las instalaciones como con RDS.		

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	• Con la configuración de un solo inquilino, su CDB de RDS para Oracle contiene 1 PDB. Esta es la configuración predeterminada cuando se crea una CDB. No puede eliminar la PDB inicial ni añadir más PDB. Más adelante, puede convertir la configuración de un solo inquilino de su CDB en la configuración de varios inquilinos, pero no podrá volver a convertirla a la configuración de un solo inquilino. Independientemente de la configuración que elija, la CDB contiene una única PDB inicial. En la configuración de varios inquilinos, puede crear más PDB más adelante mediante las API de RDS. Para obtener más información, consulte Descripción general de las CDB de RDS para Oracle.		

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Auto minor version upgrade (Actualización automática de versiones secundarias)	Elija Habilitar actualización automática de versiones secundarias para permitir que la instancia de base de datos reciba actualizaciones preferidas de la versión secundaria del motor de base de datos automáticamente cuando estén disponibles. Este es el comportamiento predeterminado. Amazon RDS realiza actualizaciones automáticas de versiones secundarias en el periodo de mantenimiento. Si no selecciona Habilitar actualización automática de versiones secundarias, la instancia de base de datos no se actualizará automáticamente cuando haya nuevas versiones secundarias disponibles.
	
	Para obtener más información, consulte Actualización automática de la versión secundaria del motor.
		Opción de la CLI:
		
		`--auto-minor-version-upgrade`
		
		`--no-auto-minor-version-upgrade`
		
		Parámetro de la API:
		
		`AutoMinorVersionUpgrade`
			Todos

Availability zone (Zona de disponibilidad)	Zona de disponibilidad de la instancia de base de datos. Utilice el valor predeterminado, No Preference, a menos que desee especificar una zona de disponibilidad.
	
	Para obtener más información, consulte Regiones, zonas de disponibilidad y Local Zones.
		Opción de la CLI:
		
		`--availability-zone`
		
		Parámetro de la API:
		
		`AvailabilityZone`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

AWS KMS key	Solo está disponible si Encryption (Cifrado) se establece en Enable encryption (Habilitar cifrado). Elija la AWS KMS key que se va a utilizar para el cifrado de esta instancia de base de datos. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.	Opción de la CLI:
		`--kms-key-id`
		Parámetro de la API:
		`KmsKeyId`
			Todos

Configuración de AWS License Manager	Escriba un nombre para la configuración de licencia de AWS License Manager. El nombre debe tener 100 caracteres o menos y solo debe incluir a-z, A-Z y 0-9. Para obtener más información, consulte the section called “Integración con AWS License Manager”.	Opción de la CLI: Para obtener más información, consulte AWS License Manager CLI. Parámetro de la API: Para obtener más información, consulte API AWS License Manager.	Db2

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
Backup replication (Replicación de copia de seguridad)	Elija la opción para habilitar replicación en otra región de AWS a fin de crear copias de seguridad en una región adicional para la recuperación de desastres. A continuación, elija la Destination Region (Región de destino) para las copias de seguridad adicionales.	No está disponible al crear una instancia de base de datos. Para obtener información acerca de cómo habilitar copias de seguridad en todas las regiones mediante la API de RDS o AWS CLI, consulte Habilitación de copias de seguridad automatizadas entre regiones.	Oracle PostgreSQL SQL Server

Backup retention period (Periodo de retención de copia de seguridad)	Número de días que se deben conservar las copias de seguridad automáticas de la instancia de base de datos. En el caso de instancias de base de datos no triviales, establezca este valor como **1** o un valor mayor.
	
	Para obtener más información, consulte Introducción a las copias de seguridad.
		Opción de la CLI:
		
		`--backup-retention-period`
		
		Parámetro de la API:
		
		`BackupRetentionPeriod`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Backup target (Destino de copia de seguridad)	Elegir Nube de AWS para almacenar copias de seguridad automatizadas e instantáneas manuales en la región de AWS principal. Elija Outposts (on-premises) (Outposts (en las instalaciones) para almacenarlos localmente en su Outpost.
	
	Esta configuración de opción solo se aplica a RDS en Outposts. Para obtener más información, consulte Creación de instancias de base de datos para Amazon RDS on AWS Outposts.
		Opción de la CLI:
		
		`--backup-target`
		
		Parámetro de la API:
		
		`BackupTarget`
			MySQL, PostgreSQL, SQL Server

Backup target (Intervalo de copia de seguridad)	Periodo de tiempo durante el cual Amazon RDS realiza automáticamente una copia de seguridad de la instancia de base de datos. A menos que desee hacer una copia de seguridad de la base de datos a una hora determinada, utilice el valor predeterminado No Preference (Sin preferencia).
	
	Para obtener más información, consulte Introducción a las copias de seguridad.
		Opción de la CLI:
		
		`--preferred-backup-window`
		
		Parámetro de la API:
		
		`PreferredBackupWindow`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Certificate authority (Autoridad de certificado)	Entidad de certificación (CA) del certificado de servidor que utiliza la instancia de base de datos.
	
	Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
		Opción de la CLI:
		
		`--ca-certificate-identifier`
		
		Parámetro de la API de RDS:
		
		`CACertificateIdentifier`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Character set (Conjunto de caracteres)	Conjunto de caracteres para la instancia de base de datos. El valor predeterminado de AL32UTF8 para el juego de caracteres de base de datos es para el juego de caracteres universales Unicode 5.0 UTF-8. No se puede cambiar el juego de caracteres de base de datos después de crear la instancia de base de datos.
	
	En una configuración de inquilino único, un conjunto de caracteres de base de datos no predeterminado afecta solo a la PDB, no a la CDB. Para obtener más información, consulte Configuración de un solo inquilino de la arquitectura CDB.
	
	El conjunto de caracteres de base de datos es diferente del conjunto de caracteres nacional, que se denomina conjunto de caracteres NCHAR. A diferencia del conjunto de caracteres de base de datos, el conjunto de caracteres NCHAR especifica la codificación para las columnas de tipos de datos NCHAR (NCHAR, NVARCHAR2 y NCLOB) sin afectar a los metadatos de la base de datos.
	
	Para obtener más información, consulte RDS para conjuntos de caracteres de Oracle.
		Opción de la CLI:
		
		`--character-set-name`
		
		Parámetro de la API:
		
		`CharacterSetName`
			Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Collation (Intercalación)	Una intercalación de nivel de servidor para la instancia de base de datos.
	
	Para obtener más información, consulte Intercalación de nivel de servidor para Microsoft SQL Server.
		Opción de la CLI:
		
		`--character-set-name`
		
		Parámetro de la API:
		
		`CharacterSetName`
			SQL Server

Copy tags to snapshots (Copiar etiquetas en instantáneas)	Esta opción copia las etiquetas de las instancias de base de datos en una instantánea de base de datos cuando se crea una instantánea.
	
	Para obtener más información, consulte Etiquetado de los recursos de y Amazon RDS.
		Opción de la CLI:
		
		`--copy-tags-to-snapshot`
		
		`--no-copy-tags-to-snapshot`
		
		Parámetro de la API de RDS:
		
		`CopyTagsToSnapshot`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Database authentication (Autenticación de bases de datos)	La opción de autenticación de la base de datos que desea usar.
	
	Elija Password authentication (Autenticación de contraseña) para autenticar solo a los usuarios de la base de datos con contraseñas de base de datos.
	
	Elija Password and IAM DB authentication (Contraseña y autenticación de base de datos de IAM) para autenticar a los usuarios de la base de datos con contraseñas y credenciales de usuario a través de usuarios y roles. Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL. Esta opción solo es compatible con MySQL y PostgreSQL.
	
	Elija Password and Kerberos authentication (Contraseña y autenticación Kerberos) para autenticar a los usuarios de la base de datos con contraseñas de base de datos y autenticación Kerberos a través de un AWS Managed Microsoft AD creado con AWS Directory Service. A continuación, elija el directorio o elija Create a new Directory (Ccrear un nuevo directorio).
		IAM:
		
		Opción de la CLI:
		
		`--enable-iam-database-authentication`
		
		`--no-enable-iam-database-authentication`
		
		Parámetro de la API de RDS:
		
		`EnableIAMDatabaseAuthentication`
		
		Kerberos:
		
		Opción de la CLI:
		
		`--domain`
		
		`--domain-iam-role-name`
		
		Parámetro de la API de RDS:
		
		`Domain`
		
		`DomainIAMRoleName`
			Varía según el tipo de autenticación

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	Para obtener más información, consulte una de las siguientes: • Uso de la autenticación de Kerberos para Amazon RDS para Db2 • Uso de la autenticación de Kerberos para Amazon RDS para MySQL • Configuración de la autenticación Kerberos con Amazon RDS for Oracle • Uso de la autenticación Kerberos con Amazon RDS para PostgreSQL		
Database management type (Tipo de administración de bases de datos)	Elija Amazon RDS si no tiene que personalizar su entorno. Elija Amazon RDS Custom si desea personalizar la base de datos, el sistema operativo y la infraestructura. Para obtener más información, consulte Amazon RDS Custom.	Para la CLI y la API, se especifica el tipo de motor de base de datos.	Oracle SQL Server

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Database management type (Puerto de base de datos)	Puerto que desea utilizar para obtener acceso a la instancia de base de datos. Se muestra el puerto predeterminado.
	
	Note
	Los firewalls de algunas compañías bloquean las conexiones al puerto predeterminado de MariaDB, MySQL y PostgreSQL. Si el firewall de su empresa bloquea el puerto predeterminado, introduzca otro puerto para la instancia de base de datos.
		Opción de la CLI:
		
		`--port`
		
		Parámetro de la API de RDS:
		
		`Port`
			Todos

DB engine version (Versión del motor de base de datos)	La versión del motor de base de datos que se desea utilizar.	Opción de la CLI:
		
		`--engine-version`
		
		Parámetro de la API de RDS:
		
		`EngineVersion`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

DB instance class (Clase de instancia de base de datos)	La configuración de su instancia de base de datos. Por ejemplo, una clase de instancia de base de datos db.t3.small tiene 2 GiB de memoria, 2 vCPU, 1 núcleo virtual, una ECU variable y una capacidad de E/S moderada.
	
	Si es posible, elija una clase de instancia de base de datos lo bastante grande como para albergar en la memoria el conjunto de trabajo de una consulta típica. Cuando los conjuntos de trabajo se albergan en la memoria, el sistema puede evitar escribir en el disco, lo que mejora su rendimiento. Para obtener más información, consulte Clases de instancia de base de datos de .
	
	En RDS for Oracle, puede seleccionar Include additional memory configurations (Incluir configuraciones de memoria adicionales). Estas configuraciones están optimizadas para una alta relación de memoria a vCPU. Por ejemplo, db.r5.6xlarge.tpc2.mem4x es una instancia de base de datos db.r5.8x que tiene 2 subprocesos por núcleo (tpc2) y 4 veces la memoria de una instancia db.r5.6xlarge estándar. Para obtener más información, consulte Clases de
		Opción de la CLI:
		
		`--db-instance-class`
		
		Parámetro de la API de RDS:
		
		`DBInstanceClass`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	instancias de base de datos de RDS para Oracle.		

DB Instance Identifier (Identificador de instancias de bases de datos)	Nombre de la instancia de base de datos. Asigne a sus instancias de base de datos el mismo nombre que a sus servidores en las instalaciones. El identificador de instancias de bases de datos puede contener un máximo de 63 caracteres alfanuméricos y debe ser único para su cuenta en la región de AWS que elija.	Opción de la CLI:
		`--db-instance-identifier`
		Parámetro de la API de RDS:
		`DBInstanceIdentifier`
			Todos

DB Parameter Group (Grupo de parámetros de base de datos)	Grupo de parámetros para la instancia de base de datos. Puede elegir el grupo de parámetros predeterminado o crear un grupo de parámetros personalizado.
	Si utiliza el modelo BYOL para RDS para Db2, antes de crear una instancia de base de datos, primero debe crear un grupo de parámetros personalizado que contenga su IBM Site ID y su IBM Customer ID. Para obtener más información, consulte Traiga su propia licencia para Db2.
	Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
		Opción de la CLI:
		`--db-parameter-group-name`
		Parámetro de la API de RDS:
		`DBParameterGroupName`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Grupo de subred de base de datos	El grupo de subredes de base de datos que desea utilizar para el clúster de base de datos.
	Seleccione Choose existing (Elegir existente) para utilizar un grupo de subredes de base de datos existente. A continuación, elija el grupo de subredes requerido en la lista desplegable Existing DB subnet groups (Grupos de subredes de base de datos existentes).
	Elija Automatic setup (Configuración automática) para permitir que RDS seleccione un grupo de subredes de base de datos compatible. Si no existe ninguno, RDS crea un nuevo grupo de subredes para el clúster.
	Para obtener más información, consulte Uso de los grupos de subredes de base de datos.
		Opción de la CLI:
		`--db-subnet-group-name`
		Parámetro de la API de RDS:
		`DBSubnetGroupName`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Volumen de registro específico	Utilice un volumen de registro específico (DLV) para almacenar los registros de transacciones de la base de datos en un volumen de almacenamiento independiente del volumen que contiene las tablas de la base de datos.
	
	Para obtener más información, consulte Uso de un volumen de registro específico (DLV).
		Opción de la CLI:
		
		`--dedicated-log-volume`
		
		Parámetro de la API de RDS:
		
		`DedicatedLogVolume`
			Todos

Deletion protection (Protección contra eliminación)	Seleccione Enable deletion protection (Habilitar la protección contra la eliminación) para evitar que se elimine la instancia de base de datos. Si crea una instancia de base de datos de producción con la AWS Management Console, se habilita de forma predeterminada la protección contra la eliminación.
	
	Para obtener más información, consulte Eliminación de una instancia de base de datos.
		Opción de la CLI:
		
		`--deletion-protection`
		
		`--no-deletion-protection`
		
		Parámetro de la API de RDS:
		
		`DeletionProtection`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Encryption (Cifrado)	Enable Encryption (Habilitar cifrado) para habilitar el cifrado en reposo para esta instancia de base de datos.
	
	Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
		Opción de la CLI:
		
		`--storage-encrypted`
		
		`--no-storage-encrypted`
		
		Parámetro de la API de RDS:
		
		`StorageEncrypted`
			Todos

Enhanced Monitoring (Supervisión mejorada)	Enable enhanced monitoring (Habilitat supervisión mejorada) para habilitar la recopilación de métricas en tiempo real para el sistema operativo en el que se ejecuta la instancia de base de datos.
	
	Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.
		Opciones de CLI:
		
		`--monitoring-interval`
		
		`--monitoring-role-arn`
		
		Parámetros de la API de RDS:
		
		`MonitoringInterval`
		
		`MonitoringRoleArn`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Tipo de motor	Elija el motor de base de datos que se va a usar para esta instancia.	Opción de la CLI:
		`--engine`
		Parámetro de la API de RDS:
		`Engine`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Initial database name (Nombre inicial de la base de datos)	Nombre de la base de datos de la instancia de base de datos. Si no proporciona un nombre, Amazon RDS no crea una base de datos en la instancia de base de datos (excepto Oracle y PostgreSQL). El nombre no puede ser una palabra reservada por el motor de base de datos y tiene otras restricciones dependiendo del motor de base de datos.
	
	Db2:
	
	• Debe tener entre 1–8 caracteres alfanuméricos.
	• Debe empezar por a-z, A-Z, @, $ o # e ir seguido de a-z, A-Z, 0-9, _, @, # o $.
	• No puede contener espacios.
	• Para obtener más información, consulte Consideraciones adicionales.
	
	MariaDB y MySQL:
	
	• Debe tener entre 1 y 64 caracteres alfanuméricos.
	
	Oracle:
		Opción de la CLI:
		
		`--db-name`
		
		Parámetro de la API de RDS:
		
		`DBName`
			Todos excepto SQL Server

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	• Debe tener entre 1–8 caracteres alfanuméricos. • No puede ser `NULL`. El valor predeterminado es `ORCL`. • Deben comenzar por una letra. PostgreSQL: • Debe tener entre 1 y 63 caracteres alfanuméricos. • Debe comenzar por una letra o un guion bajo. Los caracteres subsiguientes pueden ser letras, guiones bajos o dígitos (0-9). • El nombre inicial de la base de datos es `postgres`.		

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

License (Licencia)	Valores válidos para el modelo de licencia:
	• bring-your-own-license o marketplace-license para Db2.
	• general-public-license para MariaDB.
	• license-included para Microsoft SQL Server.
	• general-public-license para MySQL.
	• license-included o bring-your-own-license para Oracle.
	• postgresql-license para PostgreSQL.
		Opción de la CLI:
		`--license-model`
		Parámetro de la API de RDS:
		`LicenseModel`
			Todos

Log exports (Exportaciones de registros)	Los tipos de archivos de registro de base de datos que se publicarán en Amazon CloudWatch Logs.
	Para obtener más información, consulte Publicación de registros de base de datos en registros de Amazon Cloudwatch.
		Opción de la CLI:
		`--enable-cloudwatch-logs-exports`
		Parámetro de la API de RDS:
		`EnableCloudwatchLogsExports`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Periodo de mantenimiento	Periodo de 30 minutos durante el cual se aplican las modificaciones pendientes en la instancia de base de datos. Si el periodo de tiempo no es importante, elija No Preference.
	
	Para obtener más información, consulte La ventana de mantenimiento de Amazon RDS.
		Opción de la CLI:
		
		`--preferred-maintenance-window`
		
		Parámetro de la API de RDS:
		
		`PreferredMaintenanceWindow`
			Todos

Gestionar las credenciales maestras en AWS Secrets Manager	Seleccione Manage master credentials in AWS Secrets Manager (Administrar credenciales maestras en AWS Secrets Manager) para administrar la contraseña del usuario maestro en un secreto en Secrets Manager.
	
	De forma opcional, elija la clave KMS para proteger el secreto. Elija entre las claves de KMS de su cuenta o bien introduzca la clave de otra cuenta.
	
	Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.
		Opción de la CLI:
		
		`--manage-master-user-password | --no-manage-master-user-password`
		
		`--master-user-secret-kms-key-id`
		
		Parámetro de la API de RDS:
		
		`ManageMasterUserPassword`
		
		`MasterUserSecretKmsKeyId`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Master password (Contraseña maestra)	Contraseña de la cuenta del usuario maestro. La contraseña tiene el siguiente número de caracteres ASCII imprimibles (salvo `/`, `"`, un espacio y `@`) según el motor de base de datos.
	• Db2: 8–255
	• Oracle: 8–30
	• MariaDB y MySQL: 8–41
	• SQL Server y PostgreSQL: 8–128
		Opción de la CLI:
		`--master-user-password`
		Parámetro de la API de RDS:
		`MasterUserPassword`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Master Username (Nombre de usuario maestro)	Nombre que utiliza como nombre de usuario maestro para iniciar sesión en la instancia de base de datos con todos los privilegios de la base de datos. Tenga en cuenta las siguientes restricciones:
	• Puede contener 1-16 caracteres alfanuméricos y guiones bajos.
	• El primer carácter debe ser una letra.
	• El nombre no puede ser una palabra reservada por el motor de base de datos.
	
	No se puede cambiar el nombre de usuario maestro después de crear la instancia de la base de datos.
	
	En el caso de Db2, le recomendamos que utilice el mismo nombre de usuario maestro que tiene la instancia de Db2 autoadministrada.
	
	Para obtener más información sobre los privilegios concedidos al usuario maestro, consulte Privilegios de la cuenta de usuario maestro.
		Opción de la CLI:
		`--master-username`
		
		Parámetro de la API de RDS:
		`MasterUsername`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Microsoft SQL Server Windows Authentication (Autenticación de Windows de Microsoft SQL Server)	Elija Enable Microsoft SQL Server Windows authentication (Habilitar autenticación de Windows de Microsoft SQL Server) y, a continuación, Browse Directory (Examinar directorio) para elegir el directorio en el que desea permitir que los usuarios de dominio autorizados se autentiquen con esta instancia de SQL Server mediante la autenticación de Windows.	Opciones de CLI:
		`--domain`
		`--domain-iam-role-name`
		Parámetros de la API de RDS:
		`Domain`
		`DomainIAMRoleName`
			SQL Server

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Multi-AZ deployment (Implementación Multi-AZ)	Create a standby instance (Crear una instancia en espera) para crear una réplica secundaria pasiva de la instancia de base de datos en otra zona de disponibilidad para admitir el soporte si se produce algún error. Es recomendable usar varias zonas de disponibilidad Multi-AZ para las cargas de trabajo de producción con el objeto de mantener una alta disponibilidad.
	
	En el caso de desarrollo y pruebas, puede elegir Do not create a standby instance (No crear una instancia en espera).
	
	Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.
		Opción de la CLI:
		
		`--multi-az`
		
		`--no-multi-az`
		
		Parámetro de la API de RDS:
		
		`MultiAZ`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

National character set (NCHAR) (Juego de caracteres nacionales (NCHAR))	El juego de caracteres nacional para la instancia de base de datos, comúnmente denominado conjunto de caracteres NCHAR. Puede establecer el conjunto de caracteres nacionales en AL16UTF16 (predeterminado) o UTF-8. No se puede cambiar el juego de caracteres nacionales después de crear la instancia de base de datos.
	
	El juego de caracteres nacional es diferente del conjunto de caracteres DB. A diferencia del conjunto de caracteres DB, el conjunto de caracteres nacional especifica la codificación sólo para las columnas de tipos de datos NCHAR (NCHAR, NVARCHAR2 y NCLOB) sin afectar a los metadatos de la base de datos.
	
	Para obtener más información, consulte RDS para conjuntos de caracteres de Oracle.
		Opción de la CLI:
		
		`--nchar-character-set-name`
		
		Parámetro de la API:
		
		`NcharCharacterSetName`
			Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Tipo de red	Protocolos de direccionamiento IP admitidos por la instancia de base de datos.
	
	IPv4 (predeterminado) para especificar que los recursos pueden comunicarse con la instancia de base de datos solo a través del protocolo de direcciones Internet Protocol versión 4 (IPv4).
	
	Modo doble pila para especificar que los recursos pueden comunicarse con la instancia de base de datos mediante IPv4, versión 6 (IPv6) o ambos. Utilice el modo de pila doble si tiene recursos que deben comunicarse con su instancia de base de datos a través del protocolo de direccionamiento IPv6. Además, asegúrese de asociar un bloque CIDR IPv6 a todas las subredes del grupo de subredes de base de datos que especifique.
	
	Para obtener más información, consulte Direccionamiento IP de Amazon RDS.
		Opción de la CLI:
		
		`--network-type`
		
		Parámetro de la API de RDS:
		
		`NetworkType`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Option group (Grupo de opciones)	Grupo de opciones para la instancia de base de datos. Puede elegir el grupo de opciones predeterminado o crear un grupo de opciones personalizado.
	
	Para obtener más información, consulte Trabajo con grupos de opciones.
		Opción de la CLI:
		
		`--option-group-name`
		
		Parámetro de la API de RDS:
		
		`OptionGroupName`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Performance Insights	Enable Performance Insights (Habilitar Performance Insights) para monitorizar la carga de las instancias de base de datos para poder analizar y solucionar los problemas de rendimiento de la base de datos.
	
	Elija un periodo de retención para determinar durante cuánto tiempo conservar el historial de datos de Performance Insights. La configuración de retención en la capa gratuita es Default (7 days) (Predeterminado [7 días]). Para retener los datos de rendimiento durante más tiempo, especifique de 1 a 24 meses. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.
	
	Elija la clave de KMS que se utilizará para proteger la clave que se utiliza para cifrar el volumen de esta base de datos. Elija entre las claves de KMS de su cuenta o bien introduzca la clave de otra cuenta.
	
	Para obtener más información, consulte Monitoreo de la carga de base de datos
		Opciones de CLI:
		
		`--enable-performance-insights`
		
		`--no-enable-performance-insights`
		
		`--performance-insights-retention-period`
		
		`--performance-insights-kms-key-id`
		
		Parámetros de la API de RDS:
		
		`EnablePerformanceInsights`
		
		`PerformanceInsightsRetentionPeriod`
		
		`PerformanceInsightsKMSKeyId`
			Todos excepto Db2

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	con Performance Insights en Amazon RDS.		

Provisioned IOPS (IOPS aprovisionadas)	El valor de la IOPS aprovisionada (operaciones de E/S por segundo) para la instancia de base de datos. Esta configuración solo está disponible si elige una de las siguientes opciones para el tipo de almacenamiento:
	• SSD de uso general (gp3)
	• SSD de IOPS aprovisionadas (io1)
	• SSD de IOPS aprovisionadas (io2)
	
	Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.
		Opción de la CLI:
		`--iops`
		Parámetro de la API de RDS:
		`Iops`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Public access (Acceso público)	Yes (Sí) para proporcionar una dirección IP pública a la instancia de base de datos, lo que significa que es accesible desde fuera de la VPC. Para que sea accesible públicamente, la instancia de base de datos también debe estar en una subred pública de la VPC.
	
	No para hacer que la instancia de base de datos solo sea accessible desde dentro de la VPC.
	
	Para obtener más información, consulte Cómo ocultar una instancia de base de datos en una VPC desde Internet..
	
	Para conectarse a una instancia de base de datos desde afuera de su VPC, la instancia de base de datos debe ser accesible públicamente. Además, el acceso debe concederse mediante las reglas entrantes del grupo de seguridad de la instancia de base de datos. Además, deben cumplirse otros requisitos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.
	
	Si su instancia de base de datos no está accesible públicamente, use una conexión Site-to-site VPN AWS o una
		Opción de la CLI:
		
		`--publicly-accessible`
		
		`--no-publicly-accessible`
		
		Parámetro de la API de RDS:
		
		`PubliclyAccessible`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
	conexión a AWS Direct Connect para acceder a ella desde una red privada. Para obtener más información, consulte Privacidad del tráfico entre redes.		

Soporte extendido de RDS	Seleccione Habilitar el Soporte extendido de RDS para permitir que las versiones principales de los motores compatibles sigan funcionando una vez pasada la fecha de finalización del soporte estándar de RDS.
	
	Al crear una instancia de base de datos, Amazon RDS utiliza el Soporte extendido de RDS de forma predeterminada. Para evitar la creación de una nueva instancia de base de datos después de la fecha de finalización del soporte estándar de RDS y evitar cargos por el Soporte extendido de RDS, deshabilite esta configuración. Sus instancias de base de datos existentes no incurrirán en cargos hasta la fecha de inicio de los precios del Soporte extendido de RDS.
	
	Para obtener más información, consulte Soporte extendido de Amazon RDS con Amazon RDS.
		Opción de la CLI:
		
		`--engine-lifecycle-support`
		
		Parámetro de la API de RDS:
		
		`EngineLifecycleSupport`
			MySQL
			
			PostgreSQL

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles
RDS Proxy	Elija Create an RDS Proxy (Crear un RDS Proxy) para crear un proxy para la instancia de base de datos. Amazon RDS crea automáticamente un rol de IAM y un secreto de Secrets Manager para el proxy. Para obtener más información, consulte Amazon RDS Proxy .	No está disponible al crear una instancia de base de datos.	MariaDB MySQL PostgreSQL

Storage autoscaling (Escalado automático de almacenamiento)	Enable storage autoscaling (Habilitar escalado automático de almacenamiento) para que Amazon RDS aumente automáticamente el almacenamiento cuando sea necesario y evite que la instancia de base de datos se quede sin espacio de almacenamiento.
	
	Utilice la opción Maximum storage threshold (Umbral máximo de almacenamiento) para configurar el límite superior de Amazon RDS para que aumente automáticamente el almacenamiento de la instancia de base de datos. El valor predeterminado es de 1000 GiB.
	
	Para obtener más información, consulte Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS.
		Opción de la CLI:
		
		`--max-allocated-storage`
		
		Parámetro de la API de RDS:
		
		`MaxAllocatedStorage`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Storage throughput (Rendimiento de almacenamiento)	Valor de rendimiento de almacenamiento de la instancia de base de datos. Esta configuración solo está disponible si selecciona SSD de uso general (gp3) como tipo de almacenamiento.
	
	Para obtener más información, consulte Almacenamiento gp3 (recomendado).
		Opción de la CLI:
		
		`--storage-throughput`
		
		Parámetro de la API de RDS:
		
		`StorageThroughput`
			Todos

Storage type (Tipo de almacenamiento)	Tipo de almacenamiento de su instancia de base de datos.
	
	Si elige General Purpose SSD (gp3) (SSD de uso general [gp3]), puede aprovisionar IOPS aprovisionadas adicionales y un rendimiento de almacenamiento en Advanced settings (Configuración avanzada).
	
	Si selecciona SSD de IOPS aprovisionadas (io1) o SSD de IOPS aprovisionadas (io2), introduzca el valor de IOPS aprovisionadas.
	
	Para obtener más información, consulte Tipos de almacenamiento de Amazon RDS.
		Opción de la CLI:
		
		`--storage-type`
		
		Parámetro de la API de RDS:
		
		`StorageType`
			Todos

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Subnet group (Grupo de subredes)	Un grupo de subred de base de datos con el que asociar esta instancia de base de datos.
	
	Para obtener más información, consulte Uso de los grupos de subredes de base de datos.
		Opción de la CLI:
		
		`--db-subnet-group-name`
		
		Parámetro de la API de RDS:
		
		`DBSubnetGroupName`
			Todos

Nombre de la base de datos de inquilinos	El nombre de su PDB inicial en la configuración de varios inquilinos de la arquitectura Oracle. Esta configuración solo está disponible si elige Configuración de varios inquilinos en Configuración de arquitectura.
	
	El nombre de la base de datos de inquilinos debe ser diferente del nombre de la CDB, que tiene el nombre `RDSCDB`. No puede modificar el nombre de la CDB.
		Opción de la CLI:
		
		`--db-name`
		
		Parámetro de la API de RDS:
		
		`DBName`
			Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Nombre de usuario principal de la base de datos de inquilinos	Nombre que utiliza como nombre de usuario principal para iniciar sesión en la base de datos de inquilinos (PDB) con todos los privilegios de la base de datos. Esta configuración solo está disponible si elige Configuración de varios inquilinos en Configuración de arquitectura.
	
	Tenga en cuenta las siguientes restricciones sobre el nombre:
	
	• Puede contener 1-16 caracteres alfanuméricos y guiones bajos.
	• El primer carácter debe ser una letra.
	• El nombre no puede ser una palabra reservada por el motor de base de datos.
	
	No puede hacer lo siguiente:
	
	• Cambie el nombre de usuario principal del inquilino después de crear la base de datos de inquilinos.
	• Inicie sesión con el nombre de usuario principal del inquilino en la CDB.
		Opción de la CLI:
		
		`--master-username`
		
		Parámetro de la API de RDS:
		
		`MasterUsername`
			Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Contraseña principal de la base de datos de inquilinos	La contraseña para la cuenta de usuario principal de su base de datos de inquilinos (PDB). Esta configuración solo está disponible si elige Configuración de varios inquilinos en Configuración de arquitectura.
	
	La contraseña tiene entre 8 y 30 caracteres ASCII imprimibles, sin incluir /, ", un espacio y @.
		Opción de la CLI:
		
		`--master-password`
		
		Parámetro de la API de RDS:
		
		`MasterPassword`
			Oracle

Conjunto de caracteres de base de datos de inquilinos	El juego de caracteres de la base de datos de inquilinos inicial. Esta configuración solo está disponible si elige Configuración de varios inquilinos en Configuración de arquitectura. Solo se admiten las instancias de CDB de RDS para Oracle.
	
	El valor predeterminado de AL32UTF8 para el conjunto de caracteres de base de datos de inquilinos es para el conjunto de caracteres universales Unicode 5.0 UTF-8. Puede elegir un conjunto de caracteres de base de datos de inquilinos distinto del de la CDB.
	
	Para obtener más información, consulte RDS para conjuntos de caracteres de Oracle.
		Opción de la CLI:
		
		`--character-set-name`
		
		Parámetro de la API de RDS:
		
		`CharacterSetName`
			Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Conjunto de caracteres nacional de la base de datos de inquilinos	El juego de caracteres nacional para la base de datos de inquilinos, comúnmente denominado conjunto de caracteres `NCHAR`. Esta configuración solo está disponible si elige Configuración de varios inquilinos en Configuración de arquitectura. Solo se admiten las instancias de CDB de RDS para Oracle.
	
	Puede establecer el conjunto de caracteres nacionales en AL16UTF16 (predeterminado) o UTF-8. No se puede cambiar el juego de caracteres nacionales después de crear la base de datos de inquilinos.
	
	El conjunto de caracteres nacional de la base de datos de inquilinos es diferente del conjunto de caracteres de la base de datos de inquilinos. El conjunto de caracteres nacional especifica la codificación solo para las columnas que utilizan el tipo de datos `NCHAR` (`NCHAR`, `NVARCHAR2` y `NCLOB`), y no afecta a los metadatos de la base de datos.
	
	Para obtener más información, consulte RDS para conjuntos de caracteres de Oracle.
		Opción de la CLI:
		
		`--nchar-character-set-name`
		
		Parámetro de la API:
		
		`NcharCharacterSetName`
			Oracle

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Motores de bases de datos compatibles

Time zone (Zona horarioa)	Nueva zona horaria para la instancia de base de datos. Si no elige una zona horaria, la instancia de base de datos usa la zona horaria predeterminada. No puede cambiar la zona horaria después de crear la instancia de base de datos.
	
	Para obtener más información, consulte Zona horaria local para instancias de base de datos de Amazon RDS para Db2 y Zona horaria local para las instancias de base de datos de Microsoft SQL Server.
		Opción de la CLI:
		
		`--timezone`
		
		Parámetro de la API de RDS:
		
		`Timezone`
			Db2
			
			SQL Server
			
			RDS Custom para SQL Server

Virtual Private Cloud (VPC) (Nube virtual privada)	Una VPC basada en el servicio de Amazon VPC para asociar con estea instancia de base de datos. Para obtener más información, consulte VPC de Amazon y Amazon RDS.	Para la CLI y la API, especifique los ID de grupo de seguridad de la VPC.	Todos

Grupo de seguridad de VPC (firewall)	Los grupos de seguridad con los que asociar la instancia de base de datos.
	
	Para obtener más información, consulte Información general de los grupos de seguridad de VPC.
		Opción de la CLI:
		
		`--vpc-security-group-ids`
		
		Parámetro de la API de RDS:
		
		`VpcSecurityGroupIds`
			Todos

Creación de recursos de Amazon RDS con AWS CloudFormation

Amazon RDS está integrado con AWS CloudFormation, un servicio que lo ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los recursos de AWS que desee (como instancias de base de datos y grupos de parámetros de base de datos), y AWS CloudFormation aprovisiona y configura esos recursos para usted.

Cuando utiliza AWS CloudFormation, puede volver a usar la plantilla para configurar sus recursos de RDS de forma coherente y repetida. Solo tiene que describir los recursos una vez y luego aprovisionar los mismos recursos una y otra vez en varias cuentas y regiones de AWS.

RDS y plantillas de AWS CloudFormation

Las plantillas de AWS CloudFormation son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte ¿Qué es un diseñador de AWS CloudFormation? en la guía del usuario de AWS CloudFormation.

RDS admite la creación de recursos en AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para estos recursos, consulte la referencia del tipo de recurso de RDS en la guía del usuario de AWS CloudFormation.

Más información sobre AWS CloudFormation

Para conocer más información acerca de AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de AWS CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Conexión a una instancia de base de datos de Amazon RDS

Antes de conectarse a una instancia de base de datos, debe crear la instancia de base de datos. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS. Después de que Amazon RDS aprovisione su instancia de base de datos, use cualquier utilidad o aplicación cliente estándar para que su motor de base de datos se conectarse a la instancia de base de datos. En la cadena de conexión, especifique la dirección DNS del punto de conexión de la instancia de base de datos como parámetro del host. Asimismo, especifique el número de puerto del punto de enlace de la instancia de base de datos como el parámetro del puerto.

Para obtener más información sobre cómo encontrar información de conexión para una instancia de base de datos de Amazon RDS o escenarios para acceder a una instancia de base de datos en una VPC, consulte los siguientes temas.

- Búsqueda de la información de conexión para una instancia de base de datos Amazon RDS
- Situaciones para el acceso a una instancia de base de datos situada en una VPC

Búsqueda de la información de conexión para una instancia de base de datos Amazon RDS

La información de conexión de una instancia de base de datos incluye su punto de enlace, puerto y un usuario de base de datos válido, como el usuario maestro. Por ejemplo, para una instancia de base de datos MySQL, supongamos que el valor del punto de enlace es `mydb.123456789012.us-east-1.rds.amazonaws.com`. En este caso, el valor del puerto es `3306` y el usuario de la base de datos es `admin`. Dada esta información, se especifican los siguientes valores en una cadena de conexión:

- Para nombre de host o host o nombre DNS, especifique `mydb.123456789012.us-east-1.rds.amazonaws.com`.
- Para el puerto, especifique `3306`.
- Para el usuario, especifique `admin`.

El punto de enlace es único para cada instancia de base de datos y los valores del puerto y del usuario pueden variar. La siguiente lista muestra el puerto más común para cada motor de base de datos:

- Db2 – 50 000
- MariaDB – 3306
- Microsoft SQL Server – 1433
- MySQL – 3306
- Oracle – 1521
- PostgreSQL – 5432

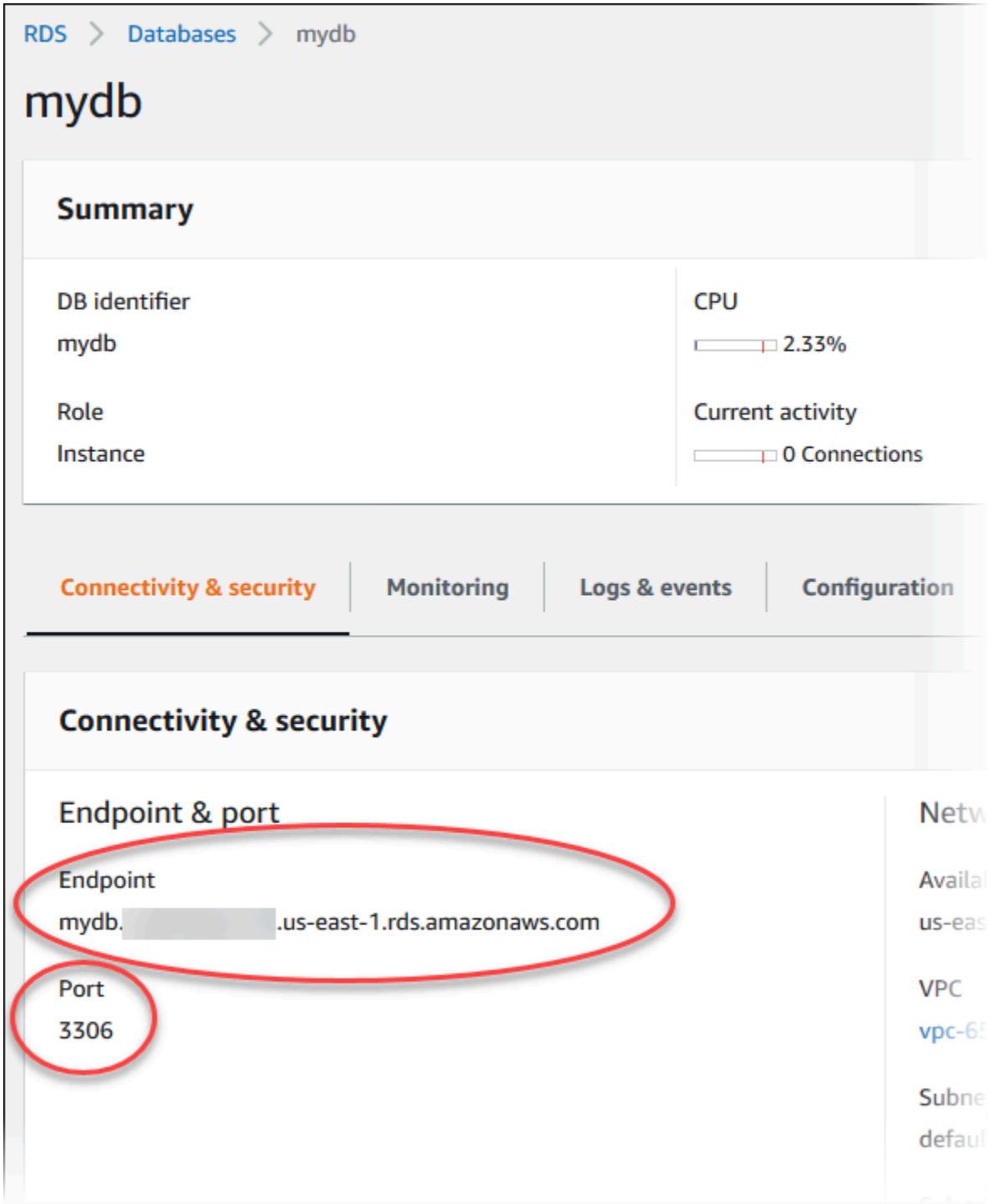
Para conectarse a una instancia de base de datos, utilice cualquier cliente para un motor de base de datos. Por ejemplo, puede usar la utilidad mysql para conectarse a una instancia de base de datos MariaDB o MySQL. Puede utilizar Microsoft SQL Server Management Studio para conectarse a una instancia de base de datos de SQL Server. Puede utilizar Oracle SQL Developer para conectarse a una instancia de base de datos de Oracle. De igual forma, puede usar una instancia local de la utilidad de línea de comandos psql para conectarse a una instancia de base de datos PostgreSQL.

Para buscar la información de conexión para una instancia de base de datos, use la AWS Management Console También puede utilizar el comando describe-db-instances de AWS Command Line Interface (AWS CLI) o la operación de la API DescribeDBInstances de RDS.

Consola

Para buscar la información de conexión para una instancia de base de datos en AWS Management Console

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) para ver una lista de las instancias de base de datos.
3. Elija el nombre de la instancia de base de datos para ver sus detalles.
4. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



5. Si necesita encontrar el nombre de usuario maestro, elija la ficha Configuration (Configuración) y vea el valor de Master username (Nombre de usuario maestro) .

AWS CLI

Para buscar la información de conexión de una instancia de base de datos mediante AWS CLI, llame al comando describe-db-instances. En la llamada, consulte el ID de instancia de base de datos, el punto de enlace, el puerto y el nombre de usuario maestro.

Para Linux, macOS o:Unix

```
aws rds describe-db-instances \
  --query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

En:Windows

```
aws rds describe-db-instances ^
  --query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

El resultado debería ser similar al siguiente.

```
[
    [
        "mydb",
        "mydb.123456789012.us-east-1.rds.amazonaws.com",
        3306,
        "admin"
    ],
    [
        "myoracledb",
        "myoracledb.123456789012.us-east-1.rds.amazonaws.com",
        1521,
        "dbadmin"
    ],
    [
        "mypostgresqldb",
        "mypostgresqldb.123456789012.us-east-1.rds.amazonaws.com",
        5432,
        "postgresadmin"
    ]
]
```

API de RDS

Para buscar la información de conexión de una instancia de base de datos mediante la API Amazon RDS, llame a la operación DescribedBInstances . En el resultado, busque los valores de la dirección del punto de enlace, el puerto del punto de enlace y el nombre de usuario maestro.

Situaciones para el acceso a una instancia de base de datos situada en una VPC

Mediante Amazon Virtual Private Cloud (Amazon VPC), puede lanzar recursos de AWS, como instancias de base de datos de Amazon RDS, en una Virtual Private Cloud (VPC). Cuando utiliza una Amazon VPC, puede controlar todos los aspectos del entorno de red virtual. Puede elegir su propio rango de direcciones IP, crear subredes y configurar listas de enrutamiento y control de acceso.

Un grupo de seguridad de VPC controla el acceso a una instancia de base de datos dentro de una VPC. Cada regla de grupo de seguridad de VPC permite a un origen específico obtener acceso a una instancia de base de datos de una VPC asociada a ese grupo de seguridad de VPC. El origen puede ser un rango de direcciones (por ejemplo, 203.0.113.0/24), u otro grupo de seguridad de VPC. Cuando se especifica un grupo de seguridad de VPC como origen, se permite el tráfico entrante procedente de todas las instancias, normalmente servidores de aplicaciones, que utilizan el grupo de seguridad de VPC.

Antes de intentar conectarse a la instancia de base de datos, configure la VPC para su caso de uso. Los siguientes escenarios son escenarios comunes para obtener acceso a una instancia de base de datos en una VPC:

- Una instancia de base de datos en una VPC a la que accede una Amazon EC2 instancia de la misma VPC – Un uso común de una instancia de base de datos en una VPC es compartir datos con un servidor de aplicaciones que se ejecuta en una instancia de EC2 en la misma VPC. La instancia de EC2 puede ejecutar un servidor web con una aplicación que interactúa con la instancia de base de datos.
- Una instancia de base de datos en una VPC a la que accede una instancia de EC2 en una VPC diferente – En algunos casos, la instancia de base de datos se encuentra en una VPC diferente de la instancia de EC2 que está utilizando para acceder a ella. Si es así, puede usar la interconexión de VPC para acceder a la instancia de base de datos.
- Una instancia de base de datos en una VPC a la que accede una aplicación cliente – a través de Internet Para acceder a una instancia de base de datos en una VPC desde una aplicación cliente

a través de Internet, configure una VPC con una única subred pública. También puede configurar una ninguna gateway de Internet para habilitar la comunicación a través de Internet.

Para conectarse a una instancia de base de datos desde afuera de su VPC, la instancia de base de datos debe ser accesible públicamente. Además, el acceso debe concederse mediante las reglas entrantes del grupo de seguridad de la instancia de base de datos y deben cumplirse otros requisitos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

- Una instancia de base de datos de una VPC a la que se accede desde una red privada: si su instancia de base de datos no es de acceso público, puede utilizar una de las siguientes opciones para acceder a ella desde una red privada:
  - Una conexión de Site-to-Site VPN de AWS.
  - Una conexión de AWS Direct Connect.
  - Una conexión de AWS Client VPN.

Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC.

Conexión a instancias de base de datos con los controladores de AWS

El conjunto de controladores de AWS se ha diseñado para permitir tiempos de transición y conmutación por error más rápidos y autenticarse con AWS Secrets Manager, AWS Identity and Access Management (IAM) e identidad federada. Los controladores de AWS se basan en la supervisión del estado de la instancia de base de datos y en el conocimiento de la topología de la instancia para determinar la nueva instancia principal. Este enfoque reduce los tiempos de transición y conmutación por error a segundos de un solo dígito, en comparación con las decenas de segundos de los controladores de código abierto.

En la tabla siguiente se enumeran las características admitidas para cada uno de los controladores. A medida que se introducen nuevas características de servicio, el objetivo del conjunto de controladores de AWS es contar con soporte integrado para estas características de servicio.

Característica	Controlador JDBC de AWS	Controlador de Python de AWS	Controlador ODBC de AWS para MySQL
Soporte de conmutación por error	Sí	Sí	Sí

Característica	Controlador JDBC de AWS	Controlador de Python de AWS	Controlador ODBC de AWS para MySQL
Supervisión mejorada de conmutación por error	Sí	Sí	Sí
División de lectura y escritura	Sí	Sí	No
Conexión de metadatos del controlador	Sí	N/A	N/A
Telemetría	Sí	Sí	No
Secrets Manager	Sí	Sí	Sí
Autenticación de IAM	Sí	Sí	Sí
Identidad federada (AD FS)	Sí	Sí	No
Identidad federada (Okta)	Sí	No	No
Clústeres de base de datos Multi-AZ	Sí	Sí	No

Para obtener más información sobre los controladores de AWS, consulte el controlador de idioma correspondiente de su instancia de base de datos RDS para MariaDB, RDS para MySQL o RDS para PostgreSQL.

> **Note**
>
> Las únicas características que se admiten con RDS para MariaDB son la autenticación con AWS Secrets Manager, AWS Identity and Access Management (IAM) y la identidad federada.

Conexión a una instancia de base de datos que ejecuta un motor de base de datos específico

Para obtener información sobre cómo conectarse a una instancia de base de datos que ejecute un motor de base de datos específico, siga las instrucciones para su motor de base de datos:

- RDS para Db2
- RDS para MariaDB
- RDS para SQL Server
- RDS para MySQL
- RDS para Oracle
- RDS para PostgreSQL

Administración de conexiones con RDS Proxy

También puede usar Amazon RDS Proxy para administrar conexiones a instancias de base de datos de RDS para MariaDB, RDS para Microsoft SQL Server, RDS para MySQL y RDS para PostgreSQL. El proxy de RDS permite a las aplicaciones agrupar y compartir conexiones de base de datos para mejorar la escalabilidad. Para obtener más información, consulte Amazon RDS Proxy .

Opciones de autenticación de bases de datos

Amazon RDS admite las siguientes formas de autenticar usuarios de bases de datos:

- Con la autenticación de contraseña,– la instancia de base de datos realiza toda la administración de las cuentas de usuario. Cree usuarios y especifique contraseñas con instrucciones SQL. Las instrucciones SQL que puede utilizar dependen de su motor de base de datos.
- AWS Identity and Access Management (IAM) con la autenticación de base de datos: no es necesario usar una contraseña al conectarse a una instancia de base de datos. En su lugar, puede usar un token de autenticación.
- Con la autenticación Kerberos– utiliza la autenticación externa de usuarios de bases de datos mediante Kerberos y Microsoft Active Directory. Kerberos es un protocolo de autenticación de red que usa tickets y criptografía de clave simétrica para eliminar la necesidad de transmitir contraseñas a través de la red. Kerberos ha sido creado en Active Directory y está diseñado para autenticar usuarios para recursos de redes, como bases de datos.

IAM la autenticación de base de datos y la autenticación Kerberos solo están disponibles para motores y versiones de base de datos específicos.

Para obtener más información, consulte Autenticación de bases de datos con Amazon RDS.

Conexiones cifradas

Puede utilizar SSL (Capa de conexión segura) o TLS (Transport Layer Security) desde una aplicación para cifrar una conexión a una instancia de base de datos. Cada motor base de datos tiene su propio proceso para implementar SSL/TLS. Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Trabajo con grupos de opciones

Algunos motores de base de datos ofrecen características adicionales que facilitan la administración de datos y bases de datos, y proporcionan seguridad adicional para su base de datos. Amazon RDS utiliza grupos de opciones para habilitar y configurar estas características. Un grupo de opciones puede especificar características, llamadas opciones, que están disponibles para una instancia de base de datos de Amazon RDS en particular. Las opciones pueden tener una configuración que especifica el funcionamiento de la opción. Cuando asocia una instancia de base de datos a un grupo de opciones, las opciones especificadas y la configuración de estas se habilitan para dicha instancia de base de datos.

Amazon RDS es compatible con opciones para los siguientes motores de base de datos:

Motor de base de datos	Documentación relacionada
`Db2`	Opciones de instancias de base de datos de RDS para Db2
`MariaDB`	Opciones para el motor de base de datos de MariaDB
`Microsoft SQL Server`	Opciones para el motor de base de datos de Microsoft SQL Server
`MySQL`	Opciones para las instancias de bases de datos MySQL
`Oracle`	Adición de opciones a instancias de base de datos de Oracle
`PostgreSQL`	PostgreSQL no utiliza opciones ni grupos de opciones. PostgreSQL utiliza extensiones y módulos para proporcionar características adicionales. Para obtener más información, consulte Versiones de extensiones de PostgreSQL compatibles.

Información general sobre grupos de opciones

Amazon RDS proporciona un grupo de opciones predeterminado vacío para cada instancia de base de datos nueva. No puede modificar este grupo de opciones predeterminado, pero cualquier grupo nuevo que cree deriva su configuración del grupo de opciones predeterminado. Para aplicar una opción a la instancia de base de datos, debe hacer lo siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Agregar una o más opciones al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

   Para asociar un grupo de opciones a una instancia de base de datos, modifique la instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Tanto las instancias de base de datos como las instantáneas de base de datos pueden asociarse a un grupo de opciones. En algunos casos, es posible que desee realizar la restauración a partir de una instantánea de copia de seguridad o realizar una restauración a un momento dado para instancia de base de datos. En esos casos, el grupo de opciones asociado a la instantánea o la instancia de base de datos se asocia, de forma predeterminada, a la instancia de base de datos restaurada. Puede asociar un grupo de opciones diferente a una instancia de base de datos restaurada. No obstante, el grupo de opciones nuevo debe contener cualquier opción persistente o permanente que se haya incluido en el grupo de opciones original. A continuación, se describen las opciones permanentes y persistentes.

Las opciones requieren memoria adicional para ejecutarse en una instancia de base de datos. Por lo tanto, tal vez deba lanzar una instancia más grande para utilizarlas, dependiendo del uso que haga actualmente de su instancia de base de datos. Por ejemplo, Oracle Enterprise Manager Database Control utiliza unos 300 MB de RAM. Si habilita esta opción para una instancia de base de datos pequeña, es posible que se produzcan problemas de rendimiento debido a errores de memoria insuficiente.

Opciones permanentes y persistentes

Dos tipos de opciones, persistentes y permanentes, exigen consideración especial cuando las agrega a un grupo de opciones.

Las opciones persistentes no se pueden eliminar de un grupo de opciones si las instancias de base de datos están asociadas al grupo de opciones. Un ejemplo es una opción persistente es la opción de TDE para el cifrado de datos transparente (TDE) de Microsoft SQL Server. Debe desasociar todas las instancias de base de datos del grupo de opciones para poder eliminar una opción persistente de dicho grupo. En algunos casos, es posible que desee restaurar o realizar una restauración a un momento dado desde una instancia de base de datos. En esos casos, si el grupo de opciones asociado a esa instantánea de base de datos contiene una opción persistente, solo puede asociar la instancia de base de datos restaurada a ese grupo de opciones.

Las opciones permanentes, por ejemplo, la opción TDE de Oracle Advanced Security, no pueden eliminarse nunca de un grupo de opciones. Puede cambiar el grupo de opciones de una instancia de base de datos que esté utilizando la opción permanente. Sin embargo, el grupo de opciones asociado a la instancia de base de datos debe incluir la misma opción permanente. En algunos casos, es posible que desee restaurar o realizar una restauración a un momento dado desde una instancia de base de datos. En esos casos, si el grupo de opciones asociado a esa instantánea de base de datos contiene una opción permanente, solo puede asociar la instancia de base de datos restaurada a ese grupo de opciones con esa opción permanente.

Para obtener las instancias de base de datos de Oracle, puede copiar las instantáneas de base de datos compartidas que tengan las opciones `Timezone` o `OLS` (o ambas). Para hacerlo, especifique un grupo de opciones de destinos que incluya estas opciones cuando copie la instantánea de base de datos. La opción OLS es permanente y persistente solo para las instancias de base de datos de Oracle que ejecuten la versión 12.2 o superior de Oracle. Para obtener más información sobre estas opciones, consulte Zona horaria Oracle y Oracle Label Security.

Consideraciones acerca del VPC

El grupo de opciones asociado a la instancia de base de datos está vinculado a la VPC de la instancia de base de datos. Esto significa que no puede utilizar el grupo de opciones asignado a una instancia de base de datos si intenta restaurar la instancia a una VPC diferente. Si restaura una instancia de base de datos en una VPC diferente, puede realizar uno de los siguientes procedimientos:

- Asignar el grupo de opciones predeterminado a la instancia de base de datos.
- Asigne un grupo de opciones que esté vinculado a esa VPC.
- Crear un nuevo grupo de opciones y asignarlo a la instancia de base de datos.

Con las opciones persistentes o permanentes, como TDE de Oracle, debe crear un grupo de opciones nuevo. Este grupo de opciones debe incluir la opción persistente o permanente cuando se restaura una instancia de BD en una VPC diferente.

La configuración de opciones controla el comportamiento de una opción. Por ejemplo, la opción de Oracle Advanced Security `NATIVE_NETWORK_ENCRYPTION` tiene una configuración que puede utilizar para especificar el algoritmo de cifrado para el tráfico de red hacia y desde la instancia de base de datos. Algunas configuraciones de opciones se han optimizado para Amazon RDS y no pueden cambiarse.

Opciones que se excluyen mutuamente

Algunas opciones se excluyen mutuamente. Puede utilizar una de las dos, pero no utilizar las dos al mismo tiempo. Las siguientes opciones se excluyen mutuamente:

- Oracle Enterprise Manager Database Express y Oracle Management Agent para Enterprise Manager Cloud Control.
- Oracle Native Network Encryption y Capa de conexión segura de Oracle.

Creación de un grupo de opciones

Puede crear un nuevo grupo de opciones que derive su configuración del grupo de opciones por defecto. Agregue entonces una o más opciones al grupo de opciones. O bien, si ya dispone de un grupo de opciones existente, puede copiarlo con todas sus opciones a un nuevo grupo de opciones. Para obtener más información, consulte Copia de un grupo de opciones.

Después de crear un grupo de opciones nuevo, no tiene opciones. Para aprender cómo agregar opciones al grupo de opciones, consulte Agregar una opción a un grupo de opciones. Una vez que haya agregado las opciones deseadas, puede asociar el grupo de opciones a la instancia de base de datos. De esta forma, las opciones estarán disponibles en la instancia de base de datos. Para obtener información sobre cómo asociar una grupo de opciones a una instancia de base de datos, consulte la documentación para su motor en Trabajo con grupos de opciones.

Consola

Una manera de crear un grupo de opciones es mediante la AWS Management Console.

Para crear un grupo de opciones nuevo mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En la ventana Create option group (Crear grupo de opciones), haga lo siguiente:
    a. En Name, escriba un nombre para el grupo de opciones que sea exclusivo dentro de su cuenta AWS. El nombre solo puede contener letras, dígitos y guiones.

b. En Description, escriba una breve descripción del grupo de opciones. La descripción se utiliza para fines de visualización.

c. En Engine, elija el motor de base de datos que desea.

d. En Major engine version (Versión de motor principal), elija la versión principal del motor de base de datos que desea.

5. Para continuar, elija Create (Crear). Para cancelar la operación, elija Cancel.

AWS CLI

Para crear un grupo de opciones, utilice el comando AWS CLI de la `create-option-group` con los siguientes parámetros obligatorios.

- `--option-group-name`
- `--engine-name`
- `--major-engine-version`
- `--option-group-description`

Example

En el siguiente ejemplo, se crea un grupo de opciones llamado `testoptiongroup`, que se asocia con el motor de base de datos Oracle Enterprise Edition. La descripción se proporciona entre comillas.

Para Linux, macOS o:Unix

```
aws rds create-option-group \
    --option-group-name testoptiongroup \
    --engine-name oracle-ee \
    --major-engine-version 19 \
    --option-group-description "Test option group for Oracle Database 19c EE"
```

En:Windows

```
aws rds create-option-group ^
    --option-group-name testoptiongroup ^
    --engine-name oracle-ee ^-
    --major-engine-version 19 ^
    --option-group-description "Test option group for Oracle Database 19c EE"
```

API de RDS

Para crear un grupo de opciones, llame a la operación `CreateOptionGroup` de la API de Amazon RDS. Incluya los siguientes parámetros:

- `OptionGroupName`
- `EngineName`
- `MajorEngineVersion`
- `OptionGroupDescription`

Copia de un grupo de opciones

Puede usar la AWS CLI o la API de Amazon RDS para copiar un grupo de opciones. Copiar un grupo de opciones puede resultar práctico. Un ejemplo es cuando se tiene un grupo de opciones existente y se quiere incluir la mayoría de sus parámetros y valores personalizados en un nuevo grupo de opciones. También es posible hacer una copia de un grupo de opciones que se utiliza en producción y modificar, a continuación, la copia para probar otra configuración de opciones.

> **Note**
>
> Actualmente, no puede copiar un grupo de opciones en una región AWS diferente.

AWS CLI

Para copiar un grupo de opciones, utilice el comando copy-option-group de la AWS CLI. Incluya las siguientes opciones obligatorias:

- `--source-option-group-identifier`
- `--target-option-group-identifier`

- `--target-option-group-description`

Example

En el siguiente ejemplo, se crea un grupo de opciones llamado `new-option-group`, que es una copia local del grupo de opciones `my-option-group`.

Para Linux, macOS o:Unix

```
aws rds copy-option-group \
    --source-option-group-identifier my-option-group \
    --target-option-group-identifier new-option-group \
    --target-option-group-description "My new option group"
```

En:Windows

```
aws rds copy-option-group ^
    --source-option-group-identifier my-option-group ^
    --target-option-group-identifier new-option-group ^
    --target-option-group-description "My new option group"
```

API de RDS

Para copiar un grupo de opciones, llame a la operación CopyOptionGroup de la API de Amazon RDS. Incluya los siguientes parámetros obligatorios.

- `SourceOptionGroupIdentifier`
- `TargetOptionGroupIdentifier`
- `TargetOptionGroupDescription`

Agregar una opción a un grupo de opciones

Puede agregar una opción a un grupo de opciones existente. Una vez que haya agregado las opciones deseadas, puede asociar el grupo de opciones a la instancia de base de datos para que las opciones estén disponibles en dicha instancia. Para obtener información sobre cómo asociar un grupo de opciones a una instancia de base de datos, consulte la documentación para su motor de base de datos específico, que podrá encontrar en Trabajo con grupos de opciones.

Los cambios en los grupos de opciones deben aplicarse de inmediato en dos casos:

- Cuando incorpora una opción que agrega o actualiza el valor de un puerto, por ejemplo, la opción `OEM`.
- Cuando agrega o elimina un grupo de opciones con una opción que incluye el valor de un puerto.

En esos casos, elija la opción Apply Immediately (Aplicar inmediatamente) en la consola. También puede incluir la opción `--apply-immediately` cuando utilice la AWS CLI o establezca el parámetro `ApplyImmediately` en `true` cuando utilice la API de Amazon RDS. Las opciones que no incluyen valores de puertos pueden aplicarse inmediatamente o durante el siguiente período de mantenimiento de la instancia de base de datos.

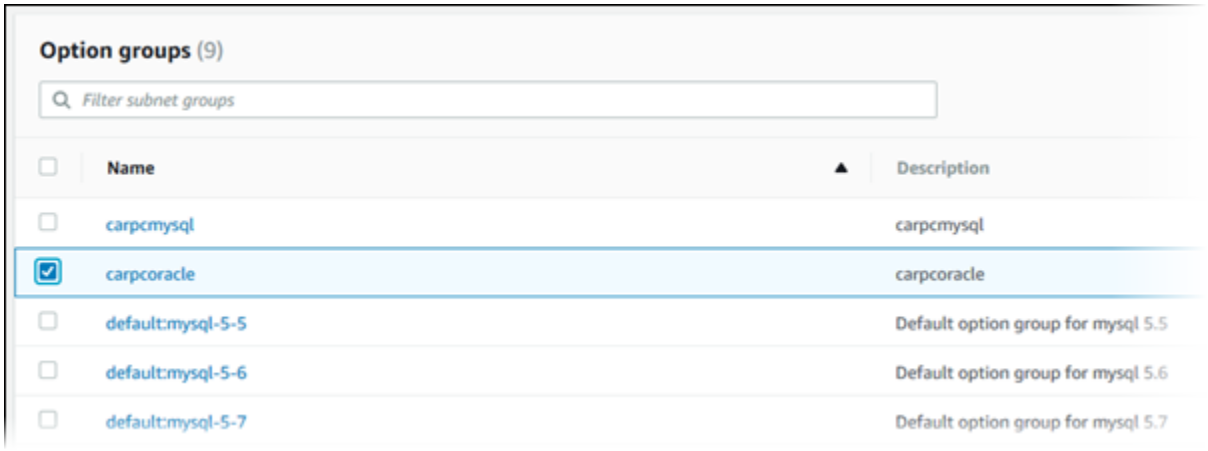
> **Note**
>
> Si especifica un grupo de seguridad como un valor para una opción de un grupo de opciones, puede administrar el grupo de seguridad modificando el grupo de opciones. No puede cambiar ni quitar este grupo de seguridad modificando una instancia de base de datos. Además, el grupo de seguridad no aparece en los detalles de la instancia de base de datos en la AWS Management Console ni en el resultado del comando de la AWS CLI `describe-db-instances`.

Consola

Puede utilizar la AWS Management Console para agregar una opción a un grupo de opciones.

Para agregar una opción a un grupo de opciones mediante la consola

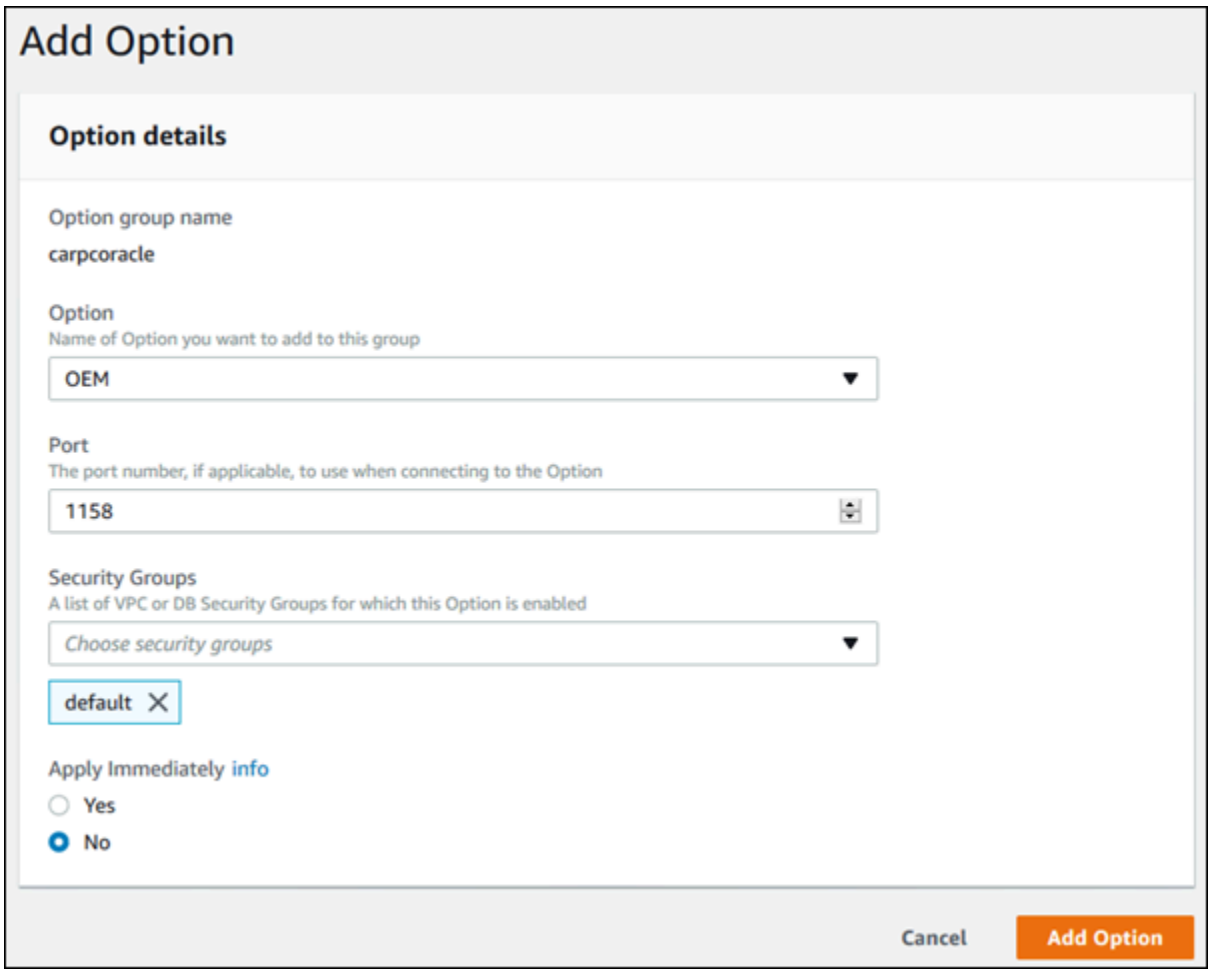
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que desea modificar y, a continuación, elija Add option (Agregar opción).



4. En la ventana Add option (Añadir opción), haga lo siguiente:

   a. Elija la opción que desea agregar. Es posible que tenga que proporcionar valores adicionales según la opción seleccionada. Por ejemplo, si elige la opción `OEM`, también debe escribir un valor de puerto y especificar un grupo de seguridad.

   b. Para habilitar la opción en todas las instancias de base de datos asociadas en cuanto la agregue, en Apply Immediately, elija Yes. Si elige No (valor predeterminado), la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento.



5. Cuando los ajustes sean los deseados, elija Add Option (Agregar opción).

AWS CLI

Para agregar una opción a un grupo de opciones, ejecute el comando add-option-to-option-group de la AWS CLI con la opción deseada. Para habilitar la opción nueva inmediatamente en todas las instancias de base de datos asociadas, incluya el parámetro `--apply-immediately`. De forma predeterminada, la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento. Incluya el siguiente parámetro obligatorio:

- `--option-group-name`

Example

En el siguiente ejemplo, se añade la opción `Timezone` con la configuración `America/Los_Angeles` a un grupo de opciones llamado `testoptiongroup` y se habilita inmediatamente.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name testoptiongroup \
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=America/
Los_Angeles}]" \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name testoptiongroup ^
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=America/
Los_Angeles}]" ^
    --apply-immediately
```

El resultado del comando es similar al siguiente:

```
...{
       "OptionName": "Timezone",
       "OptionDescription": "Change time zone",
       "Persistent": true,
       "Permanent": false,
       "OptionSettings": [
           {
               "Name": "TIME_ZONE",
               "Value": "America/Los_Angeles",
               "DefaultValue": "UTC",
               "Description": "Specifies the timezone the user wants to change the
 system time to",
               "ApplyType": "DYNAMIC",
               "DataType": "STRING",
               "AllowedValues": "Africa/Cairo,...",
               "IsModifiable": true,
               "IsCollection": false
           }
       ],
```

```
        "DBSecurityGroupMemberships": [],
        "VpcSecurityGroupMemberships": []
    }...
```

Example

En el siguiente ejemplo se añade la opción OEM de Oracle a un grupo de opciones. También especifica un puerto personalizado y un par de grupos de seguridad de VPC de Amazon EC2 que utilizar para ese puerto.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name testoptiongroup \
    --options OptionName=OEM,Port=5500,VpcSecurityGroupMemberships="sg-test1,sg-test2"
 \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name testoptiongroup ^
    --options OptionName=OEM,Port=5500,VpcSecurityGroupMemberships="sg-test1,sg-test2"
 ^
    --apply-immediately
```

El resultado del comando es similar al siguiente:

```
OPTIONGROUP  False  oracle-ee  19 arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
 Test Option Group  testoptiongroup vpc-test
OPTIONS Oracle 12c EM Express   OEM     False   False   5500
VPCSECURITYGROUPMEMBERSHIPS     active  sg-test1
VPCSECURITYGROUPMEMBERSHIPS     active  sg-test2
```

Example

El siguiente ejemplo, se agrega la opción de Oracle `NATIVE_NETWORK_ENCRYPTION` a un grupo de opciones y se especifica la configuración de opciones. Si no se especifica ninguna configuración de opciones, se utilizan los valores predeterminados.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name testoptiongroup \
    --options '[{"OptionSettings":
[{"Name":"SQLNET.ENCRYPTION_SERVER","Value":"REQUIRED"},
{"Name":"SQLNET.ENCRYPTION_TYPES_SERVER","Value":"AES256,AES192,DES"}],"OptionName":"NATIVE_NET
 \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name testoptiongroup ^
    --options "OptionSettings"=[{"Name"="SQLNET.ENCRYPTION_SERVER","Value"="REQUIRED"},
{"Name"="SQLNET.ENCRYPTION_TYPES_SERVER","Value"="AES256\,AES192\,DES"}],"OptionName"="NATIVE_N
 ^
    --apply-immediately
```

El resultado del comando es similar al siguiente:

```
...{
    "OptionName": "NATIVE_NETWORK_ENCRYPTION",
    "OptionDescription": "Native Network Encryption",
    "Persistent": false,
    "Permanent": false,
    "OptionSettings": [
        {
            "Name": "SQLNET.ENCRYPTION_TYPES_SERVER",
             "Value": "AES256,AES192,DES",
            "DefaultValue":
 "RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40",
            "Description": "Specifies list of encryption algorithms in order of
 intended use",
            "ApplyType": "STATIC",
            "DataType": "STRING",
            "AllowedValues":
 "RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40",
            "IsModifiable": true,
            "IsCollection": true
        },
        {
            "Name": "SQLNET.ENCRYPTION_SERVER",
            "Value": "REQUIRED",
```

```
            "DefaultValue": "REQUESTED",
            "Description": "Specifies the desired encryption behavior",
            "ApplyType": "STATIC",
            "DataType": "STRING",
            "AllowedValues": "ACCEPTED,REJECTED,REQUESTED,REQUIRED",
            "IsModifiable": true,
            "IsCollection": false
        },...
```

API de RDS

Para agregar una opción a un grupo de opciones mediante la API de Amazon RDS, llame a la operación ModifyOptionGroup con la opción deseada. Para habilitar la opción nueva inmediatamente en todas las instancias de base de datos asociadas, incluya el parámetro `ApplyImmediately` y establézcalo en `true`. De forma predeterminada, la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento. Incluya el siguiente parámetro obligatorio:

- `OptionGroupName`

Descripción de opciones y configuración de opciones para un grupo de opciones

Puede enumerar todas las opciones y la configuración de opciones para un grupo de opciones.

Consola

Puede utilizar la AWS Management Console para enumerar todas las opciones y la configuración de opciones para un grupo de opciones.

Para enumerar las opciones y la configuración de opciones para un grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el nombre del grupo de opciones para mostrar sus detalles. Se muestran las opciones y la configuración de opciones en el grupo de opciones.

AWS CLI

Para enumerar las opciones y la configuración de opciones para un grupo de opciones, utilice el comando AWS CLI de la `describe-option-groups`. Especifique el nombre del grupo de opciones cuyas opciones y configuración desea ver. Si no especifica un nombre de grupo de opciones, se describen todos los grupos de opciones.

Example

En el siguiente ejemplo, se enumeran las opciones y la configuración de opciones para todos los grupos de opciones.

```
aws rds describe-option-groups
```

Example

En el siguiente ejemplo, se enumeran las opciones y la configuración de opciones para un grupo de opciones llamado `testoptiongroup`.

```
aws rds describe-option-groups --option-group-name testoptiongroup
```

API de RDS

Para enumerar las opciones y la configuración de opciones para un grupo de opciones, utilice la operación `DescribeOptionGroups` de la API de Amazon RDS . Especifique el nombre del grupo de opciones cuyas opciones y configuración desea ver. Si no especifica un nombre de grupo de opciones, se describen todos los grupos de opciones.

Modificación de una configuración de opciones

Después de agregar una opción cuya configuración sea modificable, puede modificar dicha configuración en cualquier momento. Si cambia opciones o la configuración de estas en un grupo de opciones, esos cambios se aplican a todas las instancias de base de datos asociadas al grupo de opciones. Para obtener más información sobre las configuraciones disponibles para las diferentes opciones, consulte la documentación para su motor en Trabajo con grupos de opciones.

Los cambios en los grupos de opciones deben aplicarse de inmediato en dos casos:

- Cuando incorpora una opción que agrega o actualiza el valor de un puerto, por ejemplo, la opción `OEM`.

- Cuando agrega o elimina un grupo de opciones con una opción que incluye el valor de un puerto.

En esos casos, elija la opción Apply Immediately (Aplicar inmediatamente) en la consola. También puede incluir la opción `--apply-immediately` cuando utilice la AWS CLI o establezca el parámetro `ApplyImmediately` en `true` cuando utilice la API de RDS. Las opciones que no incluyen valores de puertos pueden aplicarse inmediatamente o durante el siguiente período de mantenimiento de la instancia de base de datos.

> **Note**
>
> Si especifica un grupo de seguridad como un valor para una opción de un grupo de opciones, puede administrar el grupo de seguridad modificando el grupo de opciones. No puede cambiar ni quitar este grupo de seguridad modificando una instancia de base de datos. Además, el grupo de seguridad no aparece en los detalles de la instancia de base de datos en la AWS Management Console ni en el resultado del comando de la AWS CLI `describe-db-instances`.

Consola

Puede utilizar la AWS Management Console para modificar una configuración de opciones.

Para modificar una configuración de opciones mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Seleccione el grupo de opciones cuya opción desea modificar y, a continuación, elija Modify option (Modificar opción).
4. En la ventana Modify option (Modificar opción), en Installed Options (Opciones instaladas), elija la opción cuya configuración desea modificar. Haga los cambios que desee.
5. Para habilitar la opción en cuanto la agregue, en Apply Immediately, elija Yes. Si elige No (valor predeterminado), la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento.
6. Cuando los ajustes sean los deseados, elija Modify Option.

AWS CLI

Para modificar una opción de configuración, utilice el comando AWS CLI de la `add-option-to-option-group` con el grupo de opciones y la opción que desea modificar. De forma predeterminada, la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento. Para aplicar el cambio inmediatamente en todas las instancias de base de datos asociadas, incluya el parámetro `--apply-immediately`. Para modificar una configuración de opciones, utilice el argumento `--settings`.

Example

El siguiente ejemplo, se modifica el puerto que Oracle Enterprise Manager Database Control (OEM) utiliza en un grupo de opciones llamado `testoptiongroup` y se aplica el cambio inmediatamente.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name testoptiongroup \
    --options OptionName=OEM,Port=5432,DBSecurityGroupMemberships=default \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name testoptiongroup ^
    --options OptionName=OEM,Port=5432,DBSecurityGroupMemberships=default ^
    --apply-immediately
```

El resultado del comando es similar al siguiente:

```
OPTIONGROUP   False  oracle-ee  19  arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
   Test Option Group    testoptiongroup
OPTIONS Oracle 12c EM Express   OEM     False   False   5432
DBSECURITYGROUPMEMBERSHIPS   default  authorized
```

Example

En el siguiente ejemplo, se modifica la opción de Oracle `NATIVE_NETWORK_ENCRYPTION` y se cambia la configuración de opciones.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name testoptiongroup \
    --options '[{"OptionSettings":
[{"Name":"SQLNET.ENCRYPTION_SERVER","Value":"REQUIRED"},
{"Name":"SQLNET.ENCRYPTION_TYPES_SERVER","Value":"AES256,AES192,DES,RC4_256"}],"OptionName":"NA
 \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name testoptiongroup ^
    --options "OptionSettings"=[{"Name"="SQLNET.ENCRYPTION_SERVER","Value"="REQUIRED"},
{"Name"="SQLNET.ENCRYPTION_TYPES_SERVER","Value"="AES256\,AES192\,DES
\,RC4_256"}],"OptionName"="NATIVE_NETWORK_ENCRYPTION" ^
    --apply-immediately
```

El resultado del comando es similar al siguiente:

```
OPTIONGROUP   False  oracle-ee  19  arn:aws:rds:us-east-1:1234567890:og:testoptiongroup
   Test Option Group    testoptiongroup
OPTIONS Oracle Advanced Security - Native Network Encryption
 NATIVE_NETWORK_ENCRYPTION       False   False
OPTIONSETTINGS
 RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40 STATIC
 STRING
   RC4_256,AES256,AES192,3DES168,RC4_128,AES128,3DES112,RC4_56,DES,RC4_40,DES40
 Specifies list of encryption algorithms in order of intended use
   True     True    SQLNET.ENCRYPTION_TYPES_SERVER  AES256,AES192,DES,RC4_256
OPTIONSETTINGS  ACCEPTED,REJECTED,REQUESTED,REQUIRED    STATIC  STRING  REQUESTED
 Specifies the desired encryption behavior  False   True  SQLNET.ENCRYPTION_SERVER
 REQUIRED
OPTIONSETTINGS  SHA1,MD5   STATIC  STRING  SHA1,MD5    Specifies list of
 checksumming algorithms in order of intended use      True    True
 SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER  SHA1,MD5
OPTIONSETTINGS  ACCEPTED,REJECTED,REQUESTED,REQUIRED  STATIC  STRING
 REQUESTED     Specifies the desired data integrity behavior   False   True
 SQLNET.CRYPTO_CHECKSUM_SERVER  REQUESTED
```

API de RDS

Para modificar una opción de configuración, utilice el comando `ModifyOptionGroup` de la API Amazon RDS con el grupo de opciones y la opción que desea modificar. De forma predeterminada, la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento. Para aplicar el cambio inmediatamente en todas las instancias de base de datos asociadas, incluya el parámetro `ApplyImmediately` y establézcalo en `true`.

Quitar una opción de un grupo de opciones

Algunas opciones pueden eliminarse de un grupo de opciones, mientras que otras no. Una opción persistente no puede eliminarse de un grupo de opciones hasta que no se desasocien todas las instancias de base de datos asociadas a dicho grupo. Una opción permanente no se puede eliminar nunca de un grupo de opciones. Para obtener más información sobre qué opciones pueden eliminarse, consulte la documentación para su motor específico, que podrá encontrar en Trabajo con grupos de opciones.

Si elimina todas las opciones de un grupo de opciones, Amazon RDS no elimina el grupo de opciones. Las instancias de base de datos asociadas con el grupo de opciones vacío siguen estando asociadas a él, pero no tienen ninguna opción activa. Alternativamente, para eliminar todas las opciones de una instancia de base de datos, puede asociar la instancia de base datos al grupo de opciones predeterminado (vacío).

Consola

Puede utilizar la AWS Management Console para eliminar una opción de un grupo de opciones.

Para eliminar una opción de un grupo de opciones mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Seleccione el grupo de opciones cuya opción desea eliminar y, a continuación, elija Delete option (Eliminar opción).
4. En la ventana Delete option (Eliminar opción), haga lo siguiente:
   - Seleccione la casilla de verificación correspondiente a la opción que desea eliminar.

- Para que la eliminación surta efecto en cuanto la realice, en Apply immediately (Aplicar inmediatamente), elija Yes (Sí). Si elige No (valor predeterminado), la opción se elimina para cada instancia de base de datos asociada durante su siguiente período de mantenimiento.



5. Una vez que la configuración sea la deseada, elija Yes, Delete.

AWS CLI

Para eliminar una opción de un grupo de opciones, utilice el comando de la AWS CLI `remove-option-from-option-group` con la opción que desea eliminar. De forma predeterminada, la opción se elimina de cada instancia de base de datos asociada durante su siguiente período de mantenimiento. Para aplicar el cambio inmediatamente, incluya el parámetro `--apply-immediately`.

Example

En el siguiente ejemplo, se elimina la opción Oracle Enterprise Manager Database Control (OEM) de un grupo de opciones llamado `testoptiongroup` y se aplica el cambio inmediatamente.

Para Linux, macOS o:Unix

```
aws rds remove-option-from-option-group \
    --option-group-name testoptiongroup \
    --options OEM \
    --apply-immediately
```

En:Windows

```
aws rds remove-option-from-option-group ^
    --option-group-name testoptiongroup ^
    --options OEM ^
    --apply-immediately
```

El resultado del comando es similar al siguiente:

```
OPTIONGROUP    testoptiongroup oracle-ee   19    Test option group
```

API de RDS

Para eliminar una opción de un grupo de opciones, utilice la acción `ModifyOptionGroup` de la API de Amazon RDS. De forma predeterminada, la opción se elimina de cada instancia de base de datos asociada durante su siguiente período de mantenimiento. Para aplicar el cambio inmediatamente, incluya el parámetro `ApplyImmediately` y establézcalo en `true`.

Incluya los siguientes parámetros:

- `OptionGroupName`
- `OptionsToRemove.OptionName`

Eliminación de un grupo de opciones

Solo puede eliminar un grupo de opciones si cumple los siguientes criterios:

- No está asociado a ningún recurso de Amazon RDS. Se puede asociar un grupo de opciones a una instancia de base de datos, una instantánea de base de datos o una instantánea de base de datos automatizada.
- No es un grupo de opciones predeterminado.

Para identificar los grupos de opciones que utilizan las instancias de base de datos y las instantáneas de base de datos, puede utilizar los siguientes comandos de la CLI:

```
aws rds describe-db-instances \
    --query 'DBInstances[*].
[DBInstanceIdentifier,OptionGroupMemberships[].OptionGroupName]'

aws rds describe-db-snapshots | jq -r '.DBSnapshots[] | "\(.DBInstanceIdentifier),
\(.OptionGroupName)"' | sort | uniq
```

Si intenta eliminar un grupo de opciones asociado a un recurso de RDS, se genera un error como el siguiente.

```
An error occurred (InvalidOptionGroupStateFault) when calling the DeleteOptionGroup
 operation: The option group 'optionGroupName' cannot be deleted because it is in use.
```

Para buscar los recursos de Amazon RDS asociados a un grupo de opciones, realice el siguiente procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el nombre del grupo de opción para mostrar sus detalles.
4. Compruebe la sección Associated Instances and Snapshots (Instantáneas e instancias asociadas) para los recursos de Amazon RDS asociados.

Si se asocia una instancia de base de datos a un grupo de opciones, modifique la instancia de base de datos para utilizar un grupo de opciones diferente. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Si se asocia una instantánea de base de datos manual al grupo de opciones, modifique la instantánea de base de datos para utilizar un grupo de opciones diferente. Para ello, puede usar el comando `modify-db-snapshot` de AWS CLI:

> **Note**
>
> No puede modificar el grupo de opciones de una instantánea de base de datos automatizada.

Consola

Una forma de eliminar un grupo de opciones es utilizar la AWS Management Console.

Para eliminar un grupo de opciones mediante la consola, realice el siguiente procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones.
4. Elija Delete group (Eliminar grupo).
5. En la página de confirmación, elija Delete (Eliminar) para acabar de eliminar el grupo de opciones o seleccione Cancel (Cancelar) para cancelar la eliminación.

AWS CLI

Para eliminar un grupo de opciones, utilice el comando AWS CLI de la `delete-option-group` con el siguiente parámetro necesario.

- `--option-group-name`

Example

En el siguiente ejemplo se elimina un grupo de opciones denominado `testoptiongroup`.

Para Linux, macOS o:Unix

```
aws rds delete-option-group \
    --option-group-name testoptiongroup
```

En:Windows

```
aws rds delete-option-group ^
    --option-group-name testoptiongroup
```

API de RDS

Para eliminar un grupo de opciones, llame a la operación `DeleteOptionGroup` de la API de Amazon RDS. Incluya el siguiente parámetro:

- `OptionGroupName`

Grupos de parámetros para Amazon RDS

Parámetros de la base de datos especificar cómo está configurada la base de datos. Por ejemplo, los parámetros de la base de datos pueden especificar la cantidad de recursos, como la memoria, que se asignarán a una base de datos.

Administre la configuración de la base de datos mediante la asociación de las instancias de base de datos y los clústeres de bases de datos Multi-AZ de con los grupos de parámetros. Amazon RDS define los grupos de parámetros con la configuración predeterminada. También puede definir sus propios grupos de parámetros con una configuración personalizada.

> **Note**
>
> Algunos motores de base de datos ofrecen características adicionales que puede agregar a la base de datos como opciones en un grupo de opciones. Para obtener más información acerca de los grupos de opciones, consulte Trabajo con grupos de opciones.

Temas

- Descripción general de los grupos de parámetros
- Grupos de parámetros de base de datos para instancias de Amazon RDS
- Trabajo con grupos de parámetros de clúster de base de datos para clústeres de base de datos Multi-AZ
- Comparación de grupos de parámetros de la base de datos
- Especificación de parámetros de base de datos

Descripción general de los grupos de parámetros

Un grupo de parámetros de base de datos sirve de contenedor para los valores de configuración del motor que se aplican a una o varias instancias de bases de datos.

Los grupos de parámetros de clúster de base de datos solo se aplican a clústeres de base de datos Multi-AZ. En un clúster de base de datos Multi-AZ, la configuración del grupo de parámetros del clúster de base de datos se aplica a todas las instancias de base de datos del clúster. El grupo de parámetros de base de datos predeterminado para el motor y la versión del motor de base de datos se utiliza para cada instancia de base de datos del clúster de base de datos.

Temas

- Grupos de parámetros predeterminados y personalizados
- Parámetros de instancias de base de datos estáticos y dinámicos
- Parámetros de clústeres de base de datos estáticos y dinámicos
- Parámetros del conjunto de caracteres
- Parámetros y valores de parámetros admitidos

Grupos de parámetros predeterminados y personalizados

Si crea una instancia de base de datos sin especificar un grupo de parámetros de bases de datos, la instancia de base de datos utilizará un grupo de parámetros de base de datos predeterminado. Del mismo modo, si crea un clúster de base de datos Multi-AZ de sin especificar un grupo de parámetros del clúster de base de datos, el clúster utiliza un grupo de parámetros de clúster de base de datos predeterminado. Cada grupo de parámetros predeterminado contiene los valores predeterminados del motor de base de datos, así como también los valores predeterminados del sistema Amazon RDS correspondientes al motor, la clase de computación y el almacenamiento asignado de la instancia.

La configuración de los parámetros de un grupo de parámetros predeterminado no se puede modificar. En su lugar, puede hacer lo siguiente:

1. Cree un nuevo grupo de parámetros.
2. Cambie la configuración de los parámetros que desee. No todos los parámetros del motor de base de datos pueden cambiarse en el grupo de parámetros.
3. Modifique su instancia o clúster de base de datos para asociar el nuevo grupo de parámetros .

   Al asociar un nuevo grupo de parámetros de base de datos con una instancia de base de datos, la asociación se produce de inmediato. Para obtener información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS. Para obtener más información sobre la modificación de clústeres de base de datos Multi-AZ, consulte Modificación de un clúster de base de datos multi-AZ para Amazon RDS..

   > **Note**
   >
   > Si ha modificado la instancia de base de datos para usar un grupo de parámetros personalizado y la inicia, RDS la reinicia automáticamente como parte del proceso de inicio. Para las instancias Multi-AZ de RDS para SQL Server con las opciones AlwaysOn o

Mirroring habilitadas, se espera una conmutación por error cuando la instancia se reinicie tras el proceso de startup.

RDS aplica los parámetros estáticos y dinámicos modificados en un grupo de parámetros recién asociado después de reiniciar la instancia de base de datos. Sin embargo, si modifica los parámetros dinámicos en el grupo de parámetros de base de datos después de asociarlos a la instancia de base de datos, dichos cambios se aplican inmediatamente sin reiniciar. Para obtener información sobre el cambio del grupo de parámetros de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Si actualiza los parámetros en un grupo de parámetros de base de datos, los cambios se aplican a todas las instancias de base de datos que se asocian a ese grupo de parámetros. Del mismo modo, si actualiza los parámetros dentro de un grupo de parámetros del clúster de base de datos Multi-AZ de , los cambios se aplican a todos los clústeres de base de datos de Aurora asociados a ese grupo de parámetros del clúster de base de datos.

Si no desea crear un grupo de parámetros desde cero, puede copiar un grupo de parámetros existente con los comandos de la AWS CLI copy-db-parameter-group o copy-db-clúster-parameter-group. Puede que le resulte útil copiar un grupo de parámetros en algunos casos. Por ejemplo, podría querer incluir la mayoría de los parámetros y valores personalizados de un grupo de parámetros de la base de datos existente en un grupo de parámetros de una base de datos nueva.

Parámetros de instancias de base de datos estáticos y dinámicos

Los parámetros de instancia de base de datos son estáticos o dinámicos. Se diferencian en lo siguiente:

- Cuando se cambia un parámetro estático y se guarda el grupo de parámetros de base de datos, el cambio de parámetros se aplicará después de reiniciar manualmente las instancias de base de datos asociadas. Para los parámetros estáticos, La consola siempre utiliza `pending-reboot` para la `ApplyMethod`.
- Al cambiar un parámetro dinámico, el cambio de parámetros se aplica de forma predeterminada inmediatamente, sin necesidad de reiniciar. Al utilizar la AWS Management Console para cambiar los valores de parámetros de clúster de base de datos, esta siempre utiliza `immediate` para el `ApplyMethod` para los parámetros dinámicos. Para aplazar el cambio de parámetros hasta después de reiniciar una instancia de base de datos asociada, utilice la AWS CLI o la API de RDS. Establezca `ApplyMethod` en `pending-reboot` para el cambio de parámetro.

> **Note**
>
> El uso de `pending-reboot` con parámetros dinámicos en AWS CLI o en la API de RDS en instancias base de datos de RDS for SQL Server genera un error. Utilice `apply-immediately` en RDS for SQL Server.

Para obtener más información acerca del uso de la AWS CLI para cambiar el valor de un parámetro, consulte modificy-db-parameter-group. Para obtener más información acerca del uso de la API de RDS para cambiar un valor de parámetro, consulte ModifyDBParameterGroup.

Si una instancia de base de datos no está utilizando los últimos cambios de su grupo de parámetros de base de datos asociado, la consola muestra un estado de pending-reboot para el grupo de parámetros de base de datos. Este estado no genera un reinicio automático durante la siguiente ventana de mantenimiento. Para aplicar los cambios de parámetros más recientes en esa instancia de base de datos, reinicie manualmente la instancia de base de datos.

Parámetros de clústeres de base de datos estáticos y dinámicos

Los parámetros de clúster de base de datos son estáticos o dinámicos. Se diferencian en lo siguiente:

- Cuando se cambia un parámetro estático y se guarda el grupo de parámetros de clúster de base de datos, el cambio de parámetros tendrá efecto después de reiniciar manualmente los clústeres de base de datos asociados. Para los parámetros estáticos, La consola siempre utiliza `pending-reboot` para la `ApplyMethod`.
- Al cambiar un parámetro dinámico, el cambio de parámetros se aplica de forma predeterminada inmediatamente, sin necesidad de reiniciar. Al utilizar la AWS Management Console para cambiar los valores de parámetros de clúster de base de datos, siempre se utiliza `immediate` para el `ApplyMethod` para los parámetros dinámicos. Para aplazar el cambio de parámetros hasta después de reiniciar un clúster de base de datos asociado, utilice la AWS CLI o la API de RDS. Establezca `ApplyMethod` en `pending-reboot` para el cambio de parámetro.

Para obtener más información acerca del uso de la AWS CLI para cambiar el valor de un parámetro, consulte modify-db-clúster-parameter-group. Para obtener más información acerca del uso de la API de RDS para cambiar un valor de parámetro, consulte ModifyDBclústerParameterGroup.

Parámetros del conjunto de caracteres

Antes de crear una instancia de base de datos o un clúster de base de datos Multi-AZ, establezca en su grupo de parámetros cualquier parámetro relacionado con el conjunto de caracteres o la intercalación de su base de datos. Hágalo también antes de crear una base de datos en él. De este modo, garantiza que la base de datos predeterminada y las bases de datos nuevas utilicen el conjunto de caracteres y los valores de intercalación que especifique. Si cambia los parámetros de la intercalación o del conjunto de caracteres, los cambios de parámetros no se aplicarán a las bases de datos existentes.

Para algunos motores de base de datos, puede cambiar los valores de la intercalación o del conjunto de caracteres para una base de datos existente mediante el comando `ALTER DATABASE`; por ejemplo:

```
ALTER DATABASE database_name CHARACTER SET character_set_name COLLATE collation;
```

Para obtener más información acerca de cómo cambiar el conjunto de caracteres o los valores de intercalación de una base de datos, consulte la documentación del motor de la base de datos.

Parámetros y valores de parámetros admitidos

Para determinar los parámetros compatibles con su motor de base de datos, consulte los parámetros en el grupo de parámetros de base de datos y el grupo de parámetros de clúster de base de datos utilizado por el clúster de base de datos o la instancia de base de datos. Para obtener más información, consulte Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS y Visualización de los valores de parámetros de un grupo de parámetros de clúster de base de datos .

En muchos casos, puede especificar valores de parámetros de enteros y booleanos mediante expresiones, fórmulas y funciones. Las funciones pueden incluir una expresión logarítmica matemática. Sin embargo, no todos los parámetros admiten expresiones, fórmulas y funciones para valores de parámetros. Para obtener más información, consulte Especificación de parámetros de base de datos.

Si los parámetros de un grupo de parámetros se configuran de forma incorrecta, pueden producirse efectos adversos no deseados, como la degradación del rendimiento y la inestabilidad del sistema. Realice siempre cualquier modificación de los parámetros de base de datos con cuidado y haga una copia de seguridad de los datos antes de modificar un grupo de parámetros. Pruebe los cambios de

configuración del grupo de parámetros en una instancia de base de datos o en un clúster de base de datos de prueba antes de aplicar dichos cambios a una instancia de base de datos de producción o a un clúster de base de datos.

Grupos de parámetros de base de datos para instancias de Amazon RDS

Las instancias de base de datos utilizan grupos de parámetros de base de datos. En las secciones siguientes se describe cómo configurar y administrar los grupos de parámetros de instancia de base de datos.

Temas

- Creación de un grupo de parámetros de base de datos en Amazon RDS
- Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS
- Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS
- Restablecimiento de los parámetros de un grupo de parámetros de base de datos a sus valores predeterminados en Amazon RDS
- Copia de un grupo de parámetros de base de datos en Amazon RDS
- Enumeración de grupos de parámetros de base de datos en Amazon RDS
- Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS
- Eliminación de un grupo de parámetros de base de datos en Amazon RDS

Creación de un grupo de parámetros de base de datos en Amazon RDS

Puede crear un nuevo grupo de parámetros de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS.

Se aplican las siguientes limitaciones al nombre del grupo de parámetros de base de datos:

- Debe tener de 1 a 255 letras, números o guiones.

  Los nombres de los grupos de parámetros predeterminados pueden incluir un punto, como `default.mysql8.0`. Sin embargo, los nombres de grupos de parámetros personalizados no pueden incluir un punto.
- El primer carácter debe ser una letra.

- El nombre no puede incluir dos guiones consecutivos ni finalizar con guion.

Consola

Para crear un grupo de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija Create parameter group.
4. Para Nombre del grupo de parámetros, escriba el nombre del nuevo grupo de parámetros de base de datos.
5. En Descripción, escriba una descripción del nuevo grupo de parámetros de base de datos.
6. En Tipo de motor, elija el motor de base de datos.
7. En Familia del grupo de parámetros, seleccione una familia de grupo de parámetros de base de datos.
8. En Tipo, elija Grupo de parámetros de base de datos.
9. Seleccione Create (Crear).

AWS CLI

Para crear un grupo de parámetros de base de datos, utilice el comando `create-db-parameter-group` de la AWS CLI. En el siguiente ejemplo se crea un grupo de parámetros de base de datos denominado mydbparametergroup para MySQL versión 8.0 con la descripción “My new parameter group”.

Incluya los siguientes parámetros obligatorios:

- `--db-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

Para mostrar todas las familias de grupos de parámetros disponibles, use el siguiente comando:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

> **Note**
>
> La salida contiene duplicados.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --db-parameter-group-family MySQL8.0 \
    --description "My new parameter group"
```

En:Windows

```
aws rds create-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --db-parameter-group-family MySQL8.0 ^
    --description "My new parameter group"
```

El resultado de este comando debería ser similar al siguiente:

```
DBPARAMETERGROUP  mydbparametergroup  mysql8.0  My new parameter group
```

API de RDS

Para crear un grupo de parámetros de base de datos, utilice la operación `CreateDBParameterGroup` de la API de RDS.

Incluya los siguientes parámetros obligatorios:

- `DBParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS

Puede crear sus propios grupos de parámetros de base de datos con configuraciones personalizadas. Puede asociar un grupo de parámetros de base de datos con una instancia de base de datos mediante AWS Management Console, la AWS CLI, o la API de RDS. Puede hacerlo al crear o modificar una instancia de base de datos.

Para obtener información sobre la creación de un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS. Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS. Para obtener más información sobre la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Note**
>
> Al asociar un nuevo grupo de parámetros de base de datos con una instancia de base de datos, los parámetros estáticos y dinámicos modificados se aplican solo después de reiniciar la instancia de base de datos. Sin embargo, si modifica los parámetros dinámicos en el grupo de parámetros de base de datos después de asociarlos a la instancia de base de datos, dichos cambios se aplican inmediatamente sin reiniciar.

Consola

Para asociar un grupo de parámetros de base de datos con una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify. Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. Cambie la configuración del grupo de parámetros de base de datos.
5. Elija Continue y consulte el resumen de las modificaciones.
6. (Opcional) Seleccione Apply immediately (Aplicar inmediatamente) para aplicar los cambios inmediatamente. Si se selecciona esta opción, puede producirse una interrupción en algunos

casos. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

7. En la página de confirmación, revise los cambios. Si son correctos, elija Modify DB instance (Modificar instancia de base de datos) para guardar los cambios.

   O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para asociar un grupo de parámetros de base de datos con una instancia de base de datos, utilice el comando `modify-db-instance` de AWS CLI con las siguientes opciones:

- `--db-instance-identifier`
- `--db-parameter-group-name`

En el ejemplo siguiente se asocia el `mydbpg` grupo de parámetros de base de datos con la `database-1` instancia de base de datos. Los cambios se aplican inmediatamente mediante `--apply-immediately`. Utilícelo `--no-apply-immediately` para aplicar los cambios durante la siguiente ventana de mantenimiento. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier database-1 \
    --db-parameter-group-name mydbpg \
    --apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier database-1 ^
    --db-parameter-group-name mydbpg ^
    --apply-immediately
```

API de RDS

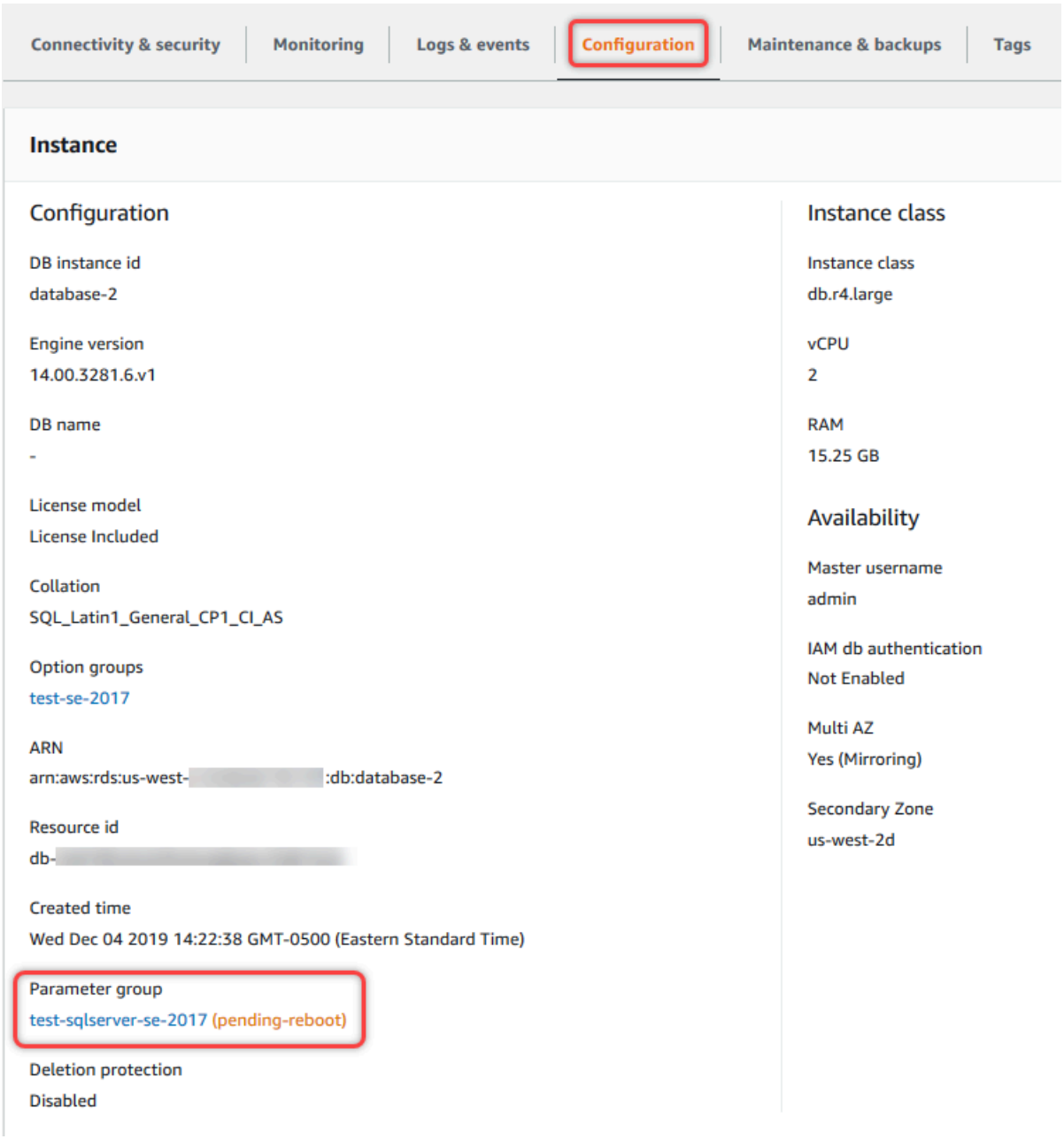
Para asociar un grupo de parámetros de base de datos con una instancia de base de datos, utilice la operación `ModifyDBInstance` de la API de RDS con los siguientes parámetros:

- `DBInstanceName`
- `DBParameterGroupName`

Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS

Es posible modificar los valores de los parámetros de un grupo de parámetros de base de datos creado por el cliente; no es posible modificar los valores de los parámetros de un grupo de parámetros de base de datos predeterminado. Los cambios realizados en los parámetros de un grupo de parámetros de base de datos creado por el cliente se aplican a todas las instancias de bases de datos asociadas al grupo de parámetros de base de datos.

Los cambios en algunos parámetros se aplican a la instancia de base de datos inmediatamente sin necesidad de reiniciar. Los cambios en otros parámetros se aplican únicamente después de reiniciar la instancia de base de datos. La consola de RDS muestra el estado del grupo de parámetros de base de datos asociado a una instancia de base de datos en la pestaña Configuration (Configuración). Por ejemplo, podría darse por ejemplo que la instancia de base de datos no está utilizando los cambios más recientes del grupo de parámetros de base de datos asociado. De ser así, la consola de RDS muestra el grupo de parámetros de base de datos con el estado pending-reboot. Para aplicar los cambios de parámetros más recientes en esa instancia de base de datos, reinicie manualmente la instancia de base de datos. Recomendamos que siempre reinicie la instancia de base de datos después de modificar los parámetros. Si no reinicia la instancia de base de datos, la operación de conmutación por error podría tardar más de lo normal.



Consola

Modificación de parámetros en un grupo de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, elija el nombre del grupo de parámetros que desea modificar.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar).

5. Cambie los valores de los parámetros que desee modificar. Puede desplazarse por los parámetros utilizando las teclas de flecha de la parte superior derecha del cuadro de diálogo.

   No puede cambiar los valores de un grupo de parámetros predeterminado.

6. Elija Save changes.

AWS CLI

Para modificar un grupo de parámetros de base de datos, utilice el AWS CLI `modify-db-parameter-group` comando con las siguientes opciones requeridas:

- `--db-parameter-group-name`
- `--parameters`

En el siguiente ejemplo se modifican los valores de `max_connections` y `max_allowed_packet` en el grupo de parámetros de base de datos denominado mydbparametergroup.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --parameters
 "ParameterName=max_connections,ParameterValue=250,ApplyMethod=immediate" \

 "ParameterName=max_allowed_packet,ParameterValue=1024,ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --parameters
 "ParameterName=max_connections,ParameterValue=250,ApplyMethod=immediate" ^

 "ParameterName=max_allowed_packet,ParameterValue=1024,ApplyMethod=immediate"
```

El comando produce un resultado similar al siguiente:

```
DBPARAMETERGROUP  mydbparametergroup
```

API de RDS

Para modificar un grupo de parámetros de base de datos, utilice la operación `ModifyDBParameterGroup` de la API de RDS con los siguientes parámetros requeridos:

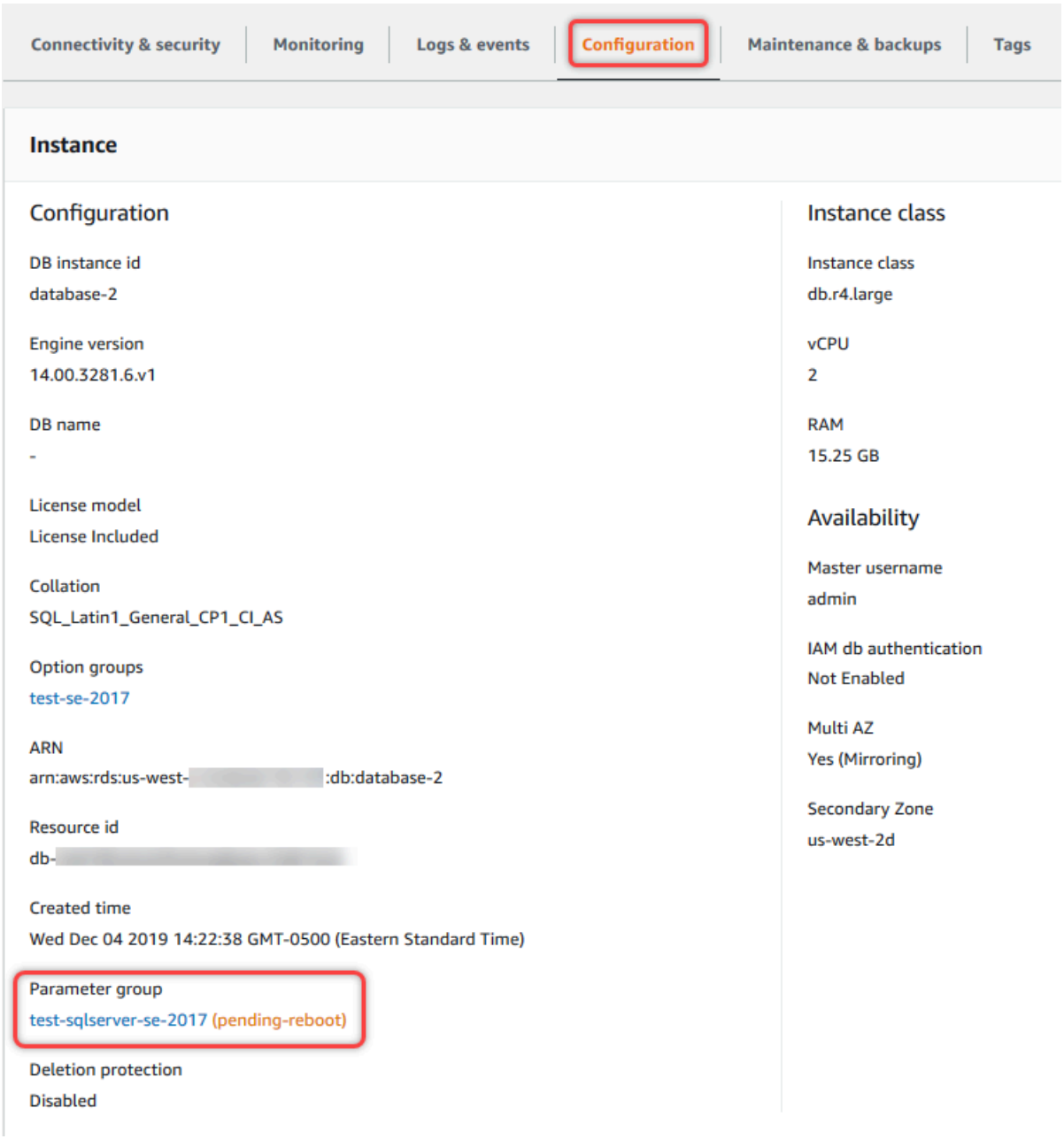
- `DBParameterGroupName`
- `Parameters`

Restablecimiento de los parámetros de un grupo de parámetros de base de datos a sus valores predeterminados en Amazon RDS

Puede restablecer los valores de los parámetros de un grupo de parámetros de base de datos creado por el cliente a sus valores predeterminados. Los cambios realizados en los parámetros de un grupo de parámetros de base de datos creado por el cliente se aplican a todas las instancias de bases de datos asociadas al grupo de parámetros de base de datos.

Cuando utiliza la consola, puede restablecer parámetros específicos a sus valores predeterminados. Sin embargo, no puede restablecer fácilmente todos los parámetros del grupo de parámetros de base de datos a la vez. Cuando utiliza la AWS CLI o la API de RDS, puede restablecer parámetros específicos a sus valores predeterminados. También puede restablecer fácilmente todos los parámetros del grupo de parámetros de base de datos a la vez.

Los cambios en algunos parámetros se aplican a la instancia de base de datos inmediatamente sin necesidad de reiniciar. Los cambios en otros parámetros se aplican únicamente después de reiniciar la instancia de base de datos. La consola de RDS muestra el estado del grupo de parámetros de base de datos asociado a una instancia de base de datos en la pestaña Configuration (Configuración). Por ejemplo, podría darse por ejemplo que la instancia de base de datos no está utilizando los cambios más recientes del grupo de parámetros de base de datos asociado. De ser así, la consola de RDS muestra el grupo de parámetros de base de datos con el estado pending-reboot. Para aplicar los cambios de parámetros más recientes en esa instancia de base de datos, reinicie manualmente la instancia de base de datos.



> **Note**
>
> En un grupo de parámetros de base de datos predeterminado, los parámetros siempre se establecen en sus valores predeterminados.

Consola

Para restablecer los parámetros de un grupo de parámetros de base de datos a sus valores predeterminados

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, elija el grupo de parámetros.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar).
5. Elija los parámetros que desea restablecer a sus valores predeterminados. Puede desplazarse por los parámetros utilizando las teclas de flecha de la parte superior derecha del cuadro de diálogo.

   No puede restablecer los valores de un grupo de parámetros predeterminado.
6. Elija Restablecer y, a continuación, confirme seleccionando Restablecer parámetros.

AWS CLI

Para restablecer algunos o todos los parámetros de un grupo de parámetros de base de datos, utilice el comando AWS CLI `reset-db-parameter-group` con la siguiente opción requerida: `--db-parameter-group-name`.

Para restablecer todos los parámetros del grupo de parámetros de base de datos, especifique la opción `--reset-all-parameters`. Para restablecer parámetros específicos, especifique la opción `--parameters`.

En el ejemplo siguiente se restablecen todos los parámetros del grupo de parámetros DB denominado mydbparametergroup a sus valores predeterminados.

Example

Para Linux, macOS o:Unix

```
aws rds reset-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --reset-all-parameters
```

En:Windows

```
aws rds reset-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --reset-all-parameters
```

En el ejemplo siguiente se restablecen las opciones `max_connections` y `max_allowed_packet` a sus valores predeterminados en el grupo de parámetros de base de datos denominado mydbparametergroup.

Example

Para Linux, macOS o:Unix

```
aws rds reset-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --parameters "ParameterName=max_connections,ApplyMethod=immediate" \
                 "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

En:Windows

```
aws rds reset-db-parameter-group ^
    --db-parameter-group-name mydbparametergroup ^
    --parameters "ParameterName=max_connections,ApplyMethod=immediate" ^
                 "ParameterName=max_allowed_packet,ApplyMethod=immediate"
```

El comando produce un resultado similar al siguiente:

```
DBParameterGroupName  mydbparametergroup
```

API de RDS

Para restablecer los parámetros de un grupo de parámetros de base de datos a sus valores predeterminados, utilice el comando `ResetDBParameterGroup` API de RDS con el siguiente parámetro requerido: `DBParameterGroupName`.

Para restablecer todos los parámetros del grupo de parámetros de base de datos, defina el parámetro `ResetAllParameters` en `true`. Para restablecer parámetros específicos, especifique el parámetro `Parameters`.

Copia de un grupo de parámetros de base de datos en Amazon RDS

Puede copiar los grupos de parámetros de base de datos personalizados que cree. Copiar un grupo de parámetros puede ser una solución práctica. Por ejemplo, podría darse cuando haya creado un grupo de parámetros de base de datos y desee incluir la mayoría de los parámetros y valores personalizados en un nuevo grupo de parámetros de base de datos. Puede copiar un grupo de parámetros de base de datos utilizando la AWS Management Console. También puede utilizar el comando AWS CLI copy-db-parameter-group o la operación CopyDBParameterGroup de la API de RDS.

Después de copiar un grupo de parámetros de base de datos, espere al menos 5 minutos antes de crear la primera instancia de base de datos que utilice ese grupo de parámetros de base de datos como grupo de parámetros predeterminado. Esto permite a Amazon RDS finalizar por completo la acción de copia antes de que se utilice el grupo de parámetros. Esto es especialmente importante para los parámetros que son críticos al crear la base de datos predeterminada de una instancia de base de datos. Un ejemplo es el conjunto de caracteres para la base de datos predeterminada definida por el parámetro `character_set_database`. Utilice la opción Parameter Groups (Grupos de parámetros) de la consola de Amazon RDS o el comando describe-db-parameters para comprobar que se ha creado el grupo de parámetros de base de datos.

> **Note**
>
> No es posible copiar un grupo de parámetros predeterminado. Sin embargo, puede crear un grupo de parámetros que se base en uno predeterminado.
> No puede copiar un grupo de parámetros de base de datos en una Cuenta de AWS o Región de AWS diferente.

Consola

Para copiar un grupo de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, seleccione el grupo de parámetros personalizado que desea copiar.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Copy (Copiar).

5. En New DB parameter group identifier (Nuevo identificador de grupo de parámetros de base de datos), escriba el nombre del nuevo grupo de parámetros.
6. En Description (Descripción), escriba una descripción para el nuevo grupo de parámetros.
7. Elija Copy.

AWS CLI

Para copiar un grupo de parámetros de base de datos, utilice el comando AWS CLI de `copy-db-parameter-group` con las siguientes opciones requeridas:

- `--source-db-parameter-group-identifier`
- `--target-db-parameter-group-identifier`
- `--target-db-parameter-group-description`

En el siguiente ejemplo se crea un nuevo grupo de parámetros de base de datos denominado `mygroup2` que es una copia del grupo de parámetros de base de datos `mygroup1`.

Example

Para Linux, macOS o:Unix

```
aws rds copy-db-parameter-group \
    --source-db-parameter-group-identifier mygroup1 \
    --target-db-parameter-group-identifier mygroup2 \
    --target-db-parameter-group-description "DB parameter group 2"
```

En:Windows

```
aws rds copy-db-parameter-group ^
    --source-db-parameter-group-identifier mygroup1 ^
    --target-db-parameter-group-identifier mygroup2 ^
    --target-db-parameter-group-description "DB parameter group 2"
```

API de RDS

Para copiar un grupo de parámetros de base de datos, utilice la operación `CopyDBParameterGroup` de la API de RDS con los siguientes parámetros obligatorios:

- `SourceDBParameterGroupIdentifier`
- `TargetDBParameterGroupIdentifier`
- `TargetDBParameterGroupDescription`

Enumeración de grupos de parámetros de base de datos en Amazon RDS

Es posible obtener un listado de los grupos de parámetros de base de datos que se han creado para una cuenta de AWS.

> **Note**
>
> Los grupos de parámetros predeterminados se crean automáticamente a partir de una plantilla de parámetros predeterminados cuando se crea una instancia de base de datos para un motor y una versión de base de datos específicos. Estos grupos de parámetros predeterminados contienen los valores preferidos para los parámetros y no se pueden modificar. Los valores de los parámetros se pueden modificar cuando se crea un grupo de parámetros personalizado.

Consola

Para obtener una lista de todos los grupos de parámetros de base de datos de una cuenta de AWS.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros de base de datos aparecen en una lista.

AWS CLI

Para obtener la lista de todos los grupos de parámetros de base de datos para una cuenta de AWS, utilice el comando AWS CLI `describe-db-parameter-groups`.

Example

En el siguiente ejemplo se obtiene la lista de todos los grupos de parámetros de base de datos disponibles en una cuenta de AWS.

```
aws rds describe-db-parameter-groups
```

El comando devuelve una respuesta similar a la siguiente:

```
DBPARAMETERGROUP  default.mysql8.0     mysql8.0  Default parameter group for MySQL8.0
DBPARAMETERGROUP  mydbparametergroup   mysql8.0  My new parameter group
```

En el siguiente ejemplo se describe el grupo de parámetros mydbparamgroup1.

Para Linux, macOS o:Unix

```
aws rds describe-db-parameter-groups \
    --db-parameter-group-name mydbparamgroup1
```

En:Windows

```
aws rds describe-db-parameter-groups ^
    --db-parameter-group-name mydbparamgroup1
```

El comando devuelve una respuesta similar a la siguiente:

```
DBPARAMETERGROUP  mydbparametergroup1  mysql8.0  My new parameter group
```

API de RDS

Para obtener la lista de todos los grupos de parámetros de base de datos de una cuenta de AWS, utilice la operación `DescribeDBParameterGroups` de la API de RDS.

Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS

Es posible obtener una lista de todos los parámetros de un grupo de parámetros de base de datos y sus valores.

Consola

Para ver los valores de los parámetros de un grupo de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros de base de datos aparecen en una lista.
3. Seleccione el nombre del grupo de parámetros para ver su lista de parámetros.

AWS CLI

Para ver los valores de los parámetros de un grupo de parámetros de base de datos, utilice el comando `describe-db-parameters` de la AWS CLI con el siguiente parámetro obligatorio.

- `--db-parameter-group-name`

Example

En el siguiente ejemplo se obtiene la lista de los parámetros y los valores de los parámetros de un grupo de parámetros de base de datos denominado mydbparametergroup.

```
aws rds describe-db-parameters --db-parameter-group-name mydbparametergroup
```

El comando devuelve una respuesta similar a la siguiente:

```
DBPARAMETER  Parameter Name           Parameter Value  Source           Data Type
 Apply Type  Is Modifiable
DBPARAMETER  allow-suspicious-udfs                    engine-default   boolean
 static      false
DBPARAMETER  auto_increment_increment                 engine-default   integer
 dynamic     true
DBPARAMETER  auto_increment_offset                    engine-default   integer
 dynamic     true
DBPARAMETER  binlog_cache_size        32768           system           integer
 dynamic     true
DBPARAMETER  socket                   /tmp/mysql.sock  system           string
 static      false
```

API de RDS

Para ver los valores de los parámetros de un grupo de parámetros de base de datos, utilice el comando `DescribeDBParameters` de la API de RDS con el siguiente parámetro obligatorio.

- `DBParameterGroupName`

Eliminación de un grupo de parámetros de base de datos en Amazon RDS

Puede eliminar un grupo de parámetros de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS. Un grupo de parámetros solo se puede eliminar si no está asociado a una instancia de base de datos.

Consola

Eliminación de un grupo de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros de base de datos aparecen en una lista.
3. Elija el nombre del grupo de parámetros que se va a eliminar.
4. Elija Acciones y, a continuación, elija Eliminar.
5. Revise los nombres de los grupos de parámetros y seleccione Eliminar.

AWS CLI

Para eliminar un grupo de parámetros de base de datos, utilice el comando `delete-db-parameter-group` de la AWS CLI con los siguientes parámetros obligatorios:

- `--db-parameter-group-name`

Example

En el siguiente ejemplo, se elimina un grupo de parámetros de base de datos con el nombre mydbparametergroup.

```
aws rds delete-db-parameter-group --db-parameter-group-name mydbparametergroup
```

API de RDS

Para eliminar un grupo de parámetros de base de datos, utilice la API `DeleteDBParameterGroup` de RDS con los siguientes parámetros obligatorios.

- `DBParameterGroupName`

Trabajo con grupos de parámetros de clúster de base de datos para clústeres de base de datos Multi-AZ

Los clústeres de base de datos Multi-AZ utilizan grupos de parámetros de clúster de base de datos. En las secciones siguientes se describe la configuración y administración de los grupos de parámetros de clúster de base de datos.

Temas

- Creación de un grupo de parámetros de clúster de base de datos
- Modificación de los parámetros en un grupo de parámetros de clúster de base de datos
- Restablecimiento de los parámetros de un grupo de parámetros de clúster de base de datos
- Copia de un grupo de parámetros de clúster de base de datos
- Enumeración de grupos de parámetros de clúster de base de datos
- Visualización de los valores de parámetros de un grupo de parámetros de clúster de base de datos
- Eliminación de un grupo de parámetros de clúster de base de datos

Creación de un grupo de parámetros de clúster de base de datos

Puede crear un nuevo grupo de parámetros de clúster de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS.

Después de crear un grupo de parámetros de clústeres de base de datos, espere al menos 5 minutos antes de crear un clúster de base de datos que utilice ese grupo de parámetros de clúster de base de datos. Esto permite a Amazon RDS crear por completo el grupo de parámetros antes de que lo utilice el nuevo clúster de base de datos. Puede utilizar la página Parameter Groups (Grupos de parámetros) de la consola de Amazon RDS o el comando describe-db-clúster-parameters para comprobar que se ha creado el grupo de parámetros de clúster de base de datos.

Se aplican las siguientes limitaciones al nombre del grupo de parámetros de clústeres de base de datos:

- Debe tener de 1 a 255 letras, números o guiones.

  Los nombres de los grupos de parámetros predeterminados pueden incluir un punto, como `default.mysql5.7`. Sin embargo, los nombres de grupos de parámetros personalizados no pueden incluir un punto.

- El primer carácter debe ser una letra.
- El nombre no puede incluir dos guiones consecutivos ni finalizar con guion.

Consola

Para crear un grupo de parámetros de clúster de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija Create parameter group.
4. En Nombre del grupo de parámetros, escriba el nombre del nuevo grupo de parámetros de clúster de bases de datos.
5. En Descripción, escriba una descripción del nuevo grupo de parámetros de clúster de bases de datos.
6. En Tipo de motor, elija el motor de base de datos.
7. En Familia del grupo de parámetros, seleccione una familia de grupo de parámetros de base de datos.
8. Seleccione Create (Crear).

AWS CLI

Para crear un grupo de parámetros de clúster de base de datos, use el comando AWS CLI de `create-db-cluster-parameter-group`.

En el siguiente ejemplo, se crea un grupo de parámetros de clúster de base de datos denominado mydbclústerparametergroup para la versión 8.0 de RDS for MySQL con la descripción “My new clúster parameter group” (Mi grupo de parámetros de clúster nuevo).

Incluya los siguientes parámetros obligatorios:

- `--db-cluster-parameter-group-name`
- `--db-parameter-group-family`
- `--description`

Para mostrar todas las familias de grupos de parámetros disponibles, use el siguiente comando:

```
aws rds describe-db-engine-versions --query "DBEngineVersions[].DBParameterGroupFamily"
```

> **Note**
>
> La salida contiene duplicados.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --db-parameter-group-family mysql8.0 \
    --description "My new cluster parameter group"
```

Para Windows:

```
aws rds create-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --db-parameter-group-family mysql8.0 ^
    --description "My new cluster parameter group"
```

El resultado de este comando debería ser similar al siguiente:

```
{
    "DBClusterParameterGroup": {
        "DBClusterParameterGroupName": "mydbclusterparametergroup",
        "DBParameterGroupFamily": "mysql8.0",
        "Description": "My new cluster parameter group",
        "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup2"
    }
}
```

API de RDS

Para crear un grupo de parámetros de clúster de base de datos, use la acción `CreateDBClusterParameterGroup` de la API de RDS.

Incluya los siguientes parámetros obligatorios:

- `DBClusterParameterGroupName`
- `DBParameterGroupFamily`
- `Description`

Modificación de los parámetros en un grupo de parámetros de clúster de base de datos

Es posible modificar parámetros de un grupo de parámetros de clúster de base de datos creado por el cliente. No puede cambiar los valores de parámetros de un grupo de parámetros de clúster de base de datos predeterminado. Los cambios realizados en los parámetros de un grupo de parámetros de clúster de base de datos creado por el cliente se aplican a todas las instancias de clústeres de bases de datos asociados al grupo de parámetros de clúster de base de datos.

Consola

Para modificar un grupo de parámetros de clúster de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, seleccione el grupo de parámetros que desea modificar.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar).
5. Cambie los valores de los parámetros que desea modificar. Puede desplazarse por los parámetros utilizando las teclas de flecha de la parte superior derecha del cuadro de diálogo.

   No puede cambiar los valores de un grupo de parámetros predeterminado.
6. Elija Save changes.
7. Reinicie la clúster para aplicar los cambios.

   Si no reinicia el clúster, una operación de conmutación por error podría tardar más de lo normal.

AWS CLI

Para modificar un grupo de parámetros de clúster de base de datos, utilice el comando `modify-db-cluster-parameter-group` de AWS CLI con los siguientes parámetros obligatorios:

- `--db-cluster-parameter-group-name`
- `--parameters`

En el siguiente ejemplo se modifican los valores de `server_audit_logging` y `server_audit_logs_upload` en el grupo de parámetros de clúster de base de datos denominado mydbclústerparametergroup.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --parameters
 "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" \

 "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --parameters
 "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" ^

 "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

El comando produce un resultado similar al siguiente:

```
DBCLUSTERPARAMETERGROUP  mydbclusterparametergroup
```

API de RDS

Para modificar un grupo de parámetros de clúster de base de datos, utilice el comando `ModifyDBClusterParameterGroup` de la API de RDS con los siguientes parámetros obligatorios:

- `DBClusterParameterGroupName`
- `Parameters`

Restablecimiento de los parámetros de un grupo de parámetros de clúster de base de datos

Puede restablecer los parámetros a sus valores predeterminados en un grupo de parámetros de clúster de base de datos creado por el cliente. Los cambios realizados en los parámetros de un grupo de parámetros de clúster de base de datos creado por el cliente se aplican a todas las instancias de clústeres de bases de datos asociados al grupo de parámetros de clúster de base de datos.

> **Note**
>
> En un grupo de parámetros de clúster de base de datos predeterminado, los parámetros siempre se establecen en sus valores predeterminados.

Consola

Para restablecer los parámetros de un grupo de parámetros de clúster de base de datos a sus valores predeterminados

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, elija el grupo de parámetros.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar).
5. Elija los parámetros que desea restablecer a sus valores predeterminados. Puede desplazarse por los parámetros utilizando las teclas de flecha de la parte superior derecha del cuadro de diálogo.

   No puede restablecer los valores de un grupo de parámetros predeterminado.
6. Elija Restablecer y, a continuación, confirme seleccionando Restablecer parámetros.
7. Reinicie la clúster de base de datos.

AWS CLI

Para restablecer los parámetros de un grupo de parámetros de clúster de base de datos a sus valores predeterminados, utilice el comando `reset-db-cluster-parameter-group` de AWS CLI con la siguiente opción requerida: `--db-cluster-parameter-group-name`.

Para restablecer todos los parámetros del grupo de parámetros de clúster de base de datos, especifique la opción `--reset-all-parameters`. Para restablecer parámetros específicos, especifique la opción `--parameters`.

En el ejemplo siguiente se restablecen todos los parámetros del grupo de parámetros DB denominado mydbparametergroup a sus valores predeterminados.

Example

Para Linux, macOS o Unix:

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbparametergroup \
    --reset-all-parameters
```

Para Windows:

```
aws rds reset-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbparametergroup ^
    --reset-all-parameters
```

En el siguiente ejemplo se modifican los valores de `server_audit_logging` y `server_audit_logs_upload` en el grupo de parámetros de clúster de base de datos denominado mydbclústerparametergroup.

Example

Para Linux, macOS o Unix:

```
aws rds reset-db-cluster-parameter-group \
    --db-cluster-parameter-group-name mydbclusterparametergroup \
    --parameters "ParameterName=server_audit_logging,ApplyMethod=immediate" \
                 "ParameterName=server_audit_logs_upload,ApplyMethod=immediate"
```

Para Windows:

```
aws rds reset-db-cluster-parameter-group ^
    --db-cluster-parameter-group-name mydbclusterparametergroup ^
    --parameters
 "ParameterName=server_audit_logging,ParameterValue=1,ApplyMethod=immediate" ^

 "ParameterName=server_audit_logs_upload,ParameterValue=1,ApplyMethod=immediate"
```

El comando produce un resultado similar al siguiente:

```
DBClusterParameterGroupName  mydbclusterparametergroup
```

API de RDS

Para restablecer los parámetros de un grupo de parámetros de clúster de base de datos a sus valores predeterminados, utilice el comando API de RDS `ResetDBClusterParameterGroup` con el siguiente parámetro requerido: `DBClusterParameterGroupName`.

Para restablecer todos los parámetros del grupo de parámetros de clúster de base de datos, defina el parámetro `ResetAllParameters` en `true`. Para restablecer parámetros específicos, especifique el parámetro `Parameters`.

Copia de un grupo de parámetros de clúster de base de datos

Puede copiar los grupos de parámetros de clúster de base de datos personalizados que cree. Copiar un grupo de parámetros es una solución conveniente cuando ya se ha creado un grupo de parámetros de clúster de base de datos y se desea incluir la mayoría de los parámetros y valores personalizados de ese grupo en un nuevo grupo de parámetros de clúster de base de datos. Puede copiar un grupo de parámetros de clúster de base de datos mediante el comando copy-db-clúster-parameter-group de la AWS CLI o la operación CopyDBclústerParameterGroup de la API de RDS.

Después de copiar un grupo de parámetros de clústeres de base de datos, espere al menos 5 minutos antes de crear un clúster de base de datos que utilice ese grupo de parámetros de clúster de base de datos. Esto permite a Amazon RDS copiar por completo el grupo de parámetros antes de que lo utilice el nuevo clúster de base de datos. Puede utilizar la página Parameter Groups (Grupos de parámetros) de la consola de Amazon RDS o el comando describe-db-clúster-parameters para comprobar que se ha creado el grupo de parámetros de clúster de base de datos.

> **Note**
>
> No es posible copiar un grupo de parámetros predeterminado. Sin embargo, puede crear un grupo de parámetros que se base en uno predeterminado.
> No puede copiar un grupo de parámetros de clúster de base de datos en una Cuenta de AWS o Región de AWS diferente.

Consola

Para copiar un grupo de parámetros de clúster de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, seleccione el grupo de parámetros personalizado que desea copiar.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Copy (Copiar).
5. En New DB parameter group identifier (Nuevo identificador de grupo de parámetros de base de datos), escriba el nombre del nuevo grupo de parámetros.
6. En Description (Descripción), escriba una descripción para el nuevo grupo de parámetros.
7. Elija Copy.

AWS CLI

Para copiar un grupo de parámetros de clúster de base de datos, utilice el comando `copy-db-cluster-parameter-group` de AWS CLI con los siguientes parámetros obligatorios:

- `--source-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-identifier`
- `--target-db-cluster-parameter-group-description`

En el siguiente ejemplo se crea un nuevo grupo de parámetros de clúster de base de datos denominado `mygroup2` que es una copia del grupo de parámetros de clúster de base de datos `mygroup1`.

Example

Para Linux, macOS o Unix:

```
aws rds copy-db-cluster-parameter-group \
    --source-db-cluster-parameter-group-identifier mygroup1 \
    --target-db-cluster-parameter-group-identifier mygroup2 \
    --target-db-cluster-parameter-group-description "DB parameter group 2"
```

Para Windows:

```
aws rds copy-db-cluster-parameter-group ^
    --source-db-cluster-parameter-group-identifier mygroup1 ^
    --target-db-cluster-parameter-group-identifier mygroup2 ^
    --target-db-cluster-parameter-group-description "DB parameter group 2"
```

API de RDS

Para copiar un grupo de parámetros de clúster de base de datos, utilice la operación `CopyDBClusterParameterGroup` de la API de RDS con los siguientes parámetros obligatorios:

- `SourceDBClusterParameterGroupIdentifier`
- `TargetDBClusterParameterGroupIdentifier`
- `TargetDBClusterParameterGroupDescription`

Enumeración de grupos de parámetros de clúster de base de datos

Es posible obtener un listado de los grupos de parámetros de clúster de base de datos que se han creado para una cuenta de AWS.

> **Note**
>
> Los grupos de parámetros predeterminados se crean automáticamente a partir de una plantilla de parámetros predeterminados cuando se crea un clúster de base de datos para un motor y una versión de base de datos específicos. Estos grupos de parámetros predeterminados contienen los valores preferidos para los parámetros y no se pueden modificar. Los valores de los parámetros se pueden modificar cuando se crea un grupo de parámetros personalizado.

Consola

Para obtener una lista de todos los grupos de parámetros de clúster de base de datos de una cuenta de AWS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros de clúster de base de datos aparecen en la lista con <guilabel>Grupo de parámetros de clúster de base de datos para Tipo.

AWS CLI

Para obtener la lista de todos los grupos de parámetros de clúster de base de datos para una cuenta de AWS, utilice el comando `describe-db-cluster-parameter-groups` de AWS CLI.

Example

En el siguiente ejemplo, se obtiene la lista de todos los grupos de parámetros de clúster de base de datos disponibles en una cuenta de AWS.

```
aws rds describe-db-cluster-parameter-groups
```

En el siguiente ejemplo se describe el grupo de parámetros mydbclústerparametergroup.

Para Linux, macOS o Unix:

```
aws rds describe-db-cluster-parameter-groups \
    --db-cluster-parameter-group-name mydbclusterparametergroup
```

Para Windows:

```
aws rds describe-db-cluster-parameter-groups ^
    --db-cluster-parameter-group-name mydbclusterparametergroup
```

El comando devuelve una respuesta similar a la siguiente:

```
{
    "DBClusterParameterGroups": [
```

```
        {
            "DBClusterParameterGroupName": "mydbclusterparametergroup2",
            "DBParameterGroupFamily": "mysql8.0",
            "Description": "My new cluster parameter group",
            "DBClusterParameterGroupArn": "arn:aws:rds:us-east-1:123456789012:cluster-
pg:mydbclusterparametergroup"
        }
    ]
}
```

API de RDS

Para obtener la lista de todos los grupos de parámetros de clúster de base de datos de una cuenta de AWS, utilice la acción `DescribeDBClusterParameterGroups` de la API de RDS.

Visualización de los valores de parámetros de un grupo de parámetros de clúster de base de datos

Es posible obtener una lista de todos los parámetros de un grupo de parámetros de clúster de base de datos y sus valores.

Consola

Para ver los valores de los parámetros de un grupo de parámetros de clúster de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros de clúster de base de datos aparecen en la lista con Grupo de parámetros de clúster de base de datos para Tipo.
3. Seleccione el nombre del grupo de parámetros de clúster de base de datos para ver su lista de parámetros.

AWS CLI

Para ver los valores de los parámetros de un grupo de parámetros de clúster de base de datos, utilice el comando `describe-db-cluster-parameters` de AWS CLI con el siguiente parámetro obligatorio.

- `--db-cluster-parameter-group-name`

Example

En el siguiente ejemplo se obtiene la lista de los parámetros y los valores de los parámetros de un grupo de parámetros de clúster de base de datos denominado mydbparametergroup, en formato JSON.

El comando devuelve una respuesta similar a la siguiente:

```
aws rds describe-db-cluster-parameters --db-cluster-parameter-group-
name mydbclusterparametergroup
```


```
{
    "Parameters": [
        {
            "ParameterName": "activate_all_roles_on_login",
            "ParameterValue": "0",
            "Description": "Automatically set all granted roles as active after the
 user has authenticated successfully.",
            "Source": "engine-default",
            "ApplyType": "dynamic",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": true,
            "ApplyMethod": "pending-reboot",
            "SupportedEngineModes": [
                "provisioned"
            ]
        },
        {
            "ParameterName": "allow-suspicious-udfs",
            "Description": "Controls whether user-defined functions that have only an
 xxx symbol for the main function can be loaded",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot",
            "SupportedEngineModes": [
                "provisioned"
            ]
        },
```

```
...
```

API de RDS

Para ver los valores de los parámetros de un grupo de parámetros de clúster de base de datos, utilice el comando `DescribeDBClusterParameters` de la API de RDS con el siguiente parámetro obligatorio.

- `DBClusterParameterGroupName`

En algunos casos, no se muestran los valores permitidos para un parámetro. Estos son siempre parámetros en los que el origen es el predeterminado del motor de base de datos.

Para ver los valores de estos parámetros, puede ejecutar las siguientes instrucciones SQL:

- MySQL:

```
-- Show the value of a particular parameter
mysql$ SHOW VARIABLES LIKE '%parameter_name%';

-- Show the values of all parameters
mysql$ SHOW VARIABLES;
```

- PostgreSQL:

```
-- Show the value of a particular parameter
postgresql=> SHOW parameter_name;

-- Show the values of all parameters
postgresql=> SHOW ALL;
```

Eliminación de un grupo de parámetros de clúster de base de datos

Puede eliminar un grupo de parámetros de clúster de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS. Un grupo de parámetros de clúster de base de datos solo se puede eliminar si no está asociado a un clúster de base de datos.

Consola

Para eliminar grupos de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros aparecen en una lista.
3. Elija el nombre del grupo de parámetros de clúster de base de datos que se va a eliminar.
4. Elija Acciones y, a continuación, elija Eliminar.
5. Revise los nombres de los grupos de parámetros y seleccione Eliminar.

AWS CLI

Para eliminar un grupo de parámetros de clúster de base de datos, utilice el comando `delete-db-cluster-parameter-group` de la AWS CLI con los siguientes parámetros obligatorios:

- `--db-parameter-group-name`

Example

En el siguiente ejemplo, se elimina un grupo de parámetros de clúster de base de datos con el nombre mydbparametergroup.

```
aws rds delete-db-cluster-parameter-group --db-parameter-group-name mydbparametergroup
```

API de RDS

Para eliminar un grupo de parámetros de clúster de base de datos, utilice el comando `DeleteDBClusterParameterGroup` de la API de RDS con los siguientes parámetros obligatorios.

- `DBParameterGroupName`

Comparación de grupos de parámetros de la base de datos

Puede usar la AWS Management Console para ver las diferencias entre dos grupos de parámetros de base de datos.

Los grupos de parámetros especificados deben ser grupos de parámetros de base de datos o ambos deben ser grupos de parámetros de clústeres de base de datos. Esto es cierto incluso si el motor de base de datos y la versión son iguales. Por ejemplo, no puede comparar un grupo de parámetros de base de datos de `aurora-mysql8.0` (Aurora MySQL versión 3) con un grupo de parámetros de clústeres de base de datos de `aurora-mysql8.0`.

Puede comparar los grupos de parámetros de base de datos de Aurora MySQL y RDS para MySQL, incluso para versiones diferentes, pero no puede comparar los grupos de parámetros de base de datos de Aurora PostgreSQL y RDS para PostgreSQL.

Para comparar dos grupos de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. En la lista, seleccione los dos grupos de parámetros que desea comparar.

   > **Note**
   >
   > Para comparar un grupo de parámetros predeterminado con un grupo de parámetros personalizado, primero elija el grupo de parámetros predeterminado en la pestaña Predeterminado y, a continuación, elija el grupo de parámetros personalizado en la pestaña Personalizado.

4. En Acciones, elija Comparar.

Especificación de parámetros de base de datos

Los tipos de parámetros de base de datos incluyen lo siguiente:

- Entero
- Booleano
- Cadena
- Largo
- Doble
- Timestamp

- Objeto de otros tipos de datos definidos
- Matriz de valores de tipo entero, booleano, en cadena, largos, dobles, temporales o de objeto

También puede especificar parámetros de enteros y booleanos mediante expresiones, fórmulas y funciones.

Para el motor de Oracle, puede utilizar la variable de la fórmula `DBInstanceClassHugePagesDefault` para especificar un parámetro de base de datos booleano. Consulte Variables de las fórmulas de parámetros de base de datos.

Para el motor PostgreSQL, puede utilizar una expresión para especificar un parámetro de base de datos booleano. Consulte Expresiones de parámetros de base de datos booleanos.

Contenido

- Fórmulas de parámetros de base de datos
  - Variables de las fórmulas de parámetros de base de datos
  - Operadores de las fórmulas de parámetros de base de datos
- Funciones de parámetros de base de datos
- Expresiones de parámetros de base de datos booleanos
- Expresiones de registro de parámetros de base de datos
- Ejemplos de valores de los parámetros de base de datos

Fórmulas de parámetros de base de datos

Una fórmula de parámetros de base de datos es una expresión que da como resultado un valor entero o un valor booleano. Se encierra la expresión entre llaves: {}. Puede especificar fórmulas para el valor de un parámetro de base de datos o como argumento de una función de parámetro de base de datos.

Sintaxis

```
{FormulaVariable}
{FormulaVariable*Integer}
{FormulaVariable*Integer/Integer}
{FormulaVariable/Integer}
```

Variables de las fórmulas de parámetros de base de datos

Cada variable de la fórmula devuelve un entero o un valor booleano. Los nombres de las variables distinguen entre mayúsculas y minúsculas.

AllocatedStorage

Devuelve un entero que representa el tamaño, en bytes, del volumen de datos.

DBInstanceClassHugePagesDefault

Devuelve un valor booleano. Actualmente solo se admite para los motores de Oracle.

Para obtener más información, consulte Activación de páginas de gran tamaño para una instancia de RDS para Oracle.

DBInstanceClassMemory

Devuelve un entero del número de bytes de memoria disponibles para el proceso de base de datos. Este número se calcula internamente. Para ello, comienza con la cantidad total de memoria de la clase de instancia de base de datos. De esto, el cálculo resta la memoria reservada del sistema operativo y los procesos de RDS que administran la instancia. Por lo tanto, el número siempre es un poco inferior al de las cifras de memoria que se muestran en las tablas de clases de instancia en Clases de instancia de base de datos de . El valor exacto depende de una combinación de factores. Estos incluyen la clase de instancia, motor de base de datos y de si aplica a una instancia de RDS o a una instancia que forme parte de un clúster de Aurora.

DBInstanceVCPU

Devuelve un entero que representa el número de unidades de procesamiento centrales virtuales (vCPU) utilizadas por Amazon RDS para administrar la instancia.

EndPointPort

Devuelve un entero que representa el puerto utilizado al conectarse a la instancia de base de datos.

TrueIfReplica

Devuelve 1 si la instancia de base de datos es una réplica de lectura y `0` si no lo es. Es el valor predeterminado del parámetro `read_only` en MySQL.

Operadores de las fórmulas de parámetros de base de datos

Las fórmulas de parámetros de base de datos admiten dos operadores: división y multiplicación.

Operador de división: /

Divide el dividendo entre el divisor, y devuelve un cociente entero. Los decimales del cociente se truncan, no se redondean.

Sintaxis

```
dividend / divisor
```

Los argumentos del dividendo y el divisor deben ser expresiones enteras.

Operador de multiplicación: *

Multiplica las expresiones, devolviendo el producto de las expresiones. Los decimales de las expresiones se truncan, no se redondean.

Sintaxis

```
expression * expression
```

Las dos expresiones deben dar como resultado valores enteros.

Funciones de parámetros de base de datos

Los argumentos de las funciones de parámetro de base de datos se especifican como enteros o fórmulas. Cada función debe tener un argumento como mínimo. Especifique varios argumentos como una lista separada por comas. La lista no puede tener ningún miembro vacío; por ejemplo, argument1,,argument3. Los nombres de las funciones no distinguen entre mayúsculas y minúsculas.

IF

Devuelve un argumento.

Actualmente solo se admite para los motores de Oracle y el único primer argumento admitido es `{DBInstanceClassHugePagesDefault}`. Para obtener más información, consulte Activación de páginas de gran tamaño para una instancia de RDS para Oracle.

Sintaxis

```
IF(argument1, argument2, argument3)
```

Devuelve el segundo argumento si el primer argumento da como resultado true. En caso contrario, devuelve el tercer argumento.

GREATEST

Devuelve el valor más grande de una lista de números enteros o fórmulas de parámetros.

Sintaxis

```
GREATEST(argument1, argument2,...argumentn)
```

Devuelve un número entero.

LEAST

Devuelve el valor más pequeño de una lista de números enteros o fórmulas de parámetros.

Sintaxis

```
LEAST(argument1, argument2,...argumentn)
```

Devuelve un número entero.

SUM

Suma los valores de los números enteros o fórmulas de parámetros especificados.

Sintaxis

```
SUM(argument1, argument2,...argumentn)
```

Devuelve un número entero.

Expresiones de parámetros de base de datos booleanos

Una expresión de parámetro de base de datos booleano se resuelve en un valor booleano de 1 o 0. La expresión se proporciona entre comillas.

> **Note**
>
> Las expresiones de parámetros de base de datos booleanos solo son compatibles con el motor PostgreSQL.

Sintaxis

```
"expression operator expression"
```

Ambas expresiones deben resolverse en enteros. Una expresión puede ser la siguiente:

- Una constante entera
- Fórmulas de parámetros de base de datos
- Funciones de parámetros de base de datos
- Variable de parámetros de base de datos

Las expresiones de parámetro de base de datos booleano admiten los siguientes operadores de desigualdad:

El operador mayor que: **>**

Sintaxis

```
"expression > expression"
```

El operador menor que: **<**

Sintaxis

```
"expression < expression"
```

Los operadores mayor que o igual a: **>=**, **=>**

Sintaxis

```
"expression >= expression"
"expression => expression"
```

Los operadores menor que o igual a: **<=**, **=<**

Sintaxis

```
"expression <= expression"
"expression =< expression"
```

Example uso de una expresión de parámetro de base de datos booleano

En el siguiente ejemplo de expresión de parámetro de base de datos booleano se compara el resultado de una fórmula de parámetro con un entero. Lo hace para modificar el parámetro `wal_compression` de base de datos booleano de una instancia de base de datos de PostgreSQL. La expresión de parámetro compara el número de vCPU con el valor 2. Si el número de vCPU es mayor que 2, entonces el parámetro de la base de datos `wal_compression` se establece en verdadero.

```
aws rds modify-db-parameter-group --db-parameter-group-name group-name \
--parameters "ParameterName=wal_compression,ParameterValue=\"{DBInstanceVCPU} > 2\" "
```

Expresiones de registro de parámetros de base de datos

Puede establecer un valor de parámetro de base de datos entero en una expresión de registro. Se encierra la expresión entre llaves: {}. Por ejemplo:

```
{log(DBInstanceClassMemory/8187281418)*1000}
```

La función `log` representa la base de registro 2. En este ejemplo también se utiliza la variable de fórmula `DBInstanceClassMemory`. Consulte Variables de las fórmulas de parámetros de base de datos.

> **Note**
>
> Actualmente, no puede especificar el parámetro `innodb_log_file_size` de MySQL con ningún valor que no sea un número entero.

Ejemplos de valores de los parámetros de base de datos

Estos ejemplos muestran el uso de fórmulas, funciones y expresiones para los valores de los parámetros de base de datos.

> **Warning**
>
> Establecer parámetros incorrectamente en un grupo de parámetros de base de datos puede tener efectos adversos no deseados. Estos pueden incluir el rendimiento degradado y la inestabilidad del sistema. Tenga cuidado siempre que modifique los parámetros de base de

datos y haga una copia de seguridad de los datos antes de modificar el grupo de parámetros de base de datos. Pruebe los cambios de los grupos de parámetros en instancias de bases de datos de prueba, creadas mediante restauraciones a un momento dado, antes de aplicar dichos cambios de grupo de parámetros a las instancias de bases de datos de producción.

Example utilizando la función de parámetro de base de datos GREATEST

Puede especificar la función `GREATEST` en un parámetro de procesos Oracle. Utilícelo para establecer el número de procesos de usuario en el mayor de 80 o `DBInstanceClassMemory` dividido por 9 868 951.

```
GREATEST({DBInstanceClassMemory/9868951},80)
```

Example uso de la función de parámetro de base de datos LEAST

Puede especificar la función `LEAST` en un valor de parámetro de MySQL `max_binlog_cache_size`. Utilícelo para establecer el tamaño máximo de caché que una transacción puede usar en una instancia de MySQL, con un mínimo de 1 MB o `DBInstanceClass`/256.

```
LEAST({DBInstanceClassMemory/256},10485760)
```

Creación de una caché de Amazon ElastiCache mediante el uso de ajustes de la instancia de base de datos de Amazon RDS

ElastiCache es un servicio de caché en memoria totalmente administrado que proporciona latencias de lectura y escritura de microsegundos que permiten que los casos de uso sean flexibles y en tiempo real. ElastiCache puede ayudarle a acelerar el rendimiento de las aplicaciones y bases de datos. Puede usar ElastiCache como almacén de datos principal para casos de uso que no requieran durabilidad de los datos, como tablas de clasificación de juegos, transmisiones y análisis de datos. ElastiCache ayuda a eliminar la complejidad propia de la implementación y la administración de un entorno de computación distribuido. Para obtener más información, consulte Common ElastiCache Use Cases and How ElastiCache Can Help para Memcached y Common ElastiCache Use Cases and How ElastiCache Can Help para Redis OSS. Puede utilizar la consola de Amazon RDS para crear cachés de ElastiCache.

Puede utilizar Amazon ElastiCache en dos formatos. Puede empezar con una memoria caché sin servidor o diseñar su propio clúster de caché. Si decide diseñar su propio clúster de caché, ElastiCache es compatible con los motores de Memcached y Redis OSS. Si no está seguro de qué motor desea utilizar, consulte Comparing Memcached and Redis OSS. Para obtener más información acerca de Amazon ElastiCache, consulte la Guía del usuario de Amazon ElastiCache.

Temas

- Información general sobre la creación de cachés de ElastiCache con ajustes de la instancia de base de datos de RDS
- Creación de una caché de ElastiCache con ajustes de una instancia de base de datos de RDS

Información general sobre la creación de cachés de ElastiCache con ajustes de la instancia de base de datos de RDS

Puede crear una caché de ElastiCache desde Amazon RDS con los mismos ajustes de configuración que un clúster de base de datos de Aurora recién creado o existente.

Algunos casos de uso para asociar una caché de ElastiCache a la instancia de base de datos:

- Puede ahorrar costos y mejorar su rendimiento si utiliza ElastiCache con RDS en lugar de solo RDS.

Por ejemplo, puede ahorrar hasta un 55 % de los costos y obtener un rendimiento de lectura hasta 80 veces más rápido si utiliza ElastiCache con RDS para MySQL en lugar de solo RDS para MySQL.

- Puede utilizar la caché de ElastiCache como almacén de datos principal para las aplicaciones que no requieran durabilidad de los datos. Las aplicaciones existentes que utilizan Redis OSS o Memcached pueden utilizar ElastiCache sin prácticamente ninguna modificación.

Al crear una caché de ElastiCache desde RDS, la caché de ElastiCache hereda los siguientes ajustes de la instancia de base de datos de RDS asociada:

- Ajustes de conectividad de ElastiCache
- Ajustes de seguridad de ElastiCache

También puede configurar los parámetros de configuración de la caché según sus necesidades.

Configuración de ElastiCache en sus aplicaciones

Debe configurar sus aplicaciones para que utilicen cachés de ElastiCache. También puede optimizar y mejorar el rendimiento de las cachés configurando las aplicaciones para que utilicen estrategias de almacenamiento en caché en función de sus requisitos.

- Para acceder a su caché de ElastiCache y comenzar a trabajar, consulte Getting started with ElastiCache (Redis OSS) y Getting started with ElastiCache (Memcached).
- Para obtener más información sobre las estrategias de almacenamiento en caché, consulte Caching strategies and best practices, para Memcached, y Caching strategies and best practices para Redis OSS.
- Para obtener más información sobre la alta disponibilidad en los clústeres de ElastiCache (Redis OSS), consulte High availability using replication groups.
- Puede incurrir en costos relacionados con el almacenamiento de copias de seguridad, la transferencia de datos dentro o entre regiones, o el uso de AWS Outposts. Para obtener más información sobre los precios, consulte Precios de Amazon ElastiCache.

Creación de una caché de ElastiCache con ajustes de una instancia de base de datos de RDS

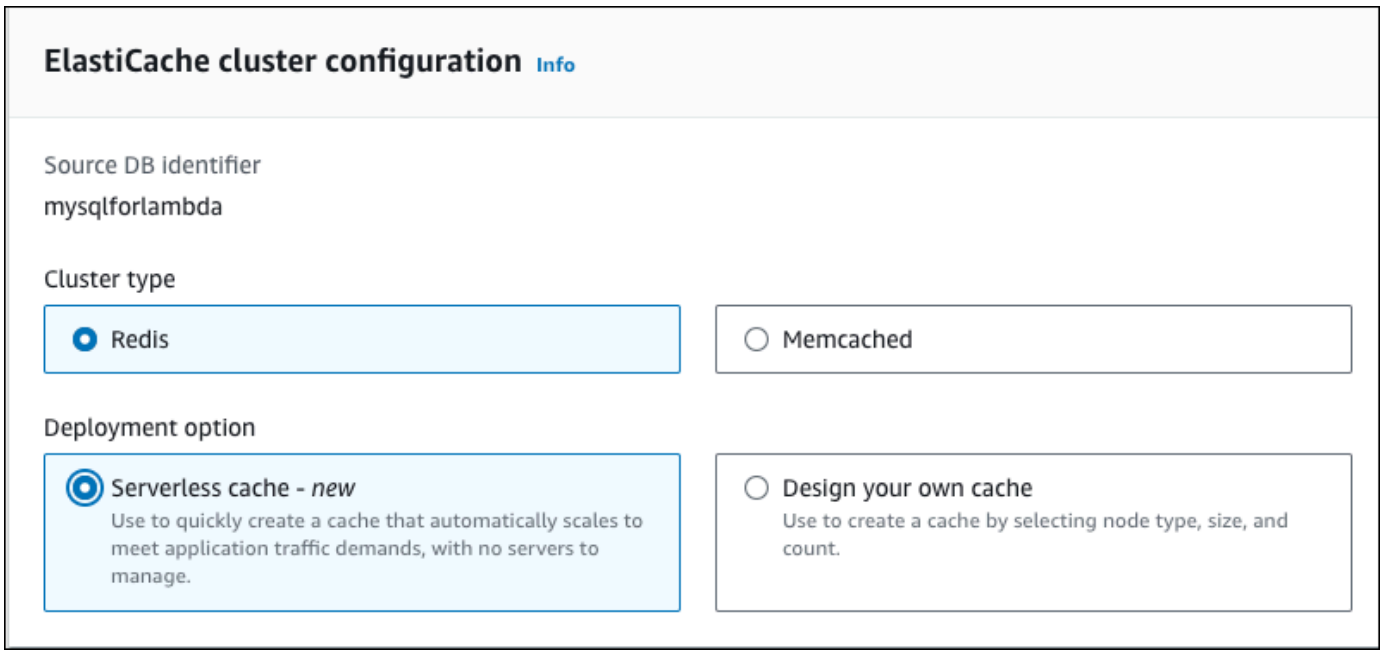
Puede crear una caché de ElastiCache para sus sus instancias de base de datos de RDS con una configuración heredada de la instancia de base de datos.

Creación de una caché de ElastiCache con ajustes de una instancia de base de datos

1. Para crear una instancia de base de datos, siga las instrucciones que se indican en Creación de una instancia de base de datos de Amazon RDS.
2. Tras crear una instancia de base de datos, la consola muestra la ventana Complementos sugeridos. Seleccione Crear un clúster de ElastiCache desde RDS con los ajustes de la base de datos.

   Para una base de datos existente, en la página Bases de datos, seleccione la instancia de base de datos que corresponda. En el menú desplegable Acciones, elija Crear clúster de ElastiCache para crear una caché de ElastiCache en RDS que tenga la misma configuración que la instancia de base de datos de RDS existente.

   En la sección de configuración de ElastiCache, el Identificador de base de datos de origen muestra de qué clúster de base de datos hereda la configuración la caché de ElastiCache.
3. Elija si desea crear un clúster de Redis OSS o Memcached. Para obtener más información, consulte Comparing Memcached and Redis OSS.



4. Después de esto, elija si desea crear una Caché sin servidor o si prefiere Diseñar su propia caché. Para obtener más información, consulte Choosing between deployment options.

   Si elige Caché sin servidor:

   a. En Configuración de caché, introduzca los valores de Nombre y Descripción.

   b. En Ver la configuración predeterminada, deje la configuración predeterminada para establecer la conexión entre la caché y la instancia de base de datos.

   c. También puede editar la configuración predeterminada seleccionando Personalizar configuración predeterminada. Seleccione Configuración de conectividad de ElastiCache, Configuración de seguridad de ElastiCache y Límites de uso máximo.

5. Si elige Diseñar su propia caché:

   a. Si elige Clúster de Redis OSS, elija si desea mantener el modo de clúster Habilitado o Deshabilitado. Para obtener más información, consulte Replication: Redis OSS (clúster Mode Disabled) vs. Redis OSS (clúster Mode Enabled).

   b. Introduzca valores para Nombre, Descripción y Versión del motor.

      En Versión del motor, el valor predeterminado recomendado es la versión del motor más reciente. También puede elegir la Versión del motor para la caché de ElastiCache que mejor se adapte a sus requisitos.

   c. Elija el tipo de nodo en la opción Tipo de nodo. Para obtener más información, consulte Administración de nodos.

      Si elige crear un clúster de Redis OSS con el Modo de clúster configurado en Habilitado, introduzca el número de particiones (particiones/grupos de nodos) en la opción Número de particiones.

      Introduzca el número de réplicas de cada partición en Número de réplicas.

      > **Note**
      >
      > El tipo de nodo seleccionado, la cantidad de particiones y la cantidad de réplicas afectan al rendimiento de la caché y a los costos de los recursos. Asegúrese de que estos ajustes se correspondan a las necesidades de su base de datos. Para obtener información sobre los precios, consulte Precios de Amazon ElastiCache.

d. Seleccione Configuración de conectividad de ElastiCache y Configuración de seguridad de ElastiCache. Puede conservar la configuración predeterminada o personalizarla según sus necesidades.

6. Compruebe la configuración predeterminada y heredada de su caché de ElastiCache. Algunos ajustes no se pueden cambiar después de la creación.

> **Note**
>
> RDS podría ajustar el periodo de copia de seguridad de la caché de ElastiCache para cumplir con el requisito del periodo mínimo de 60 minutos. El periodo de copia de seguridad de la base de datos de origen sigue siendo el mismo.

7. Cuando esté listo, elija Crear caché de ElastiCache.

La consola abre un banner de confirmación para la creación de la caché de ElastiCache. Siga el enlace del banner a la consola de ElastiCache para ver los detalles de la caché. La consola de ElastiCache muestra la caché de ElastiCache recién creada.

Migración automática de bases de datos de EC2 a Amazon RDS mediante AWS Database Migration Service

Puede utilizar la consola de RDS para migrar una base de datos de EC2 a RDS. RDS utiliza AWS Database Migration Service (AWS DMS) para migrar bases de datos de EC2 de origen. AWS DMS permite migrar bases de datos relacionales a su nube de AWS. Para obtener más información sobre AWS Database Migration Service, consulte ¿Qué es AWS Database Migration Service? en la Guía del usuario de AWS Database Migration Service.

Para comenzar la migración, debe crear una instancia de base de datos de RDS equivalente donde migrar los datos. Tras crear la base de datos de destino, puede importar la base de datos de EC2 a ella. Para las bases de datos de origen de menos de 1 TiB, esta acción de migración reduce el tiempo y los recursos necesarios para migrar los datos a RDS.

Descripción general

La consola de RDS le permite migrar bases de datos de EC2 a bases de datos de RDS equivalentes. Debe crear una base de datos de RDS para permitir la migración desde la consola.

Puede migrar las bases de datos de EC2 para los siguientes motores de bases de datos:

- MySQL
- MariaDB
- PostgreSQL

El proceso de migración consta de los pasos siguientes:

- Cree una base de datos equivalente en RDS. Para que las bases de datos sean equivalentes, deben tener el mismo motor de base de datos y versiones de motor compatibles. También deben estar en la misma VPC. Para obtener instrucciones sobre cómo crear una base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.
- Elija el tipo de replicación para la base de datos:
  - Migración a carga completa: RDS copia la base de datos de origen completa en la base de datos de destino y crea nuevas tablas en la de destino cuando es necesario.

> **Note**
>
> Esta opción provoca una interrupción en la base de datos de RDS.

- Migración a carga completa y con captura de datos de cambios (CDC): similar a la migración a carga completa, con esta opción, RDS copia la base de datos de origen completa a la base de datos de destino. Sin embargo, después de la migración a carga completa, RDS aplica todos los cambios capturados en el origen a la base de datos de destino. La captura de datos de cambios recopila los cambios en los registros de la base de datos mediante la API nativa del motor de la base de datos.

  > **Note**
  >
  > Esta opción provoca una interrupción en la base de datos de RDS.

  - Captura de datos de cambios (CDC): utilice esta opción para mantener la base de datos de destino disponible durante la migración. RDS migra los cambios continuos de la base de datos de origen a la base de datos de destino.
- RDS crea los recursos de red necesarios para facilitar la migración. Una vez que RDS crea los recursos necesarios, le notifica acerca de los recursos creados y le permite iniciar la transferencia de datos.

  El tiempo necesario para completar la migración depende del tipo de replicación y del tamaño de la base de datos de origen.

Requisitos previos

MySQL y MariaDB

Antes de comenzar a trabajar con una base de datos de MySQL o MariaDB como base de datos de origen, asegúrese de cumplir los siguientes requisitos previos. Estos requisitos previos se aplican a orígenes administrados por AWS.

Debe tener una cuenta para AWS DMS que tiene el rol de administrador de replicación. El rol necesita los siguientes privilegios:

- REPLICATION CLIENT: este privilegio es necesario solo para tareas de CDC. Es decir, las tareas de solo carga completa no necesitan este privilegio.
- REPLICATION SLAVE: este privilegio es necesario solo para tareas de CDC. Es decir, las tareas de solo carga completa no necesitan este privilegio.

El usuario de AWS DMS también debe disponer de privilegios SELECT para las tablas de origen designadas para la replicación.

Conceda los siguientes privilegios si utiliza las evaluaciones previas a la migración específicas de MySQL.

```
grant select on mysql.user to <dms_user>;
grant select on mysql.db to <dms_user>;
grant select on mysql.tables_priv to <dms_user>;
grant select on mysql.role_edges to <dms_user>  #only for MySQL version 8.0.11 and
 higher
```

PostgreSQL

Antes de migrar datos desde una base de datos de origen de PostgreSQL administrada por AWS, haga lo siguiente:

- Le recomendamos que utilice una cuenta de usuario de AWS con los permisos mínimos necesarios para la instancia de base de datos de PostgreSQL como cuenta de usuario para el punto de conexión de origen de PostgreSQL para AWS DMS. No se recomienda el uso de la cuenta principal. La cuenta debe tener el rol `rds_superuser` y el rol `rds_replication`. El rol de `rds_replication` concede permisos para administrar ranuras lógicas y para transmitir datos mediante ranuras lógicas.

> **Note**
>
> Algunas transacciones de AWS DMS están inactivas durante un tiempo antes de que el motor de DMS las utilice de nuevo. Al usar el parámetro `idle_in_transaction_session_timeout` en PostgreSQL versiones 9.6 y superiores, puede provocar transacciones inactivas en el tiempo de espera y que se devuelva un error.

Limitaciones

Se aplican las siguientes limitaciones al proceso de migración automática:

- El estado de la base de datos de destino debe ser Disponible para iniciar la migración de la base de datos de origen.
- Al migrar desde una base de datos de MySQL de origen, su cuenta de RDS debe tener el rol de administrador de replicación. También debe tener los privilegios adecuados aplicados para ese rol.
- La instancia de EC2 y la base de datos de destino deben estar en la misma VPC.
- No puede migrar la base de datos de EC2 a las siguientes bases de datos de destino cuando utiliza la acción Migrar datos desde la base de datos de EC2:
  - Base de datos que forma parte de un clúster
  - Bases de datos de Oracle, SQL Server y Db2
  - Bases de datos con una versión de MySQL inferior a la 5.7
  - Bases de datos con una versión de PostgreSQL inferior a la 10.4
  - Bases de datos con una versión de MariaDB inferior a la 10.2

Creación de recursos de IAM para migraciones homogéneas

RDS utiliza AWS DMS para migrar sus datos. Para acceder a las bases de datos y para migrar los datos, AWS DMS crea un entorno sin servidor para migraciones de datos homogéneas. En este entorno, AWS DMS requiere acceso a la interconexión de VPC, las tablas de enrutamiento, los grupos de seguridad y otros recursos de AWS. Además, AWS DMS almacena los registros, las métricas y el progreso de cada migración de datos en Amazon CloudWatch. Para crear un proyecto de migración de datos, AWS DMS necesita acceder a estos servicios.

Además, AWS DMS requiere acceso a los secretos que representan un conjunto de credenciales de usuario para autenticar la conexión de base de datos, tanto la de origen como la de destino.

> **Note**
>
> Con la acción Migrar datos de una instancia de EC2, puede utilizar la consola de RDS para generar estos recursos de IAM. Omita este paso si utiliza los recursos de IAM generados por la consola.

Para este procedimiento, necesita los siguientes recursos de IAM:

Temas

- Creación de una política de IAM para migraciones de datos homogéneas
- Creación de un rol de IAM para migraciones de datos homogéneas
- Creación de un rol y una política de acceso a un secreto
- Creación de un rol de IAM para que AWS DMS administre Amazon VPC

Creación de una política de IAM para migraciones de datos homogéneas

En este paso, se crea una política de IAM que proporciona a AWS DMS acceso a los recursos de Amazon EC2 y CloudWatch. Después, cree un rol de IAM y asocie esta política.

Creación de una política de IAM para una migración de datos

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Crear política.
4. En la página Crear política, elija la pestaña JSON.
5. Pegue el siguiente objeto JSON en el editor.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribePrefixLists",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetServiceQuota"
            ],
            "Resource": "arn:aws:servicequotas:*:*:vpc/L-0EA8095F"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DescribeLogStreams"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:dms-data-migration-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:dms-data-migration-*:log-
stream:dms-data-migration-*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:security-group-rule/*",
                "arn:aws:ec2:*:*:route-table/*",
                "arn:aws:ec2:*:*:vpc-peering-connection/*",
                "arn:aws:ec2:*:*:vpc/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group-rule/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AcceptVpcPeeringConnection",
                "ec2:ModifyVpcPeeringConnectionOptions"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-peering-connection/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:AcceptVpcPeeringConnection",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
}
```

6. Elija Siguiente: Etiquetas y Siguiente: Revisar.
7. Ingrese **`HomogeneousDataMigrationsPolicy`** para Nombre* y elija Crear política.

Creación de un rol de IAM para migraciones de datos homogéneas

En este paso, se crea un rol de IAM que proporciona acceso a AWS Secrets Manager, Amazon EC2 y CloudWatch.

Creación de un rol de IAM para migraciones de datos

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.
4. En la página Seleccionar entidad de confianza, para Tipo de entidad de confianza, elija Servicio de AWS. Para Casos de uso para otros servicios de AWS, elija DMS.
5. Seleccione la casilla de verificación DMS y elija Siguiente.
6. En la página Agregar permisos, elija HomogeneousDataMigrationsPolicy que haya creado anteriormente. Elija Siguiente.
7. En la página Asignar nombre, revisar y crear, ingrese **`HomogeneousDataMigrationsRole`** para Nombre del rol y elija Crear rol.
8. En la página Roles, escriba **`HomogeneousDataMigrationsRole`** para Nombre del rol. Elija HomogeneousDataMigrationsRole.
9. En la página HomogeneousDataMigrationsRole, elija la pestaña Relaciones de confianza. Elija Editar la política de confianza.
10. En la página Editar política de confianza, pegue el siguiente JSON en el editor y sustituya el texto existente.

    JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "dms-data-migrations.amazonaws.com",
                    "dms.your_region.amazonaws.com"
```

```
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

En el ejemplo anterior, sustituya *your_region* por el nombre de la Región de AWS.

La política anterior basada en recursos proporciona a las entidades principales de servicios de AWS DMS permisos para realizar tareas de acuerdo con la política HomogeneousDataMigrationsPolicy administrada por el cliente.

11. Elija Actualizar política.

Creación de un rol y una política de acceso a un secreto

Siga los procedimientos que se indican a continuación para crear su rol y su política de acceso a un secreto que permitan a DMS acceder a las credenciales de usuario de sus bases de datos de origen y destino.

Creación de un rol y una política de acceso a un secreto que permitan a Amazon RDS acceder a AWS Secrets Manager para acceder al secreto pertinente

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Identity and Access Management (IAM) en https://console.aws.amazon.com/iam/.
2. Elija Políticas, después elija Crear política.
3. Elija JSON e ingrese la siguiente política para permitir el acceso al secreto y el descifrado del secreto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": secret_arn,
        },
        {
             "Effect": "Allow",
```

```
            "Action": [
                      "kms:Decrypt",
                      "kms:DescribeKey"
                    ],
            "Resource": kms_key_arn,
        }
    ]
}
```

Aquí, *secret_arn* es el ARN del secreto, que puede obtener del `SecretsManagerSecretId`, según corresponda, y *kms_key_arn* es el ARN de la clave de AWS KMS que utiliza para cifrar el secreto, como en el siguiente ejemplo.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "arn:aws:secretsmanager:us-
east-2:123456789012:secret:MySQLTestSecret-qeHamH"
        },
        {
             "Effect": "Allow",
             "Action": [
                       "kms:Decrypt",
                       "kms:DescribeKey"
                     ],
             "Resource": "arn:aws:kms:us-
east-2:123456789012:key/761138dc-0542-4e58-947f-4a3a8458d0fd"
        }
    ]
}
```

> **Note**
>
> Si utiliza la clave de cifrado predeterminada creada por AWS Secrets Manager, no tiene que especificar los permisos de AWS KMS para *kms_key_arn*.

Si desea que la política proporcione acceso a ambos secretos, simplemente especifique un objeto de recurso JSON adicional para el otro *secret_arn*.

4. Revise y cree la política con un nombre descriptivo y una descripción opcional.
5. Elija Roles, después elija Crear rol.
6. Elija Servicio de AWS como tipo de entidad de confianza.
7. Elija DMS de la lista de servicios como servicio de confianza y, a continuación, elija Siguiente: Permisos.
8. Busque y asocie la política que creó en el paso 4 y, a continuación, agregue las etiquetas que desee y revise el rol. En este punto, edite las relaciones de confianza del rol para usar la entidad principal de servicio regional de Amazon RDS como entidad de confianza. Esta entidad principal tiene el formato siguiente.

```
dms.region-name.amazonaws.com
```

Aquí, *region-name* es el nombre de la región, por ejemplo `us-east-1`. Por lo tanto, le sigue una entidad principal de servicio regional de Amazon RDS para esta región.

```
dms.us-east-1.amazonaws.com
dms-data-migrations.amazonaws.com
```

Creación de un rol de IAM para que AWS DMS administre Amazon VPC

Debe crear un rol de IAM para que AWS DMS administre la configuración de VPC para sus recursos. Este rol debe estar disponible para que la migración se realice correctamente.

Creación del **`dms-vpc-role`** para la migración de la base de datos

<result>

Esto crea el rol para que DMS administre la configuración de la VPC para la migración.
</result>

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola, elija Roles y, a continuación, seleccione Crear rol.
3. Seleccione la opción Servicio de AWS para la opción Seleccionar entidad de confianza.

Para Caso de uso, seleccione DMS.

4. Para el paso Agregar permisos, seleccione `AmazonDMSVPCManagementRole` y elija Siguiente.
5. En la página Asignar nombre, revisar y crear, especifique el Nombre del rol como `dms-vpc-role` y elija Crear rol.

Configuración de la migración de datos para bases de datos de EC2

Para empezar a migrar los datos desde la base de datos de EC2 de origen, debe crear una base de datos de RDS equivalente. Para obtener instrucciones sobre cómo crear una base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

Después de crear la base de datos de destino, siga los pasos que se indican a continuación para configurar la migración de datos:

Configuración del proyecto de migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. Elija el menú desplegable Acciones y seleccione la opción Migrar datos desde la base de datos de EC2. Para ver una lista de las bases de datos admitidas, consulte Limitaciones.
3. En la sección Seleccionar la base de datos de EC2 de origen:
    1. Compruebe el Tipo de motor y asegúrese de que sea el mismo que el de la base de datos de origen.

        Compruebe también si las versiones del motor son compatibles.
    2. Para Instancia EC2, elija la instancia de EC2 en la que reside la base de datos de origen.
    3. En Puerto, introduzca el puerto en el que la base de datos de origen permite el tráfico.
    4. En Secreto, seleccione Crear y usar un secreto nuevo si aún no tiene uno. Especifique el Nombre de usuario y la Contraseña para su base de datos de origen. Elija también la clave de KMS con la que quiera cifrar su secreto.

        Si tiene un secreto existente, seleccione Usar secreto existente y elija un secreto de la lista.
    5. Para Rol de IAM para el secreto, si ya tiene un rol de IAM existente, seleccione Usar un rol de IAM existente y elija un rol de IAM del menú desplegable que pueda acceder al ID secreto del paso anterior.

Si no tiene un rol de IAM existente, elija Crear y usar un nuevo rol de IAM. Escriba un nombre para el rol en el campo Nombre del rol de IAM. Puede ver los permisos asociados a este rol en el siguiente enlace.

4. En la sección Ver la base de datos de RDS de destino:

   1. Confirme la configuración de la base de datos de destino en la parte superior de la sección.
   2. En Secreto, seleccione Crear y usar un secreto nuevo si no tiene ya uno que contenga las credenciales de su base de datos de destino.

      Si tiene un secreto existente, seleccione el secreto de la lista desplegable.
   3. En Rol de IAM para el secreto, seleccione un rol de IAM que pueda acceder al secreto en el paso anterior. También puede crear un nuevo rol de IAM si no tiene uno.

      Si el menú desplegable no rellena los roles de IAM, especifique el ARN del rol de IAM en el formato `arn:aws:iam:`*`account_id`*`:role/`*`roleName`*.
5. En la sección Configurar la migración de datos:

   1. Seleccione el tipo de migración de datos entre Carga completa, Carga completa y captura de datos de cambios (CDC) o Captura de datos de cambios (CDC). Para obtener más información sobre estas opciones, consulte Descripción general.

      No puede modificar el tipo de migración una vez iniciada la migración.
   2. Para Rol de IAM para la migración de datos, si ya tiene un rol de IAM existente, seleccione Usar un rol de IAM existente y elija un rol de IAM del menú desplegable que otorgue a DMS los permisos para crear los recursos necesarios para la migración. Si no tiene un rol de IAM existente, elija Crear y usar un nuevo rol de IAM.
6. Confirme que la pestaña Ver la configuración de migración muestra la configuración necesaria para que la migración de datos se configure correctamente.
7. Seleccione Migrar para completar la configuración de la migración.

Tras completar estos pasos, podrá ver los recursos que se están configurando para la migración de datos si selecciona Ver detalles en el panel de progreso de la consola. Una vez configurados los recursos necesarios, la migración se inicia automáticamente. Si crea

Para migrar varias bases de datos a la base de datos de destino, vuelva a iniciar este proceso con los detalles de la nueva base de datos de EC2.

Administración de migraciones de datos

Tras utilizar la acción Migrar datos desde una base de datos de EC2 desde la consola de RDS, RDS inicia la migración automáticamente.

Si utilizó la consola de AWS DMS para crear los recursos de migración, puede iniciar el proceso de migración.

Inicio de la migración de datos

Siga estos pasos para iniciar la migración de datos:

Inicio de una migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. En la página de detalles de la base de datos, elija la pestaña Migraciones de datos.
3. En la pestaña Migraciones de datos, la sección Migraciones de datos asociadas muestra las migraciones de datos disponibles.

   Las migraciones configuradas mediante la consola RDS se inician automáticamente una vez configurados los recursos necesarios.

   Las migraciones configuradas mediante la consola de DMS están configuradas como Listas.

   Para iniciar estas migraciones, seleccione el menú desplegable Acciones y, a continuación, seleccione Iniciar.
4. Esto inicia la migración de datos de su base de datos de EC2.

Detención de la migración de datos

En el caso de las migraciones de datos cuyo tipo de replicación es a plena carga, si se detiene la migración, el proceso se para y no se puede reanudar. Una vez detenida la migración, debe reiniciarse.

En el caso de las migraciones con el tipo de replicación configurado como captura de datos de cambio (CDC) o carga completa y CDC, puede detener el proceso de replicación continua y reanudarlo más adelante.

Detención de una migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. En la página de detalles de la base de datos, elija la pestaña Migraciones de datos.
3. En la pestaña Migraciones de datos, la sección Migraciones de datos asociadas muestra las migraciones de datos en curso.

   Para detener una migración, seleccione una migración de datos y elija Detener en el menú desplegable Acciones.
4. Esto detiene la migración de datos de su base de datos de EC2.

Reanudación de la migración de datos

Para las migraciones de datos cuyo tipo de replicación sea carga completa y captura de datos de cambio (CDC) o captura de datos de cambio (CDC), puede reanudar el proceso de CDC desde el último punto de parada.

Reanudación de una migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. En la página de detalles de la base de datos, elija la pestaña Migraciones de datos.
3. En la pestaña Migraciones de datos, la sección Migraciones de datos asociadas muestra las migraciones de datos detenidas.

   Para reanudar una migración, seleccione una migración de datos y elija Reanudar el procesamiento en el menú desplegable Acciones.
4. Esto reanuda la migración de datos de su base de datos de EC2.

Eliminación de la migración de datos

Para eliminar una migración de datos asociada, utilice las siguientes instrucciones

Eliminación de una migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. En la página de detalles de la base de datos, elija la pestaña Migraciones de datos.

3. Para eliminar una migración, seleccione una migración de datos y elija Eliminar en el menú desplegable Acciones.
4. Esto elimina la migración de datos.

La eliminación de una migración de datos que estuviera en curso no afecta a los datos que ya se hayan cargado en la base de datos de destino.

Reinicio de la migración de datos

Para reiniciar una migración de datos asociada desde un punto de inicio de CDC, siga estas instrucciones

Reinicio de una migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. En la página de detalles de la base de datos, elija la pestaña Migraciones de datos.
3. Para reiniciar una migración, seleccione una migración de datos y elija Reiniciar en el menú desplegable Acciones.
4. Esto reinicia la migración de datos desde un punto de inicio de CDC.

El reinicio de una migración de datos que estuviera en curso no afecta a los datos que ya se hayan cargado en la base de datos de destino.

Monitorización de migraciones de datos

Tras iniciar las migraciones de datos, puede monitorizar su estado y su progreso. Las migraciones de grandes conjuntos de datos tardan horas en completarse. Para mantener la fiabilidad, la disponibilidad y el alto rendimiento de la migración de datos, monitoree el progreso con regularidad.

Comprobación del estado y el progreso de la migración de datos

1. Seleccione la base de datos de destino en la página Bases de datos de la consola de RDS.
2. En la página de detalles de la base de datos, elija la pestaña Migraciones de datos.
3. La sección Migraciones de datos asociadas muestra las migraciones de datos. Comprobación de la columna Estado.
4. Para las migraciones de datos en curso, la columna Progreso de migración muestra el porcentaje de datos migrados.

5. Para monitorizar el proceso en CloudWatch, utilice el enlace de la columna CloudWatch.

Estados de migración

Para cada migración de datos que ejecute, la consola de RDS muestra el Estado. La siguiente lista incluye los estados:

- `Ready`: la migración de datos está lista para comenzar.
- `Starting`: RDS crea el entorno sin servidor para la migración de datos.
- `Load running`: RDS realiza la migración de carga completa.
- `Load complete, replication ongoing`: RDS ha completado la carga completa y ahora replica los cambios en curso. Este estado solo se aplica a las migraciones de carga completa y de tipo CDC.
- `Replication ongoing`: RDS está replicando los cambios en curso. Este estado solo se aplica a las migraciones de tipo CDC.
- `Stopping`: RDS está deteniendo las migraciones de datos. Este estado se aplica cuando decide detener la migración de datos desde el menú Acciones.
- `Stopped`: RDS ha detenido la migración de datos.
- `Failed`: la migración de datos ha producido un error. Para obtener más información, consulte los archivos de registro.
- `Restarting`: la migración de datos ha reiniciado una replicación de datos en curso desde un punto de partida de CDC.

Tutorial: Creación de una instancia de base de datos de MySQL con un grupo de parámetros personalizados y un grupo de opciones nuevas

En este tutorial, creará una instancia de base de datos de MySQL con un grupo de parámetros personalizados y un grupo de opciones nuevas. Para obtener más información sobre los grupos de parámetros personalizados y de opciones, consulte Grupos de parámetros para Amazon RDS y Trabajo con grupos de opciones

> **Important**
>
> La creación de una cuenta de AWS no supone ningún costo. No obstante, al completar este tutorial, puede incurrir en costos por los recursos de AWS que utilice. Puede eliminar estos recursos después de completar el tutorial si ya no son necesarios.

Para crear una instancia de base de datos con configuraciones y ajustes personalizados, puede utilizar grupos de parámetros personalizados y grupos de opciones nuevas. Los grupos de parámetros personalizados y los grupos de opciones nuevas son especialmente útiles si trabaja con varias bases de datos y desea configurar los ajustes de manera uniforme.

Al completar estos pasos, aprenderá lo siguiente:

- Cómo utilizar Amazon RDS para crear una instancia de base de datos de MySQL con un grupo de parámetros personalizados y un grupo de opciones nuevas.
- Cómo utilizar determinado parámetros y opciones para instancias de base de datos de MySQL.

Para completar este tutorial, realice las siguientes tareas:

1. Cree un grupo de parámetros personalizados con los parámetros `default_password_lifetime` y `disconnect_on_expired_password` de MySQL.
2. Cree un nuevo grupo de opciones con la característica de opciones `MariaDB Audit Plugin` de MySQL. Si desea ver los pasos necesarios para crear un grupo de opciones, consulte Trabajo con grupos de opciones.
3. Cree una instancia de base de datos de MySQL con el grupo de parámetros personalizados y un grupo de opciones nuevas que ha creado.

Temas

- Requisitos previos
- Creación de un grupo de parámetros de Amazon RDS
- Modificación de los valores de parámetro en el grupo de parámetros personalizados
- Creación de un grupo de opciones de Amazon RDS
- Cómo agregar un opción al grupo de opciones nuevas
- Creación de una instancia de base de datos de MySQL con un grupo de parámetros personalizadosy un nuevo grupo de opciones

Requisitos previos

Este tutorial requiere que tenga una Cuenta de AWS y un usuario con acceso administrativo. Si aún no los ha configurado, complete los pasos de las secciones siguientes:

- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Creación de un grupo de parámetros de Amazon RDS

En este tutorial, aprenderá a crear un grupo de parámetros personalizados con default_password_lifetime y disconnect_on_expired_password para una instancia de base de datos de MySQL en la consola. El parámetro `default_password_lifetime` controla el número de días que faltan para que la contraseña del cliente caduque automáticamente. El parámetro `disconnect_on_expired_password` controla si la instancia de base de datos de MySQL desconecta al cliente cuando caduca la contraseña. Para obtener más información sobre otros parámetros disponibles para instancias de base de datos de MySQL, consulte Parámetros de MySQL .

Para crear un grupo de parámetros

1. Abra la consola de Amazon RDS y seleccione Grupos de parámetros.
2. En Grupos de parámetros personalizados, elija Crear grupo de parámetros.
3. Establezca los detalles del grupo de parámetros.
    1. Escriba un nombre para el grupo de parámetros.

2. Introduzca la descripción del grupo de parámetros.
3. En Tipo de motor, elija MySQL Community.
4. En Familia de grupos de parámetros, elija MySQL 8.0.

4. Seleccione Crear.

El nuevo grupo de parámetros de aparece en la página Grupos de parámetros de la consola de Amazon RDS. Los siguientes pasos ilustran cómo modificar los valores de los parámetros para personalizar el grupo de parámetros.

Modificación de los valores de parámetro en el grupo de parámetros personalizados

Siga estos pasos para modificar los valores de parámetro en el grupo de parámetros que creó en Creación de un grupo de parámetros de Amazon RDS.

Modificación de los valores de parámetro en el grupo de parámetros

1. Abra la consola de Amazon RDS y seleccione Grupos de parámetros.
2. En Grupos de parámetros personalizados, elija el nombre del grupo de parámetros del que ha creado.
3. Elija Editar.
4. En el cuadro de búsqueda Filtrar los parámetros, busque el parámetro personalizado `default_password_lifetime`.
5. Seleccione la casilla de verificación situada junto al parámetro e introduzca un valor correspondiente al número de días que se va a establecer para este parámetro de duración de la contraseña.
6. Seleccione Save Changes (Guardar cambios).
7. Repita los mismos pasos para el parámetro `disconnect_on_expired_password`. Al elegir este parámetro, se le pedirá que seleccione un valor de 0 o 1 en el menú desplegable. Seleccione 1 para realizar la desconexión si la contraseña ha caducado.

El grupo de parámetros personalizado ahora está disponible para asociarlo con Amazon RDS para la instancia de base de datos de MySQL 8.0. A continuación, cree un grupo de opciones nuevas para la instancia de base de datos.

Creación de un grupo de opciones de Amazon RDS

Cree un grupo de opciones nuevas con la opción Complemento de auditoría de MariaDB. Este complemento registra la actividad del servidor para garantizar la seguridad y el cumplimiento. Para obtener más información sobre otras opciones personalizadas disponibles para las instancias de base de datos de MySQL, consulte Opciones para las instancias de bases de datos MySQL.

Creación de un grupo de opciones

1. Abra la consola de Amazon RDS y seleccione Grupos de opciones.
2. En Grupos de opciones, elija Crear grupo.
3. Establezca los detalles del grupo de opciones.
   - Introduzca un nuevo nombre para el grupo de opciones.
   - Introduzca una descripción del grupo de opciones.
   - En Motor, seleccione mysql.
   - En Versión del motor principal, seleccione 8.0.
4. Seleccione Crear.

El nuevo grupo de opciones aparecerá en la página Grupos de opciones de la consola de Amazon RDS. Los siguientes pasos muestran cómo agregar opciones al grupo de opciones.

Cómo agregar un opción al grupo de opciones nuevas

Siga estos pasos para agregar una opción al grupo de opciones nuevas que ha creado en Creación de un grupo de opciones de Amazon RDS.

Cómo agregar una opción a un grupo de opciones

1. Abra la consola de Amazon RDS y seleccione Grupos de opciones.
2. En Grupos de opciones, seleccione el nombre del grupo de opciones que ha creado.
3. En Opciones, elija Agregar opción.
4. Establezca los detalles del grupo de opciones.
   - En Nombre de la opción, elija la opción Complemento de auditoría de MariaDB, MARIADB_AUDIT_PLUGIN.

- En Configuración de opciones, deje seleccionadas todas las opciones predeterminadas.
- En Aplicar inmediatamente, elija Sí.

5. Seleccione Crear opción.

Ahora, el nuevo grupo de opciones debería estar disponible para todas las instancias de base de datos asociadas. A continuación, cree una instancia de base de datos de MySQL con el parámetro personalizado y el nuevo grupo de opciones.

Creación de una instancia de base de datos de MySQL con un grupo de parámetros personalizadosy un nuevo grupo de opciones

Por último, cree una instancia de base de datos de MySQL con el grupo de parámetros personalizados y el nuevo grupo de opciones que ha creado en los pasos anteriores. Los siguientes pasos muestran cómo crear la instancia de base de datos de MySQL con el grupo de parámetros personalizados y el nuevo grupo de opciones.

Creación de una instancia de base de datos con un grupo de parámetros personalizados y un nuevo grupo de opciones

1. Abra la consola de Amazon RDS y seleccione Bases de datos.
2. Elija Creación de base de datos.
3. En Elegir un método de creación de base de datos, elija Creación estándar.
4. En Opciones del motor, elija MySQL .
5. En Disponibilidad y durabilidad, elija Instancia de base de datos única. Este paso es necesario para admitir un grupo de parámetros personalizados o un nuevo grupo de opciones.
6. Seleccione Configuración adicional.

   - En Nombre de base de datos inicial, elija un nombre para la instancia de base de datos.
   - En la lista desplegable del grupo de parámetros de bases de datos, seleccione el nombre del grupo de parámetros personalizados que ha creado anteriormente.
   - En la lista desplegable Grupo de opciones, seleccione el nombre del nuevo grupo de opciones que ha creado anteriormente.

7. Para este tutorial, puede dejar la configuración predeterminada para cualquier otro ajuste de la base de datos o modificarla según se requiera.
8. Elija Creación de base de datos.

RDS crea una nueva instancia de base de datos de MySQL con un grupo de parámetros personalizado y un nuevo grupo de opciones. Para obtener más información sobre esta base de datos, consulte la página Bases de datos de la consola de Amazon RDS.

En este tutorial, ha configurado una instancia de base de datos de MySQL con ajustes personalizados mediante un grupo de parámetros personalizados y un nuevo grupo de opciones. Esta instancia de base de datos de MySQL de reciente creación administra la duración de la contraseña del usuario mediante el parámetro `default_password_lifetime`. Esta instancia de base de datos también desconecta a los usuarios que se conectan con una contraseña caducada mediante el parámetro `disconnect_on_expired_password`. También se utiliza la opción `MariaDB Audit Plugin` para hacer un seguimiento de la actividad del servidor. Para optimizar la base de datos, puede aplicar una configuración adicional al grupo de parámetros personalizados y agregar opciones.

Cuando haya terminado de crear el clúster de bases de datos personalizado, debe eliminar los recursos para evitar incurrir en costos no deseados. Para eliminar una instancia de base de datos, siga las instrucciones que se indican en Eliminación de una instancia de base de datos.

Administración de una instancia de base de datos de Amazon RDS

A continuación, encontrará instrucciones para administrar y mantener su instancia de base de datos de Amazon RDS.

Temas

- Parada de una instancia de base de datos de Amazon RDS temporalmente
- Inicio de una instancia de base de datos de Amazon RDS parada previamente
- Reinicio de una instancia de base de datos
- Conexión automática de una instancia de EC2 y una instancia de base de datos
- Conexión automática de una función de Lambda y una instancia de base de datos
- Modificación de una instancia de base de datos de Amazon RDS
- Mantenimiento de una instancia de base de datos
- Actualización de una versión del motor de una instancia de base de datos
- Cambio del nombre de una instancia de base de datos
- Trabajo con réplicas de lectura de instancias de base de datos
- Etiquetado de los recursos de y Amazon RDS
- Nombres de recursos de Amazon (ARN) en Amazon RDS
- Uso de almacenamiento para instancias de base de datos de Amazon RDS
- Eliminación de una instancia de base de datos
- Tutorial: Administración de un entorno de instancias de base de datos de MySQL desde el desarrollo hasta la producción

Parada de una instancia de base de datos de Amazon RDS temporalmente

Puede detener la instancia de base de datos de forma intermitente para pruebas temporales o para una actividad de desarrollo diaria, durante un máximo de 7 días consecutivos. El caso de uso más común es la optimización de costos.

El tiempo necesario para detener la instancia de base de datos varía en función de factores como la clase de instancia, el estado de la red, el tipo de motor de base de datos y el estado de la base de datos. El proceso puede durar varios minutos. El servicio debe realizar las siguientes acciones:

- Cerrar los procesos del motor de base de datos.
- Cerrar los procesos de la plataforma RDS.
- Separar los volúmenes de almacenamiento de EBS asociados a su instancia de base de datos.
- Finalizar la instancia de Amazon EC2 subyacente.

> **Warning**
>
> El inicio de una instancia de base de datos requiere la recuperación de la instancia y puede tardar desde unos minutos hasta algunas horas. Por lo tanto, si la disponibilidad de la instancia es un problema, tenga cuidado de no detener temporalmente una instancia de producción. Para obtener más información, consulte Inicio de una instancia de base de datos de Amazon RDS parada previamente.

Para detener e iniciar su instancia de base de datos en la misma operación, reinicie la instancia de base de datos. Para obtener más información, consulte Reinicio de una instancia de base de datos.

Temas

- Casos de uso para detener la instancia de base de datos
- Motores de base de datos, clases de instancia y regiones compatibles
- Detención de una instancia de base de datos en una implementación Multi-AZ
- Detención de una instancia de base de datos
- Limitaciones de la detención de la instancia de base de datos
- Consideraciones relativas al grupo de parámetros y al grupo de opciones

- Observaciones sobre direcciones IP públicas
- Parada de una instancia de base de datos temporalmente: pasos básicos

Casos de uso para detener la instancia de base de datos

Detener e iniciar una instancia de base de datos es más rápido que crear una instantánea de base de datos, detener la instancia de base de datos y, luego, restaurar la instantánea cuando desea acceder a la instancia. Estos son algunos casos de uso comunes para detener una instancia.

- Optimización de costos: en las bases de datos que no son de producción, puede parar su instancia de base de datos de Amazon RDS temporalmente para ahorrar dinero. Mientras la instancia esté detenida, no le cobrarán las horas de instancia de base de datos.

  > **Important**
  >
  > Mientras su instancia de base de datos esté detenida, se le cobrará por el almacenamiento provisionado (incluyendo las IOPS provisionadas). También se le cobra el almacenamiento de las copias de seguridad, incluidas las instantáneas manuales y las copias de seguridad automatizadas en el periodo de retención especificado. Sin embargo, no le cobrarán las horas de instancia de base de datos. Para obtener más información, consulte Preguntas frecuentes sobre facturación.

- Desarrollo diario: si mantiene una instancia de base de datos con fines de desarrollo, puede iniciarla cuando la necesite y cerrarla cuando no la necesite.
- Pruebas: es posible que necesite una instancia de base de datos temporal para probar los procedimientos de copia de seguridad y recuperación, las migraciones, las actualizaciones de aplicaciones o las actividades relacionadas. En estos casos de uso, puede detener la instancia de base de datos cuando no la necesite.
- Formación: si está realizando una formación en RDS, es posible que tenga que iniciar las instancias de base de datos durante la sesión de formación y cerrarlas después.

Motores de base de datos, clases de instancia y regiones compatibles

Puede detener e iniciar instancias de base de datos de Amazon RDS que estén ejecutando los siguientes motores:

- Db2

- MariaDB
- Microsoft SQL Server, como RDS Custom para SQL Server
- MySQL
- Oracle
- PostgreSQL

Parar e iniciar una instancia de base de datos es compatible con todas las clases de instancia de base de datos y todas las regiones de AWS.

Detención de una instancia de base de datos en una implementación Multi-AZ

Puede parar e iniciar una instancia de base de datos en una implementación multi-AZ. Presenta las siguientes limitaciones:

- Solo se puede crear una implementación Multi-AZ si su motor de base de datos lo admite. Para obtener más información sobre la compatibilidad de los motores, consulte Regiones y motores de base de datos admitidos para clústeres de bases de datos Multi-AZ en Amazon RDS.
- RDS para SQL Server no permite la detención de una instancia de base de datos en una implementación multi-AZ. Para obtener más información, consulte Limitaciones, notas y recomendaciones relativas a las implementaciones Multi-AZ de Microsoft SQL Server.
- Puede que se necesite mucho tiempo para detener una instancia de base de datos. Si dispone de al menos una copia de seguridad tras una conmutación por error anterior, puede acelerar la operación de parada realizando un reinicio con conmutación por error. Para obtener más información, consulte Reinicio de una instancia de base de datos.

Detención de una instancia de base de datos

La operación de detención se realiza en las siguientes etapas:

1. La instancia de base de datos inicia el proceso de apagado normal.

   El estado de la instancia de base de datos cambia a `stopping`.
2. La instancia deja de ejecutarse hasta un máximo de 7 días consecutivos.

   El estado de la instancia de base de datos cambia a `stopped`.

Características de una instancia de base de datos detenida

Cuando se encuentra detenida, la instancia de base de datos tiene las siguientes características:

- Cuando se detiene una instancia de base de datos, conserva lo siguiente:
  - ID de instancia
  - Punto de conexión del servidor de nombres de dominio (DNS)
  - Grupo de parámetros
  - Grupo de seguridad
  - Option group (Grupo de opciones)
  - Registros de transacciones de Amazon S3 (necesarios para una restauración a un momento dado)

  Al reiniciar una instancia de base de datos, tiene la misma configuración que al detenerla.
- Los volúmenes de almacenamiento siguen adjuntos a la instancia de base de datos y sus datos se conservan. RDS elimina los datos almacenados en la RAM de la instancia de base de datos.

  Mientras su instancia de base de datos esté detenida, se le cobrará por el almacenamiento provisionado (incluyendo las IOPS provisionadas). También se le cobra el almacenamiento de las copias de seguridad, incluidas las instantáneas manuales y las copias de seguridad automatizadas en el periodo de retención especificado.
- RDS elimina las acciones pendientes, incluidas las actualizaciones de mantenimiento programado, excepto las acciones pendientes para el grupo de opción o el grupo de parámetros de la base de datos de la instancia de base de datos.

> **Note**
>
> En ocasiones, una instancia de base de datos de RDS for PostgreSQL no se cierra de forma limpia. Si esto sucede, verá que la instancia pasa por un proceso de recuperación cuando la reinicia más tarde. Este es el comportamiento esperado del motor de base de datos, destinado a proteger la integridad de la base de datos. Algunas estadísticas y contadores basados en memoria no retienen el historial y se vuelven a iniciar tras el reinicio para capturar la carga de trabajo operativa en el futuro.

Reinicio automático de una instancia de base de datos detenida

Si no inicia manualmente la instancia de base de datos después de que haya estado detenida durante siete días consecutivos, RDS inicia automáticamente la instancia de base de datos. De esta forma, la instancia no se queda rezagada con respecto a las actualizaciones de mantenimiento necesarias. Para obtener información sobre cómo detener e iniciar la instancia según un cronograma, consulte ¿Cómo puedo utilizar Step Functions para detener una instancia de Amazon RDS por más de 7 días?.

Limitaciones de la detención de la instancia de base de datos

A continuación, se indican algunas limitaciones de la detención:

- No puede detener una instancia de base de datos que tenga una réplica de lectura o que sea una réplica de lectura.
- No puede modificar una instancia de base de datos detenida.
- Un grupo de opciones asociado a una instancia de base de datos detenida no se puede eliminar.
- No puede eliminar un grupo de parámetros de base de datos que esté asociado con una instancia de base de datos detenida.
- En una implementación Multi-AZ, tenga en cuenta las siguientes limitaciones:
  - No puede detener una instancia de base de datos de RDS para SQL Server.
  - Las zonas de disponibilidad principales y secundarias se pueden cambiar después de iniciar la instancia de base de datos.

Hay limitaciones adicionales para RDS Custom para SQL Server. Para obtener más información, consulte Iniciar y detener una instancia de base de datos de RDS Custom para SQL Server.

Consideraciones relativas al grupo de parámetros y al grupo de opciones

No se pueden eliminar las opciones persistentes (incluidas las opciones permanentes) de un grupo de opciones si hay instancias de base de datos asociadas con ese grupo de opciones. Esta funcionalidad se da también en el caso de las instancias de base de datos con un estado de `stopping`, `stopped` o `starting`.

Puede cambiar el grupo de opciones o el grupo de parámetros de la base de datos que está asociado a una instancia de la base de datos detenida. Sin embargo, el cambio no se produce hasta la próxima vez que inicia la instancia de base de datos. Si elige aplicar los cambios inmediatamente,

el cambio se produce al iniciar la instancia de base de datos. De lo contrario, el cambio se produce durante la siguiente ventana de mantenimiento una vez que el usuario inicia la instancia de base de datos.

Observaciones sobre direcciones IP públicas

Cuando se detiene la instancia de base de datos, esta retiene el punto de enlace DNS. Si se detiene una instancia de base de datos que tiene una dirección IP pública, Amazon RDS informa la dirección IP pública. Cuando se reinicia la instancia de base de datos, esta tiene una dirección IP pública diferente.

> **Note**
>
> Siempre debe conectarse a una instancia de base de datos usando el punto de enlace DNS, no la dirección IP.

Parada de una instancia de base de datos temporalmente: pasos básicos

Puede detener una base de datos mediante la AWS Management Console, la AWS CLI, o la API de RDS.

Consola

Para detener una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desea detener.
3. En Actions (Acciones), elija Stop temporarily (Detener temporalmente).
4. En la ventana Stop DB instance temporarily (Detener temporalmente la instancia de base de datos), seleccione la confirmación de que la instancia de base de datos se reiniciará automáticamente a los 7 días.
5. (Opcional) Seleccione Save the DB instance in a snapshot (Guardar la instancia de base de datos en una instantánea) e introduzca el nombre de la instantánea en Snapshot name (Nombre de instantánea). Elija esta opción si desea crear una instantánea de la instancia de base de datos antes de detenerla.

6. Elija Stop temporarily (Detener temporalmente) para detener la instancia de base de datos o elija Cancel (Cancelar) para cancelar la operación.

AWS CLI

Para detener una instancia de base de datos con la AWS CLI, llame al comando stop-db-instance con los siguientes parámetros:

- `--db-instance-identifier`: nombre de la instancia de base de datos.

Example

```
aws rds stop-db-instance --db-instance-identifier mydbinstance
```

API de RDS

Para detener una instancia de base de datos con la API de Amazon RDS, llame a la operación StopDBInstance con el siguiente parámetro:

- `DBInstanceIdentifier`: nombre de la instancia de base de datos.

Inicio de una instancia de base de datos de Amazon RDS parada previamente

En este tema, se explica cómo iniciar una instancia de base de datos de Amazon RDS que se detuvo anteriormente; además, se describen los pasos necesarios y los factores más importantes para reanudar el uso de la base de datos.

Puede parar la instancia de base de datos de Amazon RDS temporalmente para ahorrar dinero. Una vez detenida la instancia, puede reiniciarla para usarla de nuevo. Para obtener más información sobre cómo detener una instancia de base de datos, consulte Parada de una instancia de base de datos de Amazon RDS temporalmente.

Al iniciar una instancia de base de datos parada previamente, esta retiene datos como los siguientes:

- ID de instancia
- Punto de conexión del servidor de nombres de dominio (DNS)
- Grupo de parámetros de base de datos
- VPC security group (Grupo de seguridad de VPC)
- Grupo de opciones de base de datos

Amazon RDS factura las instancias de bases de datos y el almacenamiento adjunto en incrementos de un segundo. Hay un cargo mínimo de 10 minutos cuando se inicia una instancia.

Para iniciar la instancia, el servicio de Amazon RDS realiza acciones como las siguientes:

- Aprovisionamiento de la instancia de Amazon EC2 subyacente
- Inicio de los procesos de RDS
- Inicio de los procesos del motor de base de datos
- Adjuntado de los volúmenes de almacenamiento de EBS
- Habilitación de Información de rendimiento si estaba habilitada anteriormente
- Recuperación de las instancias de base de datos (la recuperación ocurre incluso después de un apagado normal)

El tiempo necesario para iniciar la instancia de base de datos varía en función de factores como la clase de instancia, el estado de la red, el tipo de motor de base de datos, el tamaño de base de datos

y el estado de la base de datos en el momento en el que se cerró la instancia. El proceso de inicio puede tardar desde unos minutos hasta algunas horas. Le recomendamos que tenga en cuenta la variabilidad del tiempo de inicio al crear el plan de disponibilidad.

Consola

Para iniciar una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee iniciar.
3. En Actions (Acciones), elija Start (Iniciar).

AWS CLI

Para iniciar una instancia de base de datos con la AWS CLI, llame al comando start-db-instance con los siguientes parámetros:

- `--db-instance-identifier`El nombre de la instancia de base de datos.

Example

```
aws rds start-db-instance --db-instance-identifier mydbinstance
```

API de RDS

Para iniciar una instancia de base de datos con la API de Amazon RDS, llame a la operación StartDBInstance con los siguientes parámetros:

- `DBInstanceIdentifier`El nombre de la instancia de base de datos.

Reinicio de una instancia de base de datos

Puede detener e iniciar el servicio de base de datos en la instancia de base de datos de RDS en una sola operación, denominada reinicio. Quizá sea necesario reiniciar para aplicar los cambios en la configuración, solucionar problemas menores o resolver problemas de red sin tener que realizar un reinicio completo o una migración de la base de datos.

> **Note**
>
> Este tema solo se aplica al reinicio de una instancia de base de datos single-AZ o multi-AZ. Para obtener instrucciones sobre el reinicio de un clúster de base de datos Multi-AZ, consulte the section called “Reinicio de un clúster de base de datos Multi-AZ”.

Temas

- Casos de uso para el reinicio de una instancia de base de datos
- Cómo funciona el reinicio de una instancia de base de datos
- Cómo funciona el reinicio de una instancia de base de datos en una implementación multi-AZ
- Observaciones sobre el reinicio de una instancia de base de datos
- Requisitos previos para el reinicio de una instancia de base de datos
- Reinicio de una instancia de base de datos : pasos básicos

Casos de uso para el reinicio de una instancia de base de datos

Normalmente, efectúa el reinicio de una instancia de base de datos por motivos de mantenimiento para que los cambios entren en vigor. Estos son algunos casos de uso comunes:

- Asociación a un nuevo grupo de parámetros: al asociar un nuevo grupo de parámetros de base de datos con una instancia de base de datos, RDS aplica los parámetros estáticos y dinámicos modificados solo después de reiniciar la instancia de base de datos. Sin embargo, si modifica los parámetros dinámicos en el grupo de parámetros de base de datos después de asociarlos a la instancia de base de datos, dichos cambios se aplican inmediatamente sin reiniciar. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
- Aplicar un cambio a un parámetro estático de un grupo de parámetros de base de datos existente: al cambiar un parámetro estático y guardar el grupo de parámetros de base de datos, el estado

de las instancias de base de datos asociadas a este grupo de parámetros en la consola cambia a pending-reboot. El cambio de parámetro solo entra en vigor después de reiniciar las instancias de base de datos asociadas. Al cambiar un parámetro dinámico en un grupo de parámetros existente, el cambio se aplica, de forma predeterminada, inmediatamente, sin necesidad de reiniciar.

> **Note**
>
> El estado pending-reboot no genera un reinicio automático durante la siguiente ventana de mantenimiento. Para aplicar los cambios de parámetros más recientes en su instancia de base de datos, reinicie manualmente la instancia de base de datos. Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

- Solución de problemas: es posible que se produzcan problemas de rendimiento u otros problemas operativos que requieran un reinicio. Por ejemplo, es posible que la instancia de base de datos no responda.

Cómo funciona el reinicio de una instancia de base de datos

Cuando Amazon RDS reinicia la instancia de base de datos, realiza las siguientes tareas secuenciales:

1. Detiene el servicio de base de datos en la instancia de base de datos
2. Inicia el servicio de base de datos en la instancia de base de datos

El proceso de reinicio provoca una breve interrupción. Durante esta interrupción, el estado de la instancia de base de datos es reiniciando. Se produce una interrupción tanto en una implementación Single-AZ como en una implementación de instancia de base de datos Multi-AZ, incluso cuando se reinicia con una conmutación por error.

Cómo funciona el reinicio de una instancia de base de datos en una implementación multi-AZ

Si la instancia de base de datos de Amazon RDS se encuentra en una implementación multi-AZ, puede reiniciar con conmutación por error. Esta operación resulta útil para simular un error en una instancia de base de datos o restaurar operaciones en la zona de disponibilidad original después de una conmutación por error.

Durante el reinicio mediante conmutación con error, Amazon RDS realiza lo siguiente:

- Interrumpe bruscamente la base de datos. Es posible que la instancia de base de datos y sus sesiones de cliente no tengan tiempo de apagarse correctamente.

  > **Warning**
  >
  > Para evitar la posibilidad de pérdida de datos, recomendamos detener las transacciones en la instancia de base de datos antes de reiniciar con una conmutación por error.

- Realiza una recuperación de bloqueo de la base de datos si es necesario.
- Cambia automáticamente a una réplica en espera en otra zona de disponibilidad. Es posible que el cambio de zona de disponibilidad no se refleje en la AWS Management Console, en las llamadas a la AWS CLI ni en la API de RDS durante algunos minutos.
- Actualiza el registro DNS de la instancia de base de datos para que apunte a la instancia de base de datos en espera. Como consecuencia, es necesario eliminar y restablecer las conexiones existentes a la instancia de base de datos. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.
- Crea un evento de Amazon RDS tras el reinicio.

En RDS para Microsoft SQL Server, la conmutación por error reinicia solo la instancia de base de datos principal. Después de la conmutación por error, la instancia de base de datos principal se convierte en la nueva instancia de base de datos secundaria. Puede que no se actualicen los parámetros para instancias Multi-AZ. Para el reinicio sin conmutación por error, las instancias de base de datos primaria y secundaria se reinician y los parámetros se actualizan después del reinicio. Si la instancia de base de datos no responde, se recomienda reiniciar sin conmutación por error.

Observaciones sobre el reinicio de una instancia de base de datos

Antes de reiniciar la instancia, tenga en cuenta lo siguiente:

- Para una instancia de base de datos con réplicas de lectura, puede reiniciar la instancia de base de datos de origen y sus réplicas de lectura de forma independiente. Cuando se complete el reinicio, la replicación se reanuda automáticamente.
- El tiempo de reinicio depende del proceso de recuperación de fallos, la actividad de la base de datos en el momento del reinicio y el comportamiento del motor de base de datos específico. Para mejorar el tiempo de reinicio, recomendamos reducir la actividad de la base de datos tanto

como sea posible durante el reinicio. Esta técnica reduce la actividad de restauración para las transacciones en tránsito.

Requisitos previos para el reinicio de una instancia de base de datos

Asegúrese de cumplir los siguientes requisitos previos:

- Su instancia de base de datos debe tener el estado `available`. Su base de datos puede no estar disponible por varias razones, como una copia de seguridad en curso, una modificación solicitada anteriormente o una operación durante un periodo de mantenimiento.
- Si fuerza una conmutación por error a una zona de disponibilidad diferente, la instancia de base de datos debe estar configurada para multi-AZ.
- Si fuerza una conmutación por error a una zona de disponibilidad diferente, le recomendamos que primero detenga las transacciones en su instancia de base de datos para evitar una posible pérdida de datos.

Reinicio de una instancia de base de datos : pasos básicos

Puede reiniciar la instancia de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para reiniciar una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee reiniciar.
3. Para Actions (Acciones), elija Reboot (Reiniciar).

   Aparece la página Reiniciar instancia de base de datos.
4. (Opcional) Seleccione Reboot with failover? (¿Reiniciar con conmutación por error?) para forzar una conmutación por error de una AZ a otra.
5. Elija Reboot para reiniciar su instancia de base de datos.

   O bien, elija Cancel.

AWS CLI

Para reiniciar una instancia de base de datos mediante la AWS CLI, llame al comando `reboot-db-instance`.

Example Reinicio sencillo

Para Linux, macOS o Unix:

```
aws rds reboot-db-instance \
    --db-instance-identifier mydbinstance
```

Para Windows:

```
aws rds reboot-db-instance ^
    --db-instance-identifier mydbinstance
```

Example Reinicio con conmutación por error

Para forzar una conmutación por error de una zona de disponibilidad a otra en un clúster de base de datos multi-AZ, utilice el parámetro `--force-failover`.

Para Linux, macOS o Unix:

```
aws rds reboot-db-instance \
    --db-instance-identifier mydbinstance \
    --force-failover
```

Para Windows:

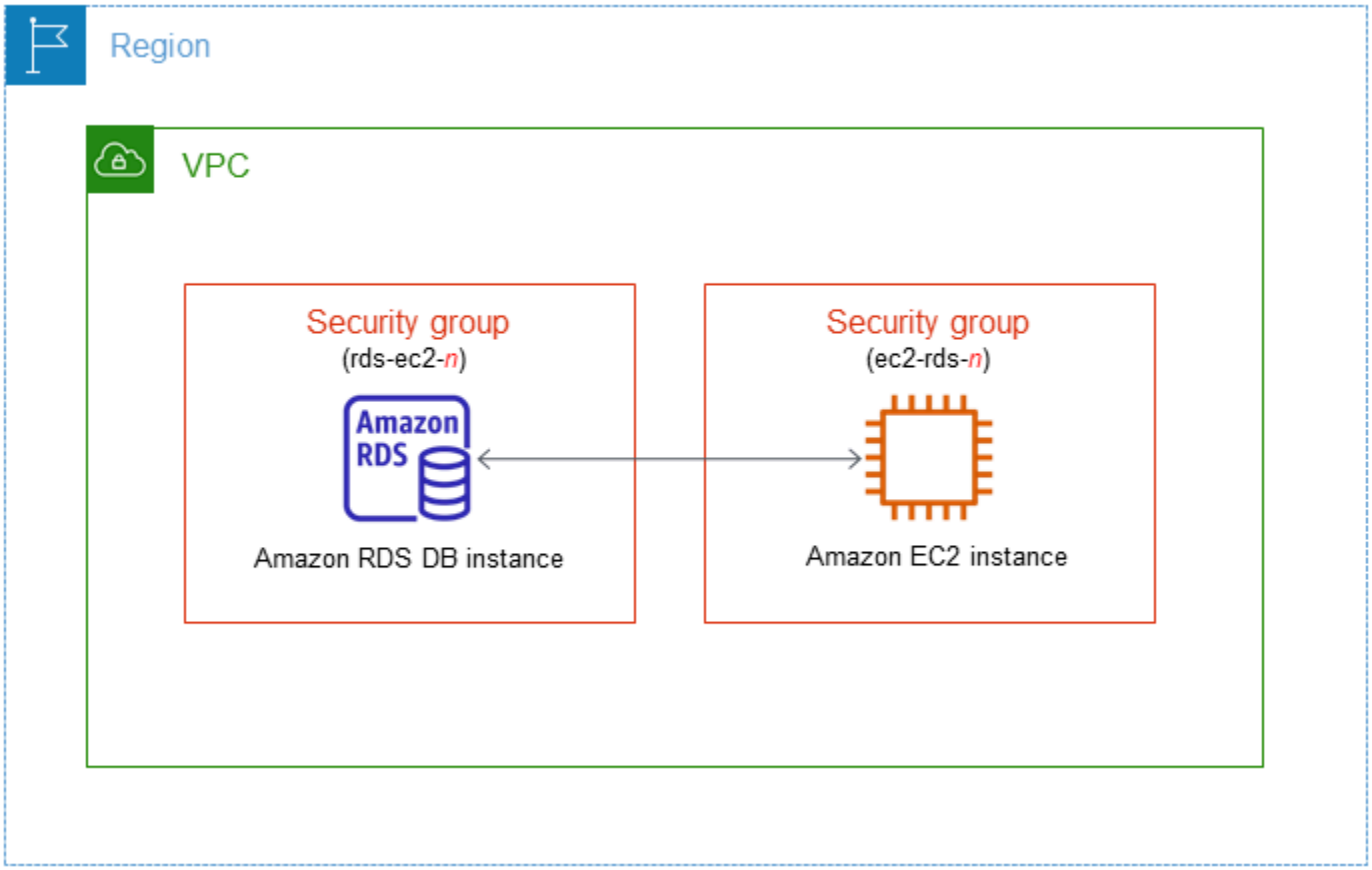
```
aws rds reboot-db-instance ^
    --db-instance-identifier mydbinstance ^
    --force-failover
```

API de RDS

Para reiniciar una instancia de base de datos mediante la Amazon RDS API, llame a la `RebootDBInstance` operación.

Conexión automática de una instancia de EC2 y una instancia de base de datos

Puede utilizar la consola de Amazon RDS para simplificar la configuración de una conexión entre una instancia de Amazon Elastic Compute Cloud (Amazon EC2) y una instancia de base de datos. A menudo, la instancia de base de datos se encuentra en una subred privada y la instancia de EC2 en una subred pública dentro de una VPC. Puede usar un cliente SQL en su instancia de EC2 para conectarse a la instancia de base de datos. La instancia de EC2 también puede ejecutar servidores web o aplicaciones que accedan a la instancia de base de datos privada. Para obtener instrucciones sobre la configuración de una conexión entre una instancia de EC2 y un clúster de base de datos Multi-AZ, consulte the section called “Conexión de una instancia de EC2 con un clúster de base de datos Multi-AZ”.



Si desea conectarse a una instancia de EC2 que no esté en la misma VPC que la instancia de base de datos, consulte los escenarios en Escenarios de acceso a una instancia de base de datos en una VPC.

Temas

- Descripción general de la conectividad automática con una instancia de EC2
- Conexión automática de una instancia de EC2 y una base de datos de RDS
- Visualización de los recursos de computación conectados
- Conexión a una instancia de base de datos que ejecuta un motor de base de datos específico

Descripción general de la conectividad automática con una instancia de EC2

Cuando se configura una conexión entre una instancia EC2 y una base de datos de RDS, Amazon RDS configura automáticamente el grupo de seguridad de la VPC para su instancia EC2 y su base de datos de RDS.

Estos son los requisitos para conectar una instancia de EC2 a una base de datos de RDS:

- La instancia de EC2 debe existir en la misma VPC que la base de datos de RDS.

  Si no existen instancias de EC2 en la misma VPC, la consola proporciona un enlace para crear una.
- El usuario que establece la conectividad debe tener permisos para realizar las siguientes operaciones de Amazon EC2:
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeSecurityGroups`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Si la instancia de la base de datos y la instancia de EC2 se encuentran en diferentes zonas de disponibilidad, su cuenta podría incurrir en costos cruzados de la zona de disponibilidad.

Cuando se establece una conexión con una instancia de EC2, Amazon RDS realiza una acción basada en la configuración actual de los grupos de seguridad asociados a la base de datos de RDS y la instancia de EC2, como se describe en la siguiente tabla.

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n* (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen.	Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `ec2-rds-`*n* (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de la base de datos de RDS como origen.	RDS no realiza ninguna acción. Ya se configuró automátic amente una conexión entre la instancia de EC2 y la base de datos de RDS. Como ya existe una conexión entre la instancia de EC2 y la base de datos de RDS, los grupos de seguridad no se modifican.
Se aplica alguna de las siguientes condiciones: • Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n*. • Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de EC2. Amazon RDS no puede usar un grupo de seguridad que no	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la instancia de EC2 con un nombre que coincida con el patrón `ec2-rds-`*n*. • Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `ec2-rds-`*n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la base de datos de RDS. Amazon RDS no puede usar un grupo de seguridad	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
tenga una regla de entrada con el grupo de seguridad de la VPC de la instancia de EC2 como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado. Los ejemplos de modificaciones incluyen agregar una regla o cambiar el puerto de una regla existente.	que no tenga una regla de salida con el grupo de seguridad de la VPC de la base de datos de RDS como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	
Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen.	Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `ec2-rds-`*n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la base de datos de RDS. Amazon RDS no puede usar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC de la base de datos de RDS como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen.	Existe un grupo de seguridad de EC2 válido para la conexión, pero no está asociado a la instancia de EC2. Este grupo de seguridad tiene un nombre que coincide con el patrón `ec2-rds-`*n*. No se ha modificado. Solo tiene una regla de salida con el grupo de seguridad de la base de datos de RDS como origen.	RDS action: associate EC2 security group

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Se aplica alguna de las siguientes condiciones: • Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n*. • Hay uno o más grupos de seguridad asociados a la base de datos de RDS con un nombre que coincide con el patrón `rds-ec2-`*n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de EC2. Amazon RDS no puede usar un grupo de seguridad que no tenga una regla de entrada con el grupo de seguridad de la VPC de la instancia de EC2 como origen. Amazon RDS tampoco puede usar un grupo de seguridad modificado.	Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `ec2-rds-`*n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de la base de datos de RDS como origen.	RDS action: create new security groups

Acción de RDS de: crear nuevos grupos de seguridad

Amazon RDS realiza las siguientes acciones:

- Crea un nuevo grupo de seguridad que coincide con el patrón `rds-ec2-`*n*. Este grupo de seguridad tiene una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2

como origen. Este grupo de seguridad que está asociado a la base de datos de RDS y permite que la instancia de EC2 acceda a la base de datos de RDS.

- Crea un nuevo grupo de seguridad que coincide con el patrón `ec2-rds-`*n*. Este grupo de seguridad tiene una regla de salida con el grupo de seguridad de la VPC de la base de datos de RDS como destino. Este grupo de seguridad está asociado a la instancia de EC2 y permite que la instancia de EC2 envíe tráfico a la base de datos de RDS.

Acción de RDS de: asociar un grupo de seguridad EC2

Amazon RDS asocia el grupo de seguridad de EC2 válido y existente con la instancia de EC2. Este grupo de seguridad permite que la instancia de EC2 envíe tráfico a la base de datos de RDS.

Conexión automática de una instancia de EC2 y una base de datos de RDS

Antes de configurar una conexión entre una instancia de EC2 y una base de datos de RDS, asegúrese de cumplir con los requisitos descritos en Descripción general de la conectividad automática con una instancia de EC2.

Si realiza cambios en los grupos de seguridad después de configurar la conectividad, los cambios pueden afectar a la conexión entre la instancia de EC2 y la base de datos RDS.

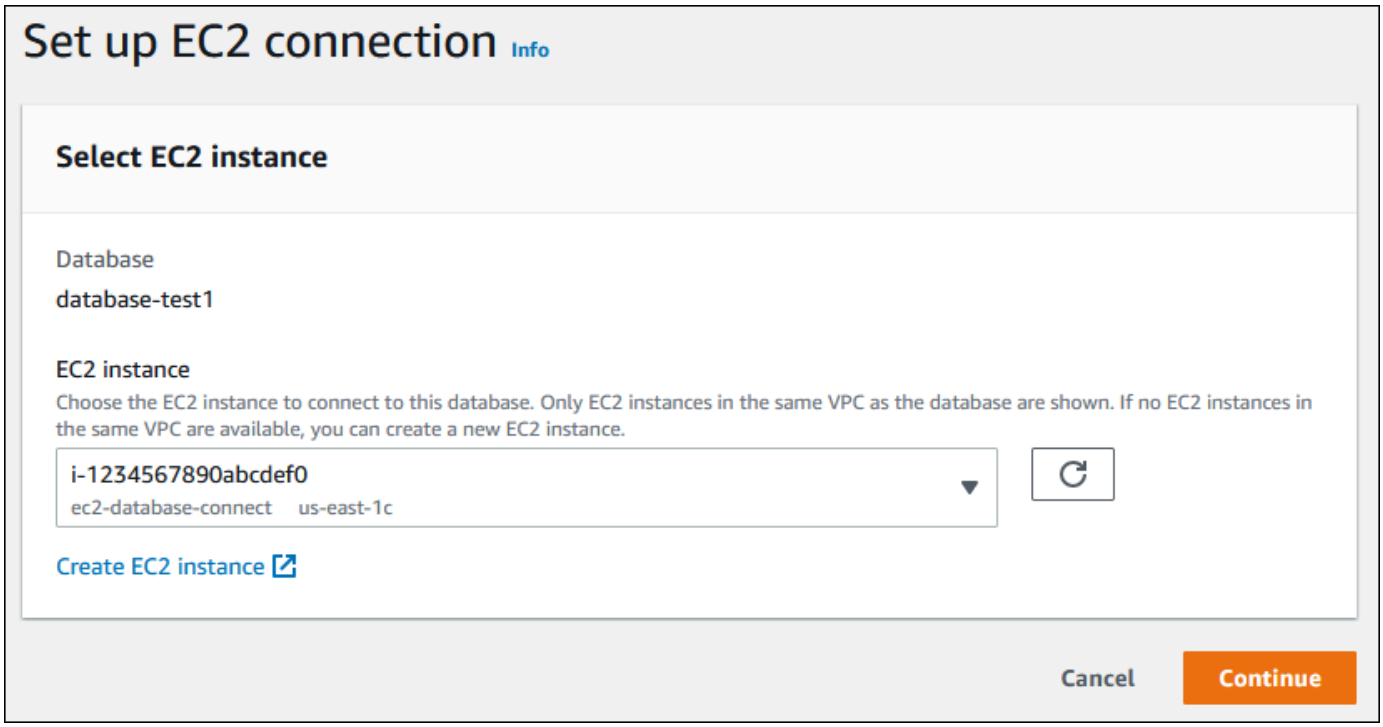
> **Note**
>
> Solo puede configurar automáticamente una conexión entre una instancia de EC2 y una base de datos de RDS automáticamente utilizando la AWS Management Console. No puede configurar una conexión automáticamente con la AWS CLI o la API de RDS.

Para conectar automáticamente de una instancia de EC2 y una base de datos de RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, luego, la instancia de base de datos.
3. En Acciones, elija Configurar conexión de EC2.

   Aparece la página Set up EC2 connection Configurar conexión de EC2).

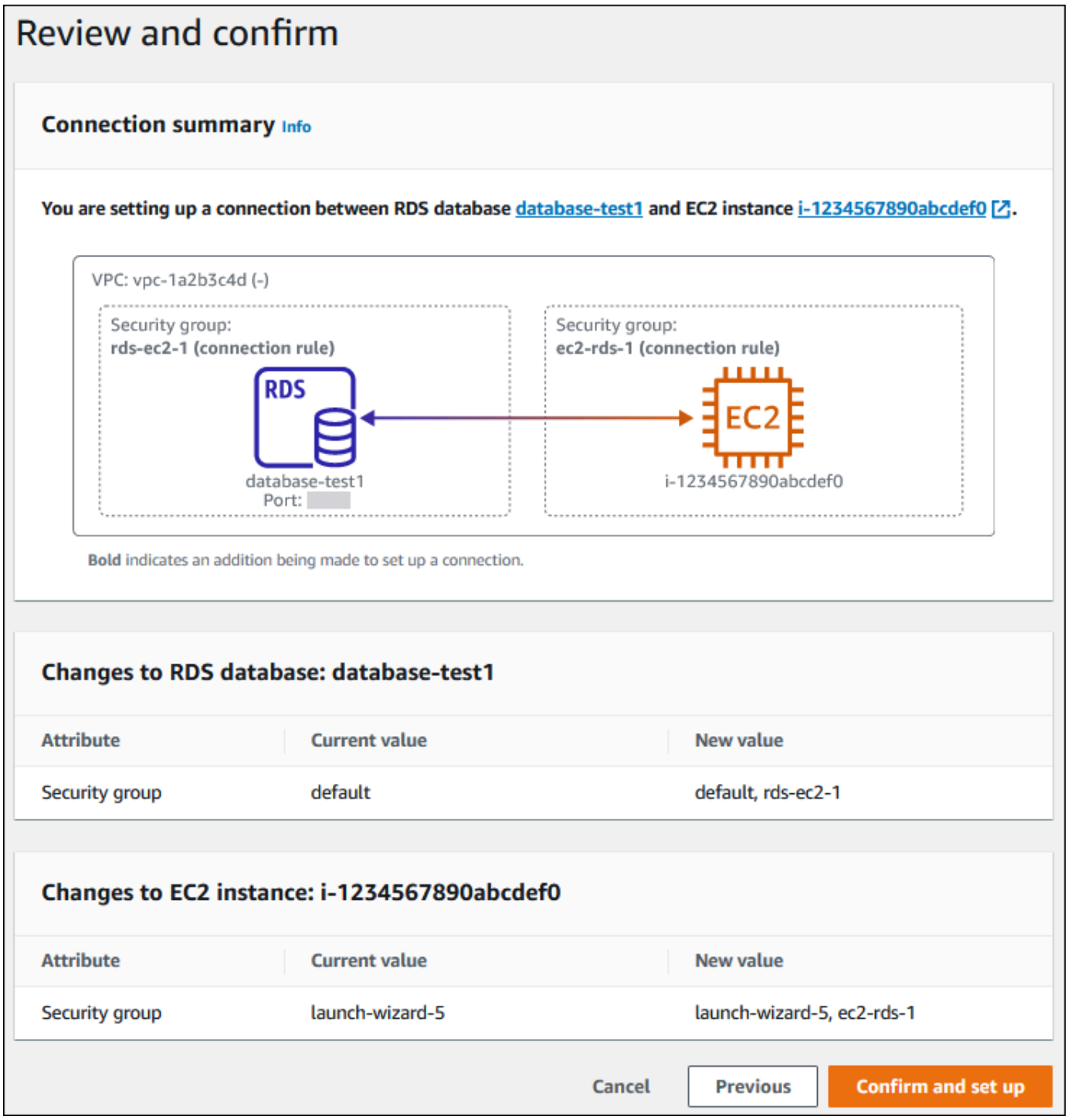
4. En la página Set up EC2 connection (Configurar conexión de EC2), elija la instancia de EC2.



   Si no existen instancias de EC2 en la misma VPC, elija Create EC2 instance (Crear instancia de EC2) para crear una. En este caso, asegúrese de que la nueva instancia de EC2 esté en la misma VPC que la base de datos de RDS.

5. Elija Continuar.

   Aparece la página Review and confirm (Revisar y confirmar).



6. En la página Review and confirm (Revisar y confirmar), revise los cambios que realizará RDS para configurar la conectividad con la instancia de EC2.

   Si los cambios son correctos, seleccione Confirmar y configurar.

   Si los cambios no son correctos, seleccione Previous (Anterior) o Cancel (Cancelar).

Visualización de los recursos de computación conectados

Puede utilizar la AWS Management Console para ver los recursos de computación que están conectados a una base de datos RDS. Los recursos que se muestran incluyen conexiones de recursos informáticos que se configuraron automáticamente. Puede definir la conectividad con los recursos informáticos de manera automática de las siguientes maneras:

- Puede seleccionar el recurso informático al crear la base de datos.

  Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS y Creación de un clúster de base de datos multi-AZ para Amazon RDS.
- Puede configurar la conectividad entre una base de datos existente y un recurso informático.

  Para obtener más información, consulte Conexión automática de una instancia de EC2 y una base de datos de RDS.

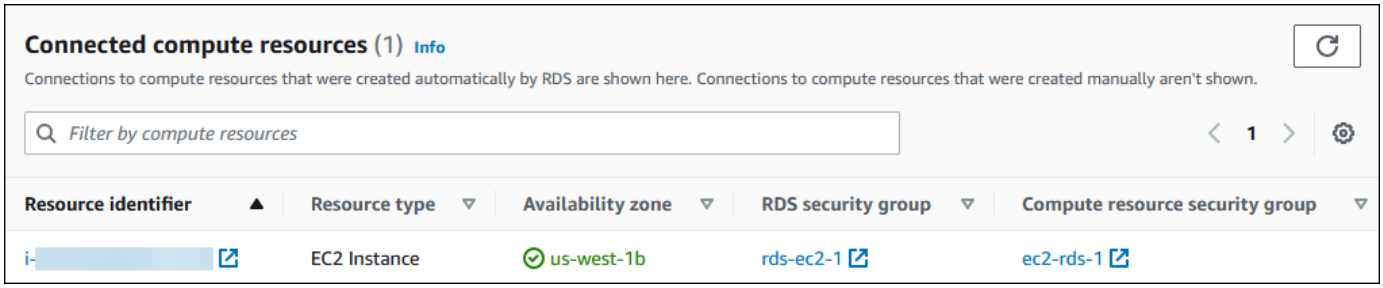
Los recursos informáticos de la lista no incluyen los que se conectaron a la base de datos manualmente. Por ejemplo, puede permitir que un recurso informático acceda a una base de datos manualmente añadiendo una regla al grupo de seguridad de la VPC asociado a la base de datos.

Para que un recurso informático coincida, se deben cumplir las siguientes condiciones:

- El nombre del grupo de seguridad asociado al recurso informático coincide con el patrón `ec2-rds-`*n* (donde *n* es un número).
- El grupo de seguridad asociado al recurso de computación tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por la base de datos RDS.
- El grupo de seguridad asociado al recurso informático tiene una regla de salida en la que el origen está establecido en un grupo de seguridad asociado a la base de datos RDS.
- El nombre del grupo de seguridad asociados a la base de datos de RDS coincide con el patrón `rds-ec2-`*n* (donde *n* es un número).
- El grupo de seguridad asociado a la base de datos de RDS tiene una regla de entrada con el rango de puertos establecido en el puerto utilizado por la base de datos de RDS.
- El grupo de seguridad asociado a la base de datos de RDS tiene una regla de entrada con el origen establecido en un grupo de seguridad asociado al recurso informático.

Para ver los recursos de computación conectados a una base de datos de RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, luego, el nombre de la instancia de base de datos.
3. En la pestaña Connectivity & security (Conectividad y seguridad), consulte los recursos informáticos en Connected compute resources (Recursos informáticos conectados).



Conexión a una instancia de base de datos que ejecuta un motor de base de datos específico

Para obtener información sobre cómo conectarse a una instancia de base de datos que ejecuta un motor de base de datos específico, siga las instrucciones para su motor de base de datos:

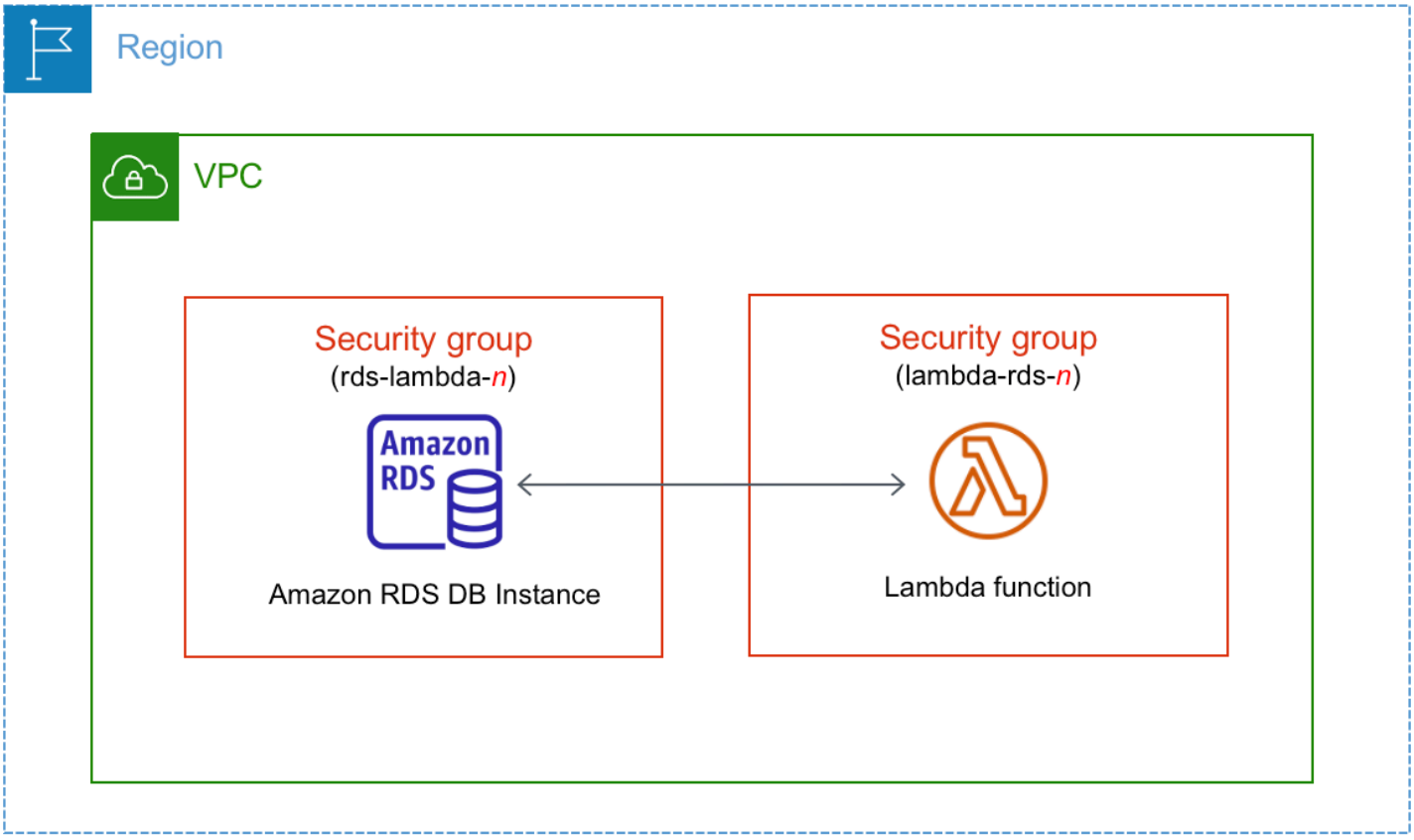
- Conexión a la instancia de base de datos de MariaDB
- Conexión a la instancia de base de datos de Microsoft SQL Server
- Conexión a la instancia de base de datos de MySQL
- Conexión a una instancia de base de datos de Oracle
- Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL

Conexión automática de una función de Lambda y una instancia de base de datos

Puede utilizar la consola de Amazon RDS para simplificar la configuración de una conexión entre una función de Lambda y una instancia de base de datos. A menudo, la instancia de base de datos se encuentra en una subred privada dentro de una VPC. Las aplicaciones pueden utilizar la función de Lambda para acceder a su instancia de base de datos privada.

Para obtener instrucciones sobre cómo configurar una conexión entre una función de Lambda y un clúster de base de datos Multi-AZ, consulte the section called “Conexión de una función de Lambda y un clúster de base de datos Multi-AZ”.

La siguiente imagen muestra una conexión directa entre su instancia de base de datos y su función de Lambda.

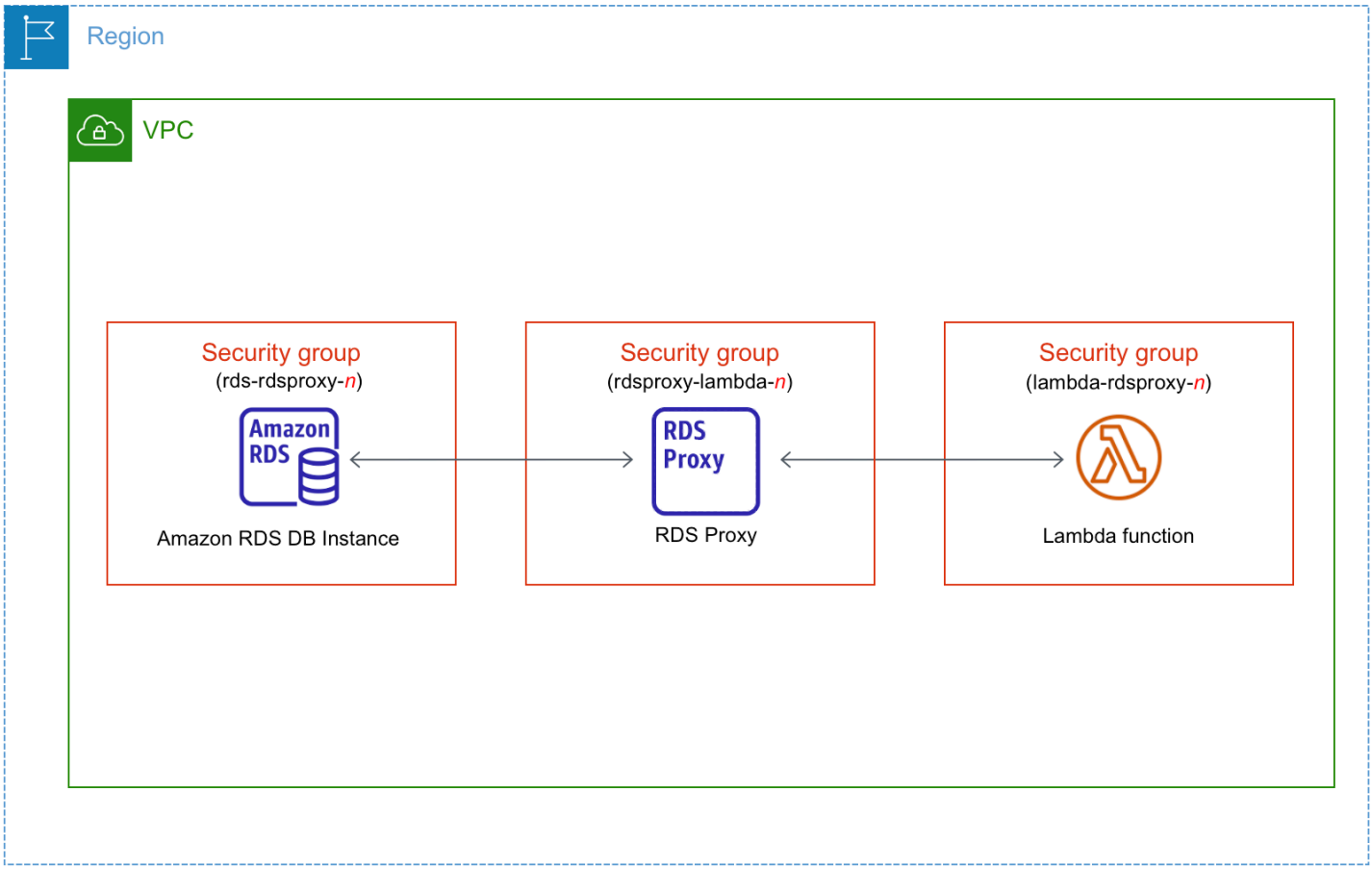


Puede configurar la conexión entre la función de Lambda y su instancia de base de datos a través de RDS Proxy para mejorar el rendimiento y la resiliencia de la base de datos. A menudo, las funciones de Lambda hacen frecuentes conexiones cortas a la base de datos que aprovechan el grupo de conexiones que ofrece RDS Proxy. Puede aprovechar cualquier autenticación de AWS Identity and

Access Management (IAM) que ya tenga para las funciones de Lambda, en lugar de administrar las credenciales de la base de datos en el código de la aplicación de Lambda. Para obtener más información, consulte Amazon RDS Proxy .

Cuando utiliza la consola para conectarse con un proxy existente, Amazon RDS actualiza el grupo de seguridad del proxy para permitir las conexiones desde su instancia de base de datos y la función de Lambda.

También puede crear un nuevo proxy desde la misma página de la consola. Al crear un proxy en la consola, para acceder a la instancia de base de datos, debe introducir las credenciales de la base de datos o seleccionar un secreto de AWS Secrets Manager.



Tip

Para conectar rápidamente una función de Lambda a una instancia de base de datos, también puede utilizar el asistente guiado integrado en la consola. Para abrir el asistente, haga lo siguiente:

1. Abra la página de Funciones en la consola de Lambda.

2. Seleccione la función a la que desea conectar una base de datos.
3. En la pestaña Configuración, seleccione Bases de datos de RDS.
4. Seleccione Conectar a la base de datos de RDS.

Después de haber conectado la función a una base de datos, podrá crear un proxy. Para ello, elija Agregar proxy.

Temas

- Información general de la conectividad automática con una función de Lambda
- Conexión automática de una función de Lambda y una base de datos de RDS
- Visualización de los recursos de computación conectados

Información general de la conectividad automática con una función de Lambda

Estos son los requisitos para conectar una función de Lambda a una base de datos de RDS:

- La función de Lambda debe encontrarse en la misma VPC que la instancia de base de datos.
- El usuario que configure la conectividad debe tener permisos para realizar las siguientes operaciones de Amazon RDS, Amazon EC2, Lambda, Secrets Manager e IAM:
  - Amazon RDS
    - `rds:CreateDBProxies`
    - `rds:DescribeDBInstances`
    - `rds:DescribeDBProxies`
    - `rds:ModifyDBInstance`
    - `rds:ModifyDBProxy`
    - `rds:RegisterProxyTargets`
  - Amazon EC2
    - `ec2:AuthorizeSecurityGroupEgress`
    - `ec2:AuthorizeSecurityGroupIngress`
    - `ec2:CreateSecurityGroup`

    - `ec2:DeleteSecurityGroup`
    - `ec2:DescribeSecurityGroups`
    - `ec2:RevokeSecurityGroupEgress`
    - `ec2:RevokeSecurityGroupIngress`
- Lambda
    - `lambda:CreateFunctions`
    - `lambda:ListFunctions`
    - `lambda:UpdateFunctionConfiguration`
- Secrets Manager
    - `secretsmanager:CreateSecret`
    - `secretsmanager:DescribeSecret`
- IAM
    - `iam:AttachPolicy`
    - `iam:CreateRole`
    - `iam:CreatePolicy`
- AWS KMS
    - `kms:describeKey`

> **Note**
>
> Si la instancia de base de datos y la función de Lambda se encuentran en diferentes zonas de disponibilidad, su cuenta podría incurrir en costes cruzados de la zona de disponibilidad.

Cuando se configura una conexión entre una función de Lambda y una base de datos de RDS, Amazon RDS configura el grupo de seguridad de la VPC para su función y su instancia de base de datos. Si usa RDS Proxy, Amazon RDS también configura el grupo de seguridad de la VPC para el proxy. Amazon RDS realiza una acción de acuerdo con la configuración actual de los grupos de seguridad asociados a la instancia de base de datos, la función de Lambda y el proxy, tal como se describe en la siguiente tabla.

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Hay uno o más grupos de seguridad asociados a la instancia de base de datos con un nombre que coincide con el patrón `rds-lambda- n` o si un proxy ya está conectado a su instancia de base de datos, RDS comprueba si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen.	Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds- n` o `lambda-rdsproxy- n` (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida bien con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como destino.	Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con el patrón `rdsproxy-lambda- n` (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene reglas de entrada y salida con los grupos de seguridad de la VPC de la función de Lambda y la instancia de base de datos.	Amazon RDS no realiza ninguna acción. Ya se configuró automáticamente una conexión entre la función de Lambda, el proxy (opcional) y la instancia de base de datos. Como ya existe una conexión entre la función, el proxy y la base de datos, los grupos de seguridad no se modifican.
Se aplica alguna de las siguientes condiciones:	Se aplica alguna de las siguientes condiciones:	Se aplica alguna de las siguientes condiciones:	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
• No hay ningún grupo de seguridad asociado a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. • Hay uno o más grupos de seguridad asociados a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. Sin embargo, ninguno de estos grupos de seguridad se puede usar para	• No hay ningún grupo de seguridad asociado a la función de Lambda con un nombre que coincida con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. • Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de base de datos. Amazon RDS no puede utilizar un grupo de seguridad que no tenga una	• No hay ningún grupo de seguridad asociado al proxy con un nombre que coincida con el patrón `rdsproxy-lambda-` *n*. • Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con `rdsproxy-lambda-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de base de datos o la función de Lambda. Amazon RDS no puede utilizar un grupo de seguridad que no tenga reglas de entrada y salida con el grupo de seguridad de la VPC	

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
la conexión con la función de Lambda. Amazon RDS no puede usar un grupo de seguridad que no tengan una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificad o. Los ejemplos de modificaciones incluyen agregar una regla o cambiar el puerto de una regla existente.	regla de salida con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como destino. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	de la instancia de base de datos y la función de Lambda. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Hay uno o más grupos de seguridad asociados a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen.	Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de base de datos. Amazon RDS no puede utilizar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como destino. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con el patrón `rdsproxy-lambda-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de base de datos o la función de Lambda. Amazon RDS no puede utilizar un grupo de seguridad que no tenga reglas de entrada y salida con el grupo de seguridad de la VPC de la instancia de base de datos y la función de Lambda. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Hay uno o más grupos de seguridad asociados a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen.	Existe un grupo de seguridad de Lambda válido para la conexión, pero no está asociado a la función de Lambda. Este grupo de seguridad tiene un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. No se ha modificado. Solo tiene una regla de salida con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como destino.	Existe un grupo de seguridad del proxy válido para la conexión, pero no está asociado al proxy. Este grupo de seguridad tiene un nombre que coincide con el patrón `rdsproxy-lambda-` *n*. No se ha modificado. Tiene reglas de entrada y salida con el grupo de seguridad de la VPC de la instancia de base de datos y la función de Lambda.	RDS action: associate Lambda security group

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda- n` o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE` . • Hay uno o más grupos de seguridad asociados a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda- n` o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE` . Sin embargo,	Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds- n` o `lambda-rdsproxy- n`. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como destino.	Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con el patrón `rdsproxy-lambda- n`. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene reglas de entrada y salida con el grupo de seguridad de la VPC de la instancia de base de datos y la función de Lambda.	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la función de Lambda o el proxy. Amazon RDS no puede usar un grupo de seguridad que no tengan una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.			

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. • Hay uno o más grupos de seguridad asociados a la instancia de base de datos con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. Sin embargo,	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la función de Lambda con un nombre que coincida con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. • Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de base de datos.	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado al proxy con un nombre que coincida con el patrón `rdsproxy-lambda-` *n*. • Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con `rdsproxy-lambda-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la instancia de base de datos o la función de Lambda. Amazon RDS no puede utilizar un grupo de seguridad	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la función de Lambda o el proxy. Amazon RDS no puede usar un grupo de seguridad que no tengan una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	Amazon RDS no puede utilizar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	que no tenga reglas de entrada y salida con el grupo de seguridad de la VPC de la instancia de base de datos y la función de Lambda. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	

Acción de RDS de: crear nuevos grupos de seguridad

Amazon RDS realiza las siguientes acciones:

- Crea un nuevo grupo de seguridad que coincide con el patrón `rds-lambda-`*n* o `rds-rdsproxy-`*n* (si elige utilizar RDS Proxy). Este grupo de seguridad tiene una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Este grupo de seguridad está asociado a la instancia de base de datos y permite que la función o el proxy accedan a la instancia de base datos.

- Crea un nuevo grupo de seguridad que coincide con el patrón `lambda-rds-`*n* o `lambda-rdsproxy-`*n*. Este grupo de seguridad tiene una regla de salida bien con el grupo de seguridad de la VPC de la instancia de base de datos o el proxy como destino. Este grupo de seguridad está asociado a la función de Lambda y permite que la función envíe tráfico a la instancia de base de datos o que envíe tráfico a través de un proxy.
- Crea un nuevo grupo de seguridad que coincide con el patrón `rdsproxy-lambda-`*n*. Este grupo de seguridad tiene reglas de entrada y salida con el grupo de seguridad de la VPC de la instancia de base de datos y la función de Lambda.

Acción de RDS : asociar un grupo de seguridad de Lambda

Amazon RDS asocia el grupo de seguridad de Lambda válido y existente a la función de Lambda. Este grupo de seguridad permite que la función envíe tráfico a la instancia de base de datos o que envíe tráfico a través de un proxy.

Conexión automática de una función de Lambda y una base de datos de RDS

Puede utilizar la consola de Amazon RDS para conectar automáticamente una función de Lambda a su instancia de base de datos. Esto simplifica el proceso de establecer una conexión entre estos recursos.

También puede usar RDS Proxy para incluir un proxy en la conexión. Las funciones de Lambda hacen frecuentes conexiones cortas a la base de datos que aprovechan el grupo de conexiones que ofrece RDS Proxy. Puede aprovechar cualquier autenticación de IAM que ya tenga para sus funciones de Lambda, en lugar de administrar las credenciales de la base de datos en el código de la aplicación de Lambda.

Puede conectar una instancia de base de datos existente a funciones de Lambda nuevas y existentes mediante la página de configuración de conexiones de Lambda. El proceso de configuración configura automáticamente los grupos de seguridad necesarios en su nombre.

Antes de configurar una conexión entre una función de Lambda y una instancia de base de datos, asegúrese de que:

- Su función de Lambda y la instancia de base de datos estén en la misma VPC.

- Tiene los permisos adecuados para su cuenta de usuario. Para obtener más información acerca de los requisitos, consulte Información general de la conectividad automática con una función de Lambda.

Si realiza cambios en los grupos de seguridad después de configurar la conectividad, los cambios podrían afectar a la conexión entre la función de Lambda y la instancia de base de datos.

> **Note**
>
> Puede configurar automáticamente una conexión entre la instancia de base de datos y una función de Lambda solo en la AWS Management Console. Para conectar una función de Lambda, la instancia de base de datos debe estar en estado Disponible.

Para conectar automáticamente una función de Lambda y una instancia de base de datos

<result>

Tras confirmar la configuración, Amazon RDS inicia el proceso de conexión de su función de Lambda, RDS Proxy (si ha utilizado un proxy) e instancia de base de datos. La consola muestra el cuadro de diálogo Detalles de la conexión, que muestra los cambios del grupo de seguridad que permiten las conexiones entre los recursos.
</result>

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, seleccione la instancia de base de datos que desea conectar a una función de Lambda.
3. En Acciones, elija Configurar la conexión de Lambda.
4. En la página Configurar la conexión de Lambda, en Seleccionar la función de Lambda, realice una de las siguientes acciones:
   - Si ya tiene una función de Lambda en la misma VPC que su instancia de base de datos, elija Elegir una función existente y, a continuación, seleccione la función.
   - Si no tiene una función de Lambda en la misma VPC, elija Crear función nueva y, a continuación, introduzca un Nombre de la función. El tiempo de ejecución predeterminado está establecido en Nodejs.18. Puede modificar la configuración de la nueva función de Lambda en la consola de Lambda después de completar la configuración de la conexión.

5. (Opcional) En RDS Proxy, seleccione Conexión mediante RDS Proxy y, a continuación, realice una de las siguientes acciones:
   - Si ya tiene un proxy que quiere usar, elija Elegir un proxy existente y, a continuación, elija el proxy.
   - Si no dispone de un proxy y desea que Amazon RDS lo cree automáticamente, elija Crear un proxy nuevo. A continuación, para Credenciales de la base de datos, realice una de las siguientes acciones:

     a. Elija Nombre de usuario y contraseña de la base de datos y, a continuación, introduzca el Nombre de usuario y la Contraseña para su instancia de base de datos.
     b. Elija Secreto de Secrets Manager. A continuación, para Seleccionar secreto, elija un secreto de AWS Secrets Manager. Si no tiene ningún secreto de Secrets Manager, elija Crear un nuevo secreto de Secrets Manager para crear un nuevo secreto. Después de crear el secreto, en Seleccionar secreto, elija el nuevo secreto.

     Después de crear el nuevo proxy, elija Elegir un proxy existente y, a continuación, elija el proxy. Tenga en cuenta que el proxy puede tardar algún tiempo en estar disponible para la conexión.
6. (Opcional) Amplíe Resumen de conexión y verifique las actualizaciones destacadas de sus recursos.
7. Elija Set up (Configurar).

Visualización de los recursos de computación conectados

Puede utilizar la AWS Management Console para ver las funciones de Lambda que están conectadas a su instancia de base de datos. Los recursos que se muestran incluyen las conexiones de los recursos de computación que Amazon RDS configuró automáticamente.

Los recursos de computación de la lista no incluyen los que se conectan manualmente a la instancia de base de datos. Por ejemplo, para permitir que un recurso de computación acceda manualmente a su instancia de base de datos puede añadir una regla al grupo de seguridad de la VPC asociado a la base de datos.

Para que la consola muestre una función de Lambda, se deben cumplir las siguientes condiciones:

- El nombre del grupo de seguridad asociado al recurso de computación coincide con el patrón `lambda-rds-`*n* o `lambda-rdsproxy-`*n* (donde *n* es un número).

- El grupo de seguridad asociado al recurso de computación tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por la instancia de base de datos o un proxy asociado. El destino de la regla de salida debe establecerse en un grupo de seguridad asociado a la instancia de base de datos o un proxy asociado.
- Si la configuración incluye un proxy, el nombre del grupo de seguridad adjunto al proxy asociado a la base de datos coincide con el patrón `rdsproxy-lambda-`*n* (donde *n* es un número).
- El grupo de seguridad asociado a la función tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por la instancia de base de datos o un proxy asociado. El destino debe establecerse en un grupo de seguridad asociado a la instancia de base de datos o un proxy asociado.

Para ver los recursos de computación conectados automáticamente a una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija la instancia de bases de datos.
3. En la pestaña Conectividad y seguridad, consulte los recursos de computación en Recursos de computación conectados.

Modificación de una instancia de base de datos de Amazon RDS

Puede cambiar la configuración de una instancia de base de datos para realizar tareas tales como añadir almacenamiento adicional o cambiar la clase de instancia de base de datos. En este tema, aprenderá a modificar una instancia de base de datos de Amazon RDS y acerca de la configuración de las instancias de base de datos.

Recomendamos que pruebe cualquier cambio en una instancia de prueba antes de modificar una instancia de producción para que pueda entender completamente el impacto de cada cambio. Esto le ayuda a comprender completamente el impacto de cada cambio. La prueba es especialmente importante al actualizar versiones de bases de datos.

La mayoría de las modificaciones realizadas en una instancia de base de datos se pueden aplicar inmediatamente o se puede posponer hasta el siguiente periodo de mantenimiento. Algunas modificaciones, como los cambios de grupo de parámetros, requieren que reinicie manualmente la instancia de base de datos para que el cambio surta efecto.

> **Important**
>
> Algunas modificaciones provocan un tiempo de inactividad porque Amazon RDS debe reiniciar la instancia de base de datos para que el cambio surta efecto. Antes de modificar la configuración de una instancia de base de datos, evalúe los efectos que puede tener en la base de datos y en las aplicaciones.

Consola

Para modificar una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify. Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. Cambie los parámetros que desee. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.
5. Cuando haya realizado todos los cambios que desee, elija Continue y compruebe el resumen de las modificaciones.

6. (Opcional) Seleccione Apply immediately (Aplicar inmediatamente) para aplicar los cambios inmediatamente. Si se selecciona esta opción, puede producirse un tiempo de inactividad en algunos casos. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.
7. En la página de confirmación, revise los cambios. Si son correctos, elija Modify DB instance (Modificar instancia de base de datos) para guardar los cambios.

   O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para modificar una instancia de base de datos mediante la AWS CLI, llame al comando modify-db-instance. Especifique el identificador de instancias de bases de datos y los valores de las opciones que desea modificar. Para obtener más información acerca de cada opción, consulte Configuración de instancias de base de datos.

Example

El siguiente código modifica `mydbinstance` configurando el período de retención de copia de seguridad en 1 semana (7 días). El código permite la protección de eliminación mediante el uso de `--deletion-protection`. Para deshabilitar la protección de eliminación, use `--no-deletion-protection`. Los cambios se aplican durante el siguiente periodo de mantenimiento si se utiliza el parámetro `--no-apply-immediately`. Utilice `--apply-immediately` para aplicar los cambios inmediatamente. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --backup-retention-period 7 \
    --deletion-protection \
    --no-apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --backup-retention-period 7 ^
```

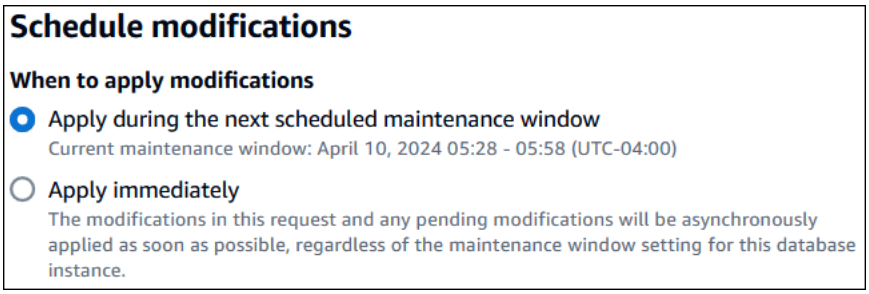
```
    --deletion-protection ^
    --no-apply-immediately
```

API de RDS

Para modificar una instancia de base de datos mediante la API de Amazon RDS, llame a la operación ModifyDBInstance. Especifique el identificador de instancias de bases de datos y los parámetros de la configuración que desea modificar. Para obtener información acerca de cada parámetro, consulte Configuración de instancias de base de datos.

Uso de la configuración de la programación de modificaciones

Al modificar la instancia de base de datos, usted decide cuándo quiere que se produzcan las modificaciones.



Para aplicar los cambios de forma inmediata en lugar de en el siguiente periodo de mantenimiento, seleccione la opción Aplicar inmediatamente en la AWS Management Console. O utilice el parámetro `--apply-immediately` al llamar a la AWS CLI o establezca el parámetro `ApplyImmediately` en `true` al usar la API de Amazon RDS.

Si decide no aplicar los cambios inmediatamente, RDS coloca estos cambios en la cola de modificaciones pendientes. RDS aplica los cambios pendientes en la cola durante el siguiente periodo de mantenimiento. Si opta por aplicar los cambios inmediatamente, se aplican los nuevos cambios y cualquier cambio de la cola de modificaciones pendientes.

Para ver las modificaciones pendientes para la siguiente ventana de mantenimiento, utilice el comando describe-db-instances de la AWS CLI y marque el campo `PendingModifiedValues`.

> **Important**
>
> Si alguna de las modificaciones pendientes requiere que la instancia de base de datos no esté disponible temporalmente (tiempo de inactividad), la elección de la opción aplicar inmediatamente puede provocar un tiempo de inactividad inesperado.

Al elegir aplicar un cambio inmediatamente, cualquier modificación pendiente se aplica también inmediatamente, en lugar de durante el siguiente periodo de mantenimiento. Si no desea que se aplique un cambio pendiente en el siguiente periodo de mantenimiento, puede modificar la instancia de base de datos para revertir el cambio. Para ello, utilice la AWS CLI y especifique la opción `--apply-immediately`.

Los cambios en algunos ajustes de la base de datos se aplican de inmediato, incluso si elige aplazarlos. Para ver cómo interactúan los distintos ajustes de la base de datos con la configuración de aplicación inmediata, consulte Configuración de instancias de base de datos.

Configuración de instancias de base de datos

En la siguiente tabla, encontrará detalles sobre qué configuración puede y no puede modificar. También podrá encontrar cuándo se pueden aplicar los cambios y si los cambios causan tiempo de inactividad en la instancia de base de datos. Con el uso de características de Amazon RDS como Multi-AZ, puede minimizar el tiempo de inactividad si modifica posteriormente la instancia de base de datos. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Puede modificar una instancia de base de datos mediante la consola, el comando de la CLI `modify-db-instance` o la operación de la API de RDS `ModifyDBInstance`.

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Allocated storage (Almacenamiento asignado) El almacenamiento, en gibibytes, que se desea asignar a la instancia de base de datos. Solo puede aumentar el almacenam	Opción de la CLI: `--allocated-storage`	Si decide aplicar el cambio inmediatamente, surte efecto	No se produce un tiempo de inactividad durante este cambio. El desempeño	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
iento asignado. No puede reducir el almacenamiento asignado. No es posible modificar el almacenamiento de algunas instancias de base de datos antiguas ni de instancias de base de datos restauradas a partir de instantáneas de base de datos antiguas. La nueva opción Allocated Storage (Almacenamiento asignado) estará desactivada en la consola si la instancia de base de datos no es elegible. Puede comprobar si puede asignar más almacenamiento mediante el comando de la CLI describe-valid-db-instance-modifications. Este comando devuelve las opciones de almacenamiento válidas para su instancia de base de datos. El almacenamiento asignado no se puede modificar si el estado de instancia de base de datos es storage-optimization. El almacenamiento asignado para una instancia de base de datos	Parámetro de la API de RDS: `AllocatedStorage`	inmediatamente. Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.	se puede degradar durante el cambio.	

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
tampoco se puede modificar durante las últimas seis horas. El máximo almacenamiento permitido depende del motor de la base de datos y el tipo de almacenamiento. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.				

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Configuración de arquitectura Una configuración que permite que varias bases de datos de inquilino residan en su instancia de base de datos. Actualmente, solo admiten esta configuración las bases de datos de contenedores (CDB) de RDS para Oracle. Si la CDB se encuentra en la configuración de un solo inquilino, puede modificarla para usar la configuración de varios inquilinos. En esta configuración, puede usar las API de RDS para crear de 1 a 30 bases de datos de inquilino, según la edición de la base de datos y las licencias opcionales requeridas. No se admiten las PDB de aplicaciones ni las PDB proxy. La configuración de varios inquilinos es permanente, lo que significa que no podrá convertir de nuevo la CDB a la configuración de un solo inquilino.	Opción de la CLI: `--multi-tenant` (configuración de varios inquilinos de la arquitectura CDB) `--no-multi-tenant` (configuración de un solo inquilino de la arquitectura CDB) Parámetro de la API: `MultiTenant`	El cambio se produce inmediatamente.	No se produce un tiempo de inactividad durante este cambio.	Oracle

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Note La configuración de Amazon RDS se denomina “de varios inquilinos”, en lugar de “multitenencia”, ya que es una capacidad de la plataforma RDS, no solo del motor de base de datos de Oracle. De manera similar, el término “inquilino” de RDS se refiere a cualquier inquilino en una configuración de RDS, no solo a las PDB de Oracle. En la documentación de RDS, el término “de varios inquilinos de Oracle” sin guion se refiere exclusivamente a la arquitectura CDB de la base de datos de Oracle, que es compatible tanto con las implementaciones en las instalaciones como con RDS.				

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Para obtener más información, consulte Descripción general de las CDB de RDS para Oracle.				

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Architecture settings (Configuración de arquitectura) Arquitectura de la base de datos de Oracle: CDB o no CDB. Si elige una arquitectura multitenencia de Oracle, RDS para Oracle convierte la base de datos no CDB en una CDB con configuración de un solo inquilino. Esta configuración solo se admite si la base de datos no es una CDB y ejecuta Oracle Database 19c con una RU de abril de 2021 o superior. Tras la conversión, la CDB contendrá una base de datos conectable (PDB). El cambio de arquitectura es permanente, lo que significa que no puede volver a convertir la CDB en una base de datos no CDB. **Note** Para convertir una CDB de un solo inquilino en una CDB con configura	Opción de la CLI: `--engine oracle-ee-cdb` (Oracle multitenencia) `--engine oracle-se2-cdb` (Oracle multitenencia) Parámetro de la API: `Engine`	Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente. Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.	Se produce un tiempo de inactividad durante este cambio.	Oracle

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
ción de varios inquilinos, modifique nuevamente la instancia de CDB y elija Configuración de varios inquilinos como Configuración de la arquitectura. Para obtener más información, consulte Configuración de un solo inquilino de la arquitectura CDB.				

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Auto minor version upgrade (Actualización automática de versiones secundarias)
 	
Elija Habilitar actualización automática de versiones secundarias para permitir que la instancia de base de datos reciba actualizaciones preferidas de la versión secundaria del motor de base de datos automáticamente cuando estén disponibles. Este es el comportamiento predeterminado. Amazon RDS realiza actualizaciones automáticas de versiones secundarias en el periodo de mantenimiento. Si no selecciona Habilitar actualización automática de versiones secundarias, la instancia de base de datos no se actualizará automáticamente cuando haya nuevas versiones secundarias disponibles.
 	
Para obtener más información, consulte Actualización automática de la versión secundaria del motor.
	Opción de la CLI:
	
	`--auto-minor-version-upgrade | --no-auto-minor-version-upgrade`
	
	Parámetro de la API de RDS:
	
	`AutoMinorVersionUpgrade`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Backup replication (Replicación de copia de seguridad) Elija Enable replication to another AWS Region (Habilitar replicación en otra región de) para crear copias de seguridad en una región adicional para la recuperación de desastres. A continuación, elija la Destination Region (Región de destino) para las copias de seguridad adicionales.	No está disponible al modificar una instancia de base de datos. Para obtener información acerca de cómo habilitar copias de seguridad en todas las regiones mediante la API de RDS o AWS CLI, consulte Habilitación de copias de seguridad automatizadas entre regiones.	El cambio se aplica de forma asíncrona, tan pronto como sea posible.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Backup retention period (Periodo de retención de copia de seguridad)
 	
El número de días que se conservan las copias de seguridad automáticas. Para desactivar las copias de seguridad automáticas, establezca período de retención de copia de seguridad en cero.
 	
Para obtener más información, consulte Introducción a las copias de seguridad.
 	
Note
Si se utiliza AWS Backup para administrar las copias de seguridad, esta opción no aparecerá. Para obtener más información AWS Backup, consulte la Guía del desarrolladorAWS de copiasde seguridad.
	Opción de la CLI:
	
	`--backup-retention-period`
	
	Parámetro de la API de RDS:
	
	`BackupRetentionPeriod`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no elige la opción de aplicar inmediatamente y cambia la configuración de un valor distinto de cero a otro valor distinto de cero, el cambio se aplica de forma asíncrona, tan pronto como sea posible. De lo contrario, el cambio se produce
			Se produce un tiempo de inactividad si se cambia el valor de cero a un valor distinto de cero o de un valor distinto de cero a cero.
			
			Esto es aplicable a las instancias de base de datos Single-AZ y Multi-AZ.
				Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
		durante el siguiente período de mantenimiento.		

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Backup window (Ventana de copìa de seguridad)
 	
El intervalo de tiempo durante el que se realizan las copias de seguridad automáticas de las bases de datos. Backup Window se expresa mediante una hora de inicio en tiempo universal coordinado (UTC) y una duración en horas.
 	
Para obtener más información, consulte Introducción a las copias de seguridad.
 	
Note
Si se utiliza AWS Backup para administrar las copias de seguridad, esta opción no aparecerá. Para obtener más información sobre AWS Backup, consulte la Guía para desarrolladores de AWS Backup.
	Opción de la CLI:
	
	`--preferred-backup-window`
	
	Parámetro de la API de RDS:
	
	`PreferredBackupWindow`
		El cambio se aplica de forma asíncrona, tan pronto como sea posible.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Certificate authority (Autoridad de certificado)
 	
Entidad de certificación (CA) del certificado de servidor que utiliza la instancia de base de datos.
 	
Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
	Opción de la CLI:
	
	`--ca-certificate-identifier`
	
	Parámetro de la API de RDS:
	
	`CACertificateIdentifier`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Solo se produce una interrupción si el motor de base de datos no admite la rotación sin reinicio. Puede utilizar el comando de la AWS CLI describe-db-engine-versions para determinar si el motor de base de datos admite la rotación sin reinicio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Copy Tags To Snapshots (Copiar etiquetas en instantáneas)
 	
Si tiene etiquetas de instancias de bases de datos, habilite esta opción para copiarlas al crear una instantánea de base de datos.
 	
Para obtener más información, consulte Etiquetado de los recursos de y Amazon RDS.
	Opción de la CLI:
	
	`--copy-tags-to-snapshot` o `--no-copy-tags-to-snapshot`
	
	Parámetro de la API de RDS:
	
	`CopyTagsToSnapshot`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Database port (Puerto de base de datos)
 	
El puerto que desea utilizar para obtener acceso a la instancia de base de datos.
 	
El valor del puerto no debe coincidir con ninguno de los valores de puertos especificados para las opciones del grupo de opciones que se asocia a la instancia de base de datos.
 	
Para obtener más información, consulte Conexión a una instancia de base de datos de Amazon RDS.
	Opción de la CLI:
	
	`--db-port-number`
	
	Parámetro de la API de RDS:
	
	`DBPortNumber`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	La instancia de base de datos se reinicia inmediatamente.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

DB engine version (Versión del motor de base de datos)
 	
La versión del motor de base de datos que desea utilizar. Antes de actualizar las instancias de bases de datos de producción, recomendamos que pruebe el proceso de actualización en una instancia de base de datos de prueba. Esto ayuda a verificar su duración y a validar las aplicaciones.
 	
Para obtener más información, consulte Actualización de una versión del motor de una instancia de base de datos.
	Opción de la CLI:
	
	`--engine-version`
	
	Parámetro de la API de RDS:
	
	`EngineVersion`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

DB instance class (Clase de instancia de base de datos)
 	
Clase de instancia de base de datos que desea utilizar.
 	
Para obtener más información, consulte Clases de instancia de base de datos de .
	Opción de la CLI:
	
	`--db-instance-class`
	
	Parámetro de la API de RDS:
	
	`DBInstanceClass`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

DB Instance Identifier (Identificador de instancias de bases de datos)
 	
El nuevo identificador de instancias de bases de datos. Este valor se almacena como una cadena en minúsculas.
 	
Para obtener más información acerca de los efectos de cambiar el nombre de una instancia de base de datos, consulte Cambio del nombre de una instancia de base de datos.
	Opción de la CLI:
	
	`--new-db-instance-identifier`
	
	Parámetro de la API de RDS:
	
	`NewDBInstanceIdentifier`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Durante este cambio, se produce un tiempo de inactividad, a menos que la versión del motor de base de datos admita la carga SSL dinámica. Para determinar si su versión requiere un reinicio, ejecute lo siguiente comanc CLI:
			
			`aws rds describe-db-engine-versions \ --default-only \ --engine your-db-engine \`
				Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
			`--query 'DBEngineVersions[*].SupportsCertificateRotationWithoutRestart'`	

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

DB Parameter Group (Grupo de parámetros de base de datos)
 	
El grupo de parámetros de la base de datos que desea asociar a la instancia de base de datos.
 	
Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
	Opción de la CLI:
	
	`--db-parameter-group-name`
	
	Parámetro de la API de RDS:
	
	`DBParameterGroupName`
		La asociación del nuevo grupo de parámetros de base de datos con la instancia de base de datos se produce de forma inmediata.	El tiempo de inactividad no se produce cuando asocia un nuevo grupo de parámetros de base de datos con su instancia de base de datos.
			
			La asociación de un grupo de parámetros de base de datos es diferente de la aplicación de cambios de parámetros dentro de un grupo de parámetros. RDS aplica la configuración modificada de los parámetros estáticos y dinámicos al
				Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
			grupo recién asociado después de reiniciar manualmente la instancia de base de datos. Sin embargo, si modifica los parámetros dinámicos en el grupo de parámetros de base de datos después de asociarlos a la instancia de base de datos, esa configuración de parámetros se aplica inmediatamente sin necesidad de reinicio. Para obtener más informaci	

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
			ón, consulte Grupos de parámetros para Amazon RDS y Reinicio de una instancia de base de datos.	

Volumen de registro específico
 	
Utilice un volumen de registro específico (DLV) para almacenar los registros de transacciones de la base de datos en un volumen de almacenamiento independiente del volumen que contiene las tablas de la base de datos.
 	
Para obtener más información, consulte Uso de un volumen de registro específico (DLV).
	Opción de la CLI:
	
	`-dedicated-log-volume`
	
	Parámetro de la API de RDS:
	
	`DedicatedLogVolume`
		El cambio se aplica después de reiniciar la instancia de base de datos.	Hay un tiempo de inactividad mientras la instancia de base de datos se reinicia.	MariaDB, MySQL, PostgreSQL

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Deletion protection (Protección contra eliminación)
 	
Seleccione Enable deletion protection (Habilitar la protección contra la eliminación) para evitar que se elimine la instancia de base de datos.
 	
Para obtener más información, consulte Eliminación de una instancia de base de datos.
	Opción de la CLI:
	
	`--deletion-protection|--no-deletion-protection`
	
	Parámetro de la API de RDS:
	
	`DeletionProtection`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Enhanced Monitoring (Supervisión mejorada)
 	
Enable enhanced monitoring (Habilitar la monitorización mejorada) para habilitar la recopilación de métricas en tiempo real para el sistema operativo en el que se ejecuta la instancia de base de datos.
 	
Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.
	Opción de la CLI:
	
	`--monitoring-interval` y `--monitoring-role-arn`
	
	Parámetro de la API de RDS:
	
	`MonitoringInterval` y `MonitoringRoleArn`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

IAM DB authentication (Autenticación de base de datos de IAM)
 	
Enable IAM DB authentication (Habilitar la autenticación de base de datos de IAM) para autenticar usuarios de bases de datos a través de usuarios y roles.
 	
Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.
	Opción de la CLI:
	
	`--enable-iam-database-authentication |--no-enable-iam-database-authentication`
	
	Parámetro de la API de RDS:
	
	`EnableIAMDatabaseAuthentication`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			No se produce un tiempo de inactividad durante este cambio.	Solo MariaDB, MySQL y PostgreSQL

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Kerberos authentication (Autenticación Kerberos)
 	
Elija el Active Directory al que mover la instancia de base de datos. El directorio debe existir antes de esta operación. Si ya hay un directorio seleccionado, puede especificar None (Ninguno) para quitar la instancia de base de datos de su directorio actual.
 	
Para obtener más información, consulte Autenticación Kerberos.
	Opción de la CLI:
	
	`--domain` y `--domain-iam-role-name`
	
	Parámetro de la API de RDS:
	
	`Domain` y `DomainIAMRoleName`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Durante este cambio se produce un breve tiempo de inactividad.	Solo Microsoft SQL Server, MySQL, Oracle y PostgreSQL

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

License model (Modelo de licencia)
 	
Elija bring-your-own-license para utilizar su licencia para Db2 y Oracle.
 	
Elija license-included (licencia incluida) para utilizar el acuerdo de licencia general de Microsoft SQL Server u Oracle.
 	
Para obtener más información, consulte Opciones de licencias de Amazon RDS para Db2, Licencias de Microsoft SQL Server en Amazon RDS y Opciones de licencias de RDS para Oracle.
	Opción de la CLI:
	
	`--license-model`
	
	Parámetro de la API de RDS:
	
	`LicenseModel`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Se produce un tiempo de inactividad durante este cambio.	Solo Microsoft SQL Server y Oracle

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Log exports (Exportaciones de registros)
 	
Los tipos de archivos de registro de base de datos que se publicarán en Amazon CloudWatch Logs.
 	
Para obtener más información, consulte Publicación de registros de base de datos en registros de Amazon Cloudwatch.
	Opción de la CLI:
	
	`--cloudwatch-logs-export-configuration`
	
	Parámetro de la API de RDS:
	
	`CloudwatchLogsExportConfiguration`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Maintenance window (Periodo de mantenimiento)
 	
El intervalo de tiempo durante el que se produce el mantenimiento del sistema. El mantenimiento del sistema incluye actualizaciones, si procede. El periodo de mantenimiento se expresa mediante una hora de inicio en tiempo universal coordinado (UTC) y una duración en horas.
 	
Si establece un intervalo que incluya la hora actual, debe haber al menos 30 minutos entre la hora actual y el final del intervalo. Este tiempo ayuda a garantizar que se apliquen los cambios pendientes.
 	
Para obtener más información, consulte La ventana de mantenimiento de Amazon RDS.
	Opción de la CLI:
	
	`--preferred-maintenance-window`
	
	Parámetro de la API de RDS:
	
	`PreferredMaintenanceWindow`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	Si hay una o varias acciones pendientes que provocan un tiempo de inactividad y el periodo de mantenimiento se cambia para incluir la hora actual, las acciones pendientes se aplican inmediatamente y se produce un tiempo de inactividad.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Gestionar las credenciales maestras en AWS Secrets Manager
 	
Seleccione Manage master credentials in AWS Secrets Manager (Administrar credenciales maestras en AWS Secrets Manager) para administrar la contraseña del usuario maestro en un secreto en Secrets Manager.
 	
De forma opcional, elija la clave KMS para proteger el secreto. Elija entre las claves de KMS de su cuenta o bien introduzca la clave de otra cuenta.
 	
Si RDS ya administra la contraseña de usuario maestra de la instancia de base de datos, puede rotar la contraseña del usuario maestro seleccionando Rotate secret immediately (Rotar el secreto inmediatamente).
 	
Para obtener más información, consulte Administración de
	Opción de la CLI:
	
	`--manage-master-user-password | --no-manage-master-user-password`
	
	`--master-user-secret-kms-key-id`
	
	`--rotate-master-user-password | --no-rotate-master-user-password`
	
	Parámetro de la API de RDS:
		Si activa o desactiva la administración automática de contraseñas de usuario maestro, el cambio se produce inmediatamente. Este cambio omite la configuración de aplicación inmediata.
		
		Si va a rotar la contraseña del usuario maestro, debe especificar que el cambio se aplique inmediatamente.
			No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

contraseñas con Amazon RDS y AWS Secrets Manager.	`ManageMasterUserPassword`
	
	`MasterUserSecretKmsKeyId`
	
	`RotateMasterUserPassword`			

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Multi-AZ deployment (Implementación Multi-AZ)
 	
Seleccione Yes (Sí) para implementar la instancia de base de datos en varias zonas de disponibilidad. De lo contrario, seleccione No.
 	
Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.
	Opción de la CLI:
	
	`--multi-az|--no-multi-az`
	
	Parámetro de la API de RDS:
	
	`MultiAZ`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			No se produce un tiempo de inactividad durante este cambio. Sin embargo, existe un posible impacto en el rendimiento. Para obtener más información, consulte Conversión de una instancia de base de datos en una implementación multi-AZ para Amazon RDS.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Tipo de red
 	
Protocolos de direccionamiento IP admitidos por la instancia de base de datos.
 	
IPv4 para especificar que los recursos se pueden comunicar con la instancia de base de datos solo a través del protocolo de direcciones Internet Protocol versión 4 (IPv4).
 	
Modo de pila doble para especificar que los recursos se pueden comunicar con la instancia de base de datos mediante IPv4, versión 6 (IPv6) o ambos. Utilice el modo de pila doble si tiene recursos que deben comunicarse con su instancia de base de datos a través del protocolo de direccionamiento IPv6. Además, asegúrese de asociar un bloque CIDR IPv6 a todas las subredes del grupo de subredes de base de datos que especifique.
	Opción de la CLI:
	
	`--network-type`
	
	Parámetro de la API de RDS:
	
	`NetworkType`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Es posible un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Para obtener más información, consulte Direccionamiento IP de Amazon RDS.				

New master password (Nueva contraseña maestra)
 	
La contraseña para el usuario maestro. La contraseña debe incluir 8–41 caracteres alfanuméricos.
	Opción de la CLI:
	
	`--master-user-password`
	
	Parámetro de la API de RDS:
	
	`MasterUserPassword`
		El cambio se aplica de forma asíncrona, tan pronto como sea posible. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Option group (Grupo de opciones)
 	
El grupo de opciones que desea asociar a la instancia de base de datos.
 	
Para obtener más información, consulte Trabajo con grupos de opciones.
	Opción de la CLI:
	
	`--option-group-name`
	
	Parámetro de la API de RDS:
	
	`OptionGroupName`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			No se produce un tiempo de inactividad durante este cambio. Una excepción es añadir el complemento de auditoría de MariaDB a una instancia de base de datos de RDS para MariaDB o RDS para MySQL, lo que podría provocar una interrupción.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Performance Insights (Información sobre rendimiento)
 	
Enable Performance Insights (Información sobre rendimiento) para monitorizar la carga de las instancias de base de datos para poder analizar y solucionar los problemas de rendimiento de la base de datos.
 	
Información sobre rendimiento no está disponible para algunas versiones de motor de base de datos y clases de instancia de base de datos. La sección Performance Insights no aparece en la consola si no está disponible para su instancia de base de datos.
 	
Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS y El motor de base de datos de Amazon RDS, la región y la clase de instancia son compatibles con Información de rendimiento.
	Opción de la CLI:
	
	`--enable-performance-insights| --no-enable-performance-insights`
	
	Parámetro de la API de RDS:
	
	`EnablePerformanceInsights`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos excepto Db2

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Performance InsightsAWS KMS key (Información sobre rendimiento)
 	
El identificador de la clave de AWS KMS para AWS KMS key para el cifrado de datos de Información sobre rendimiento. El identificador de clave es el nombre de recurso de Amazon (ARN), el identificador de clave de AWS KMS o el alias de clave de la CMK.
 	
Para obtener más información, consulte Activación y desactivación de Información de rendimiento de Amazon RDS.
	Opción de la CLI:
	
	`--performance-insights-kms-key-id`
	
	Parámetro de la API de RDS:
	
	`PerformanceInsightsKMSKeyId`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos excepto Db2

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Performance Insights Retention period (Periodo de retención de información sobre rendimiento)
 	
El tiempo, en días, durante los que se conservan los datos de información sobre rendimiento. La configuración de retención en la capa gratuita es Default (7 days) (Predeterminado [7 días]). Para retener los datos de rendimiento durante más tiempo, especifique de 1 a 24 meses. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.
 	
Para obtener más información, consulte Activación y desactivación de Información de rendimiento de Amazon RDS.
	Opción de la CLI:
	
	`--performance-insights-retention-period`
	
	Parámetro de la API de RDS:
	
	`PerformanceInsightsRetentionPeriod`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos excepto Db2

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Processor features (Características del procesador)
 	
El número de núcleos de CPU y el número de subprocesos por núcleo para la clase de instancia de la instancia de base de datos.
 	
Para obtener más información, consulte Configuración del procesador de una clase de instancias de base de datos en RDS para Oracle.
	Opción de la CLI:
	
	`--processor-features` y `--use-default-processor-features` | `--no-use-default-processor-features`
	
	Parámetro de la API de RDS:
	
	`ProcessorFeatures` y `UseDefaultProcessorFeatures`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Se produce un tiempo de inactividad durante este cambio.	Solo Oracle

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Provisioned IOPS (IOPS aprovisionadas)
 	
El valor de la IOPS aprovisionada (operaciones de E/S por segundo) para la instancia de base de datos. Esta configuración solo está disponible si elige una de las siguientes opciones para el tipo de almacenamiento:
 	
• SSD de uso general (gp3)
• SSD de IOPS aprovisionadas (io1)
• SSD de IOPS aprovisionadas (io2)
 	
Para obtener más información, consulte the section called “Almacenamiento de IOPS aprovisionadas” y the section called “Almacenamiento gp3 (recomendado)”.
	Opción de la CLI:
	
	`--iops`
	
	Parámetro de la API de RDS:
	
	`Iops`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Public access (Acceso público)
 	
Publicly accesible (Accesible públicamente) para proporcionar una dirección IP pública a la instancia de base de datos, lo que significa que es accesible desde fuera de la VPC. Para que sea accesible públicamente, la instancia de base de datos también debe estar en una subred pública de la VPC.
 	
Not publicly accesible (No es accesible públicamente) para que la instancia de base de datos sea accesible solo desde dentro de la VPC.
 	
Para obtener más información, consulte Cómo ocultar una instancia de base de datos en una VPC desde Internet..
 	
Para conectarse a una instancia de base de datos desde afuera de su VPC, la instancia de base de datos debe ser accesible públicamente. Además, el acceso debe concederse mediante
	Opción de la CLI:
	
	`--publicly-accessible | --no-publicly-accessible`
	
	Parámetro de la API de RDS:
	
	`PubliclyAccessible`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
las reglas entrantes del grupo de seguridad de la instancia de base de datos. Además, deben cumplirse otros requisitos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS. Si su instancia de base de datos no está accesible públicamente, también puede usar una conexión Site-to-site VPN AWS o una conexión a AWS Direct Connect para acceder a ella desde una red privada. Para obtener más información, consulte Privacidad del tráfico entre redes.				

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Security group (Grupo de seguridad)
 	
El grupo de seguridad de la VPC que desea asociar a la instancia de base de datos.
 	
Para obtener más información, consulte Control de acceso con grupos de seguridad.
	Opción de la CLI:
	
	`--vpc-security-group-ids`
	
	Parámetro de la API de RDS:
	
	`VpcSecurityGroupIds`
		El cambio se aplica de forma asíncrona , tan pronto como sea posible. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Storage autoscaling (Escalado automático de almacenamiento)
 	
Enable storage autoscaling (Habilitar escalado automático de almacenamiento) para que Amazon RDS aumente automáticamente el almacenamiento cuando sea necesario y evite que la instancia de base de datos se quede sin espacio de almacenamiento.
 	
Utilice la opción Maximum storage threshold (Umbral máximo de almacenamiento) para configurar el límite superior de Amazon RDS para que aumente automáticamente el almacenamiento de la instancia de base de datos. El valor predeterminado es de 1000 GiB.
 	
Para obtener más información, consulte Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS.
	Opción de la CLI:
	
	`--max-allocated-storage`
	
	Parámetro de la API de RDS:
	
	`MaxAllocatedStorage`
		El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Rendimiento de almacenamiento
 	
Valor de rendimiento de almacenamiento nuevo para la instancia de base de datos. Esta configuración solo está disponible si selecciona SSD de uso general (gp3) como tipo de almacenamiento.
 	
Para obtener más información, consulte the section called “Almacenamiento gp3 (recomendado)”.
	Opción de la CLI:
	
	`--storage-throughput`
	
	Parámetro de la API de RDS:
	
	`StorageThroughput`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			No se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Storage type (Tipo de almacenamiento)
 	
El tipo de almacenamiento que desea utilizar.
 	
Si elige General Purpose SSD (gp3) (SSD de uso general [gp3]), puede aprovisionar IOPS aprovisionadas adicionales y Storage throughput (Rendimiento de almacenamiento) en Advanced settings (Configuración avanzada).
 	
Si selecciona SSD de IOPS aprovisionadas (io1) o SSD de IOPS aprovisionadas (io2), introduzca el valor de IOPS aprovisionadas.
 	
Cuando Amazon RDS empieza a modificar la instancia de base de datos para cambiar el tamaño o el tipo de almacenamiento, no se puede enviar otra solicitud para cambiar dicho tamaño, rendimiento o tipo de almacenamiento durante 6 horas.
	Opción de la CLI:
	
	`--storage-type`
	
	Parámetro de la API de RDS:
	
	`StorageType`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Los siguientes cambios producen un breve tiempo de inactividad mientras se inicia el proceso. Después de eso, puede usar la base de datos con normalidad mientras se produce el cambio.
			
			• De General Purpose (SSD) [Uso general (SSD)] o Provisioned IOPS (SSD) [IOPS aprovisionadas (SSD)] a
				Todos los motores DB

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles
Para obtener más información, consulte Tipos de almacenamiento de Amazon RDS.			Magnetic (Magnético). • De Magnetic (Magnético) a General Purpose (SSD) [Uso general (SSD)] o Provisioned IOPS (SSD) [IOPS aprovisionadas (SSD)].	

Configuración y descripción de la consola	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad	Motores de bases de datos compatibles

Grupo de subredes de base de datos
 	
El grupo de subredes base de datos de la instancia de base de datos. Puede utilizar este ajuste para mover la instancia de base de datos a otra VPC.
 	
Para obtener más información, consulte VPC de Amazon y Amazon RDS.
	Opción de la CLI:
	
	`--db-subnet-group-name`
	
	Parámetro de la API de RDS:
	
	`DBSubnetGroupName`
		Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
		
		Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
			Se produce un tiempo de inactividad durante este cambio.	Todos los motores DB

Mantenimiento de una instancia de base de datos

Amazon RDS realiza tareas de mantenimiento periódicas en los recursos de Amazon RDS.

Temas

- Descripción general de las actualizaciones de mantenimiento de instancias de base de datos DB
- Visualización de actualizaciones de mantenimiento pendientes
- Aplicación de actualizaciones a una instancia de base de datos
- Mantenimiento de implementaciones Multi-AZ
- La ventana de mantenimiento de Amazon RDS
- Ajuste de la ventana de mantenimiento preferida para una instancia de base de datos
- Actualizaciones del sistema operativo de instancias de base de datos de RDS

Descripción general de las actualizaciones de mantenimiento de instancias de base de datos DB

El mantenimiento suele implicar actualizaciones de los siguientes recursos de su instancia de base de datos:

- Hardware subyacente
- Sistema operativo (SO) subyacente
- Versión del motor de base de datos

Las actualizaciones del sistema operativo suelen deberse a motivos de seguridad. Se recomienda que las haga lo antes posible. Para obtener más información sobre las actualizaciones de sistemas operativos, consulte Aplicación de actualizaciones a una instancia de base de datos.

Temas

- Recursos sin conexión durante las actualizaciones de mantenimiento
- Modificaciones diferidas de instancias de base de datos
- Consistencia final de la API DescribependingMaintenanceActions

Recursos sin conexión durante las actualizaciones de mantenimiento

Algunos elementos de mantenimiento requieren que Amazon RDS desconecte su instancia de base de datos durante un breve plazo de tiempo. Entre los elementos de mantenimiento que requieren que un recurso esté desconectado están el sistema operativo necesario o la aplicación de parches a la base de datos. Los parches obligatorios que tienen que ver con la seguridad y la fiabilidad de la instancia son los únicos que se programan automáticamente. Estos parches se producen con poca frecuencia, normalmente una vez cada pocos meses. Rara vez se requiere más de una fracción de su período de mantenimiento.

Modificaciones diferidas de instancias de base de datos

Las modificaciones de instancias de base de datos diferidas que haya decidido no aplicar inmediatamente se aplican durante el periodo de mantenimiento. Por ejemplo, puede elegir cambiar la clase o el grupo de parámetros de la instancia de base de datos durante el periodo de mantenimiento. Las modificaciones que especifique mediante la configuración de reinicio pendiente no se muestran en la lista Mantenimiento pendiente. Para obtener más información acerca de la modificación de una instancia de base de datos , consulte Modificación de una instancia de base de datos de Amazon RDS.

Para ver las modificaciones pendientes para la siguiente ventana de mantenimiento, utilice el comando describe-db-instances de la AWS CLI y marque el campo `PendingModifiedValues`.

Consistencia final de la API DescribependingMaintenanceActions

La API `DescribePendingMaintenanceActions` de Amazon RDS sigue un modelo de consistencia final. Esto significa que el resultado del comando `DescribePendingMaintenanceActions` puede que no sea visible inmediatamente para todos los comandos de RDS posteriores. Tenga esto en cuenta cuando utilice `DescribePendingMaintenanceActions` inmediatamente después de usar un comando de API anterior.

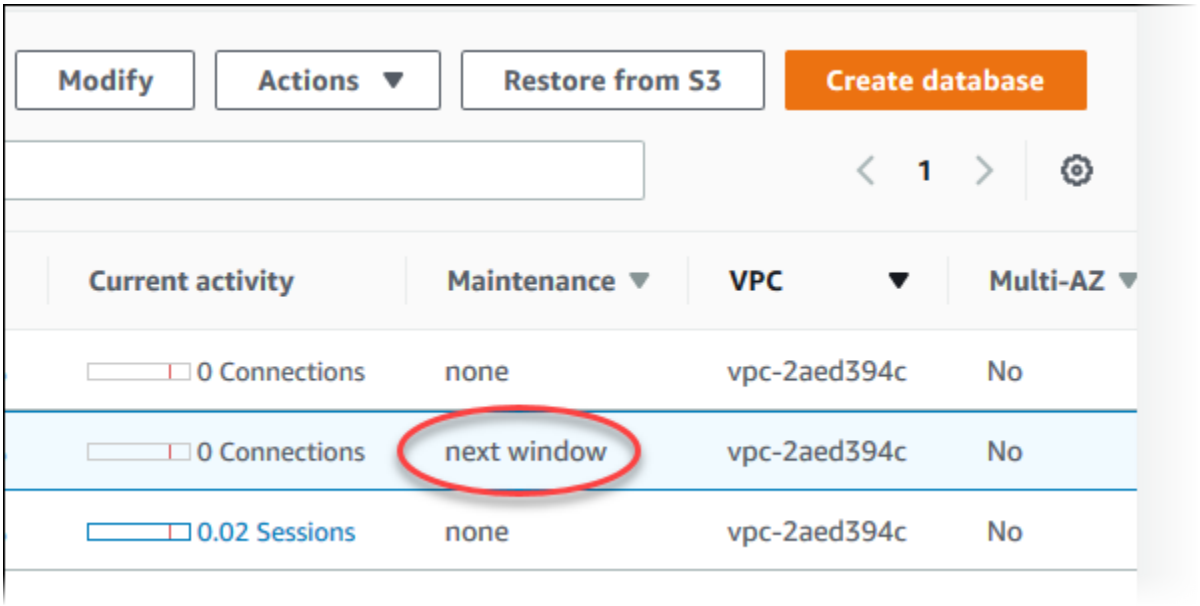
La consistencia final puede afectar a la forma en que ha administrado las actualizaciones de mantenimiento. Por ejemplo, si ejecuta el comando `ApplyPendingMaintenanceActions` para actualizar la versión del motor de base de datos de una instancia de base de datos, al final será visible en `DescribePendingMaintenanceActions`. En este escenario, `DescribePendingMaintenanceActions` podría indicar que la acción de mantenimiento no se aplicó a pesar de que sí se hizo.

Para administrar la consistencia final, puede hacer lo siguiente:

- Confirme el estado de la instancia de base de datos antes de ejecutar un comando para modificarlo. Ejecute el comando `DescribePendingMaintenanceActions` correspondiente mediante un algoritmo de retroceso exponencial para asegurarse de que dispone de tiempo suficiente para que el comando anterior se propague en el sistema. Para ello, ejecute el comando `DescribePendingMaintenanceActions` varias veces, empezando con un par de segundos de espera y aumentando gradualmente hasta cinco minutos.
- Agregue tiempo de espera entre los comandos siguientes, incluso si un comando `DescribePendingMaintenanceActions` devuelve una respuesta precisa. Aplique un algoritmo de retroceso exponencial comenzando con un par de segundos de tiempo de espera y aumente gradualmente hasta unos cinco minutos de tiempo de espera.

Visualización de actualizaciones de mantenimiento pendientes

Compruebe si hay disponible una actualización de mantenimiento para una instancia de base de datos, use la consola de RDS, la AWS CLI o la API de RDS. Si hay disponible una actualización, se indicará en la columna Maintenance (Mantenimiento) para la instancia de base de datos en la consola Amazon RDS, como se muestra a continuación.



Si no hay ninguna actualización de mantenimiento disponible para una instancia de base de datos, el valor de columna es none (ninguno).

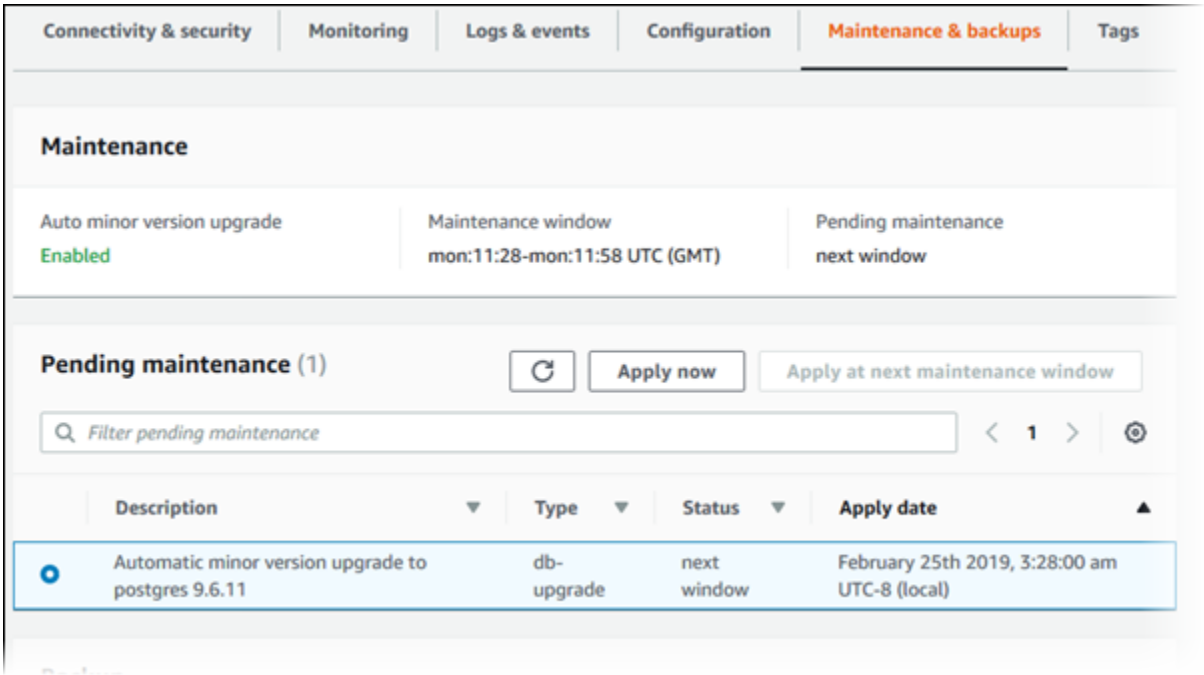
Si una actualización de mantenimiento está disponible para una instancia, son posibles los siguientes valores de columna:

- required (obligatorio): la acción de mantenimiento se aplicará al recurso y no se podrá aplazar indefinidamente.
- available (disponible): la acción de mantenimiento está disponible, pero no se aplicará al recurso automáticamente. Puede aplicarla manualmente.
- next window (siguiente periodo): la acción de mantenimiento se aplicará al recurso durante el siguiente periodo de mantenimiento.
- In progress (en curso): la acción de mantenimiento está en proceso de aplicarse al recurso.

Si hay una actualización disponible, puede realizar una de las acciones:

- Si el valor de mantenimiento es next window (siguiente periodo), aplace los elementos de mantenimiento eligiendo defer upgrade (aplazar actualización) en Actions (Acciones). No puede aplazar una acción de mantenimiento si ya se ha iniciado.
- Aplicar inmediatamente los elementos de mantenimiento.
- Programar los elementos de mantenimiento para que se inicien en la siguiente ventana de mantenimiento.
- No realice ninguna acción.

Para realizar una acción, elija la instancia para mostrar sus detalles y, a continuación, elija Maintenance & backups (Mantenimiento y copias de seguridad). Aparecerán los elementos de mantenimiento pendientes.



El periodo de mantenimiento determina el momento en que comienzan las operaciones pendientes, pero no limita su tiempo de ejecución total. No existen garantías de que las operaciones de mantenimiento finalicen antes de que termine el periodo de mantenimiento, de modo que pueden continuar más allá de la hora de finalización establecida. Para obtener más información, consulte La ventana de mantenimiento de Amazon RDS.

Para ver si hay disponible una actualización de mantenimiento para una instancia de base de datos, puede ejecutar el comando `describe-pending-maintenance-actions` de la AWS CLI.

Para obtener información sobre la aplicación de actualizaciones de mantenimiento, consulte Aplicación de actualizaciones a una instancia de base de datos.

Aplicación de actualizaciones a una instancia de base de datos

Con Amazon RDS puede elegir el momento en que desea aplicar las operaciones de mantenimiento. Puede indicar cuándo Amazon RDS debe aplicar las actualizaciones usando la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> En el caso de RDS para SQL Server, se puede aplicar una actualización del sistema operativo subyacente deteniendo e iniciando la instancia de base de datos o subiendo y bajando la clase de instancia de base de datos.

Consola

Para administrar la actualización de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione la instancia de base de datos que tenga una actualización necesaria.
4. En Acciones, elija una de las siguientes opciones:
   - Aplicar parches ahora
   - Aplicar parches en el siguiente periodo

   > **Note**
   >
   > Si elige Aplicar parches en el siguiente periodo y después desea aplazar la actualización, puede seleccionar Aplazar actualización. No puede aplazar una acción de mantenimiento si ya se ha iniciado.
   > Para cancelar una acción de mantenimiento, modifique la instancia de base de datos y deshabilite la Auto minor version upgrade (Actualización automática de versiones secundarias).

AWS CLI

Para aplicar una actualización pendiente a una instancia de base de datos, use el comando apply-pending-maintenance-action de la AWS CLI.

Example

Para Linux, macOS o Unix:

```
aws rds apply-pending-maintenance-action \
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db \
    --apply-action system-update \
    --opt-in-type immediate
```

En Windows:

```
aws rds apply-pending-maintenance-action ^
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db ^
    --apply-action system-update ^
    --opt-in-type immediate
```

> **Note**
>
> Para aplazar una acción de mantenimiento, especifique `undo-opt-in` para `--opt-in-type`. No se puede especificar `undo-opt-in` para `--opt-in-type` si la acción de mantenimiento ya se ha iniciado.
> Para cancelar una acción de mantenimiento, ejecute el comando de la AWS CLI modify-db-instance y especifique `--no-auto-minor-version-upgrade`.

Para obtener una lista de los recursos con al menos una actualización pendiente, use el comando describe-pending-maintenance-actions de la AWS CLI.

Example

Para Linux, macOS o Unix:

```
aws rds describe-pending-maintenance-actions \
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

Para Windows:

```
aws rds describe-pending-maintenance-actions ^
    --resource-identifier arn:aws:rds:us-west-2:001234567890:db:mysql-db
```

También puede obtener una lista de recursos de una instancia de base de datos mediante la especificación del parámetro `--filters` del comando `describe-pending-maintenance-actions` de la AWS CLI. El formato del comando `--filters` es `Name=`*`filter-name`*`,Value=`*`resource-id`*`,...`.

Los valores aceptados para el parámetro `Name` de un filtro son los siguientes:

- `db-instance-id`: acepta una lista de identificadores o nombres de recurso de Amazon (ARN) de instancias de base de datos. La lista obtenida solo incluirá las operaciones de mantenimiento pendientes para las instancias de base de datos referidas por esos identificadores o ARN.
- `db-cluster-id`: acepta una lista de identificadores o ARN de clústeres de base de datos para Amazon Aurora. La lista obtenida solo incluirá las operaciones de mantenimiento pendientes para los clústeres de base de datos referidos por esos identificadores o ARN.

Por ejemplo, en el ejemplo siguiente se obtienen las operaciones de mantenimiento pendientes para las instancias de base de datos `sample-instance1` y `sample-instance2`.

Example

Para Linux, macOS o Unix:

```
aws rds describe-pending-maintenance-actions \
 --filters Name=db-instance-id,Values=sample-instance1,sample-instance2
```

Para Windows:

```
aws rds describe-pending-maintenance-actions ^
 --filters Name=db-instance-id,Values=sample-instance1,sample-instance2
```

API de RDS

Para aplicar una actualización a una instancia de base de datos, llame a la operación `ApplyPendingMaintenanceAction` de la API de Amazon RDS.

Para obtener una lista de los recursos con al menos una actualización pendiente, llame a la operación `DescribePendingMaintenanceActions` de la API Amazon RDS.

Mantenimiento de implementaciones Multi-AZ

Ejecutar una instancia de base de datos como una Implementación multi-AZ AZ puede reducir aún más el impacto de un evento de mantenimiento. Este resultado se debe a que Amazon RDS aplica las actualizaciones del sistema operativo siguiendo estos pasos:

1. Realización del mantenimiento en la instancia en espera.
2. Promoción de la instancia en espera a principal.
3. Realización del mantenimiento en la antigua instancia principal, que se convierte en la nueva instancia en espera.

Si actualiza el motor de base de datos para su instancia de base de datos en una implementación multi-AZ, Amazon RDS modifica tanto la instancia de base de datos principal como la secundaria a la vez. En este caso, tanto la instancia de base de datos principal como la secundaria en la implementación multi-AZ no estarán disponibles durante la actualización. Esta operación generará un tiempo de inactividad hasta que se complete la actualización. El tiempo que dura la interrupción varía según el tamaño de la instancia de base de datos.

Si hay parches subyacentes del sistema operativo que deban aplicarse, es necesario realizar una breve conmutación por error multi-AZ para aplicar los parches en la instancia de base de datos principal. Esta conmutación por error suele durar menos de un minuto.

Si su instancia de base de datos ejecuta RDS para MySQL, RDS para PostgreSQL o RDS para MariaDB, puede minimizar el tiempo de inactividad necesario para la actualización usando una implementación azul/verde. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos. Si actualiza una instancia de base de datos de RDS para SQL Server o RDS Custom para SQL Server en una implementación multi-AZ, Amazon RDS realizará actualizaciones sucesivas, de manera que la interrupción sea solo mientras dure la conmutación por error. Para obtener más información, consulte Consideraciones de Multi-AZ.

Si su instancia de base de datos ejecuta RDS para SQL Server en una implementación Multi-AZ, puede aplicarle una actualización al sistema operativo subyacente mediante uno de los siguientes métodos:

- Modifique la clase de instancia de base de datos a un tamaño diferente y, a continuación, vuelva a modificarla al tamaño original.
- Aumente el tamaño de la instancia de la base de datos y vuelva a reducirlo al tamaño original.

- Modifique la instancia de base de datos de Multi-AZ a Single-AZ, detenga e inicie la instancia de base de datos y, a continuación, cámbiela de nuevo a Multi-AZ.

Para obtener más información sobre las implementaciones Multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

La ventana de mantenimiento de Amazon RDS

Los periodos de mantenimiento son un intervalo de tiempo semanal durante los que se aplican los cambios del sistema. Cada instancia de base de datos tiene un periodo de mantenimiento semanal. El periodo de mantenimiento es una oportunidad para controlar cuándo ocurrirán las modificaciones y los parches de software. Para obtener más información sobre el ajuste del periodo de mantenimiento, consulte Ajuste de la ventana de mantenimiento preferida para una instancia de base de datos.

RDS consume algunos de los recursos de su instancia de base de datos mientras se aplica el mantenimiento. Es posible que observe un efecto mínimo en el desempeño. Para una instancia de base de datos, en raras ocasiones puede ser necesaria una conmutación por error Multi-AZ para que se complete una actualización de mantenimiento.

Si hay un evento de mantenimiento programado para una semana determinada, se iniciará durante la ventana de mantenimiento que identifique. La mayoría de los eventos de mantenimiento también se completan durante la ventana de mantenimiento de 30 minutos, aunque otros eventos de mantenimiento pueden tardar más de 30 minutos en completarse. El periodo de mantenimiento se detiene cuando se detiene la instancia de la base de datos.

La ventana de mantenimiento de 30 minutos se selecciona al azar dentro de un bloque de 8 horas por región. Si no especifica una ventana de mantenimiento al crear una instancia de base de datos, RDS asigna una ventana de mantenimiento de 30 minutos un día de la semana seleccionado al azar.

A continuación, puede encontrar los bloques de horas de cada región desde los que se asignan las ventanas predeterminadas de mantenimiento.

Nombre de la región	Región	Bloque de tiempo
Este de EE. UU. (Ohio)	us-east-2	03:00 — 11:00 UTC

Nombre de la región	Región	Bloque de tiempo
Este de EE. UU. (Norte de Virginia)	us-east-1	03:00–11:00 UTC
Oeste de EE. UU. (Norte de California)	us-west-1	06:00 — 14:00 UTC
Oeste de EE. UU. (Oregón)	us-west-2	06:00–14:00 UTC
África (Ciudad del Cabo)	af-south-1	03:00–11:00 UTC
Asia-Pacífico (Hong Kong)	ap-east-1	06:00–14:00 UTC
Asia-Pacífico (Hyderabad)	ap-south-2	06:30 – 14:30 UTC
Asia-Pacífico (Yakarta)	ap-southeast-3	08:00 a 16:00 h UTC
Asia-Pacífico (Melbourne)	ap-southeast-4	11:00–19:00 UTC
Asia Pacífico (Bombay)	ap-south-1	06:00–14:00 UTC
Asia Pacific (Osaka)	ap-northeast-3	22:00 — 23:59 UTC
Asia Pacific (Seoul)	ap-northeast-2	13:00 — 21:00 UTC
Asia-Pacífico (Singapur)	ap-southeast-1	14:00 — 22:00 UTC
Asia Pacífico (Sídney)	ap-southeast-2	12:00 — 20:00 UTC
Asia Pacífico (Tokio)	ap-northeast-1	13:00 — 21:00 UTC

Nombre de la región	Región	Bloque de tiempo
Canadá (centro)	ca-central-1	03:00 — 11:00 UTC
Oeste de Canadá (Calgary)	ca-west-1	18:00 — 02:00 UTC
China (Pekín)	cn-north-1	06:00–14:00 UTC
China (Ningxia)	cn-northwest-1	06:00–14:00 UTC
Europe (Fráncfort)	eu-central-1	21:00 — 05:00 UTC
Europe (Irlanda)	eu-west-1	22:00 — 06:00 UTC
Europe (Londres)	eu-west-2	22:00 — 06:00 UTC
Europa (Milán)	eu-south-1	02:00 — 10:00 UTC
Europa (París)	eu-west-3	23:59–07:29 UTC
Europa (España)	eu-south-2	02:00 — 10:00 UTC
Europa (Estocolmo)	eu-north-1	23:00 — 07:00 UTC
Europa (Zúrich)	eu-central-2	02:00 — 10:00 UTC
Israel (Tel Aviv)	il-central-1	03:00 — 11:00 UTC
Medio Oriente (Baréin)	me-south-1	06:00–14:00 UTC
Medio Oriente (EAU)	me-central-1	05:00 a 13:00 h UTC
América del Sur (São Paulo)	sa-east-1	00:00–08:00 UTC
AWS GovCloud (EE. UU. Este)	us-gov-east-1	17:00 — 01:00 UTC

Nombre de la región	Región	Bloque de tiempo
AWS GovCloud (Oeste de EE. UU.)	us-gov-west-1	06:00–14:00 UTC

Ajuste de la ventana de mantenimiento preferida para una instancia de base de datos

La ventana de mantenimiento debe corresponder al momento de mínimo uso y, por tanto, podría ser preciso modificarla cada cierto tiempo. La instancia de base de datos solo dejan de estar disponibles durante este periodo si se están aplicando cambios en el sistema, por ejemplo, se está realizando una operación de escalado del almacenamiento o un cambio de clase de instancia y se requiere una interrupción. Su instancia de base de datos solo dejará de estar disponible durante el tiempo mínimo requerido para realizar los cambios necesarios.

En el siguiente ejemplo, se ajusta la ventana de mantenimiento preferida para una instancia de base de datos.

En este ejemplo, supondremos que una instancia de base de datos llamada mydbinstance existe y que tiene una ventana de mantenimiento preferida de "Sun:05:00-Sun:06:00" UTC.

Consola

Para ajustar la ventana de mantenimiento preferida

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desea modificar.
3. Elija Modify. Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. En la sección Maintenance (Mantenimiento), actualice el periodo de mantenimiento.

> **Note**
>
> La ventana de mantenimiento y la ventana de backup de la instancia de base de datos no se pueden solapar. Si escribe un valor para la ventana de mantenimiento que se superponga con la ventana de backup, aparece un mensaje de error.

5. Elija Continue.

   En la página de confirmación, revise los cambios.

6. Para aplicar los cambios al periodo de mantenimiento de forma inmediata, seleccione Apply immediately (Aplicar inmediatamente).

7. Seleccione Modificar la instancia de base de datos para guardar los cambios.

   O bien, elija Back para editar los cambios o Cancel para cancelarlos.

AWS CLI

Para ajustar la ventana de mantenimiento preferida, use el comando AWS CLI de la `modify-db-instance` con los siguientes parámetros:

- `--db-instance-identifier`
- `--preferred-maintenance-window`

Example

En el siguiente ejemplo de código, el periodo de mantenimiento se define para los martes de 4:00 a 4:30 UTC.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
--db-instance-identifier mydbinstance \
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

En Windows:

```
aws rds modify-db-instance ^
--db-instance-identifier mydbinstance ^
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

API de RDS

Para ajustar el plazo de mantenimiento preferido, utilice la operación `ModifyDBInstance` de la API de Amazon RDS con los siguientes parámetros:

- `DBInstanceIdentifier`

- `PreferredMaintenanceWindow`

Actualizaciones del sistema operativo de instancias de base de datos de RDS

En ocasiones, las instancias de base de datos de RDS para Db2, RDS para MariaDB, RDS para PostgreSQL y RDS para Oracle requieren actualizaciones del sistema operativo. Amazon RDS actualiza el sistema operativo a una versión más reciente para mejorar el rendimiento de la base de datos y la posición de seguridad general de los clientes. Normalmente, las actualizaciones tardan unos 10 minutos en completarse. Las actualizaciones del sistema operativo no cambian la versión del motor de la base de datos ni la clase de instancia de la base de datos.

Las actualizaciones del sistema operativo pueden ser opcionales u obligatorias:

- Se puede aplicar una actualización opcional en cualquier momento. Aunque estas actualizaciones son opcionales, le recomendamos que las aplique periódicamente para mantener su flota de RDS al día. RDS no aplica estas actualizaciones automáticamente.

  Para recibir una notificación cuando haya un nuevo parche del sistema operativo opcional disponible, puede suscribirse al RDS-EVENT-0230 en la categoría de eventos de parches de seguridad. Para obtener información sobre cómo suscribirse a los eventos de RDS, consulte Suscripción a notificaciones de eventos de Amazon RDS.

  > **Note**
  >
  > `RDS-EVENT-0230` no se aplica a las actualizaciones de distribución del sistema operativo.

  > **Note**
  >
  > Si ha recibido `RDS-EVENT-0230` para una instancia de base de datos de RDS para SQL Server, la actualización del sistema operativo no se puede aplicar mediante la acción `apply-pending-maintenance`. Para obtener más información, consulte Aplicación de actualizaciones a una instancia de base de datos.

- Se requiere una actualización obligatoria y tiene una fecha de aplicación. Planifique la actualización antes de dicha fecha. Después de la fecha de aplicación especificada, Amazon RDS

actualiza automáticamente el sistema operativo de la instancia de base de datos a la última versión durante uno de los períodos de mantenimiento asignados.

> **Note**
>
> Mantenerse al día en todas las actualizaciones opcionales y obligatorias podría ser necesario para cumplir varias obligaciones de conformidad. Le recomendamos que aplique todas las actualizaciones que RDS pone a disposición de los usuarios de forma rutinaria durante los periodos de mantenimiento.

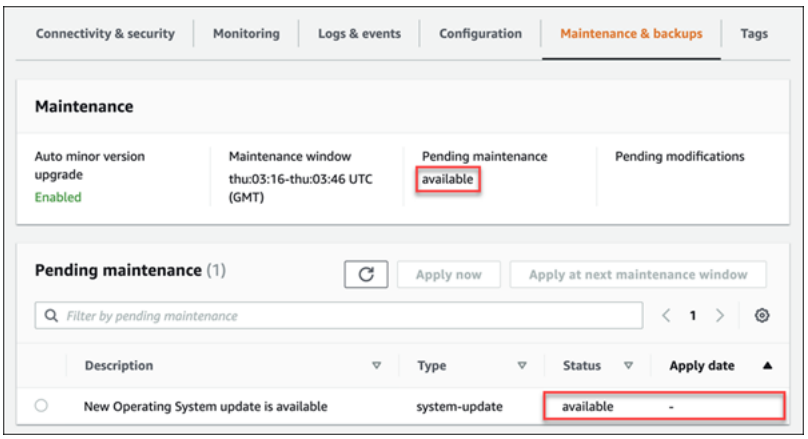
Puede utilizar la AWS Management Console o la AWS CLI para obtener información sobre el tipo de actualización del sistema operativo.

Consola

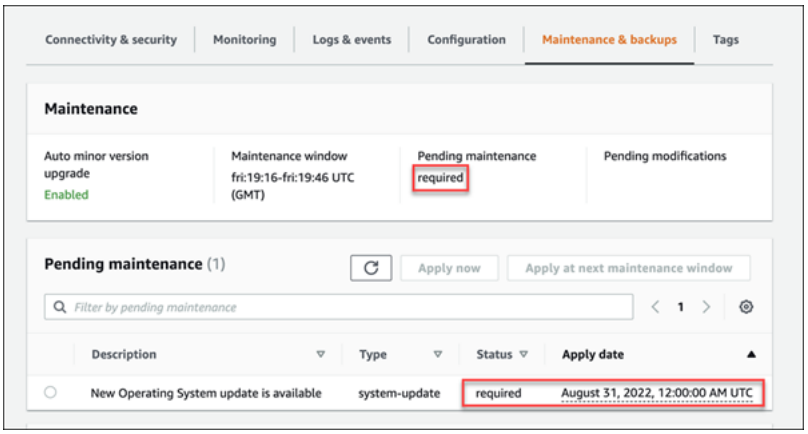
Para obtener información de actualización mediante la AWS Management Console

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos.
3. Seleccione Mantenimiento y copias de seguridad.
4. En la sección Mantenimiento pendiente, busque la actualización del sistema operativo y consulte el valor Estado.

En la AWS Management Console, una actualización opcional tiene el valor de Estado de mantenimiento establecido como disponible y no tiene un valor en Fecha de aplicación, como se muestra en la siguiente imagen.



Una actualización obligatoria tiene el valor de Estado de mantenimiento establecido como obligatorio y tiene un valor en Fecha de aplicación, como se muestra en la siguiente imagen.



AWS CLI

Para obtener información de actualización de la AWS CLI, use el comando describe-pending-maintenance-actions.

```
aws rds describe-pending-maintenance-actions
```

Una actualización obligatoria del sistema operativo los valores `AutoAppliedAfterDate` y `CurrentApplyDate`. Una actualización opcional del sistema operativo no incluye estos valores.

La siguiente salida muestra una actualización obligatoria del sistema operativo.

```
{
  "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:mydb1",
  "PendingMaintenanceActionDetails": [
    {
```

```
      "Action": "system-update",
      "AutoAppliedAfterDate": "2022-08-31T00:00:00+00:00",
      "CurrentApplyDate": "2022-08-31T00:00:00+00:00",
      "Description": "New Operating System update is available"
    }
  ]
}
```

La siguiente salida muestra una actualización opcional del sistema operativo.

```
{
  "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:mydb2",
  "PendingMaintenanceActionDetails": [
    {
      "Action": "system-update",
      "Description": "New Operating System update is available"
    }
  ]
}
```

Disponibilidad de las actualizaciones del sistema operativo

Las actualizaciones del sistema operativo son específicas para la versión del motor de base de datos y la clase de instancia de base de datos. Por lo tanto, las instancias de base de datos reciben o requieren actualizaciones en diferentes momentos. Cuando una actualización del sistema operativo está disponible para su instancia de base de datos en función de su versión del motor y de la clase de instancia, la actualización aparece en la consola. También puede verse ejecutando el comando describe-pending-maintenance-actions de la AWS CLI o llamando a la operación de la API de RDS DescribePendingMaintenanceActions. Si hay una actualización disponible para su instancia, puede actualizar el sistema operativo siguiendo las instrucciones de Aplicación de actualizaciones a una instancia de base de datos.

Actualización de una versión del motor de una instancia de base de datos

Amazon RDS proporciona versiones posteriores de cada motor de base de datos compatible, por lo que puede mantener la instancia al día. Las nuevas versiones pueden incluir correcciones de errores, mejoras de seguridad y otras mejoras para el motor de base de datos. Cuando Amazon RDS es compatible con una nueva versión de un motor de base de datos, puede elegir cuándo y cómo actualizar sus instancias de base de datos.

Hay dos tipos de actualizaciones: actualizaciones de versiones principales y actualizaciones de versiones secundarias. En general, una actualización de la versión principal del motor puede introducir cambios incompatibles con las aplicaciones existentes. Por contraste, una actualización de una versión secundaria solo incluye cambios compatibles con las versiones anteriores de las aplicaciones.

En el caso de los clústeres de bases de datos Multi-AZ, las actualizaciones de la versión principal solo son compatibles con RDS para PostgreSQL. Las actualizaciones de versiones secundarias son compatibles con todos los motores que admiten clústeres de base de datos Multi-AZ. Para obtener más información, consulte the section called “Actualización de un clúster de base de datos multi-AZ”.

La secuencia del número de versión es específica para cada motor de base de datos. Por ejemplo, RDS para MySQL 5.7 y 8.0 son versiones principales del motor y la actualización desde cualquier versión 5.7 hasta cualquier versión 8.0 es una actualización de versión principal. Las versiones de RDS para MySQL 5.7.22 y 5.7.23 son versiones secundarias y la actualización de 5.7.22 a 5.7.23 es una actualización de versiones secundarias.

> **Important**
>
> No puede modificar una instancia de base de datos cuando está en proceso de actualización. Durante una actualización, el estado de la instancia de base de datos es `upgrading`.

Para obtener más información acerca de las actualizaciones de las versiones principales y secundarias de un motor de base de datos específico, consulte la documentación del motor de base de datos que se indica a continuación:

- Actualizaciones del motor de base de datos de MariaDB
- Actualizaciones del motor de base de datos de Microsoft SQL Server

- Actualizaciones del motor de base de datos de RDS para MySQL
- Actualización del motor de base de datos de RDS para Oracle
- Actualizaciones del motor de base de datos de RDS para PostgreSQL

Para las actualizaciones de versiones principales, debe modificar manualmente la versión del motor de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS. En el caso de actualizaciones de versiones secundarias, puede modificar manualmente la versión del motor o elegir habilitar la opción Actualización automática de versiones secundarias.

> **Note**
>
> Las actualizaciones del motor de base de datos requieren tiempo de inactividad Puede minimizar el tiempo de inactividad necesario para la actualización de la instancia de base de datos mediante una implementación azul/verde. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Temas

- Actualización manual de la versión del motor
- Actualización automática de la versión secundaria del motor

Actualización manual de la versión del motor

Para actualizar manualmente la versión del motor de una instancia de base de datos, puede utilizar la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para actualizar la versión del motor de una instancia de base de datos con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, elija la instancia de base de datos que desea actualizar.
3. Elija Modify. Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. Para DB engine version, elija la nueva versión.

5. Elija Continue y consulte el resumen de las modificaciones.
6. Decida cuándo programar la actualización:

   - Para incluir los cambios en la cola de modificaciones pendientes, elija Aplicar durante la próxima ventana de mantenimiento programada. RDS aplica los cambios pendientes en la cola durante el siguiente periodo de mantenimiento.
   - Para aplicar los cambios inmediatamente, elija Apply immediately. Si se selecciona esta opción, puede producirse una interrupción en algunos casos. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.
7. En la página de confirmación, revise los cambios. Si son correctos, elija Modify DB instance (Modificar instancia de base de datos) para guardar los cambios.

   O bien, elija Back para editar los cambios o Cancel para cancelarlos.

AWS CLI

Para actualizar la versión del motor de una instancia de base de datos, utilice el comando modify-db-instance de la CLI. Especifique los siguientes parámetros:

- `--db-instance-identifier`: nombre de la instancia de base de datos.
- `--engine-version`: número de versión del motor de base de datos al que se va a actualizar.

  Para obtener información sobre versiones de motores válidas, utilice el comando describe-db-engine-versions de la AWS CLI.
- `--allow-major-version-upgrade`: para actualizar la versión principal.
- `--no-apply-immediately`–: para aplicar los cambios en el siguiente periodo de mantenimiento. Para aplicar los cambios inmediatamente, use `--apply-immediately`.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --engine-version new_version \
    --allow-major-version-upgrade \
    --no-apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --engine-version new_version ^
    --allow-major-version-upgrade ^
    --no-apply-immediately
```

API de RDS

Para actualizar la versión del motor de una instancia de base de datos, utilice la acción ModifyDBInstance. Especifique los siguientes parámetros:

- `DBInstanceIdentifier` – nombre de la instancia de base de datos, por ejemplo *`mydbinstance`*.
- `EngineVersion`: número de versión del motor de base de datos al que se va a actualizar. Para obtener información sobre versiones de motores válidas, utilice la operación DescribeDBEngineVersions.
- `AllowMajorVersionUpgrade`: si se permite una actualización de versión principal. Para ello, defina el valor en `true`.
- `ApplyImmediately`: indica si se deben aplicar los cambios inmediatamente o en la siguiente ventana de mantenimiento. Para aplicar los cambios inmediatamente, establezca el valor en `true`. Para aplicar los cambios en el siguiente periodo de mantenimiento, establezca el valor en `false`.

Actualización automática de la versión secundaria del motor

Las actualizaciones automáticas de las versiones secundarias actualizan periódicamente la base de datos a versiones recientes del motor de base de datos. Sin embargo, es posible que la actualización no siempre incluya la versión más reciente del motor de base de datos. Si necesita mantener las bases de datos en versiones específicas en momentos determinados, le recomendamos que las actualice manualmente a las versiones de base de datos que necesite según el calendario requerido. En caso de problemas de seguridad críticos o cuando una versión alcance su fecha de fin de soporte, Amazon RDS podría aplicar una actualización de la versión secundaria aunque no haya habilitado la opción Actualización automática de versión secundaria. Para obtener más información, consulte la documentación de actualización para el motor de base de datos específico.

- Actualizaciones de versiones secundarias automáticas de RDS para PostgreSQL

- Actualizaciones de versiones secundarias automáticas de RDS para MySQL
- Actualizaciones de versiones secundarias automáticas de RDS para MariaDB
- Actualizaciones de la versión secundaria de Oracle
- Actualizaciones del motor de base de datos de Microsoft SQL Server
- Versiones de Db2 en Amazon RDS

Temas

- Cómo funcionan las actualizaciones automáticas de versiones secundarias
- Activar las actualizaciones automáticas de versiones secundarias
- Determinación de la disponibilidad de las actualizaciones de mantenimiento
- Búsqueda de destinos de las actualizaciones automáticas de versiones secundarias

Cómo funcionan las actualizaciones automáticas de versiones secundarias

El destino de actualización es la versión del motor de base de datos a la que Amazon RDS actualiza la base de datos. Una versión de motor secundaria se designa como destino de actualización cuando se cumplen las siguientes condiciones:

- La base de datos ejecuta una versión secundaria del motor de la base de datos menor que la versión de motor secundaria de destino.

  Para encontrar la versión de motor actual de la instancia de base de datos, consulte la pestaña Configuración de la página de detalles de la base de datos o ejecute el comando de la CLI `describe-db-instances`.
- La base de datos tiene habilitada la actualización automática de versiones secundarias.

RDS programa la actualización para que se realice automáticamente en el periodo de mantenimiento. Durante la actualización, RDS hace lo siguiente:

1. Ejecuta una comprobación previa del sistema para asegurarse de que la base de datos esté en buen estado y lista para actualizarse
2. Actualiza el motor de base de datos a la versión de motor secundaria destino
3. Realiza las comprobaciones posteriores
4. Marca la actualización de la base de datos como finalizada

Las actualizaciones automáticas provocan tiempos de inactividad. La duración del tiempo de inactividad depende de varios factores, como el tipo de motor de base de datos y el tamaño de la base de datos.

Activar las actualizaciones automáticas de versiones secundarias

Puede controlar si las actualizaciones automáticas de versiones secundarias están habilitadas para una instancia de base de datos al realizar las siguientes tareas:

- Creación de una instancia de base de datos
- Modificación de una instancia de base de datos
- Creación de una réplica de lectura
- Restauración de una instancia de base de datos desde una instantánea
- Restauración de una instancia de base de datos a un momento especificado
- Importación de una instancia de base de datos desde Amazon S3 (para una copia de seguridad de MySQL en Amazon S3)

A realizar estas tareas, puede controlar si está habilitada la actualización automática de versiones secundarias para la instancia de la base de datos de las siguientes formas:

- Con la consola, establezca la opción Auto minor version upgrade (Actualización automática de versiones secundarias).
- Con la AWS CLI, establezca la opción `--auto-minor-version-upgrade|--no-auto-minor-version-upgrade`.
- Con la API de RDS, establezca el parámetro `AutoMinorVersionUpgrade`.

Determinación de la disponibilidad de las actualizaciones de mantenimiento

Para determinar si una actualización de mantenimiento, como una actualización de la versión del motor de base de datos, está disponible para su instancia de base de datos, puede utilizar la consola, la AWS CLI o la API de RDS. También puede actualizar manualmente la versión de la base de datos y ajustar el periodo de mantenimiento. Para obtener más información, consulte Mantenimiento de una instancia de base de datos.

Búsqueda de destinos de las actualizaciones automáticas de versiones secundarias

Puede utilizar el siguiente comando de la AWS CLI para determinar la versión actual de destino de actualización secundaria automática para una versión secundaria del motor de base de datos especificada en una Región de AWS específica. Puede encontrar los valores de `--engine` posibles para este comando en la descripción del parámetro `Engine` en CreateDBInstance.

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine engine \
--engine-version minor-version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine engine ^
--engine-version minor-version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

Por ejemplo, el siguiente comando de la AWS CLI determina el destino de actualización secundaria automática para la versión secundaria 8.0.11 de MySQL en la región de AWS de Este de EE. UU. (Ohio) (us-east-2).

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
--engine-version 8.0.11 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version 8.0.11 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Su resultado es similar al siguiente.

```
---------------------------------
|    DescribeDBEngineVersions    |
+--------------+-----------------+
|  AutoUpgrade |  EngineVersion  |
+--------------+-----------------+
|  False       |  8.0.15         |
|  False       |  8.0.16         |
|  False       |  8.0.17         |
|  False       |  8.0.19         |
|  False       |  8.0.20         |
|  False       |  8.0.21         |
|  True        |  8.0.23         |
|  False       |  8.0.25         |
+--------------+-----------------+
```

En este ejemplo, el valor `AutoUpgrade` es `True` para la versión 8.0.23 de MySQL. Por lo tanto, el destino de actualización secundaria automática es la versión 8.0.23 de MySQL, que está resaltado en el resultado.

> **Important**
>
> Si planea migrar una instancia de base de datos de RDS for PostgreSQL a un clúster de base de datos de Aurora PostgreSQL pronto, se recomienda encarecidamente que desactive las actualizaciones automáticas de versiones secundarias para la instancia de base de datos al principio de la fase inicial durante la planificación. La migración a Aurora PostgreSQL podría retrasarse si la versión de RDS para PostgreSQL aún no es compatible con Aurora PostgreSQL. Para obtener información acerca de Aurora PostgreSQL las versiones, vea Versiones del motor para Amazon Aurora PostgreSQL.

Cambio del nombre de una instancia de base de datos

Puede cambiar el nombre de una instancia de base de datos con la AWS Management Console, el comando `modify-db-instance` de la AWS CLI o la acción `ModifyDBInstance` de la API de Amazon RDS. Cambiar el nombre de una instancia de base de datos puede tener grandes repercusiones. A continuación, se muestra una lista de consideraciones que debe tener en cuenta antes de cambiar el nombre de una instancia de base de datos.

- Cuando cambia el nombre de una instancia de base de datos, se modifica su punto de conexión, porque la URL incluye el nombre asignado a dicha instancia. Deberá redirigir siempre el tráfico desde la URL antigua a la nueva.
- Si cambia el nombre de una instancia de base de datos, el nombre DNS anterior que utilizaba la instancia se elimina de inmediato, si bien puede quedar almacenado en la caché durante varios minutos. El nuevo nombre DNS de la instancia de base de datos se hace efectivo, aproximadamente, a los 10 minutos. La instancia de base de datos en cuestión no estará disponible hasta que se haga efectivo el nombre nuevo.
- Si cambia el nombre de una instancia, no puede usar el nombre de una instancia de base de datos existente.
- Todas las réplicas de lectura asociadas a una instancia de base de datos quedan asociadas a esa instancia después de que se le cambia el nombre. Por ejemplo, suponga que tiene una instancia de base de datos que atiende a su base de datos de producción y que esa instancia tiene varias réplicas de lectura asociadas. Si cambia el nombre de la instancia de base de datos y, luego, lo reemplaza en el entorno de producción con una instantánea de base de datos, la instancia de base de datos cuyo nombre cambió sigue teniendo esas réplicas de lectura asociadas.
- Las métricas y los eventos asociados con el nombre de una instancia de base de datos se mantienen si reutiliza un nombre. Por ejemplo, si promociona una réplica de lectura y le asigna el nombre de la instancia de base de datos primaria anterior, los eventos y las métricas asociados a la instancia de base de datos primaria se asocian a la instancia con el nuevo nombre.
- Las etiquetas de la instancia de base de datos permanecen con dicha instancia, independientemente del cambio de nombre.
- Las instantáneas de base de datos se conservan para una instancia de base de datos a la que se le haya cambiado el nombre.

> **Note**
>
> Una instancia de base de datos es un entorno de base de datos aislado que se ejecuta en la nube. Una instancia de base de datos puede alojar varias bases de datos o una única base de datos de Oracle con varios esquemas. Para obtener información sobre cómo cambiar el nombre de una base de datos, consulte la documentación de su motor de base de datos.

Cambio de nombre para sustituir una instancia de base de datos existente

Los motivos más habituales por los que se cambia el nombre de una instancia de base de datos son la promoción de una réplica de lectura o la restauración de datos a partir de una instantánea de base de datos o mediante la recuperación a un momento dado (PITR). Al cambiar el nombre de la base de datos, puede sustituir la instancia de base de datos sin tener que cambiar ningún código de la aplicación que haga referencia a la instancia. En estos casos, haría lo siguiente:

1. Detener todo el tráfico que va hacia la instancia de base de datos primaria. Esto puede implicar el redireccionamiento del tráfico para evitar que tenga acceso a las bases de datos de la instancia o cualquier otro método.
2. Cambie el nombre de la instancia de base de datos primaria por un nombre que indique que ya no es la instancia de base de datos primaria, como se describe más adelante en este tema.
3. Crear una nueva instancia de base de datos primaria restaurándola desde una instantánea de base de datos o promoviendo una réplica de lectura y, a continuación, asignar a la nueva instancia el nombre de la instancia de base de datos primaria anterior.
4. Asociar las réplicas de lectura a la nueva instancia de base de datos primaria.

Si elimina la instancia de base de datos primaria antigua, deberá eliminar todas las instantáneas de base de datos no deseadas de la instancia primaria antigua.

Para obtener información acerca de la promoción de una réplica de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

> **Important**
>
> La instancia de base de datos se reinicia cuando se cambia de nombre. Para las instancias Multi-AZ de RDS para SQL Server con las opciones AlwaysOn o Mirroring habilitadas, se

espera una conmutación por error cuando la instancia se reinicie tras la operación de cambio de nombre.

Consola

Para cambiar el nombre de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea cambiar de nombre.
4. Elija Modify.
5. En Settings (Configuración), escriba un nuevo nombre para DB instance identifier (Identificador de instancia de base de datos).
6. Elija Continue.
7. Para aplicar los cambios inmediatamente, elija Apply immediately. Si se selecciona esta opción, puede producirse una interrupción en algunos casos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
8. En la página de confirmación, revise los cambios. Si son correctos, elija Modify DB Instance para guardarlos.

   O bien, elija Back para editar los cambios o Cancel para cancelarlos.

AWS CLI

Para cambiar el nombre de una instancia de base de datos, utilice el comando AWS CLI de la `modify-db-instance`. Proporcione el nombre nuevo de la instancia de base de datos al valor `--db-instance-identifier` y al parámetro `--new-db-instance-identifier` actuales.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier DBInstanceIdentifier \
    --new-db-instance-identifier NewDBInstanceIdentifier
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier DBInstanceIdentifier ^
    --new-db-instance-identifier NewDBInstanceIdentifier
```

API de RDS

Para cambiar el nombre de una instancia de base de datos, llame a la operación de la API de Amazon RDS `ModifyDBInstance` con los siguientes parámetros:

- `DBInstanceIdentifier`: nombre actual de la instancia
- `NewDBInstanceIdentifier`: nombre nuevo de la instancia

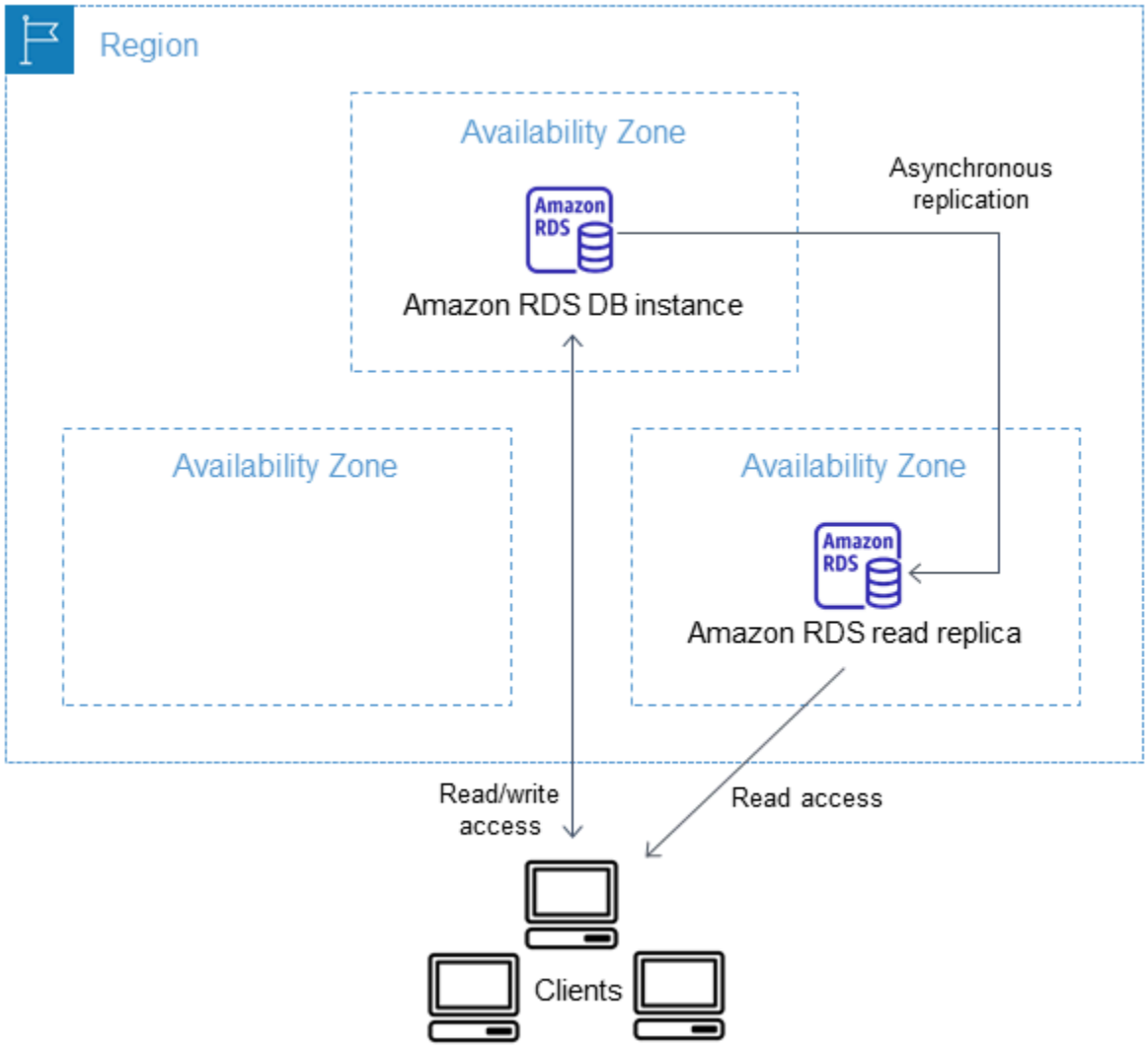
Trabajo con réplicas de lectura de instancias de base de datos

Una réplica de lectura es una copia de solo lectura de una instancia de base de datos. Puede reducir la carga de la instancia de la base de datos principal enrutando las consultas de sus aplicaciones a la réplica de lectura. De este modo, puede ajustar la escala horizontalmente y de manera elástica por encima de las restricciones de capacidad de una instancia de base de datos para las cargas de trabajo de las bases de datos con operaciones intensivas de lectura.

Para crear una réplica de lectura a partir de una instancia de base de datos de origen, Amazon RDS usa las características de replicación integradas del motor de base de datos. Para obtener información sobre la utilización de las réplicas de lectura con un motor específico, consulte las secciones siguientes:

- Trabajo con las réplicas de Amazon RDS para Db2
- Uso de réplicas de lectura de MariaDB
- Uso de réplicas de lectura para Microsoft SQL Server en Amazon RDS
- Uso de réplicas de lectura de MySQL
- Trabajo con las réplicas de lectura para Amazon RDS para Oracle
- Uso de réplicas de lectura para Amazon RDS para PostgreSQL

Tras crear una réplica de lectura a partir de una instancia de base de datos de origen, el origen se convierte en la instancia de base de datos principal. Al realizar actualizaciones en la instancia de base de datos principal, Amazon RDS las copia de forma asíncrona en la réplica de lectura. El siguiente diagrama muestra una instancia de base de datos de origen que se replica en una réplica de lectura en una zona de disponibilidad (AZ) diferente. Los clientes tienen acceso de lectura/escritura a la instancia de base de datos principal y acceso de solo lectura a la réplica.



Las réplicas de lectura se facturan como instancias de base de datos estándar con las mismas tarifas que la clase de instancia de base de datos utilizada para la réplica. No se le cobrará por los gastos de transferencia de datos en los que se incurra al replicar datos entre la instancia de base de datos de origen y la réplica de lectura de la misma Región de AWS. Para obtener más información, consulte Costos de la replicación entre regiones y Facturación de instancia de base de datos para Amazon RDS.

Temas

- Información general de las réplicas de lectura de Amazon RDS
- Diferencias entre réplicas de lectura para motores de base de datos
- Creación de una réplica de lectura
- Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente

- Monitoreo de la replicación de lectura
- Creación de una réplica de lectura en una Región de AWS distinta

Información general de las réplicas de lectura de Amazon RDS

En las siguientes secciones se describen las réplicas de lectura de instancia de base de datos. Para obtener más información acerca de las réplicas de lectura de clúster de base de datos multi-AZ, consulte the section called “Trabajo con réplicas de lectura de clústeres de base de datos Multi-AZ”.

Temas

- Casos de uso de réplicas de lectura
- Cómo funcionan las réplicas de lectura
- Lectura de réplicas en una implementación multi-AZ
- Réplicas de lectura entre regiones
- Tipos de almacenamiento de las réplicas de lectura
- Restricciones para crear una réplica a partir de una réplica
- Consideraciones a la hora de borrar réplicas

Casos de uso de réplicas de lectura

La implementación de una o varias réplicas de lectura para una instancia de base de datos de origen puede tener sentido en diversas situaciones, como las siguientes:

- Aumentar la escala por encima de la capacidad de E/S o de computación de una instancia de base de datos para las cargas de trabajo de las bases de datos con operaciones intensivas de lectura. Puede dirigir este exceso del tráfico de lectura a una o varias réplicas de lectura.
- Servir tráfico de lectura cuando la instancia de base de datos de origen no está disponible. En algunos casos, es posible que su instancia de base de datos de origen no pueda aceptar solicitudes de E/S, por ejemplo, debido a la suspensión de E/S para las copias de seguridad o el mantenimiento programado. En estos casos, puede dirigir el tráfico de lectura a sus réplicas de lectura. En este caso de uso, recuerde que los datos de la réplica de lectura pueden estar "obsoletos" porque la instancia de base de datos de origen no está disponible.
- Las situaciones de informes de negocios o de almacenamiento de datos en las que se desea que las consultas de informes de negocios se ejecuten en una réplica de lectura y no en la instancia de base de datos de producción.

- Implementación de recuperación de desastres Puede promocionar una réplica de lectura en la instancia independiente como solución de recuperación de desastres si la instancia de base de datos principal produce un error.

Cómo funcionan las réplicas de lectura

Cuando se crea una réplica de lectura, se especifica una instancia de base de datos existente como origen. A continuación, Amazon RDS realiza una instantánea de la instancia de origen y crea una instancia de solo lectura a partir de la instantánea. Luego, Amazon RDS utiliza el método de reproducción asíncrono para que el motor de base de datos actualice la réplica de lectura cuando se produzca un cambio en la instancia de base de datos primaria.

La réplica de lectura funciona como una instancia de base de datos que permite únicamente conexiones de solo lectura. Las excepciones son los motores de base de datos RDS para Db2 y RDS para Oracle, que admiten bases de datos de réplica en modo de espera y en modo montado, respectivamente. Una réplica en espera y una réplica montada no aceptan conexiones de usuario, por lo que no pueden servir cargas de trabajo de solo lectura. El uso principal de las réplicas en espera y las réplicas montadas es la recuperación ante desastres entre regiones. Para obtener más información, consulte Trabajo con las réplicas de Amazon RDS para Db2 y Trabajo con las réplicas de lectura para Amazon RDS para Oracle.

Las aplicaciones se conectan a una réplica de lectura de la misma forma que a cualquier instancia de base de datos. Amazon RDS replica todas las bases de datos de la instancia de base de datos de origen.

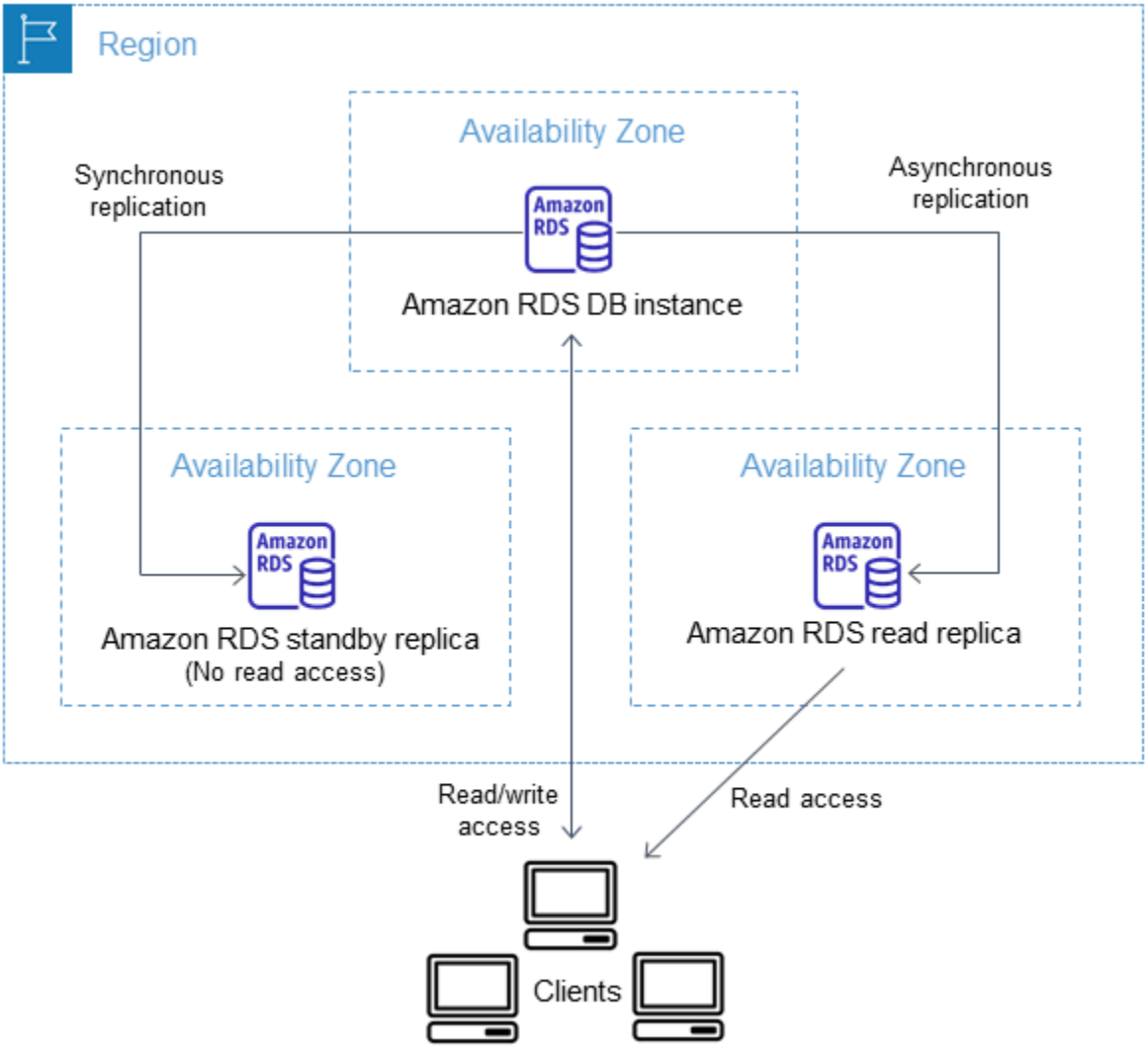
Debe crear réplicas de lectura manualmente. RDS no admite el escalado automático de réplicas de lectura, que es la acción de agregar o eliminar automáticamente réplicas de lectura a medida que cambia la demanda de lectura.

Lectura de réplicas en una implementación multi-AZ

Se puede configurar una réplica de lectura para una instancia de base de datos que también tenga una réplica en espera configurada para alta disponibilidad en una implementación Multi-AZ. Una replicación con la réplica en espera es sincrónica. A diferencia de una réplica de lectura, una réplica en espera no puede servir tráfico de lectura.

En el siguiente escenario, los clientes tienen acceso de lectura/escritura a una instancia de base de datos principal en una AZ. La instancia principal copia las actualizaciones de forma asincrónica en

una réplica de lectura en una segunda AZ y también las copia de forma sincrónica en una réplica en espera en una tercera AZ. Los clientes solo tienen acceso de lectura a la réplica de lectura.



Para obtener más información acerca de las réplicas de alta disponibilidad y en espera, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Réplicas de lectura entre regiones

En algunos casos, una réplica de lectura reside en una Región de AWS distinta de la de su instancia de base de datos principal. En esos casos, Amazon RDS configura un canal de comunicaciones seguro entre la instancia de base de datos primaria y la réplica de lectura. Amazon RDS establece cualquier configuración de seguridad de AWS necesarias para habilitar el canal seguro, por ejemplo agregar entradas de grupo de seguridad. Para obtener información sobre las réplicas de lectura entre regiones, consulte Creación de una réplica de lectura en una Región de AWS distinta.

La información de este capítulo hace referencia a la creación de réplicas de lectura de Amazon RDS, ya sea en la misma Región de AWS que la instancia de base de datos de origen o en una Región de AWS diferente. La siguiente información no es válida para configurar la replicación con una instancia que se ejecute en una instancia de Amazon EC2 o que esté instalada localmente.

Tipos de almacenamiento de las réplicas de lectura

De forma predeterminada, una réplica de lectura se crea con el mismo tipo de almacenamiento que la instancia de base de datos de origen. Sin embargo, puede crear una réplica de lectura que tenga un tipo de almacenamiento distinto del de la instancia de base de datos de origen en función de las opciones que se muestran en la siguiente tabla.

Tipo de almacenamiento de la instancia de base de datos de origen	Asignación de almacenamiento de la instancia de base de datos de origen	Opciones del tipo de almacenamiento de las réplicas de lectura
Provisioned IOPS (IOPS aprovisionadas)	100 GiB–64 TiB	IOPS aprovisionadas, uso general, magnético
Uso general	100 GiB–64 TiB	IOPS aprovisionadas, uso general, magnético
Uso general	<100 GiB	Uso general, magnético
Magnético	100 GiB–6 TiB	IOPS aprovisionadas, uso general, magnético
Magnético	<100 GiB	Uso general, magnético

> **Note**
>
> Cuando aumenta el almacenamiento asignado de una réplica de lectura, debe ser de al menos un 10 por ciento. Si intenta aumentar el valor en menos del 10 por ciento, obtendrá un error.

Restricciones para crear una réplica a partir de una réplica

Amazon RDS no admite la replicación circular. No puede configurar una instancia de base de datos para que sirva como origen de replicación para una instancia de base de datos existente. Solo puede crear una nueva réplica de lectura desde una instancia de base de datos existente. Por ejemplo, si **`MySourceDBInstance`** se replica en **`ReadReplica1`**, no puede configurar **`ReadReplica1`** para volverse a replicar en **`MySourceDBInstance`**.

Para RDS para MariaDB y RDS para MySQL, y en determinadas versiones de RDS para PostgreSQL, puede crear una réplica de lectura a partir de una réplica de lectura existente. Por ejemplo, puede crear una réplica de lectura nueva **`ReadReplica2`** a partir de una réplica **`ReadReplica1`** existente. En RDS para Db2, RDS para Oracle y RDS para SQL Server, no puede crear una réplica de lectura a partir de una réplica de lectura existente.

Consideraciones a la hora de borrar réplicas

RDS no admite el escalado automático de réplicas de lectura. Por lo tanto, RDS no aumentará el número de réplicas cuando la demanda aumente ni disminuirá el número de réplicas cuando la demanda disminuya. Si ya no necesita réplicas de lectura, elimínelas manualmente con los mismos mecanismos que emplea para eliminar una instancia de base de datos. Si elimina una instancia de base de datos de origen sin eliminar las réplicas de lectura en la misma Región de AWS, cada réplica se convertirá en una instancia de base de datos independiente.

Para obtener más información sobre la eliminación de instancias de base de datos, consulte Eliminación de una instancia de base de datos. Para obtener información sobre la promoción de réplicas de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente. Para obtener información relacionada con la eliminación de la instancia de base de datos de origen para una réplica de lectura entre regiones, consulte Consideraciones relativas a la replicación entre regiones.

Diferencias entre réplicas de lectura para motores de base de datos

Dado que los motores de base de datos de Amazon RDS implementan la replicación de forma diferente, existen varias diferencias importantes que debe conocer.

Db2

Las réplicas para RDS para Db2 tienen las siguientes características y comportamientos:

- Método de replicación: replicación física.

- Purga de registros de transacciones: RDS para Db2 purga los registros de la instancia de base de datos principal cuando se han cumplido las siguientes condiciones:
  - Los registros tienen al menos dos horas de antigüedad.
  - Ha pasado la configuración de horas de retención de registros de archivo.
  - RDS para Db2 ha replicado correctamente los registros en todas las instancias de base de datos de réplica.

  Esto se aplica tanto a instancias de base de datos de la misma Región de AWS como a instancias de base de datos de distintas regiones. Para obtener información acerca de cómo configurar las horas de retención del registro de archivo, consulte rdsadmin.set_archive_log_retention.
- Réplicas que se pueden escribir: una réplica de Db2 es una copia física y Db2 no permite escribir en una réplica. Puede promocionar la réplica para que sea de escritura. La réplica promocionada tiene los datos replicados hasta el momento en que se realizó la solicitud para promocionarla.
- Copias de seguridad: las réplicas de RDS para Db2 admiten copias de seguridad automáticas e instantáneas manuales.
- Replicación paralela: los datos del registro de archivo siempre se transmiten en paralelo desde la base de datos principal a todas las réplicas.
- Estado en espera: el uso principal de las réplicas en espera es la recuperación ante desastres entre regiones. Para obtener más información, consulta Trabajo con las réplicas de Amazon RDS para Db2.

MariaDB y MySQL

Las réplicas de lectura para RDS para MariaDB y RDS para MySQL tienen las siguientes características y comportamientos:

- Método de replicación: replicación lógica.
- Purga de registros de transacciones: RDS para MariaDB y RDS para MySQL conservan todos los registros binarios que no se han aplicado.
- Réplicas que se pueden escribir: puede habilitar la réplica de lectura de MariaDB o MySQL para que se pueda escribir.
- Copias de seguridad: las copias de seguridad automáticas y las instantáneas manuales se admiten en las réplicas de lectura de RDS para MariaDB o RDS para MySQL.
- Replicación paralela: todas las versiones de MariaDB y MySQL compatibles permiten subprocesos de replicación paralela.

- Estado montado: no se admite.

Oracle

Las réplicas de lectura para RDS para Oracle tienen las siguientes características y comportamientos:

- Método de replicación: replicación física.
- Purga de registros de transacciones: si una instancia de base de datos principal no tiene réplicas de lectura entre regiones, Amazon RDS para Oracle mantiene durante un mínimo de dos horas los registros de transacciones en la instancia de base de datos de origen. Los registros se purgan de la base de datos de origen después de dos horas o cuando hayan pasado las horas de retención del registro del archivo establecidas, lo que lleve más tiempo. Los registros se purgan de la réplica de lectura después de haber pasado las horas de retención del registro del archivo establecidas solo si se han aplicado correctamente a la base de datos.

  En algunos casos, es posible que una instancia de base de datos principal tenga una o más réplicas de lectura entre regiones. Si esto ocurre, Amazon RDS para Oracle mantiene los registros de transacción en la instancia de base de datos de origen hasta que se hayan transmitido y aplicado a todas las réplicas de lectura entre regiones.

  Para obtener información acerca de cómo configurar las horas de retención del registro de archivo, consulte Retención de los registros REDO archivados.
- Réplicas que se pueden escribir: una réplica de lectura de Oracle es una copia física y Oracle no permite escribir en una réplica de lectura. Puede promocionar la réplica de lectura para que sea de escritura. La réplica de lectura promocionada tiene los datos replicados hasta el momento en el que se hizo la solicitud para promocionarla.
- Copias de seguridad: las copias de seguridad automáticas y las instantáneas manuales se admiten las réplicas de lectura de RDS para Oracle.
- Replicación paralela: los datos de registro de REDO siempre se transmiten en paralelo desde la base de datos principal a todas las réplicas de lectura.
- Estado montado: el uso principal de las réplicas montadas es la recuperación ante desastres entre regiones. No se requiere una licencia Active Data Guard para las réplicas montadas. Para obtener más información, consulte Trabajo con las réplicas de lectura para Amazon RDS para Oracle.

PostgreSQL

Las réplicas de lectura para RDS para PostgreSQL tienen las siguientes características y comportamientos:

- Método de replicación: replicación física.
- Purga de registros de transacciones: PostgreSQL cuenta con el parámetro `wal_keep_segments`, que establece cuántos archivos de registro de escritura previa (WAL) se conservan para proporcionar datos a las réplicas de lectura. El valor del parámetro especifica el número de registros que conservar.
- Réplicas que se pueden escribir: una réplica de lectura de PostgreSQL es una copia física y PostgreSQL no permite que una réplica de lectura sea de escritura.
- Copias de seguridad: se admiten instantáneas manuales para las réplicas de lectura de RDS para PostgreSQL. Las copias de seguridad automatizadas para réplicas de lectura se admiten únicamente para RDS para PostgreSQL 14.1 y versiones posteriores. No puede activar las copias de seguridad automatizadas para las réplicas de lectura de RDS para PostgreSQL de versiones anteriores a 14.1. Para RDS para PostgreSQL 13 y versiones anteriores, cree una instantánea a partir de una réplica de lectura si desea realizar una copia de seguridad de ella.
- Replicación paralela: PostgreSQL tiene un único proceso para gestionar la replicación.
- Estado montado: no se admite.

SQL Server

Las réplicas de lectura para RDS para SQL Server tienen las siguientes características y comportamientos:

- Método de replicación: replicación física.
- Purga de registros de transacciones: el archivo de registro virtual (VLF) del archivo de registro de transacciones en la réplica principal se puede truncar después de que ya no sea necesario para las réplicas secundarias.

  El VLF solo se puede marcar como inactivo cuando los registros se han reforzado en las réplicas. Independientemente de lo rápido que los subsistemas de disco estén en la réplica principal, el registro de transacciones mantendrá los VLF hasta que la réplica más lenta se haya reforzado.
- Réplicas que se pueden escribir: una réplica de lectura de SQL Server es una copia física y SQL Server no permite escribir en una réplica de lectura. Puede promocionar la réplica de lectura

para que sea de escritura. La réplica de lectura promocionada tiene los datos replicados hasta el momento en el que se hizo la solicitud para promocionarla.

- Copias de seguridad: las copias de seguridad automáticas y las instantáneas manuales no se admiten en las réplicas de lectura de RDS para SQL Server.
- Replicación paralela: los datos de registro de REDO siempre se transmiten en paralelo desde la base de datos principal a todas las réplicas de lectura.
- Estado montado: no se admite.

Creación de una réplica de lectura

Se puede crear una réplica de lectura a partir de una instancia de base de datos existente, utilizando AWS Management Console, AWS CLI, o la API de RDS. Para crear una réplica de lectura, debe especificar `SourceDBInstanceIdentifier`, que es el identificador de instancias de base de datos de la instancia de base de datos de origen desde la que desea replicar.

Cuando se crea una réplica de lectura, Amazon RDS realiza una instantánea de base de datos de la instancia de base de datos de origen y comienza la replicación. La instancia de base de datos de origen experimenta una suspensión de E/S muy breve cuando comienza la operación de instantánea de base de datos. La suspensión de E/S suele durar un segundo. Puede evitar la suspensión de E/S si la instancia de base de datos de origen es una implementación Multi-AZ, porque en ese caso la instantánea se toma de la instancia de base de datos secundaria.

Una transacción activa de ejecución prolongada puede ralentizar el proceso de creación de la réplica de lectura. Le recomendamos que espere a que se completen las transacciones de ejecución prolongada antes de crear una réplica de lectura. Si crea varias réplicas de lectura en paralelo a partir de la misma instancia de base de datos de origen, Amazon RDS solo realiza una instantánea cuando comienza la primera acción de creación.

Cuando se crea una réplica de lectura, hay varias cosas que se deben tener en cuenta. En primer lugar, debe habilitar las copias de seguridad automáticas en la instancia de base de datos de origen estableciendo el periodo de retención de copia de seguridad en un valor distinto de 0. Este requisito también es válido para una réplica de lectura que sea la instancia de base de datos de origen de otra réplica de lectura. Para habilitar las copias de seguridad automáticas en una réplica de lectura de RDS para My SQL, primero cree la réplica de lectura y modifíquela a continuación para habilitar las copias de seguridad automáticas.

> **Note**
>
> En una Región de AWS, recomendamos encarecidamente crear todas las réplicas de lectura en la misma nube privada virtual (VPC) basándose en Amazon VPC como instancia de base de datos de origen. Si crea una réplica de lectura en una VPC diferente de la instancia de base de datos de origen, los rangos de enrutamiento entre dominios sin clases (CIDR) pueden superponerse entre la réplica y el sistema RDS. La superposición de CIDR hace que la réplica sea inestable, lo que puede afectar negativamente a las aplicaciones que se conectan a ella. Si obtiene un error al crear la réplica de lectura, elija un grupo de subred de base de datos de destino diferente. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.
>
> No existe una forma directa de crear una réplica de lectura en otra Cuenta de AWS mediante la consola o AWS CLI.

Consola

Para crear una réplica de lectura a partir de una instancia de base de datos de origen

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione la instancia de base de datos que desea usar como origen de una réplica de lectura
4. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).
5. En DB instance identifier (Identificador de instancias de bases de datos), escriba un nombre para la réplica de lectura.
6. Elija la configuración de la instancia. Es recomendable usar la misma clase de instancia de base de datos y el mismo tipo de almacenamiento o mayores que la instancia de base de datos de origen para la réplica de lectura.
7. Para la Región de AWS, especifique la región de destino de la réplica de lectura.
8. En Almacenamiento, especifique el tamaño del almacenamiento asignado y si quiere utilizar el autoescalado de almacenamiento.

   Si la instancia de base de datos de origen no dispone de la última configuración de almacenamiento, la opción Actualizar la configuración del sistema de archivos de almacenamiento estará disponible. Puede habilitar esta opción para actualizar el sistema

de archivos de almacenamiento de la réplica de lectura a la configuración preferida. Para obtener más información, consulte the section called “Actualización del sistema de archivos de almacenamiento”.

9. En Disponibilidad, elija si quiere crear una réplica en espera en otra zona de disponibilidad para permitir la conmutación por error de la réplica.

> **Note**
>
> La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.

10. Especifique otros ajustes de la instancia de base de datos. Para obtener información acerca de cada configuración disponible, consulte Configuración de instancias de base de datos.
11. Para crear una réplica de lectura cifrada, expanda Configuración adicional y especifique la configuración siguiente:

    a. Elija Habilitar el cifrado.

    b. Para AWS KMS key, elija el identificador AWS KMS key de la clave de KMS.

> **Note**
>
> La instancia de base de datos de origen debe estar cifrada. Para obtener más información acerca del cifrado de la instancia de base de datos de origen, consulte Cifrado de recursos de Amazon RDS.

12. Elija Create read replica (Crear réplica de lectura).

Después de crear la réplica de lectura, puede verla en la página Bases de datos de la consola de RDS. Muestra Réplica en la columna Rol .

AWS CLI

Para crear una réplica de lectura a partir de una instancia de base de datos de origen, utilice el comando create-db-instance-read-replica de la AWS CLI. En este ejemplo, también se establece el tamaño de almacenamiento asignado, se habilita el autoescalado de almacenamiento y se actualiza el sistema de archivos a la configuración preferida.

Puede especificar otras opciones. Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

> **Note**
>
> Para crear una réplica en espera de RDS para Db2, incluya `--replica-mode mounted` en el siguiente comando de la AWS CLI.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier myreadreplica \
    --source-db-instance-identifier mydbinstance \
    --allocated-storage 100 \
    --max-allocated-storage 1000 \
    --upgrade-storage-config
```

Para Windows:

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --source-db-instance-identifier mydbinstance ^
    --allocated-storage 100 ^
    --max-allocated-storage 1000 ^
    --upgrade-storage-config
```

API de RDS

Para crear una réplica de lectura a partir de una instancia de base de datos MySQL, MariaDB, Oracle, PostgreSQL o SQL Server de origen, llame a la operación CreateDBInstanceReadReplica de la API de Amazon RDS con los siguientes parámetros obligatorios:

- `DBInstanceIdentifier`
- `SourceDBInstanceIdentifier`

> **Note**
>
> Para crear una réplica en espera de RDS para Db2, establezca la operación `ReplicaMode` opcional en `mounted`.

Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente

Puede promover una réplica de lectura a una instancia de base de datos independiente. Si una instancia de base de datos de origen tiene varias réplicas de lectura, promocionar una de las réplicas de lectura a instancia de base de datos no tiene ningún efecto en las otras réplicas.

Cuando se promociona una réplica de lectura, RDS reinicia la instancia de base de datos antes de que esté disponible. Este proceso de promoción puede tardar unos minutos o más, según el tamaño de la réplica de lectura.



Casos de uso para promocionar una réplica de lectura

Hay varios motivos por los que promocionar una réplica de lectura a una instancia de base de datos independiente:

- Implementación de recuperación de errores: puede utilizar la promoción de réplica de lectura como esquema de recuperación de datos si la instancia de base de datos principal produce un error. Este enfoque complementa la replicación sincrónica, la detección automática de errores y la conmutación por error.

Si es consciente de las ramificaciones y limitaciones de la replicación asíncrona y a pesar de ello quiere usar la promoción de réplicas de lectura para la recuperación de datos, puede hacerlo. Para ello, cree primero una réplica de lectura y, a continuación, monitoree la instancia de base de datos principal para ver si se producen errores. En caso de error, haga lo siguiente:

1. Promocione la réplica de lectura.
2. Dirija el tráfico de la base de datos a la instancia de base de datos promocionada.
3. Cree una réplica de lectura de reemplazo que tenga la instancia de base de datos promocionada como origen.

- Actualización de la configuración de almacenamiento: si la instancia de base de datos de origen no tiene la configuración de almacenamiento preferida, puede crear una réplica de lectura de la instancia y actualizar la configuración del sistema de archivos de almacenamiento. Esta opción migra el sistema de archivos de la réplica de lectura a la configuración preferida. Luego, puede promover la réplica de lectura en una instancia independiente.

  Puede utilizar esta opción para superar las limitaciones de escalado de almacenamiento y tamaño de archivos de los sistemas de archivos de 32 bits más antiguos. Para obtener más información, consulte the section called “Actualización del sistema de archivos de almacenamiento”.

  Esta opción solo está disponible si su instancia de base de datos de origen no tiene la configuración de almacenamiento más reciente o si va a cambiar la clase de instancia de base de datos en la misma solicitud.

- Fragmentación: la fragmentación es un tipo de arquitectura en el que no se comparte nada y, en esencia, consiste en dividir una base de datos grande en varias bases de datos más pequeñas. Una forma habitual de partir una base de datos es dividir las tablas que no están unidas en la misma consulta entre diferentes hosts. Otro método es duplicar una tabla entre varios hosts y, a continuación, usar un algoritmo de hash para determinar qué host recibe una actualización determinada. Puede crear réplicas de lectura correspondientes a cada uno de sus particiones (bases de datos más pequeñas) y promocionarlas cuando decida convertirlas en particiones independientes. A continuación puede separar el espacio de claves (si va a dividir filas) o la distribución de las tablas para cada uno de los fragmentos dependiendo de sus necesidades.

- Realización de operaciones DDL (solo MySQL y MariaDB): las operaciones DDL, como la creación o la reconstrucción de índices, pueden requerir tiempo y tener un impacto considerable en el desempeño de una instancia de base de datos. Puede realizar estas operaciones en una réplica de lectura de MySQL o MariaDB una vez que la réplica de lectura se haya sincronizado con la

instancia de base de datos principal. A continuación, puede promocionar la réplica de lectura y dirigir sus aplicaciones para que usen la instancia promocionada.

> **Note**
>
> Si su réplica de lectura es una instancia de base de datos de RDS para Oracle, puede realizar una transición en lugar de una promoción. En una transición, la instancia de base de datos de origen pasa a ser la nueva réplica y la réplica pasa a ser la nueva instancia de base de datos de origen. Para obtener más información, consulte Realización de una conmutación de Oracle Data Guard.

Características de una réplica de lectura promocionada

Una vez que haya promocionado la réplica de lectura, dejará de funcionar como tal y pasará a ser una instancia de base de datos independiente. La nueva instancia de base de datos independiente tiene las siguientes características:

- La instancia de base de datos independiente conserva el grupo de opciones y el grupo de parámetros de la réplica de lectura previa a la promoción.
- Puede crear réplicas de lectura a partir de la instancia de base de datos independiente y realizar operaciones de restauración a un momento dado.
- No puede usar la instancia de base de datos como déstino de la réplica, puesto que ya no es una réplica de lectura.

Requisitos previos para promocionar una réplica de lectura

Antes de promocionar una réplica de lectura, siga este procedimiento:

- Revise su estrategia de copia de seguridad:
  - Le recomendamos que habilite las copias de seguridad y que complete al menos una de ellas. La duración de la copia de seguridad es una función del número de cambios en la base de datos desde la copia de seguridad anterior.
  - Si ha habilitado las copias de seguridad en la réplica de lectura, configure el intervalo de copia de seguridad automática para que las copias de seguridad diarias no interfieran en la promoción de la réplica de lectura.

  - Asegúrese de que la réplica de lectura no tenga el estado `backing-up`. No puede promocionar una réplica de lectura si se encuentra en ese estado.
- Detenga la escritura de transacciones en la instancia de base de datos principal y, a continuación, espere hasta que RDS haya realizado todas las actualizaciones en la réplica de lectura.

  Las actualizaciones de la base de datos se producen en la réplica de lectura después de haberse producido en la instancia de la base de datos principal. Este retardo en la réplica puede variar considerablemente. Utilice la métrica `Replica Lag` para determinar cuándo se han completado todas las actualizaciones en la réplica de lectura.
- (Solo para MySQL y MariaDB) Para realizar cambios en una réplica de lectura MySQL o MariaDB antes de promocionarla, establezca el parámetro `read_only` en `0` en el grupo de parámetros de base de datos para la réplica de lectura. A continuación, puede llevar a cabo todas las operaciones DDL necesarias, como la creación de índices, en la réplica de lectura. Las acciones realizadas en la réplica de lectura no afectan al rendimiento de la instancia de base de datos principal.

Promoción de una réplica de lectura: pasos básicos

Los siguientes pasos muestran el proceso general para promocionar una réplica de lectura a instancia de base de datos:

1. Promueva la réplica de lectura mediante la opción Promote (Promover) de la consola de Amazon RDS, el comando de la AWS CLI `promote-read-replica` o la operación `PromoteReadReplica` de la API de Amazon RDS.

   > **Note**
   >
   > El proceso de promoción tarda algunos minutos en completarse. Cuando se promociona una réplica de lectura, RDS detiene la réplica y la reinicia. Una vez completado el reinicio, la réplica de lectura pasa a estar disponible como nueva instancia de base de datos.

2. (Opcional) Modifique la nueva instancia de base de datos para que sea una implementación Multi-AZ. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS y Configuración y administración de una implementación multi-AZ para Amazon RDS.

Consola

Para promover una réplica de lectura a una instancia de base de datos independiente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos).

   Aparece el panel Databases (Bases de datos). Cada réplica de lectura muestra Replica (Réplica) en la columna Role (Rol).
3. Elija la réplica de lectura que desea promocionar.
4. En Actions (Acciones), seleccione Promote (Promover).
5. En la página Promote Read Replica (Promocionar réplica de lectura), escriba el periodo de retención de copia de seguridad y el periodo de copia de seguridad para la instancia de base de datos recientemente promocionada.
6. Cuando la configuración sea la que desea, elija Continue.
7. En la página de confirmación, elija Promote Read Replica (Promocionar réplica de lectura).

AWS CLI

Para promover una réplica de lectura a una instancia de base de datos independiente, use el comando AWS CLI `promote-read-replica`.

Example

Para Linux, macOS o Unix:

```
aws rds promote-read-replica \
    --db-instance-identifier myreadreplica
```

Para Windows:

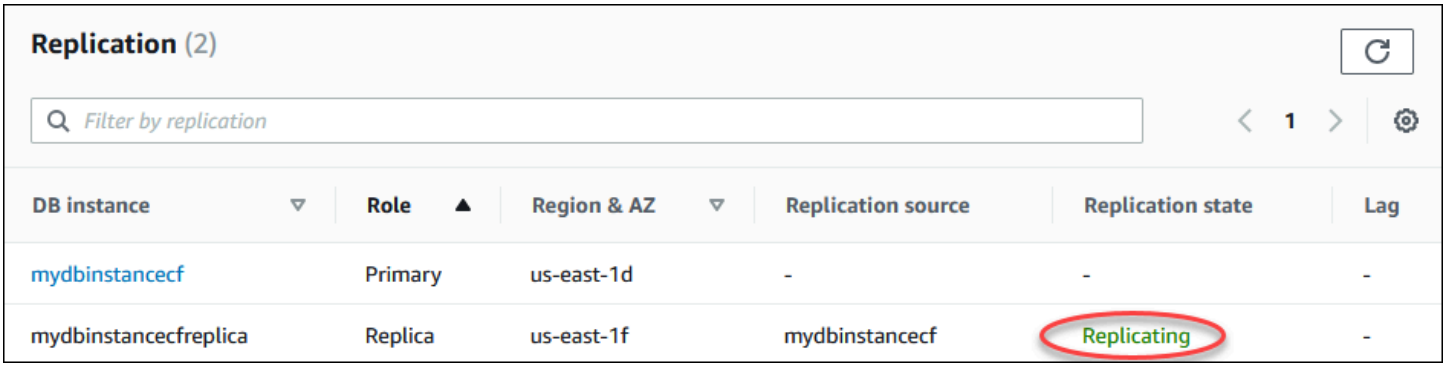
```
aws rds promote-read-replica ^
    --db-instance-identifier myreadreplica
```

API de RDS

Para promover una réplica de lectura a una instancia de base de datos independiente, llame a la operación `PromoteReadReplica` de la API de Amazon RDS con el parámetro `DBInstanceIdentifier` requerido.

Monitoreo de la replicación de lectura

Puede monitorear el estado de una réplica de lectura de varias formas. La consola de Amazon RDS muestra el estado de una réplica de lectura en la sección Replicación de la pestaña Conectividad y seguridad, en los detalles de la réplica de lectura. Para ver los detalles de una réplica de lectura, elija el nombre de la réplica de lectura en la lista de instancias de base de datos en la consola de Amazon RDS.



También puede ver el estado de una réplica de lectura con el comando `describe-db-instances` de la AWS CLI o la operación `DescribeDBInstances` de la API de Amazon RDS.

El estado de una réplica de lectura puede ser uno de los siguientes:

- replicating (replicando): la réplica de lectura se está replicando correctamente.
- Replicación degradada (solo SQL Server y PostgreSQL): las réplicas reciben datos de la instancia principal, pero una o más bases de datos no están recibiendo actualizaciones. Esto puede ocurrir, por ejemplo, cuando una réplica se encuentra en el proceso de configuración de las bases de datos recién creadas. También puede ocurrir cuando se realizan cambios en objetos grandes o en DDL no compatibles en el entorno azul de una implementación azul/verde.

  El estado no pasa de `replication degraded` a `error`, a menos que se produzca un error durante el estado degradado.
- error: se ha producido un error durante la replicación. Compruebe el campo Replication Error (Error de replicación) en la consola de Amazon RDS o el registro de eventos para determinar el error

exacto. Para obtener más información acerca de resolución de problemas de replicación, consulte Solución de problemas de réplicas de lectura de MySQL.

- terminated (terminada) (solo MariaDB, MySQL o PostgreSQL): la replicación se ha terminado. Esto sucede si la replicación se ha detenido durante más de 30 días consecutivos, ya sea manualmente o por un error de replicación. En ese caso, Amazon RDS termina la reproducción entre la instancia de base de datos primaria y todas las réplicas de lectura. Amazon RDS realiza ese procedimiento para impedir que aumenten los requisitos de almacenamiento en la instancia de base de datos de origen y que se incrementen los tiempos de conmutación por error.

  La replicación no completada puede afectar al almacenamiento, ya que los registros pueden aumentar en tamaño y en número debido al alto volumen de mensajes de error que se escriben en el registro. La replicación no completada puede afectar también a la recuperación de errores debido al tiempo que Amazon RDS necesita para mantener y procesar el elevado número de registros durante la recuperación.
- terminated (terminado) (solo Oracle): la replicación ha terminado. Esto sucede si la replicación se ha detenido durante más de 8 horas por no haber suficiente espacio de almacenamiento en la réplica de lectura. En ese caso, Amazon RDS termina la replicación entre la instancia de base de datos primaria y la réplica de lectura afectada. Este estado es terminal y la réplica leída debe volver a crearse.
- stopped (detenida) (solo MariaDB or MySQL): la replicación se ha detenido a petición de un cliente.
- replication stop point set (punto de detención de replicación establecidoI) (solo MySQL): se ha establecido un punto de detención iniciado por el cliente con el procedimiento almacenado mysql.rds_start_replication_until y la replicación se encuentra en curso.
- replication stop point reached (punto de detención de replicación alcanzado) (solo MySQL): se ha establecido un punto de detención iniciado por el cliente con el procedimiento almacenado mysql.rds_start_replication_until y la replicación se ha detenido porque se ha llegado al punto de detención.

Puede ver dónde se está replicando una instancia de base de datos y, si es así, comprobar su estado de replicación. En la página Bases de datos de la consola de RDS, muestra Principal en la columna Rol . Elija su nombre de instancia de base de datos. En su página de detalles, en la ficha Conectividad y seguridad , su estado de replicación se encuentra en Replicación.

Monitoreo de retraso de la replicación

Puede monitorizar el retardo de replicación en Amazon CloudWatch mediante la visualización de la métrica `ReplicaLag` de Amazon RDS.

Para Db2, la métrica `ReplicaLag` es el retardo máximo de las bases de datos que se han retrasado, en segundos. Por ejemplo, si tiene dos bases de datos que se retrasan 5 segundos y 10 segundos, respectivamente, entonces `ReplicaLag` es 10 segundos. Las bases de datos sin estados de recuperación ante desastres de alta disponibilidad (HADR) disponibles no se incluyen en el cálculo.

Para MariaDB y MySQL, la métrica `ReplicaLag` indica el valor del campo de `Seconds_Behind_Master` del comando `SHOW REPLICA STATUS`. Los motivos comunes de retardo de la replicación para MySQL y MariaDB son los siguientes:

- Una interrupción de la red.
- Escritura en tablas con índices en una réplica de lectura. Si el parámetro `read_only` no se ha establecido en 0 en la réplica de lectura, puede interrumpirse la replicación.
- Uso de un motor de almacenamiento no transaccional como MyISAM. La replicación solo se admite para el motor de almacenamiento InnoDB en MySQL y el motor de almacenamiento XtraDB en MariaDB.

> **Note**
>
> Versiones anteriores de MariaDB utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MariaDB anterior a la 10.5, utilice `SHOW SLAVE STATUS`.

Cuando la métrica `ReplicaLag` llegue a 0, la réplica estará funcionando al mismo ritmo que la instancia de base de datos principal. Si la métrica `ReplicaLag` devuelve `-1`, la replicación no está activa. `ReplicaLag = -1` es equivalente a `Seconds_Behind_Master = NULL`.

En Oracle, la métrica `ReplicaLag` es la suma del valor `Apply Lag` y la diferencia entre la hora actual y el valor de `DATUM_TIME` del retraso de aplicación. El valor `DATUM_TIME` es la última hora en la que la réplica de lectura recibió datos de su instancia de base de datos de origen. Para obtener más información, consulte V$DATAGUARD_STATS en la documentación de Oracle.

Para SQL Server, la métrica `ReplicaLag` es el retraso máximo de las bases de datos que se han retrasado, en segundos. Por ejemplo, si tiene dos bases de datos que se retrasan 5 segundos y 10 segundos, respectivamente, entonces `ReplicaLag` son 10 segundos. La métrica `ReplicaLag` devuelve el valor de la siguiente consulta.

```
SELECT MAX(secondary_lag_seconds) max_lag FROM sys.dm_hadr_database_replica_states;
```

Para obtener más información, consulte secondary_lag_seconds en la documentación de Microsoft.

`ReplicaLag` devuelve `-1` si RDS no puede determinar el retraso, como durante la configuración de la réplica, o cuando la réplica de lectura está en el estado `error`.

> **Note**
>
> Las nuevas bases de datos no se incluyen en el cálculo del retraso hasta que estén accesibles en la réplica de lectura.

Para PostgreSQL, la métrica `ReplicaLag` devuelve el valor de la siguiente consulta.

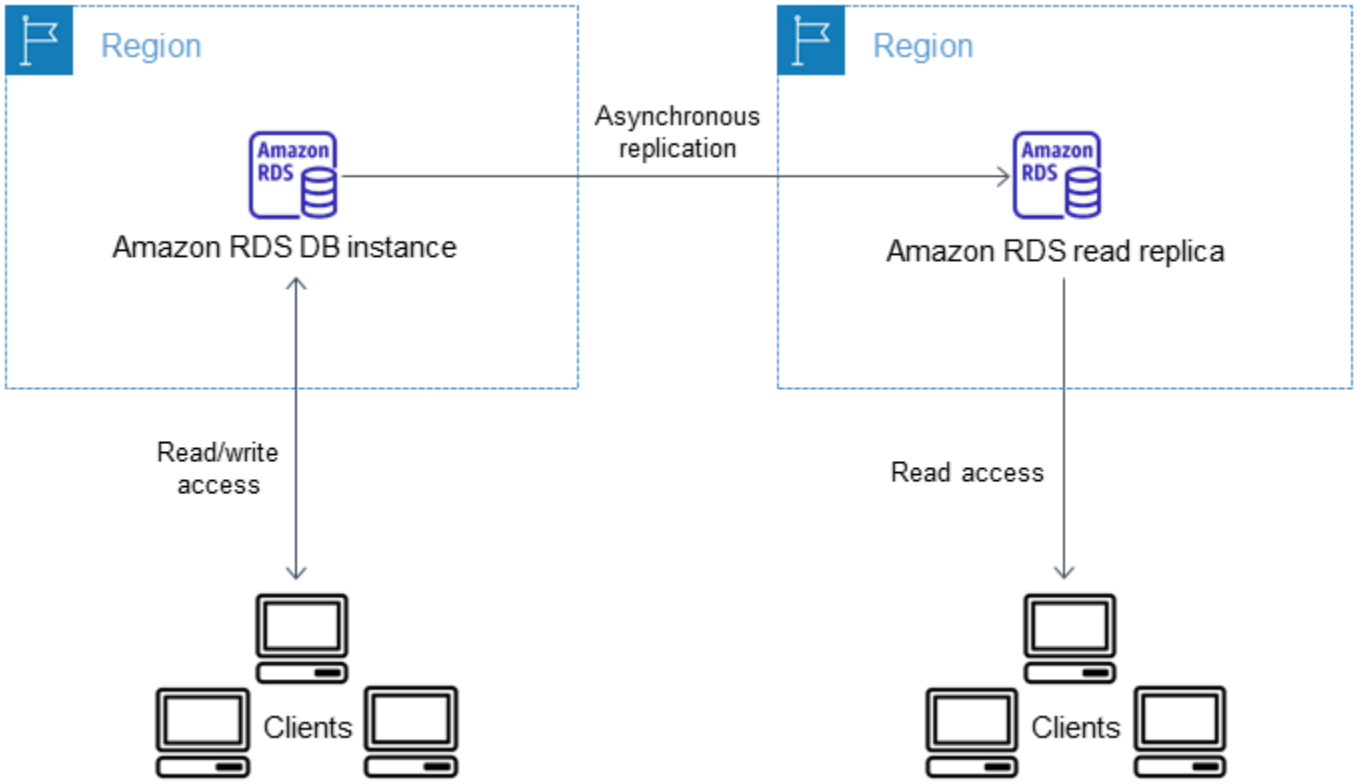
```
SELECT extract(epoch from now() - pg_last_xact_replay_timestamp()) AS reader_lag
```

Las versiones 9.5.2 y más recientes de PostgreSQL utilizan ranuras de replicación física para administrar la retención del registro de escritura previa (WAL) en la instancia de origen. Para cada instancia de réplica de lectura entre regiones, Amazon RDS crea una ranura de replicación física y la asocia con la instancia. Dos métricas de Amazon CloudWatch, `Oldest Replication Slot Lag` y `Transaction Logs Disk Usage`, muestran el retardo de la réplica con más retraso en términos de datos de WAL recibidos y la cantidad de almacenamiento que se está usando para los datos de WAL. El valor de `Transaction Logs Disk Usage` puede aumentar sustancialmente cuando una réplica de lectura entre regiones tiene mucho retraso.

Para obtener más información acerca de la monitorización de una instancia de base de datos con CloudWatch, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.

Creación de una réplica de lectura en una Región de AWS distinta

Con Amazon RDS, puede crear una réplica de lectura en una región de Región de AWS diferente que la de la instancia de base de datos de origen.



Cree una réplica de lectura en una Región de AWS diferente para lo siguiente:

- Mejorar la capacidad de recuperación de desastres.
- Escalar las operaciones de lectura en una Región de AWS más cercana a sus usuarios.
- Facilitar la migración de un centro de datos de una Región de AWS a un centro de datos de otra Región de AWS.

Crear una réplica de lectura en una Región de AWS distinta a la de la instancia de origen es similar a crear una réplica en la misma Región de AWS. Puede utilizar la AWS Management Console, ejecutar el comando `create-db-instance-read-replica` o llamar a la operación `CreateDBInstanceReadReplica` de la API.

> **Note**
>
> Para crear una réplica de lectura cifrada en una Región de AWS distinta a la de la instancia de base de datos de origen, la instancia de base de datos de origen debe estar cifrada.

Temas

- Disponibilidad en regiones y versiones
- Creación de una réplica de lectura entre regiones
- Cómo realiza Amazon RDS la replicación entre regiones
- Consideraciones relativas a la replicación entre regiones
- Costos de la replicación entre regiones

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de la replicación entre regiones, consulte Regiones y motores de bases de datos admitidos para réplicas de lectura entre regiones en Amazon RDS.

Creación de una réplica de lectura entre regiones

Los siguientes procedimientos muestran cómo crear una réplica de lectura a partir de una instancia de base de datos de MariaDB, Microsoft SQL Server, MySQL, Oracle o PostgreSQL de origen en una Región de AWS diferente.

Consola

Puede crear una réplica de lectura entre Regiones de AWS usando la AWS Management Console.

Para crear una réplica de lectura entre Regiones de AWS con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Seleccione la instancia de base de datos de MariaDB, Microsoft SQL Server, MySQL, Oracle o PostgreSQL que desee usar como origen para una réplica de lectura.
4. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).
5. En DB instance identifier (Identificador de instancias de bases de datos), escriba un nombre para la réplica de lectura.
6. Elija la Destination Region (Región de destino).
7. Elija las especificaciones de la instancia que desee usar. Se recomienda usar la misma clase de instancia de base de datos y el mismo tipo de almacenamiento o mayores para la réplica de lectura.

8. Para crear una réplica de lectura cifrada en otra Región de AWS:

   a. Elija Habilitar el cifrado.

   b. En AWS KMS key, elija el identificador AWS KMS key de la clave de KMS en la Región de AWS de destino.

   > **Note**
   >
   > Para crear una réplica de lectura cifrada, la instancia de base de datos de origen debe estar cifrada. Para obtener más información acerca del cifrado de la instancia de base de datos de origen, consulte Cifrado de recursos de Amazon RDS.

9. Elija otras opciones, como el escalado automático de almacenamiento.
10. Elija Create read replica (Crear réplica de lectura).

AWS CLI

Para crear una réplica de lectura a partir de una instancia de base de datos de MariaDB, Microsoft SQL Server, MySQL, Oracle o PostgreSQL de origen en una Región de AWS diferente, puede utilizar el comando `create-db-instance-read-replica`. En este caso, se usa `create-db-instance-read-replica` desde la Región de AWS en la que se desea situar la réplica de lectura (región de destino) y se especifica el nombre de recurso de Amazon (ARN) para la instancia de base de datos de origen. Un ARN identifica de forma única a un recurso creado en Amazon Web Services.

Por ejemplo, si la instancia de base de datos de origen está en la región US East (N. Virginia), el ARN tendrá un aspecto similar al siguiente.

```
arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

Para obtener información acerca de los ARN, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

Para crear una réplica de lectura cifrada en una Región de AWS distinta de la instancia de base de datos de origen, puede usar el comando AWS CLI`create-db-instance-read-replica` desde la Región de AWS de destino. Los siguientes parámetros son necesarios para crear una réplica de lectura en otra Región de AWS:

- `--region`: la Región de AWS de destino donde se crea la réplica de lectura.

- `--source-db-instance-identifier` – Identificador de instancia de base de datos para la instancia de base de datos de origen. Este identificador debe estar en el formato del ARN para la Región de AWS de origen.
- `--db-instance-identifier`: el identificador de la réplica de lectura en la Región de AWS de destino.

Example de una réplica de lectura entre regiones

El siguiente código crea una réplica de lectura en la región EE.UU. Oeste (Oregón) desde una instancia de base de datos de origen en la regiónUS East (N. Virginia).

Para Linux, macOS o Unix:

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier myreadreplica \
    --region us-west-2 \
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

Para Windows:

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --region us-west-2 ^
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

Los siguientes parámetros también son necesarios para crear una réplica de lectura cifrada en otra Región de AWS:

- `--kms-key-id`: identificador de AWS KMS key de la clave de KMS que se va a utilizar para cifrar la réplica de lectura en Región de AWS de destino.

Example de una réplica de lectura cifrada entre regiones

El siguiente código crea una réplica de lectura cifrada en la región EE.UU. Oeste (Oregón) de una instancia de base de datos de origen en la región US East (N. Virginia).

Para Linux, macOS o Unix:

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier myreadreplica \
```

```
    --region us-west-2 \
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance
 \
    --kms-key-id my-us-west-2-key
```

Para Windows:

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --region us-west-2 ^
    --source-db-instance-identifier arn:aws:rds:us-east-1:123456789012:db:mydbinstance
 ^
    --kms-key-id my-us-west-2-key
```

La opción `--source-region` es necesaria cuando se crea una réplica de lectura cifrada entre las AWS GovCloud (Este de EE. UU.) y AWS GovCloud (EE. UU. Oeste). Para `--source-region`, especifique la Región de AWS de la instancia de base de datos de origen.

Si no se ha especificado `--source-region`, especifique un valor de `--pre-signed-url`. Una URL prefirmada es una URL que contiene una solicitud firmada de Signature Version 4 para el comando `create-db-instance-read-replica` que se llama en la Región de AWS de origen. Para obtener más información acerca de la opción `pre-signed-url`, consulte create-db-instance-read-replica en la Referencia de los comandos de AWS CLI.

API de RDS

Para crear una réplica de lectura a partir de una instancia de base de datos de MariaDB, MySQL, Microsoft SQL Server, Oracle o PostgreSQL de origen en una Región de AWS diferente, puede llamar a la operación CreateDBInstanceReadReplica de la API de Amazon RDS. En este caso, debe llamar a CreateDBInstanceReadReplica desde la Región de AWS en la que se desea colocar la réplica de lectura (región de destino) y especificar el nombre de recurso de Amazon (ARN) de la instancia de base de datos de origen. Un ARN identifica de forma única a un recurso creado en Amazon Web Services.

Para crear una réplica de lectura cifrada en una Región de AWS diferente que la instancia de base de datos de origen, puede usar la operación de la API de Amazon RDS `CreateDBInstanceReadReplica` desde la Región de AWS de destino. Para crear una réplica de lectura cifrada en otra Región de AWS, debe especificar un valor para

`PreSignedURL`. `PreSignedURL` debe contener una solicitud para llamar a la operación `CreateDBInstanceReadReplica` en la Región de AWS de origen en la que se crea la réplica de lectura. Para obtener más información acerca de la `PreSignedUrl`, consulte `CreateDBInstanceReadReplica`.

Por ejemplo, si la instancia de base de datos de origen está en la región US East (N. Virginia), el ARN tendrá un aspecto similar al siguiente.

```
arn:aws:rds:us-east-1:123456789012:db:mydbinstance
```

Para obtener información acerca de los ARN, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

Example

```
https://us-west-2.rds.amazonaws.com/
    ?Action=CreateDBInstanceReadReplica
    &KmsKeyId=my-us-east-1-key
    &PreSignedUrl=https%253A%252F%252Frds.us-west-2.amazonaws.com%252F
         %253FAction%253DCreateDBInstanceReadReplica
         %2526DestinationRegion%253Dus-east-1
         %2526KmsKeyId%253Dmy-us-east-1-key
         %2526SourceDBInstanceIdentifier%253Darn%25253Aaws%25253Ards%25253Aus-
west-2%123456789012%25253Adb%25253Amydbinstance
         %2526SignatureMethod%253DHmacSHA256
         %2526SignatureVersion%253D4%2526SourceDBInstanceIdentifier%253Darn%25253Aaws
%25253Ards%25253Aus-west-2%25253A123456789012%25253Ainstance%25253Amydbinstance
         %2526Version%253D2014-10-31
         %2526X-Amz-Algorithm%253DAWS4-HMAC-SHA256
         %2526X-Amz-Credential%253DAKIADQKE4SARGYLE%252F20161117%252Fus-west-2%252Frds
%252Faws4_request
         %2526X-Amz-Date%253D20161117T215409Z
         %2526X-Amz-Expires%253D3600
         %2526X-Amz-SignedHeaders%253Dcontent-type%253Bhost%253Buser-agent%253Bx-amz-
content-sha256%253Bx-amz-date
         %2526X-Amz-Signature
%253D255a0f17b4e717d3b67fad163c3ec26573b882c03a65523522cf890a67fca613
    &DBInstanceIdentifier=myreadreplica
    &SourceDBInstanceIdentifier=&region-arn;rds:us-east-1:123456789012:db:mydbinstance
    &Version=2012-01-15
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
```

```
    &Timestamp=2012-01-20T22%3A06%3A23.624Z
    &AWSAccessKeyId=<&AWS; Access Key ID>
    &Signature=<Signature>
```

Cómo realiza Amazon RDS la replicación entre regiones

Amazon RDS usa el siguiente proceso para crear una réplica de lectura entre regiones. En función de las Regiones de AWS implicadas y de la cantidad de datos de la base de datos, este proceso puede tardar horas en completarse. Puede usar esta información para determinar cuánto ha avanzado el proceso cuando cree una réplica de lectura entre regiones:

1. Amazon RDS comienza a configurar la instancia de base de datos de origen como origen de la replicación y define el estado como modifying.
2. Amazon RDS comienza a configurar la réplica de lectura especificada en la Región de AWS de destino y define el estado como creating.
3. Amazon RDS crea una instantánea de base de datos automatizada de la instancia de base de datos de origen en la Región de AWS de origen. El formato del nombre de la instantánea de base de datos es `rds:<InstanceID>-<timestamp>`, donde `<InstanceID>` es el identificador de la instancia de origen y `<timestamp>` corresponde a la fecha y la hora en las que se inició la copia. Por ejemplo, `rds:mysourceinstance-2013-11-14-09-24` se creó a partir de la instancia `mysourceinstance` en `2013-11-14-09-24`. Durante la creación de una instantánea de base de datos automatizada, el estado de la instancia de base de datos de origen sigue siendo modifying (modificando), el estado de las réplicas de lectura sigue siendo creating (creando) y el estado de la instantánea de base de datos es creating (creando). La columna de progreso de la página de la instantánea de base de datos de la consola indica cuánto ha avanzado la creación de la instantánea de base de datos. Cuando la instantánea de base de datos se haya completado, el estado tanto de la instantánea de base de datos como de la instancia de base de datos de origen se definirá como available.
4. Amazon RDS comienza una copia de la instantánea entre regiones para la transferencia de datos inicial. La copia de la instantánea aparece como instantánea automatizada en la Región de AWS de destino con el estado creating. Tiene el mismo nombre que la instantánea de base de datos de origen. La columna de progreso de la página de la instantánea de base de datos indica cuánto ha avanzado la copia. Cuando la copia se haya completado, el estado de la copia de la instantánea de base de datos se definirá como available.
5. A continuación, Amazon RDS usa la instantánea de base de datos copiada para la carga de datos inicial en la réplica de lectura. Durante esta fase, la réplica de lectura está en la lista de instancias de base de datos del destino con el estado creating (creando). Cuando la carga se

haya completado, el estado de la réplica de lectura se definirá como available (disponible) y se eliminará la copia de la instantánea de base de datos.

6. Cuando la réplica de lectura llega al estado disponible, Amazon RDS comienza a replicar los cambios realizados en la instancia de origen desde el comienzo de la operación de creación de la réplica de lectura. Durante esta fase, el retraso de replicación para la réplica de lectura es mayor que 0.

   Para obtener información sobre el retardo de replicación, consulte Monitoreo de la replicación de lectura.

Consideraciones relativas a la replicación entre regiones

Todas las consideraciones relativas a la realización de la replicación dentro de una Región de AWS son válidas para la replicación entre regiones. Las siguientes consideraciones adicionales se deben tener en cuenta al replicar entre Regiones de AWS:

- Una instancia de base de datos de origen puede tener réplicas de lectura entre regiones en en varias Regiones de AWS. Debido al límite del número de entradas de la lista de control de acceso (ACL) de una VPC de origen, RDS no puede garantizar más de cinco instancias de base de datos de réplica de lectura entre regiones.
- Puede replicar entre las regiones GovCloud (Este de EE. UU.) y GovCloud (Oeste de EE. UU.), pero no dentro o fuera de GovCloud (EE. UU.).
- Para los siguientes motores de RDS, puede crear una réplica de lectura de Amazon RDS entre regiones a partir de una instancia de base de datos de origen de Amazon RDS solo cuando no sea una réplica de lectura de otra instancia de base de datos de Amazon RDS:
  - RDS para SQL Server
  - RDS para Oracle
  - RDS para PostgreSQL versiones menores de 14.1

  Esta limitación no se aplica a instancias de base de datos que ejecutan RDS para PostgreSQL versión 14.1 y versiones superiores, RDS para MariaDB y RDS para MySQL.
- Puede esperar ver un nivel superior de retraso para cualquier réplica de lectura que esté en una Región de AWS diferente que la instancia de origen. Este retardo procede de los canales de red más largos entre los centros de datos regionales.

- En las réplicas de lectura entre regiones, cualquiera de los comandos para crear réplicas de lectura que definan el parámetro `--db-subnet-group-name` debe especificar un grupo de subredes de base de datos de la misma VPC.
- En la mayoría de los casos, la réplica de lectura utiliza el grupo de parámetros de base de datos predeterminado y el grupo de opción de base de datos para el motor de base de datos especificado.

  Para el motor de base de datos de Db2, debe especificar un grupo de parámetros personalizados para la réplica. Para las réplicas que utilizan el modelo BYOL, este grupo de parámetros personalizado debe incluir IBM Site ID e IBM Customer ID. Puede especificar este grupo de parámetros personalizado para la réplica mediante la AWS Management Console, la AWS CLI o la API de RDS. Para obtener más información, consulte ID de IBM para Traiga su propia licencia para Db2.

  Para los motores de base de datos de MySQL y Oracle, puede especificar un grupo de parámetros personalizado para la réplica de lectura en la opción `--db-parameter-group-name` del comando create-db-instance-read-replica de la AWS CLI. No puede especificar un grupo de parámetros personalizado cuando utiliza la AWS Management Console.
- La réplica de lectura utiliza el grupo de seguridad predeterminado.
- Para las instancias de base de datos de MariaDB, Microsoft SQL Server, MySQL y Oracle, cuando se elimina la instancia de base de datos de origen para una réplica de lectura entre regiones, la réplica de lectura se promociona.
- Para instancias de base de datos de PostgreSQL, cuando se elimina la instancia de base de datos de origen de una réplica de lectura entre regiones, el estado de la reproducción de la réplica de lectura se establece como `terminated`. Sin embargo, la réplica de lectura no se promociona.

  Debe promocionar la réplica de lectura de forma manual o eliminarla.

Solicitud de una réplica de lectura entre regiones

Para comunicarse con la región de origen y solicitar la creación de una réplica de lectura entre regiones, el solicitante (rol de IAM o usuario de IAM) debe tener acceso a la instancia de base de datos de origen y a la región de origen.

Ciertas condiciones en la política de IAM del solicitante pueden generar un error en la solicitud. En los siguientes ejemplos se supone que la instancia de base de datos de origen está en EE.UU.

Este (Ohio) y que la réplica de lectura se crea en US East (N. Virginia). Estos ejemplos muestran condiciones en la política de IAM del solicitante que generan un error en la solicitud:

- La política del solicitante tiene una condición para la `aws:RequestedRegion`.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": "us-east-1"
    }
}
```

  La solicitud falla porque la política no permite el acceso a la región de origen. Para que una solicitud sea correcta, se deben especificar las regiones de origen y destino.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": [
            "us-east-1",
            "us-east-2"
        ]
    }
}
```

- La política del solicitante no permite el acceso a la instancia de base de datos de origen.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "arn:aws:rds:us-east-1:123456789012:db:myreadreplica"
...
```

  Para que una solicitud sea correcta, se deben especificar la instancia de origen y la réplica.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": [
    "arn:aws:rds:us-east-1:123456789012:db:myreadreplica",
    "arn:aws:rds:us-east-2:123456789012:db:mydbinstance"
]
...
```

- La política del solicitante niega `aws:ViaAWSService`.

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "Bool": {"aws:ViaAWSService": "false"}
}
```

  La comunicación con la región de origen la efectúa RDS en nombre del solicitante. Para que una solicitud sea correcta, no deniegue las llamadas realizadas por los servicios de AWS.

- La política del solicitante tiene una condición para `aws:SourceVpc` o `aws:SourceVpce`.

  Estas solicitudes pueden fallar porque cuando RDS realiza la llamada a la región remota, esta no procede del punto de conexión de la VPC o la VPC especificada.

Si es necesario utilizar una de las condiciones anteriores que generarían un error en una solicitud, se puede incluir una segunda instrucción con `aws:CalledVia` en la política para que la solicitud se realice correctamente. Por ejemplo, se puede usar `aws:CalledVia` con `aws:SourceVpce`, como se muestra aquí:

```
...
"Effect": "Allow",
"Action": "rds:CreateDBInstanceReadReplica",
"Resource": "*",
"Condition": {
    "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
```

```
     }
},
{
    "Effect": "Allow",
    "Action": [
        "rds:CreateDBInstanceReadReplica"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "rds.amazonaws.com"
            ]
        }
    }
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Autorización de la réplica de lectura

Luego de que una solicitud de creación de réplica de lectura de base de datos en varias regiones devuelva `success`, RDS iniciará la creación de la réplica en segundo plano. Se crea una autorización para que RDS acceda a la instancia de base de datos de origen. Esta autorización vincula la instancia de base de datos de origen a la réplica de lectura y permite que RDS copie solo en la réplica de lectura especificada.

La autorización es verificada por RDS mediante el permiso `rds:CrossRegionCommunication` en el rol de IAM vinculado al servicio. Si la réplica es autorizada, RDS se comunica con la región de origen y completa la creación de la réplica.

RDS no tiene acceso a instancias de base de datos que no hayan sido autorizadas previamente por una solicitud `CreateDBInstanceReadReplica`. La autorización se revoca cuando se completa la creación de la réplica de lectura.

RDS utiliza el rol vinculado a servicios para verificar la autorización en la región de origen. Si se elimina el rol vinculado a servicios durante el proceso de creación de replicación, se produce un error en la creación.

Para obtener más información, consulte Usar roles vinculados a servicios en la Guía del usuario de IAM.

Uso de credenciales de AWS Security Token Service

Los tokens de sesión del punto de conexión global de AWS Security Token Service (AWS STS) son válidos únicamente en Regiones de AWS que están habilitadas de forma predeterminada (regiones comerciales). Si utiliza credenciales de la operación de la API `assumeRole` en AWS STS, utilice el punto de conexión regional si la región de origen es una región registrada. De lo contrario, la solicitud devuelve un error. Esto ocurre porque las credenciales deben ser válidas en ambas regiones, lo cual se cumple para las regiones registradas solo cuando se utiliza el punto de conexión regional de AWS STS.

Para utilizar el punto de conexión global, asegúrese de que está habilitado para operaciones en ambas regiones. Establezca el punto de conexión global en `Valid in all Regiones de AWS` en la configuración de la cuenta de AWS STS.

La misma regla se aplica a las credenciales del parámetro URL prefirmado.

Para obtener más información, consulte Administración de AWS STS en una Región de AWS en la guía del usuario de IAM.

Costos de la replicación entre regiones

Los datos transferidos para la replicación entre regiones incurren en cargos por transferencia de datos de Amazon RDS. Las siguientes acciones de replicación entre regiones generan cargos para los datos transferidos fuera de la Región de AWS de origen:

- Cuando se crea una réplica de lectura, Amazon RDS realiza una instantánea de la instancia de origen y transfiere la instantánea a la Región de AWS de la réplica de lectura.
- Para cada modificación de datos realizada en las bases de datos de origen, Amazon RDS transfiere los datos de la Región de AWS de origen a la Región de AWS de la réplica de lectura.

Para obtener más información acerca de los precios de las transferencias de datos, consulte Precios de Amazon RDS.

Para las instancias de MySQL y MariaDB, puede limitar los costos de transferencia de datos reduciendo el número de réplicas de lectura entre regiones que crea. Por ejemplo, imagine que tiene una instancia de base de datos de origen en una Región de AWS y que quiere tres réplicas de lectura en otra Región de AWS. En ese caso, cree solo una de las réplicas de lectura de la instancia de base de datos de origen. Cree las otras dos réplicas a partir de la primera réplica de lectura en lugar de la instancia de base de datos de origen.

Por ejemplo, si tiene `source-instance-1` en una Región de AWS, puede hacer lo siguiente:

- Cree `read-replica-1` en la nueva Región de AWS especificando `source-instance-1` como origen.
- Cree `read-replica-2` a partir de `read-replica-1`.
- Cree `read-replica-3` a partir de `read-replica-1`.

En este ejemplo, solo se le cobrará por los datos transferidos desde `source-instance-1` a `read-replica-1`. No se le cobrará por los datos transferidos desde `read-replica-1` a las otras dos réplicas porque todas están en la misma Región de AWS. Si crea las tres réplicas directamente desde `source-instance-1` en otra Región de AWS, se le cobrará por las transferencias de datos a las tres réplicas.

Etiquetado de los recursos de y Amazon RDS

Una etiqueta de Amazon RDS es un par nombre-valor que define y asocia a un recurso de Amazon RDS, como una instancia de base de datos o una instantánea de base de datos. El nombre es la clave. Opcionalmente, puede proporcionar un valor para la clave.

Puede utilizar la AWS Management Console, la AWS CLI o la API de Amazon RDS para agregar, enumerar y eliminar etiquetas de recursos de Amazon RDS. Si utiliza la CLI de o la API, asegúrese de proporcionar el nombre de recurso de Amazon (ARN) correspondiente al recurso de RDS con el que desee trabajar. Para obtener más información sobre cómo crear un ARN, consulte Creación de un nombre ARN para Amazon RDS.

Puede utilizar etiquetas para agregar metadatos a sus recursos de Amazon RDS. Puede utilizar las etiquetas para agregar sus propias notaciones sobre instancias de base de datos, instantáneas, Aurora clústeres, etc. Si lo hace, puede ayudarle a documentar sus recursos de Amazon RDS. También puede utilizar las etiquetas con procedimientos de mantenimiento automatizados.

En concreto, puede utilizar estas etiquetas con las políticas de IAM. Puede utilizarlas para administrar el acceso a los recursos de Amazon RDS y controlar qué acciones se pueden aplicar a estos recursos. También puede utilizar estas etiquetas para realizar un seguimiento de los costos al agrupar los gastos de recursos etiquetados de forma similar.

Puede etiquetar los siguientes recursos de Amazon RDS:

- Instancias de base de datos
- Clústeres de base de datos
- Clústeres globales de Aurora
- Puntos de conexión de clústeres de base de datos
- Réplicas de lectura
- Instantáneas de base de datos
- Instantáneas de clúster de base de datos
- Instancias de base de datos reservadas
- Suscripciones de eventos
- Grupos de opciones de base de datos
- Grupos de parámetros de base de datos
- Grupos de parámetros de clúster de bases de datos

- Grupos de subred de base de datos
- Proxies de RDS Proxy
- Puntos de enlace de RDS Proxy
- Implementaciones azul/verde
- Integraciones sin ETL

> **Note**
>
> Actualmente, no puede etiquetar los proxies de RDS ni los puntos de conexión de proxies de RDS mediante la AWS Management Console.

Temas

- ¿Por qué usar etiquetas de recursos de Amazon RDS?
- Funcionamiento de las etiquetas de recursos de Amazon RDS
- Prácticas recomendadas para el etiquetado de los recursos de Amazon RDS
- Copia de etiquetas a instantáneas de base de datos
- Añadido y eliminación de etiquetas en Amazon RDS
- Tutorial: especificar qué instancias de base de datos se deben detener mediante etiquetas

¿Por qué usar etiquetas de recursos de Amazon RDS?

Puede usar etiquetas para hacer lo siguiente:

- Clasifique sus recursos de RDS por aplicación, proyecto, departamento, entorno, etc. Por ejemplo, puede usar una clave de etiqueta para definir una categoría en la que el valor de la etiqueta sea un elemento dentro de esa categoría. Podría crear la etiqueta `environment=prod`. También podría definir una clave de etiqueta de `project` y un valor de etiqueta de `Salix` para indicar que se ha asignado un recurso de Amazon RDS al proyecto Salix.
- Automatice las tareas de administración de recursos. Por ejemplo, podría crear una ventana de mantenimiento para las instancias etiquetadas con `environment=prod` que sea diferente de la ventana para las instancias etiquetadas con `environment=test`. También puede configurar instantáneas de bases de datos automáticas para las instancias etiquetadas con `environment=prod`.

- Controle el acceso a los recursos de RDS dentro de una política de IAM. Para ello, utilice la clave de condición `aws:ResourceTag/tag-key` global. Por ejemplo, una política podría permitir que solo los usuarios del grupo `DBAdmin` modifiquen las instancias de base de datos etiquetadas con `environment=prod`. Para obtener más información sobre la administración del acceso a los recursos etiquetados con políticas de IAM, consulte Administración de la identidad y el acceso en Amazon RDS y Control del acceso a los recursos de AWS en la Guía del usuario de AWS Identity and Access Management.
- Supervise los recursos en función de una etiqueta. Por ejemplo, puede crear un panel de Amazon CloudWatch para instancias de base de datos etiquetadas con `environment=prod`.
- Realice un seguimiento de los costos agrupando los gastos por recursos con etiquetas similares. Por ejemplo, si etiqueta los recursos de RDS asociados al proyecto de Salix con `project=Salix`, puede generar informes de costos y asignar los gastos a este proyecto. Para obtener más información, consulte Funcionamiento de la facturación de AWS con etiquetas en Amazon RDS.

Funcionamiento de las etiquetas de recursos de Amazon RDS

AWS no aplica ningún significado semántico a las etiquetas. Las etiquetas se interpretan estrictamente como cadenas de caracteres.

Temas

- Conjuntos de etiquetas en Amazon RDS
- Estructura de etiquetas en Amazon RDS
- Recursos de Amazon RDS aptos para el etiquetado
- Funcionamiento de la facturación de AWS con etiquetas en Amazon RDS

Conjuntos de etiquetas en Amazon RDS

Cada recurso de Amazon RDS tiene un contenedor denominado conjunto de etiquetas. El contenedor incluye todas las etiquetas asignadas al recurso. Un recurso tiene exactamente un conjunto de etiquetas.

Un conjunto de etiquetas contiene de 0 a 50 etiquetas. Si agrega una etiqueta a un recurso de RDS con la misma clave que una etiqueta existente, el nuevo valor sobrescribirá al antiguo.

Estructura de etiquetas en Amazon RDS

La estructura de una etiqueta de RDS es la siguiente:

Clave de etiqueta

La clave de la etiqueta es el nombre obligatorio de la etiqueta. El valor de la cadena debe tener una longitud de entre 1 y 128 caracteres Unicode y no puede llevar el prefijo `aws:` ni `rds:`. La cadena puede contener únicamente el conjunto de letras Unicode, dígitos, espacio en blanco, `_`, `.`, `:`, `/`, `=`, `+`, `-` y `@`. La expresión regular de Java es `"^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$"`. Las claves de etiqueta distinguen entre mayúsculas y minúsculas. Por lo tanto, las claves `project` y `Project` son distintas.

Una clave es única en un conjunto de etiquetas. Por ejemplo, en un conjunto de etiquetas no puede haber claves iguales pero con valores diferentes, como `project=Trinity` y `project=Xanadu`.

Valor de etiqueta

El valor es un valor de cadena opcional en la etiqueta. El valor de la cadena debe tener una longitud de entre 1 y 256 caracteres Unicode. La cadena puede contener únicamente el conjunto de letras Unicode, dígitos, espacio en blanco, `_`, `.`, `:`, `/`, `=`, `+`, `-` y `@`. La expresión regular de Java es `"^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-@]*)$"`. Los valores distinguen entre mayúsculas y minúsculas. Por lo tanto, los valores `prod` y `Prod` son distintos.

Los valores no tienen que ser únicos dentro de un conjunto de etiquetas y también pueden ser nulos. Por ejemplo, es posible tener en un conjunto de etiquetas los pares clave-valor `project=Trinity` y `cost-center=Trinity`.

Recursos de Amazon RDS aptos para el etiquetado

Puede etiquetar los siguientes recursos de Amazon RDS:

- Instancias de base de datos
- Clústeres de base de datos
- Puntos de conexión de clústeres de base de datos
- Réplicas de lectura
- Instantáneas de base de datos
- Instantáneas de clúster de base de datos
- Instancias de base de datos reservadas
- Suscripciones de eventos
- Grupos de opciones de base de datos

- Grupos de parámetros de base de datos
- Grupos de parámetros de clúster de bases de datos
- Grupos de subred de base de datos
- Proxies de RDS Proxy
- Puntos de enlace de RDS Proxy

> **Note**
>
> Actualmente, no puede etiquetar los proxies de RDS ni los puntos de conexión de proxies de RDS mediante la AWS Management Console.

- Implementaciones azul/verde
- Integraciones sin ETL (versión preliminar)

Funcionamiento de la facturación de AWS con etiquetas en Amazon RDS

Puede usar etiquetas para organizar la factura de AWS de modo que refleje su propia estructura de costos. Para ello, inscríbase para obtener una factura de Cuenta de AWS que incluya valores de clave de etiquetas. A continuación, para ver los costos de los recursos combinados, organice la información de facturación de acuerdo con los recursos con los mismos valores de clave de etiquetas. Por ejemplo, puede etiquetar varios recursos con un nombre de aplicación específico y luego organizar su información de facturación para ver el costo total de la aplicación en distintos servicios. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

Funcionamiento de las etiquetas de asignación de costos con las instantáneas de de bases de datos

Puede añadir una etiqueta a una instantánea de de base de datos. Sin embargo, la factura no reflejará esta agrupación. Para que las etiquetas de asignación de costos se apliquen a las instantáneas de de base de datos, se deben cumplir las siguientes condiciones:

- Las etiquetas se deben asociar a la instancia de base de datos principal.
- La instancia de base de datos principal debe existir en la misma Cuenta de AWS que la instantánea del de base de datos.
- La instancia de base de datos principal debe existir en la misma Región de AWS que la instantánea del de base de datos.

Las instantáneas de base de datos se consideran huérfanas si no existen en la misma región que la instancia de base de datos principal, o bien si la instancia de base de datos principal se elimina. Las instantáneas de bases de datos huérfanas no admiten etiquetas de asignación de costos. Los costos de las instantáneas huérfanas se agregan en un único elemento de línea sin etiquetar. Las instantáneas de de bases de datos entre cuentas no se consideran huérfanas cuando se cumplen las siguientes condiciones:

- Existen en la misma región que la instancia de base de datos principal.
- La instancia de base de datos principal es propiedad de la cuenta de origen.

> **Note**
>
> Si la instancia de base de datos principal pertenece a una cuenta diferente, las etiquetas de asignación de costos no se aplican a las instantáneas entre cuentas de la cuenta de destino.

Prácticas recomendadas para el etiquetado de los recursos de Amazon RDS

Al utilizar etiquetas, le sugerimos que siga las siguientes prácticas recomendadas:

- Documente las convenciones sobre el uso de etiquetas que siguen todos los equipos de su organización. En concreto, asegúrese de que los nombres sean descriptivos y coherentes. Por ejemplo, estandarice el formato `environment:prod` en lugar de etiquetar algunos recursos con `env:production`.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas.

- Automatice el etiquetado para garantizar la coherencia. Por ejemplo, puede utilizar las siguientes técnicas:
  - Incluya etiquetas en una plantilla de AWS CloudFormation. Al crear recursos con la plantilla, los recursos se etiquetan automáticamente.
  - Defina y aplique etiquetas mediante funciones de AWS Lambda.

  - Cree un documento SSM que incluya los pasos para añadir etiquetas a sus recursos de RDS.
- Use las etiquetas solo cuando sea necesario. Puede añadir hasta 50 etiquetas para un único recurso de RDS, pero se recomienda evitar la complejidad y la proliferación innecesarias de etiquetas.
- Revise las etiquetas periódicamente para comprobar su relevancia y precisión. Elimine o modifique las etiquetas obsoletas según sea necesario.
- Plantéese la posibilidad de crear etiquetas con el editor de etiquetas de AWS en la AWS Management Console. Puede utilizar el editor de etiquetas para añadir etiquetas a varios recursos de AWS compatibles, incluidos los recursos de RDS, al mismo tiempo. Para obtener más información, consulte el Editor de etiquetas en la Guía del usuario de grupos de recursos de AWS.

Copia de etiquetas a instantáneas de base de datos

Cuando crea o restaura una instancia de base de datos, puede especificar que las etiquetas de dicha instancia se copien en instantáneas de la instancia de base de datos. La copia de las etiquetas garantiza que los metadatos para las instantáneas coincidan con los de la instancia de base de datos de origen. Además, garantiza que cualquier política de acceso para las instantáneas de base de datos también coincida con la de la instancia de base de datos de origen.

Puede especificar que las etiquetas se copien en las instantáneas de base de datos para las siguientes acciones:

- Creación de una instancia de base de datos
- Restauración de una instancia de base de datos
- Creación de una réplica de lectura
- Copia de una instantánea de base de datos

Para copiar las etiquetas de las acciones anteriores, elija Copiar etiquetas a las instantáneas en la AWS Management Console, o especifique `--copy-tags-to-snapshot` en la AWS CLI.

En la mayoría de los casos, las etiquetas no se copian de forma predeterminada. Sin embargo, al restaurar una instancia de base de datos desde una instantánea de base de datos, RDS verifica si se especifican nuevas etiquetas. En caso afirmativo, las nuevas etiquetas se agregan a la instancia de base de datos restaurada. Si no hay etiquetas nuevas, RDS agrega las etiquetas de la instancia de base de datos de origen al crear la instantánea de la instancia de base de datos restaurada.

Para evitar que se agreguen etiquetas desde instancias de base de datos de origen a instancias de base de datos restauradas, le recomendamos que especifique nuevas etiquetas al restaurar una instancia de base de datos.

> **Note**
>
> En algunos casos, puede incluir un valor para el`--tags` parámetro delAWS CLI comando create-db-snapshot. O puede proporcionar al menos una etiqueta a la operación de la API CreateDBSnapshot. En estos casos, RDS no copia las etiquetas de la instancia de base de datos de origen a la nueva instantánea de base de datos. Esta funcionalidad se aplica incluso si la instancia de base de datos de origen tiene la opción `--copy-tags-to-snapshot` (`CopyTagsToSnapshot`) activada.
> Si adopta este enfoque, puede crear una copia de una instancia de base de datos a partir de una instantánea de base de datos. Este enfoque evita añadir etiquetas que no se apliquen a la nueva instancia de base de datos. La instantánea de base de datos se crea mediante el comando `create-db-snapshot` de AWS CLI (o la operación de la API `CreateDBSnapshot` RDS). Después de crear la instantánea de la base de datos, puede añadir etiquetas como se describe más adelante en este tema.

Añadido y eliminación de etiquetas en Amazon RDS

Puede hacer lo siguiente:

- Cree etiquetas al crear un recurso, por ejemplo, al ejecutar el comando `create-db-instance` de la AWS CLI.
- Añada etiquetas a un recurso existente con el comando `add-tags-to-resource`.
- Enumere las etiquetas asociadas a un recurso específico con el comando `list-tags-for-resource`.
- Actualice las etiquetas con el comando `add-tags-to-resource`.
- Elimine las etiquetas de un recurso con el comando `remove-tags-from-resource`.

Los procedimientos siguientes muestran cómo realizar operaciones de etiquetado típicas en recursos relacionados con instancias de base de datos. Tenga en cuenta que las etiquetas se almacenan en caché con fines de autorización. Por este motivo, al añadir o actualizar etiquetas en los recursos de Amazon RDS, pueden pasar varios minutos hasta que las modificaciones estén disponibles.

Consola

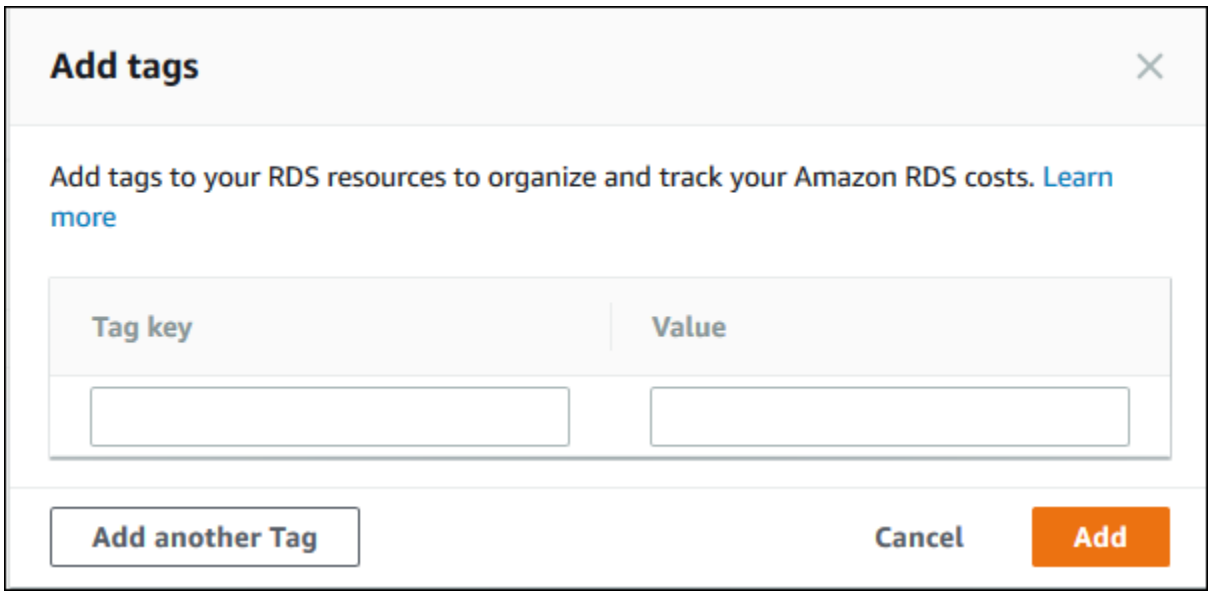
El proceso para etiquetar un recurso de Amazon RDS es similar para todos los recursos. El siguiente procedimiento muestra cómo etiquetar una instancia de base de datos de Amazon RDS.

Para agregar una etiqueta a una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

> **Note**
>
> Para filtrar la lista de instancias de base de datos en el panel Databases (Bases de datos), escriba una cadena de texto para Filter databases (Filtrar bases de datos). Solo aparecen instancias de base de datos que contienen la cadena.

3. Seleccione el nombre de la instancia de base de datos que desea etiquetar para mostrar sus detalles.
4. En la sección de detalles, desplácese hasta la sección Tags (Etiquetas).
5. Elija Add (Añadir). Aparece la ventana Add tags (Añadir etiquetas).



6. Escriba un valor para Tag key (Clave de etiqueta) y Value (Valor).
7. Para añadir otra etiqueta, puede elegir Add another Tag (Añadir otra etiqueta) y escribir un valor para Tag key (Clave de etiqueta) y Value (Valor).

Repita este paso tantas veces como sea necesario.

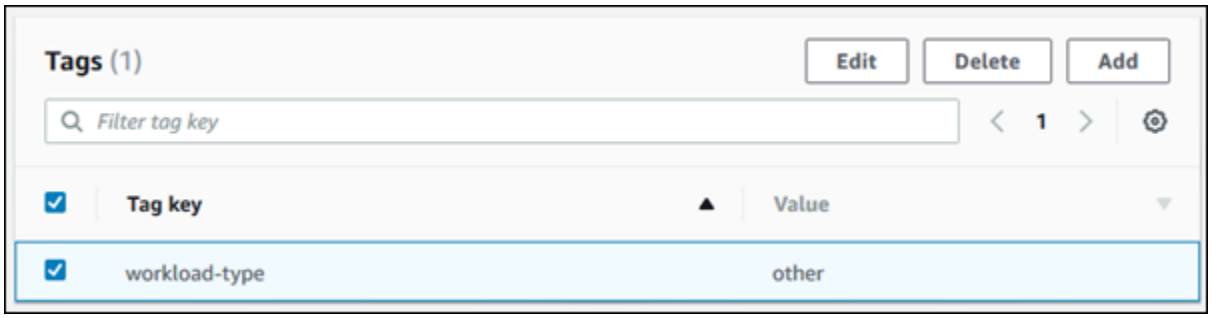
8. Elija Add (Añadir).

Para eliminar una etiqueta de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

> **Note**
>
> Para filtrar la lista de instancias de base de datos en el panel Databases (Bases de datos), escriba una cadena de texto en el cuadro Filter databases (Filtrar bases de datos). Solo aparecen instancias de base de datos que contienen la cadena.

3. Seleccione el nombre de la instancia de base de datos para mostrar sus detalles.
4. En la sección de detalles, desplácese hasta la sección Tags (Etiquetas).
5. Elija la etiqueta desea eliminar.



6. Elija Delete (Eliminar) y después elija (Eliminar) en la ventana Delete tags (Eliminar etiquetas).

AWS CLI

Puede utilizar la para agregar, listar o eliminar etiquetas de una instancia de base de dato AWS CLI.

- Para agregar una o más etiquetas a un recurso de Amazon RDS, utilice el comando `add-tags-to-resource` de la AWS CLI.
- Para ver una lista de las etiquetas de un recurso de Amazon RDS, utilice el comando `list-tags-for-resource` de la AWS CLI.

- Para eliminar una o más etiquetas de un recurso de Amazon RDS, utilice el comando `remove-tags-from-resource` de la AWS CLI.

Para obtener más información acerca de cómo crear el ARN requerido, consulte Creación de un nombre ARN para Amazon RDS.

API de RDS

Puede utilizar la API de Amazon RDS para agregar, listar o eliminar etiquetas de una instancia de base de datos.

- Para añadir una etiqueta a un recurso de Amazon RDS, utilice la operación `AddTagsToResource`.
- Para ver una lista de las etiquetas asignadas a un recurso de Amazon RDS, utilice `ListTagsForResource`.
- Para eliminar etiquetas de un recurso de Amazon RDS, utilice la operación `RemoveTagsFromResource`.

Para obtener más información acerca de cómo crear el ARN requerido, consulte Creación de un nombre ARN para Amazon RDS.

Cuando se trabaja con XML mediante la API de Amazon RDS, las etiquetas utilizan el esquema siguiente:

```
<Tagging>
      <TagSet>
          <Tag>
              <Key>Project</Key>
              <Value>Trinity</Value>
          </Tag>
          <Tag>
              <Key>User</Key>
              <Value>Jones</Value>
          </Tag>
      </TagSet>
  </Tagging>
```

La tabla siguiente proporciona una lista de las etiquetas XML permitidas y sus características. Los valores de `Key` y `Value` distinguen entre mayúsculas y minúsculas. Por ejemplo, `project=Trinity` y `PROJECT=Trinity` son dos etiquetas diferentes.

Elemento de etiquetado	Descripción
TagSet	Los conjuntos de etiquetas contienen todas las etiquetas asignadas a un recurso de Amazon RDS. Solo puede haber un conjunto de etiquetas por recurso. Solo puede trabajar con conjuntos de etiquetas a través de la API de Amazon RDS.
Tag	Las etiquetas son pares clave-valor que define el usuario. En un conjunto de etiquetas puede haber entre 1 y 50 etiquetas.
Key	La clave es el nombre obligatorio de la etiqueta. Para conocer las restricciones, consulte Estructura de etiquetas en Amazon RDS. El valor de la cadena puede tener una longitud de entre 1 y 128 caracteres Unicode y no puede llevar el prefijo `aws:` ni `rds:`. La cadena solo puede contener el conjunto de letras, dígitos y espacio en blanco Unicode, '_', '.', '/', '=', '+', '-' (Java regex: "^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$"). Las claves deben ser únicas dentro de un conjunto de etiquetas. Por ejemplo, en un conjunto de etiquetas no puede haber claves iguales pero con valores diferentes, como proyecto/Trinity y proyecto/Xanadu.
Valor	El valor es la parte opcional de la etiqueta. Para conocer las restricciones, consulte Estructura de etiquetas en Amazon RDS. El valor de la cadena puede tener una longitud de entre 1 y 256 caracteres Unicode y no puede llevar el prefijo `aws:` ni `rds:`. La cadena solo puede contener el conjunto de letras, dígitos y espacio en blanco Unicode, '_', '.', '/', '=', '+', '-' (Java regex: "^([\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*)$"). Los valores no deben ser únicos dentro de un conjunto de etiquetas y también pueden ser nulos. Por ejemplo, puede tener un par clave-valor en un conjunto de etiquetas en proyecto/Trinity y centro-de-costos/Trinity.

Tutorial: especificar qué instancias de base de datos se deben detener mediante etiquetas

Este tutorial supone que tiene varias instancias de base de datos en un entorno de desarrollo o prueba. Debe mantener todas estas instancias de base de datos durante varios días. Algunas instancias de base de datos puede ejecutar pruebas por la noche, mientras que otras se pueden detener durante la noche y volver a iniciarse al día siguiente.

El siguiente tutorial muestra cómo asignar una etiqueta a instancias de base de datos que son adecuadas para detenerse durante la noche. El tutorial muestra cómo un script puede detectar qué instancias de base de datos tienen esa etiqueta y, a continuación, detener esas instancias de base de datos. En este ejemplo, la parte del valor del par clave-valor no importa. La presencia de la `stoppable` etiqueta significa que la instancia de base de datos tiene esta propiedad definida por el usuario.

En el siguiente tutorial, los comandos y las API de etiquetado funcionan con ARN, lo que permite a RDS funcionar sin problemas en regiones de AWS, cuentas de AWS y diferentes tipos de recursos que pueden tener nombres cortos idénticos. Puede especificar el ARN en lugar del ID de instancia de base de datos en los comandos CLI que operan en instancias de base de datos.

Para especificar qué instancias de base de datos se deben detener

1. Determine el ARN de una instancia de base de datos que queremos designar como detenible.

   En el siguiente ejemplo, sustituya el nombre de las propias instancias de base de datos por *`dev-test-db-instance`*. En comandos posteriores que utilicen parámetros ARN, sustituya el ARN de la propia instancia de base de datos. El ARN incluye el propio ID de cuenta de AWS y el nombre de la región de AWS donde se encuentra la instancia de base de datos.

   ```
   $ aws rds describe-db-instances --db-instance-identifier dev-test-db-instance \
     --query "*[].{DBInstance:DBInstanceArn}" --output text
   arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance
   ```

2. Agregue la etiqueta `stoppable` a esta instancia de base de datos.

   Usted elige el nombre de esta etiqueta. Dado que en este ejemplo se trata la etiqueta como un atributo presente o ausente, se omite la `Value=` parte del `--tags` parámetro. Este enfoque significa que puede evitar diseñar una convención de nomenclatura que codifique toda la

información relevante en los nombres. En una convención de este tipo, puede codificar la información en el nombre de la instancia de base de datos o en los nombres de otros recursos.

```
$ aws rds add-tags-to-resource \
  --resource-name arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance \
  --tags Key=stoppable
```

3. Confirme que la etiqueta está presente en la instancia de base de datos.

   Los siguientes comandos recuperan la información de etiqueta para la instancia de base de datos en formato JSON y en texto sin formato separado por tabulaciones.

```
$ aws rds list-tags-for-resource \
  --resource-name arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance
{
    "TagList": [
        {
            "Key": "stoppable",
            "Value": ""

        }
    ]
}
aws rds list-tags-for-resource \
  --resource-name arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance --
output text
TAGLIST stoppable
```

4. Detenga todas las instancias de base de datos designadas como `stoppable`.

   En el siguiente ejemplo, se crea un archivo de texto que enumera todas las instancias de base de datos. El comando de intérprete de comandos recorre la lista y comprueba si cada instancia de base de datos está etiquetada con el atributo correspondiente y ejecuta el comando `aws rds stop-db-instance` para cada instancia de base de datos.

```
$ aws rds describe-db-instances --query "*[].[DBInstanceArn]" --output text >/tmp/
db_instance_arns.lst
$ for arn in $(cat /tmp/db_instance_arns.lst)
do
  match="$(aws rds list-tags-for-resource --resource-name $arn --output text | grep
 stoppable)"
  if [[ ! -z "$match" ]]
```

```
  then
      echo "DB instance $arn is tagged as stoppable. Stopping it now."
# Note that you need to get the DB instance identifier from the ARN.
      dbid=$(echo $arn | sed -e 's/.*://')
      aws rds stop-db-instance --db-instance-identifier $dbid
  fi
done

DB instance arn:arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance is
 tagged as stoppable. Stopping it now.
{
    "DBInstance": {
        "DBInstanceIdentifier": "dev-test-db-instance",
        "DBInstanceClass": "db.t3.medium",
        ...
```

Puede ejecutar un script como el anterior al final de cada día para asegurarse de que se detienen las instancias de base de datos no esenciales. También puede programar un trabajo al usar una utilidad como `cron` para realizar dicha comprobación cada noche. Por ejemplo, puede hacer esto en caso de que algunas instancias de base de datos siguieran ejecutándose por error. Aquí, puede ajustar el comando que prepara la lista de instancias de base de datos para comprobar.

El siguiente comando produce una lista de las instancias de base de datos, pero sólo las que están en `available` estado. El script puede ignorar las instancias de base de datos que ya están detenidas, porque tendrán valores de estado diferentes, como `stopped` o `stopping`.

```
$ aws rds describe-db-instances \
  --query '*[].{DBInstanceArn:DBInstanceArn,DBInstanceStatus:DBInstanceStatus}|[?
DBInstanceStatus == `available`]|[].{DBInstanceArn:DBInstanceArn}' \
  --output text
arn:aws:rds:us-east-1:123456789102:db:db-instance-2447
arn:aws:rds:us-east-1:123456789102:db:db-instance-3395
arn:aws:rds:us-east-1:123456789102:db:dev-test-db-instance
arn:aws:rds:us-east-1:123456789102:db:pg2-db-instance
```

> **Tip**
>
> Puede utilizar la asignación de etiquetas y la búsqueda de instancias de base de datos con esas etiquetas para reducir costos de otras maneras. Por ejemplo, veamos este escenario con instancias de base de datos utilizadas para el desarrollo y las pruebas. En este caso,

puede designar algunas instancias de base de datos para que se eliminen al final de cada día. O puede designarlos para que sus instancias de base de datos se cambien a clases de instancias de base de datos pequeñas durante los períodos de uso escaso previsto.

Nombres de recursos de Amazon (ARN) en Amazon RDS

Cada recurso que se crea en Amazon Web Services se identifica de forma inequívoca mediante un nombre de recurso de Amazon (ARN). Para determinadas operaciones de Amazon RDS, debe identificar de forma inequívoca un recurso de Amazon RDS mediante su ARN. Por ejemplo, al crear una réplica de lectura de una instancia de base de datos de RDS, debe proporcionar el ARN de la instancia de base de datos de origen.

Para obtener información sobre la creación de un ARN y la obtención de un ARN existente, consulte los siguientes temas.

Temas

- Creación de un nombre ARN para Amazon RDS
- Obtención de un ARN existente para Amazon RDS

Creación de un nombre ARN para Amazon RDS

Cada recurso que se crea en Amazon Web Services se identifica de forma inequívoca mediante un nombre de recurso de Amazon (ARN). Puede crear un ARN para un recurso de Amazon RDS utilizando la siguiente sintaxis.

`arn:aws:rds:<region>:<account number>:<resourcetype>:<name>`

Nombre de la región	Región	Punto de conexión	Protocolo	
Este de EE. UU. (Ohio)	us-east-2	rds.us-east-2.amazonaws.com	HTTPS	
		rds-fips.us-east-2.api.aws	HTTPS	
		rds.us-east-2.api.aws	HTTPS	
		rds-fips.us-east-2.amazonaws.com	HTTPS	
Este de EE. UU. (Norte de Virginia)	us-east-1	rds.us-east-1.amazonaws.com	HTTPS	
		rds-fips.us-east-1.api.aws	HTTPS	

Nombre de la región	Región	Punto de conexión	Protocolo
		rds-fips.us-east-1.amazonaws.com	HTTPS
		rds.us-east-1.api.aws	HTTPS
Oeste de EE. UU. (Norte de California)	us-west-1	rds.us-west-1.amazonaws.com	HTTPS
		rds.us-west-1.api.aws	HTTPS
		rds-fips.us-west-1.amazonaws.com	HTTPS
		rds-fips.us-west-1.api.aws	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	rds.us-west-2.amazonaws.com	HTTPS
		rds-fips.us-west-2.amazonaws.com	HTTPS
		rds.us-west-2.api.aws	HTTPS
		rds-fips.us-west-2.api.aws	HTTPS
África (Ciudad del Cabo)	af-south-1	rds.af-south-1.amazonaws.com	HTTPS
		rds.af-south-1.api.aws	HTTPS
Asia-Pacífico (Hong Kong)	ap-east-1	rds.ap-east-1.amazonaws.com	HTTPS
		rds.ap-east-1.api.aws	HTTPS
Asia-Pacífico (Hyderabad)	ap-south-2	rds.ap-south-2.amazonaws.com	HTTPS
		rds.ap-south-2.api.aws	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Yakarta)	ap-southeast-3	rds.ap-southeast-3.amazonaws.com rds.ap-southeast-3.api.aws	HTTPS HTTPS
Asia-Pacífico (Malasia)	ap-southeast-5	rds.ap-southeast-5.amazonaws.com	HTTPS
Asia-Pacífico (Melbourne)	ap-southeast-4	rds.ap-southeast-4.amazonaws.com rds.ap-southeast-4.api.aws	HTTPS HTTPS
Asia-Pacífico (Bombay)	ap-south-1	rds.ap-south-1.amazonaws.com rds.ap-south-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Osaka)	ap-northeast-3	rds.ap-northeast-3.amazonaws.com rds.ap-northeast-3.api.aws	HTTPS HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	rds.ap-northeast-2.amazonaws.com rds.ap-northeast-2.api.aws	HTTPS HTTPS
Asia-Pacífico (Singapur)	ap-southeast-1	rds.ap-southeast-1.amazonaws.com rds.ap-southeast-1.api.aws	HTTPS HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	rds.ap-southeast-2.amazonaws.com rds.ap-southeast-2.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Asia-Pacífico (Taipéi)	ap-east-2	rds.ap-east-2.amazonaws.com	HTTPS
Asia-Pacífico (Tailandia)	ap-southeast-7	rds.ap-southeast-7.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	rds.ap-northeast-1.amazonaws.com rds.ap-northeast-1.api.aws	HTTPS HTTPS
Canadá (centro)	ca-central-1	rds.ca-central-1.amazonaws.com rds.ca-central-1.api.aws rds-fips.ca-central-1.api.aws rds-fips.ca-central-1.amazonaws.com	HTTPS HTTPS HTTPS HTTPS
Oeste de Canadá (Calgary)	ca-west-1	rds.ca-west-1.amazonaws.com rds-fips.ca-west-1.amazonaws.com	HTTPS HTTPS
Europa (Fráncfort)	eu-central-1	rds.eu-central-1.amazonaws.com rds.eu-central-1.api.aws	HTTPS HTTPS
Europa (Irlanda)	eu-west-1	rds.eu-west-1.amazonaws.com rds.eu-west-1.api.aws	HTTPS HTTPS
Europa (Londres)	eu-west-2	rds.eu-west-2.amazonaws.com rds.eu-west-2.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
Europa (Milán)	eu-south-1	rds.eu-south-1.amazonaws.com rds.eu-south-1.api.aws	HTTPS HTTPS
Europa (París)	eu-west-3	rds.eu-west-3.amazonaws.com rds.eu-west-3.api.aws	HTTPS HTTPS
Europa (España)	eu-south-2	rds.eu-south-2.amazonaws.com rds.eu-south-2.api.aws	HTTPS HTTPS
Europa (Estocolmo)	eu-north-1	rds.eu-north-1.amazonaws.com rds.eu-north-1.api.aws	HTTPS HTTPS
Europa (Zúrich)	eu-central-2	rds.eu-central-2.amazonaws.com rds.eu-central-2.api.aws	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	rds.il-central-1.amazonaws.com rds.il-central-1.api.aws	HTTPS HTTPS
México (central)	mx-central-1	rds.mx-central-1.amazonaws.com	HTTPS
Medio Oriente (Baréin)	me-south-1	rds.me-south-1.amazonaws.com rds.me-south-1.api.aws	HTTPS HTTPS
Medio Oriente (EAU)	me-central-1	rds.me-central-1.amazonaws.com rds.me-central-1.api.aws	HTTPS HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo
América del Sur (São Paulo)	sa-east-1	rds.sa-east-1.amazonaws.com rds.sa-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	rds.us-gov-east-1.amazonaws.com rds.us-gov-east-1.api.aws	HTTPS HTTPS
AWS GovCloud (Oeste de EE.UU.)	us-gov-west-1	rds.us-gov-west-1.amazonaws.com rds.us-gov-west-1.api.aws	HTTPS HTTPS

En la siguiente tabla se muestra el formato que debe utilizar al crear un ARN para un tipo de recurso concreto de Amazon RDS.

Tipo de recurso	Formato de ARN
Instancia de base de datos	arn:aws:rds:*<region>*:*<account>* :db:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :db:my-mysql-instance-1`
Clúster de base de datos	arn:aws:rds:*<region>*:*<account>* :clúster:*<name>* Por ejemplo:

Tipo de recurso	Formato de ARN
	`arn:aws:rds: us-east-2 :123456789012 :cluster: my-aurora-cluster-1`
Suscripción a eventos	arn:aws:rds:*<region>*:*<account>* :es:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :es:my-subscription`
Grupo de opciones de base de datos	arn:aws:rds:*<region>*:*<account>* :og:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :og:my-og`
DB Parameter Group (Grupo de parámetros de base de datos)	arn:aws:rds:*<region>*:*<account>* :pg:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :pg:my-param-enable-logs`
Grupo de parámetros de clúster de base de datos	arn:aws:rds:*<region>*:*<account>* :clúster-pg:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :cluster-pg: my-cluster-param-timezone`
Instancia de base de datos reservada	arn:aws:rds:*<region>*:*<account>* :ri:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :ri:my-reserved-postgresql`

Tipo de recurso	Formato de ARN
Grupo de seguridad de base de datos	arn:aws:rds:*<region>*:*<account>* :secgrp:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :secgrp:my-public`
Instantánea de base de datos automatizada	arn:aws:rds:*<region>*:*<account>* :snapshot:rds:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :snapshot:rds: my-mysql-db-2019-07-22-07-23`
Instantánea de clúster de base de datos automatizada	arn:aws:rds:*<region>*:*<account>* :clúster-snapshot:rds:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :cluster-snapshot:rds: my-aurora-cluster-2019-07-22-16-16`
Instantánea de base de datos manual	arn:aws:rds:*<region>*:*<account>* :snapshot:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :snapshot: my-mysql-db-snap`
Instantánea de un clúster de base de datos manual	arn:aws:rds:*<region>*:*<account>* :clúster-snapshot:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :cluster-snapshot: my-aurora-cluster-snap`

Tipo de recurso	Formato de ARN
Grupo de subred de base de datos	arn:aws:rds:*<region>*:*<account>* :subgrp:*<name>* Por ejemplo: `arn:aws:rds: us-east-2 :123456789012 :subgrp:my-subnet -10`

Obtención de un ARN existente para Amazon RDS

Puede obtener el ARN de un recurso de RDS mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de RDS.

Consola

Para obtener un ARN desde la AWS Management Console, vaya al recurso cuyo ARN desea obtener y consulte los detalles de ese recurso.

Por ejemplo, puede obtener el ARN de una instancia de base de datos desde la pestaña Configuración de los detalles de la instancia de base de datos.

AWS CLI

Para obtener el ARN de un recurso concreto de RDS desde la AWS CLI, se utiliza el comando `describe` con dicho recurso. En la siguiente tabla se muestran los distintos comandos de AWS CLI, junto con la propiedad ARN que se utiliza con el comando para obtener un ARN.

AWS CLI command	Propiedad ARN
describe-event-subscriptions	EventSubscriptionArn
describe-certificates	CertificateArn
describe-db-parameter-groups	DBParameterGroupArn
describe-db-clúster-parameter-groups	DBclústerParameterGroupArn

AWS CLI command	Propiedad ARN
describe-db-instances	DBInstanceArn
describe-db-security-groups	DBSecurityGroupArn
describe-db-snapshots	DBSnapshotArn
describe-events	SourceArn
describe-reserved-db-instances	ReservedDBInstanceArn
describe-db-subnet-groups	DBSubnetGroupArn
describe-option-groups	OptionGroupArn
describe-db-clústers	DBclústerArn
describe-db-clúster-snapshots	DBclústerSnapshotArn

Por ejemplo, el siguiente comando de la AWS CLI obtiene el ARN de una instancia de base de datos.

Example

Para Linux, macOS o:Unix

```
aws rds describe-db-instances \
--db-instance-identifier DBInstanceIdentifier \
--region us-west-2 \
--query "*[].{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceArn:DBInstanceArn}"
```

En:Windows

```
aws rds describe-db-instances ^
--db-instance-identifier DBInstanceIdentifier ^
--region us-west-2 ^
--query "*[].{DBInstanceIdentifier:DBInstanceIdentifier,DBInstanceArn:DBInstanceArn}"
```

El resultado de ese comando es como el siguiente:

```
[
    {
        "DBInstanceArn": "arn:aws:rds:us-west-2:account_id:db:instance_id",
        "DBInstanceIdentifier": "instance_id"
    }
]
```

API de RDS

Para obtener el ARN de un recurso concreto de RDS, puede llamar a las siguientes operaciones de la API de RDS y utilizar las propiedades ARN que se muestran a continuación.

Operación de la API de RDS	Propiedad ARN
DescribeEventSubscriptions	EventSubscriptionArn
DescribeCertificates	CertificateArn
DescribeDBParameterGroups	DBParameterGroupArn
DescribeDBclústerParameterGroups	DBclústerParameterGroupArn
DescribeDBInstances	DBInstanceArn
DescribeDBSecurityGroups	DBSecurityGroupArn
DescribeDBSnapshots	DBSnapshotArn
DescribeEvents	SourceArn
DescribeReservedDBInstances	ReservedDBInstanceArn
DescribeDBSubnetGroups	DBSubnetGroupArn
DescribeOptionGroups	OptionGroupArn
DescribeDBclústers	DBclústerArn
DescribeDBclústerSnapshots	DBclústerSnapshotArn

Uso de almacenamiento para instancias de base de datos de Amazon RDS

Para especificar cómo quiere que se almacenen sus datos en Amazon RDS, elija un tipo de almacenamiento y proporcione un tamaño de almacenamiento cuando cree o modifique una instancia de base de datos. Más tarde, puede aumentar la cantidad o cambiar el tipo de almacenamiento modificando la instancia de base de datos. Para obtener información sobre qué tipo de almacenamiento debe usar para su carga de trabajo, consulte Tipos de almacenamiento de Amazon RDS.

Temas

- Aumento de la capacidad de almacenamiento de la instancia de base de datos
- Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS
- Actualización del sistema de archivos de almacenamiento para una instancia de base de datos
- Modificación de la configuración del almacenamiento de SSD de las IOPS aprovisionadas
- Modificaciones en el almacenamiento con uso intensivo de E/S
- Modificación de la configuración del almacenamiento SDD de uso general (gp3)
- Uso de un volumen de registro específico (DLV)

Aumento de la capacidad de almacenamiento de la instancia de base de datos

Si necesita espacio para datos adicionales, puede aumentar el almacenamiento de una instancia de base de datos existente. Para ello, puede usar la consola de administración de Amazon RDS, la API de Amazon RDS o la AWS Command Line Interface (AWS CLI). Para obtener información sobre los límites de almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

> **Note**
>
> No puede reducir la cantidad de almacenamiento de una instancia de base de datos una vez que se ha asignado el almacenamiento. Cuando aumente el almacenamiento asignado, este aumento debe ser de al menos el 10 por ciento. Si intenta aumentar el valor en menos del 10 por ciento, obtendrá un error.

El aumento de almacenamiento para instancias de base de datos de RDS para SQL Server solo es compatible con los tipos de almacenamiento de SSD de uso general y SSD de IOPS aprovisionadas.

Recomendamos que cree una alarma de Amazon CloudWatch para monitorizar la cantidad de almacenamiento libre de la instancia de base de datos para que pueda reaccionar cuando sea necesario. Para obtener más información sobre la configuración de alarmas de CloudWatch, consulte Uso de alarmas de CloudWatch.

Por lo general, la escalabilidad del almacenamiento no causa ninguna interrupción o merma de rendimiento en la instancia de base de datos. Después de modificar el tamaño de almacenamiento para una instancia de base de datos, el estado de la instancia de base de datos es storage-optimization (optimización del almacenamiento).

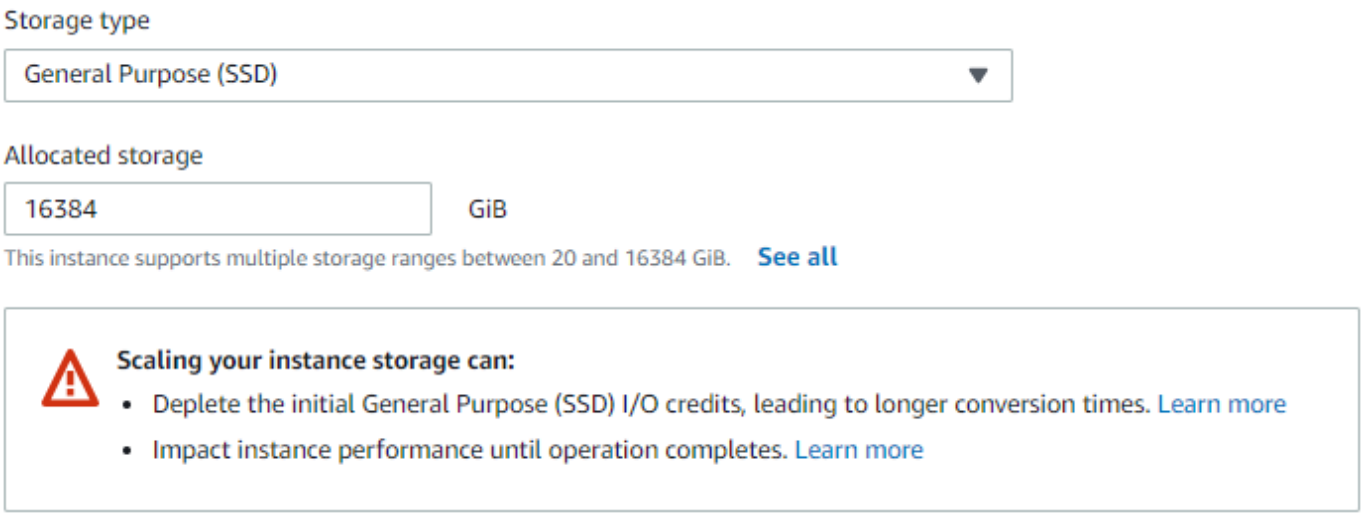
Note

La optimización del almacenamiento puede tardar varias horas. No puede hacer modificaciones de almacenamiento adicionales hasta seis (6) horas o después de que se haya completado la optimización de almacenamiento en la instancia, lo que tarde más tiempo. Puede ver el progreso de la optimización del almacenamiento en la AWS Management Console o mediante el comando de la AWS CLI describe-db-instances.

Consola

Para aumentar el almacenamiento de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea modificar.
4. Elija Modify.
5. Escriba un nuevo valor para Allocated Storage (Almacenamiento asignado). Debe ser mayor que el valor actual.



6. Elija Continue (Continuar) para pasar a la siguiente pantalla.
7. Para aplicar los cambios a la instancia de base de datos inmediatamente, seleccione Apply Immediately (Aplicar inmediatamente) en la sección Scheduling of modifications (Programación de modificaciones).

   También puede elegir Apply during the next scheduled maintenance window (Aplicar durante la próxima ventana de mantenimiento programada) para aplicar los cambios durante el próximo período de mantenimiento.
8. Cuando los ajustes sean los deseados, elija Modify DB instance (Modificar instancia de base de datos).

AWS CLI

Para aumentar el almacenamiento de una instancia de base de datos, utilice el comando AWS CLI de la `modify-db-instance`. Establezca los siguientes parámetros:

- `--allocated-storage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente.

  También puede utilizar `--no-apply-immediately` (valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento. Se produce una interrupción inmediata cuando se aplican los cambios.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

API de RDS

Para aumentar el almacenamiento de una instancia de base de datos, utilice la operación de la API de Amazon RDS `ModifyDBInstance`. Establezca los siguientes parámetros:

- `AllocatedStorage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `ApplyImmediately`: establezca esta opción en `True` para aplicar los cambios de almacenamiento inmediatamente. Establezca esta opción en `False` (valor predeterminado) para aplicar los cambios durante el siguiente período de mantenimiento. Se produce una interrupción inmediata cuando se aplican los cambios.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS

Si su carga de trabajo es impredecible, puede habilitar el escalado automático de almacenamiento para una instancia de base de datos de Amazon RDS. Para ello, puede usar la consola de Amazon RDS, la API de Amazon RDS o la AWS CLI.

Por ejemplo, puede usar esta característica para una nueva aplicación de juegos para dispositivos móviles que los usuarios están adoptando rápidamente. En este caso, una carga de trabajo de aumento rápido podría superar el almacenamiento de base de datos disponible. Para evitar tener que ampliar manualmente el almacenamiento de la base de datos, puede usar el escalado automático de almacenamiento de Amazon RDS.

Con la opción de escalado automático de almacenamiento habilitada, si Amazon RDS detecta que se está quedando sin espacio en la base de datos, aumenta automáticamente el almacenamiento. Amazon RDS inicia una modificación en el almacenamiento para una instancia de base de datos habilitada con la opción de escalado automático cuando se aplican los siguientes factores:

- El espacio libre disponible es inferior o igual al 10 por ciento del almacenamiento asignado.
- La condición de almacenamiento bajo dura al menos cinco minutos.

- Han pasado al menos seis horas desde la última modificación del almacenamiento o se ha completado la optimización del almacenamiento en la instancia, lo que tarde más tiempo.

El almacenamiento adicional se produce en incrementos de lo que sea superior a continuación:

- 10 GiB
- 10 % del almacenamiento asignado actualmente.
- El crecimiento previsto del almacenamiento superará el tamaño de almacenamiento asignado actualmente en las próximas 7 horas en función de las métricas `FreeStorageSpace` de la última hora. Para obtener más información sobre métricas, consulte Monitoreo con Amazon CloudWatch.

El umbral máximo de almacenamiento es el límite que se establece para el escalado automático de la instancia de base de datos. Se dan las siguientes restricciones:

- Debe establecer el umbral máximo de almacenamiento en al menos un 10 % más que el almacenamiento asignado actual. Recomendamos configurarlo en al menos un 26 % más para evitar recibir una notificación de evento para indicar que el tamaño de almacenamiento se acerca al umbral de almacenamiento máximo.

  Por ejemplo, si tiene una instancia de base de datos con 1000 GiB de almacenamiento asignado, establezca el umbral máximo de almacenamiento en al menos 1100 GiB. Si no, aparecerá un error indicando que el tamaño máximo de almacenamiento no es válido para *`nombre_motor`*. Sin embargo, recomendamos establecer el umbral máximo de almacenamiento en al menos 1260 GiB para evitar la notificación de evento.
- Para una instancia de base de datos que utiliza almacenamiento de IOPS aprovisionadas (io1 o io2 Block Express), la relación entre IOPS y umbral máximo de almacenamiento (en GiB) debe estar dentro de un rango determinado. Para obtener más información, consulte Almacenamiento de SSD de IOPS aprovisionadas.
- No puede establecer el umbral de almacenamiento máximo en las instancias habilitadas con la opción de escalado automático en un valor superior al almacenamiento máximo asignado para el motor de base de datos y la clase de instancia de base de datos.

  Por ejemplo, SQL Server Standard Edition en db.m5.xlarge tiene un almacenamiento asignado predeterminado para la instancia de 20 GiB (el mínimo) y un almacenamiento asignado máximo de 16 384 GiB. El umbral de almacenamiento máximo predeterminado para el escalado automático es de 1000 GiB. Si utiliza esta opción como predeterminada, la instancia no escala de forma

automática por encima de los 1000 GiB. Es cierto aunque el almacenamiento máximo asignado para la instancia es 16 384 GiB.

> **Note**
>
> Le recomendamos que elija cuidadosamente el umbral máximo de almacenamiento en función de los patrones de uso y las necesidades del cliente. Si hay aberraciones en los patrones de uso, el umbral de almacenamiento máximo puede evitar que el almacenamiento escale a un valor inesperadamente alto cuando el escalado automático predice un umbral muy alto. Después de que una instancia de base de datos se ha escalado automáticamente, su almacenamiento asignado no se puede reducir.

Temas

- Limitaciones del escalado automático de almacenamiento
- Habilitación del escalado automático de almacenamiento para una nueva instancia de base de datos
- Cambio de la configuración de escalado automático de almacenamiento para una instancia de base de datos
- Reducción vertical u horizontal de forma manual de la instancia de base de datos
- Apagado del escalado automático de almacenamiento para una instancia de base de datos

Limitaciones del escalado automático de almacenamiento

Se aplican las siguientes limitaciones al escalado automático del almacenamiento:

- No se produce el escalado automático si se supera el umbral de almacenamiento máximo debido al incremento del almacenamiento.
- Al escalar automáticamente, RDS predice el tamaño del almacenamiento de información para las operaciones de escalado automático posteriores. Si se prevé que una operación posterior supere el umbral máximo de almacenamiento, RDS se escalará automáticamente al umbral máximo de almacenamiento.
- El escalado automático no puede evitar completamente situaciones de almacenamiento completo para cargas de datos de gran tamaño. Esto se debe a que no es posible hacer modificaciones

de almacenamiento adicionales durante seis (6) horas o hasta que se haya completado la optimización de almacenamiento en la instancia, lo que tarde más tiempo.

Si realiza una carga de datos grande y el escalado automático no proporciona suficiente espacio, la base de datos puede permanecer en el estado de almacenamiento completo durante varias horas. Esto puede dañar la base de datos.

- Si inicia una operación de escalado de almacenamiento al mismo tiempo que Amazon RDS inicia una operación de escalado automático, la modificación realizada en su almacenamiento tendrá prioridad. Por tanto, se cancela la operación de escalado automático.
- El ajuste de escala automático no puede reducir el almacenamiento asignado. No puede reducir la cantidad de almacenamiento de una instancia de base de datos una vez que se ha asignado el almacenamiento.
- El escalado automático no se puede usar con almacenamiento magnético.
- El escalado automático no se puede usar con las siguientes clases de instancia de generación anterior que tienen menos de 6 TiB de almacenamiento ordenable: db.m3.large, db.m3.xlarge y db.m3.2xlarge.
- Las operaciones de escalado automático no están registradas por AWS CloudTrail. Para obtener más información acerca de CloudTrail, consulte Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail.

Aunque el escalado automático le ayuda a aumentar dinámicamente el almacenamiento en su instancia de base de datos de Amazon RDS, debe configurar el almacenamiento inicial de la instancia de base de datos con un tamaño adecuado para una carga de trabajo típica.

Habilitación del escalado automático de almacenamiento para una nueva instancia de base de datos

Cuando cree una nueva instancia de base de datos de Amazon RDS, podrá elegir si habilitar el escalado automático de almacenamiento. También puede establecer un límite superior en el almacenamiento que Amazon RDS puede asignar en la instancia de base de datos.

> **Note**
>
> Cuando clona una instancia de base de datos de Amazon RDS que tiene habilitada el escalado automático de almacenamiento, la instancia clonada no hereda automáticamente esa configuración. La nueva instancia de la base de datos tiene la misma cantidad de almacenamiento asignado que la instancia original. Puede volver a activar el escalado

automático de almacenamiento para la nueva instancia si la instancia clonada sigue aumentando sus requisitos de almacenamiento.

Consola

Para habilitar el escalado automático de almacenamiento para una nueva instancia de base de datos, realice el siguiente procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Elija Create database (Crear base de datos). En la página Select engine (Seleccionar motor), elija el motor de base de datos y especifique la información de la instancia de base de datos como se describe en Introducción a Amazon RDS.
5. En la sección Storage Autoscaling (Escalado automático de almacenamiento), establezca el valor Maximum storage threshold (Umbral de almacenamiento máximo) de la instancia de base de datos.
6. Especifique el resto de información de su instancia de base de datos como se describe en Introducción a Amazon RDS.

AWS CLI

Para habilitar el escalado automático de almacenamiento para una nueva instancia de base de datos, utilice el comando de la AWS CLI `create-db-instance`. Establezca el siguiente parámetro:

- `--max-allocated-storage`: activa el escalado automático de almacenamiento y establece el límite superior de tamaño de almacenamiento en gibibytes.

Para comprobar que el escalado automático de almacenamiento de Amazon RDS está disponible para su instancia de base de datos, utilice el comando de la AWS CLI `describe-valid-db-instance-modifications`. Para realizar la comprobación según la clase de instancia antes de crear una instancia, utilice el comando `describe-orderable-db-instance-options`. Compruebe el siguiente campo en el valor de retorno:

- `SupportsStorageAutoscaling`: indica si la instancia de base de datos o la clase de instancia admiten el escalado automático de almacenamiento.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

API de RDS

Para habilitar el escalado automático de almacenamiento de una nueva instancia de base de datos, utilice la operación de la API de Amazon RDS `CreateDBInstance`. Establezca el siguiente parámetro:

- `MaxAllocatedStorage`: activa el escalado automático de almacenamiento de Amazon RDS y establece el límite superior de tamaño de almacenamiento en gibibytes.

Para comprobar que el escalado automático de almacenamiento de Amazon RDS está disponible para su instancia de base de datos, use la operación `DescribeValidDbInstanceModifications` de la API de Amazon RDS para una instancia existente o la operación `DescribeOrderableDBInstanceOptions` antes de crear una instancia. Compruebe el siguiente campo en el valor de retorno:

- `SupportsStorageAutoscaling`: indica si la instancia de base de datos admite el escalado automático de almacenamiento.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Cambio de la configuración de escalado automático de almacenamiento para una instancia de base de datos

Puede activar el escalado automático de almacenamiento para una instancia de base de datos de Amazon RDS. También puede cambiar el límite superior en el almacenamiento que Amazon RDS puede asignar en la instancia de base de datos.

Consola

Para cambiar la configuración de escalado automático de almacenamiento para una instancia de base de datos, realice el siguiente procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione la instancia de base de datos que desea modificar y elija Modify (Modificar). Aparece la página Modify DB instance.
4. Cambie el límite de almacenamiento en la sección Autoscaling (Escalado automático). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
5. Cuando haya realizado todos los cambios que desee, elija Continue (Continuar) y compruebe sus modificaciones.
6. En la página de confirmación, revise los cambios. Si son correctos, elija Modificar la instancia de base de datos para guardarlos. Si no son correctos, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

   El cambio del límite de escalado automático se produce de forma inmediata. Esta opción no tiene en cuenta la opción Apply immediately.

AWS CLI

Para cambiar la configuración de escalado automático de almacenamiento para una instancia de base de datos, utilice el comando de la AWS CLI `modify-db-instance`. Establezca el siguiente parámetro:

- `--max-allocated-storage`: establece el límite superior del tamaño de almacenamiento en gibibytes. Si el valor es superior al parámetro `--allocated-storage`, se activa el escalado automático de almacenamiento. Si el valor es el mismo que el parámetro `--allocated-storage`, el escalado automático de almacenamiento se desactiva.

Para comprobar que el escalado automático de almacenamiento de Amazon RDS está disponible para su instancia de base de datos, utilice el comando de la AWS CLI `describe-valid-db-instance-modifications`. Para realizar la comprobación según la clase de instancia antes

de crear una instancia, utilice el comando `describe-orderable-db-instance-options`. Compruebe el siguiente campo en el valor de retorno:

- `SupportsStorageAutoscaling`: indica si la instancia de base de datos admite el escalado automático de almacenamiento.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

API de RDS

Para cambiar la configuración de escalado automático de almacenamiento de una instancia de base de datos, utilice la operación de la API de Amazon RDS `ModifyDBInstance`. Establezca el siguiente parámetro:

- `MaxAllocatedStorage`: establece el límite superior del tamaño de almacenamiento en gibibytes.

Para comprobar que el escalado automático de almacenamiento de Amazon RDS está disponible para su instancia de base de datos, use la operación `DescribeValidDbInstanceModifications` de la API de Amazon RDS para una instancia existente o la operación `DescribeOrderableDBInstanceOptions` antes de crear una instancia. Compruebe el siguiente campo en el valor de retorno:

- `SupportsStorageAutoscaling`: indica si la instancia de base de datos admite el escalado automático de almacenamiento.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Reducción vertical u horizontal de forma manual de la instancia de base de datos

Amazon RDS ofrece escalado automático del almacenamiento para satisfacer la creciente demanda. Sin embargo, existen limitaciones en cuanto a la reducción vertical u horizontal:

- Almacenamiento de RDS: aunque RDS admite el escalado vertical automático del almacenamiento a medida que aumenta la demanda, no se reduce verticalmente de forma automática.

- Réplicas de lectura: RDS no admite escalar horizontalmente (agregar) o reducir horizontalmente (eliminar) réplicas de lectura de forma automática. Debe agregar o eliminar manualmente las réplicas de lectura según los requisitos de carga.

Para reducir verticalmente los recursos de RDS, lleve a cabo las siguientes acciones manuales:

- Para el almacenamiento, no puede reducir manualmente el almacenamiento asignado de una instancia de base de datos mediante el comando `modify-db-instance`. En su lugar, elija una de las siguientes técnicas:
  - Utilice una implementación azul/verde si el motor de base de datos lo admite. Cree una base de datos verde con un tamaño de almacenamiento menor y, a continuación, ascienda la base de datos verde a base de datos azul. Para obtener más información, consulte Modificación de la configuración de almacenamiento y rendimiento.
  - Cree una nueva instancia de base de datos con menos almacenamiento asignado, migre manualmente los datos de la base de datos actual a la instancia de base de datos recién creada y cambie los puntos de conexión de base de datos.
- En el caso de las réplicas de lectura, elimine manualmente las réplicas no utilizadas a través de la consola de RDS o AWS CLI.

Apagado del escalado automático de almacenamiento para una instancia de base de datos

Si ya no necesita que Amazon RDS aumente automáticamente el almacenamiento de una instancia de base de datos de Amazon RDS, puede desactivar el escalado automático de almacenamiento. Una vez que realice esa operación, podrá seguir aumentando manualmente la cantidad de almacenamiento para su instancia de base de datos.

Consola

Para apagar el escalado automático de almacenamiento para una instancia de base de datos, realice el siguiente procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

3. Seleccione la instancia de base de datos que desea modificar y elija Modify (Modificar). Aparece la página Modify DB instance.
4. Elimine la marca de la casilla de verificación Enable storage autoscaling (Habilitar escalado automático de almacenamiento) de la sección Storage autoscaling (Escalado automático de almacenamiento). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
5. Cuando haya realizado todos los cambios que desee, elija Continue (Continuar) y compruebe las modificaciones.
6. En la página de confirmación, revise los cambios. Si son correctos, elija Modificar la instancia de base de datos para guardarlos. Si no son correctos, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

El cambio del límite de escalado automático se produce de forma inmediata. Esta opción no tiene en cuenta la opción Apply immediately.

AWS CLI

Para apagar el escalado automático de almacenamiento para una instancia de base de datos, utilice el comando de la AWS CLI `modify-db-instance` y el siguiente parámetro:

- `--max-allocated-storage`: especifique un valor igual al ajuste `--allocated-storage` para evitar un escalado automático de almacenamiento de Amazon RDS posterior para la instancia de base de datos especificada.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

API de RDS

Para desactivar el escalado automático de almacenamiento de una instancia de base de datos, utilice la operación de la API de Amazon RDS `ModifyDBInstance`. Establezca el siguiente parámetro:

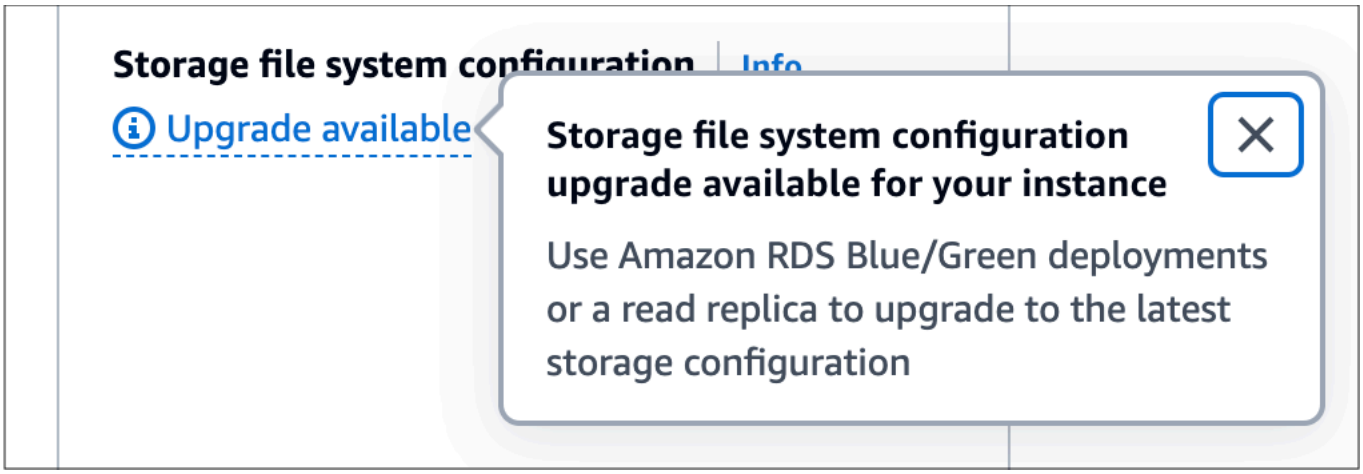
- `MaxAllocatedStorage`: especifique un valor igual al ajuste `AllocatedStorage` para evitar un escalado automático de almacenamiento de Amazon RDS posterior para la instancia de base de datos especificada.

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Actualización del sistema de archivos de almacenamiento para una instancia de base de datos

La mayoría de las instancias de base de datos de RDS ofrecen un tamaño de almacenamiento máximo de 64 TiB para las bases de datos MariaDB, MySQL y PostgreSQL. Sin embargo, algunos sistemas de archivos antiguos de 32 bits tienen capacidades de almacenamiento más bajas. Para determinar la capacidad de almacenamiento de la instancia de base de datos, use el comando de la AWS CLI describe-valid-db-instance-modifications.

RDS comprueba si el sistema de almacenamiento tiene un tamaño de almacenamiento de 16 TiB, un límite de tamaño de archivo de 2 TiB o escrituras no optimizadas. Si las instancias de base de datos cumplen estas condiciones, RDS le avisa de que la configuración del sistema de archivos es apta para una actualización. Puede comprobar si la instancia de base de datos puede actualizarse en el panel Almacenamiento de la página de detalles de la instancia de base de datos.



Si la instancia de base de datos cumple los requisitos para una actualización del sistema de archivos, utilice cualquiera de las siguientes técnicas:

- Cree una implementación azul/verde y especifique Actualizar la configuración del sistema de archivos de almacenamiento.

  Esta opción actualiza el sistema de archivos del entorno verde en la configuración preferida. A continuación, puede conmutar la implementación azul/verde para que el entorno verde sea el nuevo entorno de producción. Para obtener instrucciones detalladas, consulta the section called “Creación de una implementación azul/verde”.

- Cree una réplica de lectura de la instancia de base de datos y especifique Actualizar la configuración del sistema de archivos de almacenamiento.

  Esta opción actualiza el sistema de archivos de la réplica de lectura a la configuración preferida. Luego, puede promover una réplica de lectura en una instancia independiente. Para obtener instrucciones detalladas, consulta the section called “Creación de una réplica de lectura”.

Durante el proceso de actualización del almacenamiento, el motor de base de datos no está disponible. La actualización de la configuración de almacenamiento es una operación que requiere un uso intensivo de E/S y prolonga los tiempos de creación en las réplicas de lectura y las implementaciones azul/verde. El proceso de actualización del almacenamiento es más rápido cuando se cumplen las dos condiciones siguientes:

- La instancia de base de datos de origen utiliza un almacenamiento SSD de IOPS aprovisionadas (io1 o io2 Block Express).
- Ha aprovisionado el entorno verde o la réplica de lectura con un tamaño de instancia 4xlarge o superior.

Las actualizaciones de almacenamiento que implican el almacenamiento de SSD de uso general (gp2) pueden agotar el saldo de créditos de E/S, lo que puede generar retrasos en la actualización. Para obtener más información, consulte the section called “Almacenamiento de instancias de base de datos”.

Durante una actualización de almacenamiento, RDS aumenta el tamaño de almacenamiento asignado en un 10 % para la instancia verde o la réplica de lectura si se cumplen las dos condiciones siguientes:

- El consumo de almacenamiento de la instancia de base de datos de origen es superior o igual al 90 % del tamaño de almacenamiento asignado.
- El escalado automático de almacenamiento está habilitado.

RDS desactiva el escalado automático cuando el nuevo tamaño de almacenamiento es superior o igual al almacenamiento máximo asignado que se estableció para la instancia. Si el escalado automático de almacenamiento está desactivado antes de que empiece la actualización del almacenamiento, el tamaño del almacenamiento no aumenta durante la actualización.

Modificación de la configuración del almacenamiento de SSD de las IOPS aprovisionadas

Puede modificar la configuración de una instancia de base de datos que utiliza el almacenamiento de SSD de IOPS aprovisionadas mediante la consola de administración de Amazon RDS, la AWS CLI o la API de Amazon RDS. Especifique el tipo de almacenamiento, el almacenamiento asignado y la cantidad de IOPS aprovisionadas que necesita. El intervalo depende del motor de base de datos y del tipo de instancia.

Aunque puede reducir la cantidad de IOPS aprovisionadas de su instancia, no puede reducir el tamaño de almacenamiento.

En la mayoría de los casos, el aumento del almacenamiento no requiere ninguna interrupción y no degrada el rendimiento del servidor. Después de modificar el tamaño de IOPS de almacenamiento para una instancia de base de datos, el estado de la instancia de base de datos es storage-optimization (optimización del almacenamiento).

> **Note**
>
> La optimización del almacenamiento puede tardar varias horas. No puede hacer modificaciones de almacenamiento adicionales hasta seis (6) horas o después de que se haya completado la optimización de almacenamiento en la instancia, lo que tarde más tiempo.

Para obtener información sobre los rangos de almacenamiento asignado y las IOPS aprovisionadas disponibles para cada motor de base de datos, consulte Almacenamiento de SSD de IOPS aprovisionadas.

Consola

Para cambiar la configuración de IOPS aprovisionadas de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

Para filtrar la lista de instancias de base de datos, en Filter databases (Filtrar bases de datos), escriba una cadena de texto para que Amazon RDS la utilice para filtrar los resultados. Solo aparecen instancias de base de datos cuyos nombres contengan la cadena.

3. Elija la instancia de base de datos con almacenamiento de IOPS aprovisionadas que desea modificar.
4. Elija Modify.
5. En la página Modificar instancia de base de datos, elija SSD de IOPS aprovisionadas (io1) o SSD de IOPS aprovisionadas (io2) en Tipo de almacenamiento.
6. Introduzca un valor para Provisioned IOPS (IOPS aprovisionadas).

   Si el valor que especifica para Allocated storage (Almacenamiento asignado) o Provisioned IOPS (IOPS provisionadas) está fuera de los límites admitidos por el otro parámetro, se muestra un mensaje de advertencia. Este mensaje indica el intervalo de valores necesario para el otro parámetro.
7. Elija Continue.
8. Para aplicar los cambios a la instancia de base de datos inmediatamente, seleccione Apply Immediately (Aplicar inmediatamente) en la sección Scheduling of modifications (Programación de modificaciones). También puede elegir Apply during the next scheduled maintenance window (Aplicar durante la próxima ventana de mantenimiento programada) para aplicar los cambios durante el próximo período de mantenimiento.
9. Revise los parámetros que se cambiarán y elija Modify DB Instance (Modificar instancia de base de datos) para completar la modificación.

   El valor nuevo para el almacenamiento asignado o para IOPS aprovisionadas aparece en la columna Status (Estado).

AWS CLI

Para cambiar la configuración de IOPS aprovisionadas de una instancia de base de datos, utilice el comando AWS CLI de la `modify-db-instance`. Establezca los siguientes parámetros:

- `--storage-type`: establézcalo en `io1` o `io2` para IOPS aprovisionadas.
- `--allocated-storage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.

- `--iops`: nueva cantidad de IOPS aprovisionadas para la instancia de base de datos, expresada en operaciones de E/S por segundo.
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente. Utilice `--no-apply-immediately` (el valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento.

API de RDS

Para cambiar la configuración de IOPS aprovisionadas de una instancia de base de datos, utilice la operación de la API de Amazon RDS `ModifyDBInstance`. Establezca los siguientes parámetros:

- `StorageType`: establézcalo en `io1` o `io2` para IOPS aprovisionadas.
- `AllocatedStorage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `Iops`: nueva tasa de IOPS para la instancia de base de datos, expresada en operaciones de E/S por segundo.
- `ApplyImmediately`: establezca esta opción en `True` para aplicar los cambios inmediatamente. Establezca esta opción en `False` (el valor predeterminado) para aplicar los cambios durante el siguiente período de mantenimiento.

Modificaciones en el almacenamiento con uso intensivo de E/S

Las instancias de base de datos de Amazon RDS usan volúmenes de Amazon Elastic Block Store (EBS) para el almacenamiento de registros. En función de la cantidad de almacenamiento solicitada, RDS (excepto RDS para SQL Server) realiza automáticamente una división en franjas entre varios volúmenes de Amazon EBS para mejorar el rendimiento. Las instancias de base de datos de RDS con tipos de almacenamiento SSD están respaldadas por uno o cuatro volúmenes de Amazon EBS divididos en franjas en una configuración RAID 0. Por diseño, las operaciones de modificación del almacenamiento de una instancia de base de datos de RDS tienen un impacto mínimo en las operaciones de la base de datos.

En la mayoría de los casos, las modificaciones de escalado del almacenamiento se descargan por completo en la capa de Amazon EBS y son transparentes para la base de datos. Este proceso suele completarse en unos pocos minutos. Sin embargo, algunos volúmenes de almacenamiento RDS más antiguos requieren un proceso diferente para modificar el tamaño, las IOPS aprovisionadas o el tipo

de almacenamiento. Esto implica hacer una copia completa de los datos mediante una operación que potencialmente hace un uso intensivo de E/S.

La modificación del almacenamiento utiliza una operación que hace un uso intensivo de E/S si se aplica alguno de los siguientes factores:

- El tipo de almacenamiento de origen es magnético. El almacenamiento magnético no admite la modificación del volumen elástico.
- La instancia de base de datos de RDS no se encuentra en un diseño de Amazon EBS de uno o cuatro volúmenes. Puede ver el número de volúmenes de Amazon EBS en uso en sus instancias de base de datos de RDS mediante las métricas de monitorización mejorada. Para obtener más información, consulte Visualización de métricas OS en la consola de RDS.
- El tamaño objetivo de la solicitud de modificación aumenta el almacenamiento asignado por encima de 400 GiB para instancias de RDS para MariaDB, MySQL y PostgreSQL, y 200 GiB para RDS para Oracle. Las operaciones de escalado automático del almacenamiento tienen el mismo efecto cuando aumentan el tamaño de almacenamiento asignado de la instancia de base de datos por encima de estos umbrales.

Si la modificación del almacenamiento implica una operación que hace un uso intensivo de E/S, consume recursos de E/S y aumenta la carga de la instancia de base de datos. Las modificaciones del almacenamiento con operaciones que hacen un uso intensivo de E/S que implican el almacenamiento de SSD de uso general (gp2) pueden agotar el saldo de créditos de E/S, lo que puede aumentar los tiempos de conversión.

Como práctica recomendada, recomendamos programar estas solicitudes de modificación de almacenamiento fuera de las horas pico para ayudar a reducir el tiempo necesario para completar la operación de modificación del almacenamiento. De forma alternativa, puede crear una réplica de lectura de la instancia de base de datos y realizar la modificación del almacenamiento en la réplica de lectura. Esto hará que la réplica se convierta en la instancia de base de datos principal. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Para obtener más información, consulte Why is an Amazon RDS DB instance stuck in the modifying state when I try to increase the allocated storage? (¿Por qué una instancia de base de datos de Amazon RDS se queda atascada en el estado de modificación cuando intento aumentar el almacenamiento asignado?)

Modificación de la configuración del almacenamiento SDD de uso general (gp3)

Puede modificar la configuración de una instancia de base de datos que utiliza el almacenamiento de SSD de uso general (gp3) mediante la consola de Amazon RDS, la AWS CLI o la API de Amazon RDS. Especifique el tipo de almacenamiento, el almacenamiento asignado, la cantidad de IOPS aprovisionadas y el rendimiento de almacenamiento que necesita.

Aunque puede reducir la cantidad de IOPS aprovisionadas y el rendimiento de almacenamiento para su instancia de base de datos, no puede reducir el tamaño de almacenamiento.

En la mayoría de los casos, no es necesario interrumpir el aumento del almacenamiento. Después de modificar el tamaño de IOPS de almacenamiento para una instancia de base de datos, el estado de la instancia de base de datos es storage-optimization (optimización del almacenamiento). Puede esperar latencias elevadas, pero dentro del rango de milisegundos de un solo dígito, durante la optimización del almacenamiento. La instancia de base de datos es totalmente operativa después de una modificación de almacenamiento.

> **Note**
>
> No puede hacer modificaciones de almacenamiento adicionales hasta seis (6) horas después de que se haya completado la optimización de almacenamiento en la instancia.

Para obtener información sobre los rangos de almacenamiento asignado, las IOPS aprovisionadas y el rendimiento de almacenamiento disponibles para cada motor de base de datos, consulte Almacenamiento gp3 (recomendado).

Consola

Para cambiar la configuración de rendimiento de almacenamiento para una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

Para filtrar la lista de instancias de base de datos, en Filter databases (Filtrar bases de datos), escriba una cadena de texto para que Amazon RDS la utilice para filtrar los resultados. Solo aparecen instancias de base de datos cuyos nombres contengan la cadena.

3. Elija la instancia de bases de datos con almacenamiento gp3 que desea modificar.
4. Elija Modificar.
5. En la página Modificar instancia de base de datos, elija SSD de uso general (gp3) para Tipo de almacenamiento y haga lo siguiente:

   a. Elija un valor para Provisioned IOPS (IOPS aprovisionadas).

      Si el valor que especifica para Allocated storage (Almacenamiento asignado) o Provisioned IOPS (IOPS provisionadas) está fuera de los límites admitidos por el otro parámetro, aparece un mensaje de advertencia. Este mensaje indica el intervalo de valores necesario para el otro parámetro.

   b. Elija un valor para Storage throughput (Rendimiento de almacenamiento).

      Si el valor que especifica para Storage throughput (Rendimiento de almacenamiento) o Provisioned IOPS (IOPS provisionadas) está fuera de los límites admitidos por el otro parámetro, aparece un mensaje de advertencia. Este mensaje indica el intervalo de valores necesario para el otro parámetro.

6. Elija Continue.
7. Para aplicar los cambios a la instancia de base de datos inmediatamente, seleccione Apply Immediately (Aplicar inmediatamente) en la sección Scheduling of modifications (Programación de modificaciones). También puede elegir Apply during the next scheduled maintenance window (Aplicar durante la próxima ventana de mantenimiento programada) para aplicar los cambios durante el próximo período de mantenimiento.
8. Revise los parámetros que se cambiarán y elija Modify DB Instance (Modificar instancia de base de datos) para completar la modificación.

   El valor nuevo para IOPS aprovisionadas aparece en la columna Status (Estado).

AWS CLI

Para cambiar la configuración de rendimiento de almacenamiento para una instancia de base de datos, utilice el comando AWS CLI de la `modify-db-instance`. Establezca los siguientes parámetros:

- `--storage-type`: establezca `gp3` para SSD de uso general (gp3).
- `--allocated-storage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `--iops`: nueva cantidad de IOPS aprovisionadas para la instancia de base de datos, expresada en operaciones de E/S por segundo.
- `--storage-throughput`: nuevo rendimiento de almacenamiento para la instancia de base de datos, expresada en MiBps.
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente. Utilice `--no-apply-immediately` (el valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento.

API de RDS

Para cambiar la configuración de rendimiento de almacenamiento de una instancia de base de datos, utilice la operación `ModifyDBInstance` de la API de Amazon RDS. Establezca los siguientes parámetros:

- `StorageType`: establezca `gp3` para SSD de uso general (gp3).
- `AllocatedStorage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `Iops`: nueva tasa de IOPS para la instancia de base de datos, expresada en operaciones de E/S por segundo.
- `StorageThroughput`: nuevo rendimiento de almacenamiento para la instancia de base de datos, expresada en MiBps.
- `ApplyImmediately`: establezca esta opción en `True` para aplicar los cambios inmediatamente. Establezca esta opción en `False` (el valor predeterminado) para aplicar los cambios durante el siguiente período de mantenimiento.

Uso de un volumen de registro específico (DLV)

Puede utilizar un volumen de registro específico (DLV) para una instancia de base de datos que utilice el almacenamiento de IOPS aprovisionadas (PIOPS). Un DLV transporta los registros de transacciones de la base de datos de PostgreSQL y los registros redo y registros binarios de MySQL/MariaDB a un volumen de almacenamiento independiente del volumen que contiene las tablas

de la base de datos. Un DLV hace que el registro de escritura de transacciones sea más eficiente y uniforme. Los DLV son ideales para bases de datos con gran capacidad de almacenamiento asignado, requisitos elevados de E/S por segundo (IOPS) o cargas de trabajo donde la latencia es muy importante.

Los DLV son compatibles con el almacenamiento PIOPS (io1 y io2 Block Express) y se crean con un tamaño fijo de 1024 GiB y 3000 IOPS aprovisionadas.

Amazon RDS es compatible con los DLV en todas las Regiones de AWS para las siguientes versiones:

- MariaDB 10.6.7 y versiones 10 superiores
- MySQL versión 8.0.28 y posteriores a la 8.0, MySQL versión 8.4.3 y posteriores a la 8.4
- PostgreSQL 13.10 y versiones 13 superiores, 14.7 y versiones 14 superiores y 15.2 y versiones 15 superiores

RDS es compatible con DLV con implementaciones Multi-AZ Al modificar o crear una instancia multi-AZ, se crea un DLV tanto para la instancia principal como para la secundaria.

RDS admite DLV con réplicas de lectura. Si la instancia de base de datos principal tiene un DLV habilitado, todas las réplicas de lectura creadas después de habilitar el DLV también tendrán un DLV. Las réplicas de lectura creadas antes del cambio a DLV no la tendrán habilitada, a menos que se modifiquen explícitamente para ello. Es recomendable que todas las réplicas de lectura conectadas a una instancia principal antes de activar el DLV también se modifiquen manualmente para que tengan un DLV.

> **Note**
>
> Es recomendable emplear volúmenes de registro específicos para configuraciones de bases de datos de 5 TiB o más.

Para obtener más información sobre las ventajas de los DLV, consulte las siguientes entradas del blog:

- Mejore el rendimiento de las bases de datos con los volúmenes de registro dedicados de Amazon RDS
- Compare Amazon RDS para PostgreSQL con volúmenes de registro dedicados

- Maximizar el rendimiento de AWS RDS para MySQL con volúmenes de registro dedicados en la documentación de Percona

Para obtener información sobre los rangos de almacenamiento asignado, las IOPS aprovisionadas y el rendimiento de almacenamiento disponibles para cada motor de base de datos, consulte Almacenamiento de SSD de IOPS aprovisionadas.

Temas

- Observaciones sobre la activación o desactivación del DLV
- Habilitación de DLV al crear una instancia de base de datos
- Habilitación de DLV en una instancia de base de datos existente
- Supervisión del almacenamiento del DLV

Observaciones sobre la activación o desactivación del DLV

La activación y desactivación del DLV puede llevar mucho tiempo y provocar tiempos de inactividad. El proceso consiste en copiar todos los registros de transacciones, o los registros binarios y REDO (en función del motor de base de datos), en el nuevo volumen al activarlo, o bien en devolverlo al almacenamiento original al desactivarlo. La duración de esta operación depende de varios factores:

- Número de registros de transacciones:
  - Las bases de datos más grandes y con más transacciones generan más registros, lo que aumenta el tiempo necesario para copiarlos.
  - Los registros de transacciones se pueden acumular en la instancia de base de datos principal si las ranuras de replicación están inactivas o si la replicación está retrasada, lo que aumenta el tiempo necesario para realizar la copia. Asegúrese de que la replicación esté actualizada y elimine las ranuras innecesarias.
- Configuración de almacenamiento:
  - Ancho de banda de EBS de la instancia de base de datos: un mayor ancho de banda permite una transferencia de datos más rápida.
  - Número de IOPS aprovisionadas: un mayor número de operaciones de entrada/salida por segundo (IOPS) puede acelerar el proceso de copia.
- Actividad de la base de datos: los niveles altos de actividad de la base de datos durante la configuración pueden ralentizar el proceso.

Para minimizar el tiempo de inactividad, le recomendamos que planifique y programe los periodos de baja actividad o de mantenimiento.

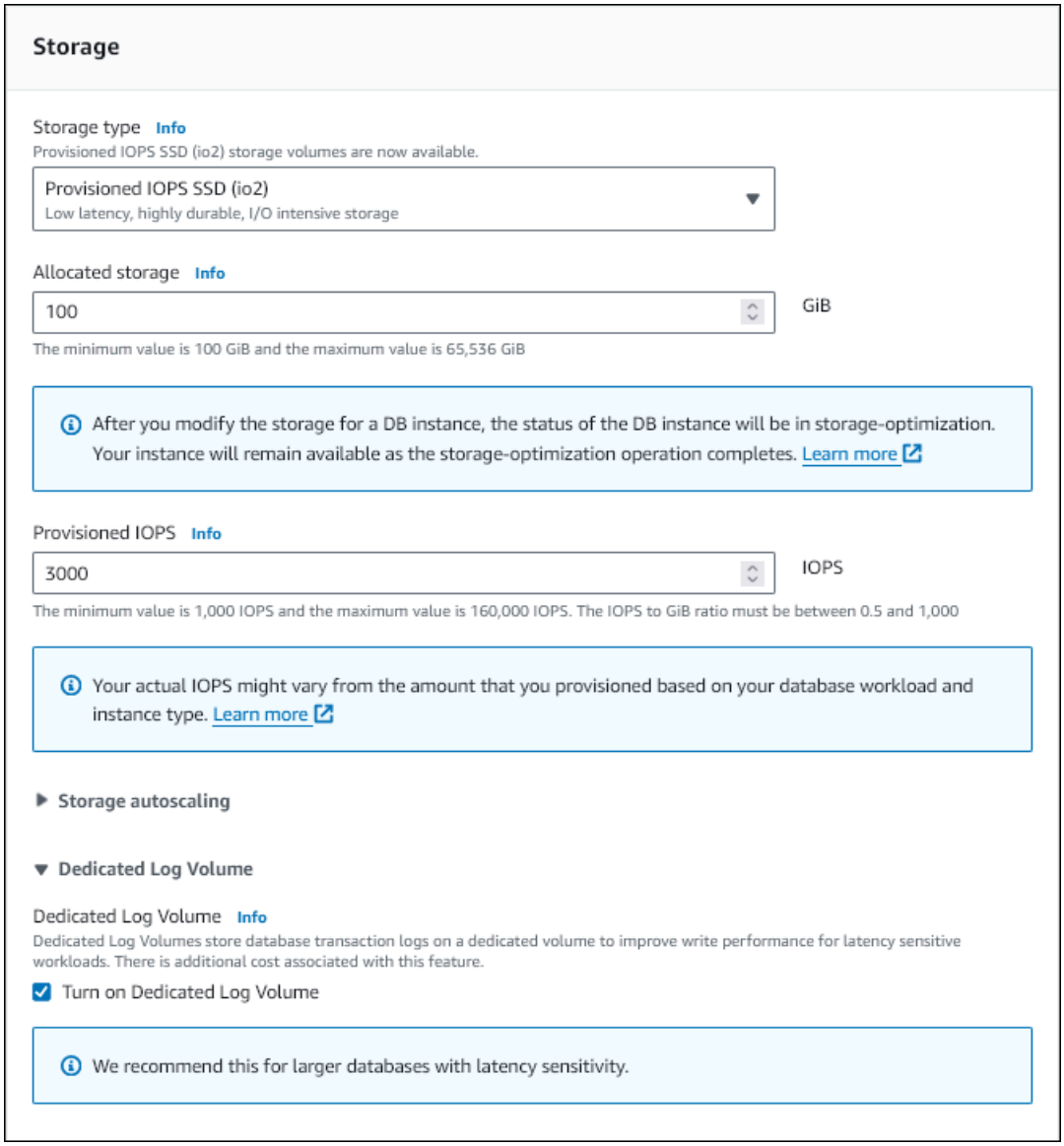
Habilitación de DLV al crear una instancia de base de datos

Puede usar la AWS Management Console, la AWS CLI o la API de RDS para crear una instancia de base de datos con DLV habilitado.

Consola

Habilitación de DLV en una nueva instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Create database (Crear base de datos).
3. En la página Crear instancia de base de datos, elija un motor de base de datos compatible con DLV.
4. En Almacenamiento:
    a. Elija entre SSD de IOPS aprovisionadas (io1) o SSD de IOPS aprovisionadas (io2).
    b. Introduzca el Almacenamiento asignado y las IOPS aprovisionadas que desee.
    c. Expanda Volumen de registro dedicado y seleccione Activar el volumen de registro dedicado.



5. Seleccione el resto de ajustes según sea necesario.
6. Elija Creación de base de datos.

Una vez creada la base de datos, el valor del volumen de registro dedicado aparece en la pestaña Configuración de la página de detalles de la base de datos.

CLI

Para habilitar DLV cuando cree una instancia de base de datos mediante el almacenamiento de IOPS aprovisionadas, use el comando de la AWS CLI create-db-instance. Establezca los siguientes parámetros:

- `--dedicated-log-volume`: habilita un volumen de registro específico.
- `--storage-type`: establézcalo en `io1` o `io2` para IOPS aprovisionadas.
- `--allocated-storage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `--iops`: nueva cantidad de IOPS aprovisionadas para la instancia de base de datos, expresada en operaciones de E/S por segundo.

API de RDS

Para habilitar DLV al crear una instancia de base de datos utilizando el almacenamiento de IOPS aprovisionadas, utilice la operación CreateDBInstance de la API de Amazon RDS. Establezca los siguientes parámetros:

- `DedicatedLogVolume`: se configura en `true` para habilitar un volumen de registro dedicado.
- `StorageType`: establézcalo en `io1` o `io2` para IOPS aprovisionadas.
- `AllocatedStorage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes.
- `Iops`: tasa de IOPS para la instancia de base de datos, expresada en operaciones de E/S por segundo.

Habilitación de DLV en una instancia de base de datos existente

Puede utilizar la AWS Management Console, la AWS CLI o la API de RDS para modificar una instancia de base de datos y habilitar DLV.

Una vez que haya modificado la configuración de DLV de una instancia de base de datos, debe reiniciar la instancia de base de datos.

Consola

Habilitación de DLV en una instancia de base de datos existente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

Para filtrar la lista de instancias de base de datos, en Filter databases (Filtrar bases de datos), escriba una cadena de texto para que Amazon RDS la utilice para filtrar los resultados. Solo aparecen instancias de base de datos cuyos nombres contengan la cadena.

3. Elija la instancia de base de datos con almacenamiento de IOPS aprovisionadas que desea modificar.
4. Elija Modificar.
5. En la página Modificar instancia de base de datos:
   - En Almacenamiento, expanda Volumen de registro dedicado y seleccione Activar el volumen de registro dedicado.
6. Elija Continuar.
7. Para aplicar los cambios inmediatamente a la instancia de base de datos, elija Aplicar inmediatamente. También puede elegir Apply during the next scheduled maintenance window (Aplicar durante la próxima ventana de mantenimiento programada) para aplicar los cambios durante el próximo período de mantenimiento.
8. Revise los parámetros que se cambiarán y elija Modify DB Instance (Modificar instancia de base de datos) para completar la modificación.

El nuevo valor del volumen de registro dedicado aparece en la pestaña Configuración de la página de detalles de la base de datos.

CLI

Para habilitar o deshabilitar el DLV en una instancia de base de datos existente mediante el almacenamiento de IOPS aprovisionadas, use el comando `modify-db-instance` de la AWS CLI. Establezca los siguientes parámetros:

- `--dedicated-log-volume`: habilita un volumen de registro dedicado.

  Utilice `--no-dedicated-log-volume` (predeterminado) para deshabilitar un volumen de registro dedicado.
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente.

  Utilice `--no-apply-immediately` (el valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento.

API de RDS

Para habilitar o deshabilitar el DLV en una instancia de base de datos existente mediante el almacenamiento de IOPS aprovisionadas, use la operación `ModifyDBInstance` de la API de Amazon RDS. Establezca los siguientes parámetros:

- `DedicatedLogVolume`: configure esta opción en `true` para habilitar un volumen de registro dedicado.

  Configure esta opción en `false` para deshabilitar un volumen de registro dedicado. Este es el valor predeterminado.
- `ApplyImmediately`: establezca esta opción en `True` para aplicar los cambios inmediatamente.

  Establezca esta opción en `False` (el valor predeterminado) para aplicar los cambios durante el siguiente período de mantenimiento.

Supervisión del almacenamiento del DLV

Puede supervisar el uso del almacenamiento del DLV con la métrica `FreeStorageSpaceLogVolume` en CloudWatch.

Puede utilizar la siguiente consulta de RDS para PostgreSQL a fin de encontrar el tamaño ocupado por los registros de transacciones:

```
SELECT pg_size_pretty(COALESCE(sum(size), 0)) AS total_wal_generated_size
FROM pg_catalog.pg_ls_waldir();
```

Si el DLV se queda sin espacio de almacenamiento, la instancia de base de datos entrará en el estado `storage-full`, lo que provocará un tiempo de inactividad.

Eliminación de una instancia de base de datos

Puede eliminar una instancia de base de datos mediante la consola de AWS Management Console, la AWS CLI o la API de RDS. Si quiere eliminar una instancia de base de datos de un clúster de base de datos de Aurora, consulte Eliminación de clústeres e instancias de base de datos de Aurora.

Temas

- Requisitos previos para eliminar una instancia de base de datos
- Consideraciones a la hora de eliminar una instancia de base de datos
- Eliminación de una instancia de base de datos

Requisitos previos para eliminar una instancia de base de datos

Antes de intentar eliminar la instancia de base de datos, asegúrese de que la protección contra eliminación esté desactivada. La protección contra eliminación está activada de forma predeterminada en las instancias de base de datos que se han creado con la consola.

Si la instancia de base de datos tiene activada la protección contra eliminación, puede desactivarla modificando la configuración de la instancia. Elija Modificar en la página de detalles de la base de datos o llame al comando modify-db-instance. Esta operación no produce una interrupción. Para obtener más información, consulte Configuración de instancias de base de datos.

Consideraciones a la hora de eliminar una instancia de base de datos

La eliminación de una instancia de base de datos afecta a la capacidad de recuperación de la instancia, la disponibilidad de las copias de seguridad y el estado de la réplica de lectura. Tenga en cuenta lo siguiente:

- Puede elegir si quiere crear una instantánea de base de datos final. Dispone de las opciones siguientes:
  - Si crea una instantánea final, se puede utilizar para restaurar la instancia de base de datos eliminada. RDS retiene tanto la instantánea final como cualquier instantánea manual que haya creado anteriormente. No puede crear una instantánea de base de datos final de la instancia de base de datos si no tiene el estado `Available` Para obtener más información, consulte Visualización del estado de la instancia de base de datos de en un clúster de Aurora.
  - Si no crea una instantánea final, la eliminación de la instancia es más rápida. La desventaja es que no existe una instantánea final que pueda restaurar posteriormente. Si decide restaurar la

instancia de base de datos eliminada, retenga las copias de seguridad automatizadas o utilice una instantánea manual anterior para restaurar la instancia de base de datos al momento en que se creó la instantánea anterior.

- Puede elegir si quiere retener las copias de seguridad automatizadas. Dispone de las opciones siguientes:
  - Si retiene las copias de seguridad automatizadas, RDS las conserva durante el período de retención establecido para la instancia de base de datos en el momento de eliminarla. Puede utilizar copias de seguridad automatizadas para restaurar la instancia de base de datos a un momento que esté incluido en el periodo de retención, pero no después de él. El periodo de retención establecido se aplica independientemente de si crea o no una instantánea de base de datos final. Para eliminar una copia de seguridad automatizada retenida, consulte Eliminación de las copias de seguridad automatizadas retenidas.
  - Las copias de seguridad automatizadas y las instantáneas manuales retenidas incurrirán en cargos de facturación hasta que se eliminen. Para obtener más información, consulte Costos de retención.
  - Si no retiene las copias de seguridad automatizadas, RDS elimina las que residen en la misma Región de AWS que la instancia de base de datos. Estas copias de seguridad no se pueden recuperar. Si sus copias de seguridad automatizadas se han replicado en otra Región de AWS, RDS las conserva aunque no haya elegido retenerlas. Para obtener más información, consulte Replicación de las copias de seguridad automatizadas en otra Región de AWS.

    > **Note**
    >
    > Normalmente, no es necesario retener las copias de seguridad automatizadas si crea una instantánea de base de datos final.

- Al eliminar la instancia de base de datos, RDS no elimina las instantáneas de base de datos manuales. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
- Si desea eliminar todos los recursos de RDS, tenga en cuenta que se cobra por los siguientes recursos:
  - Instancias de base de datos
  - Instantáneas de base de datos
  - Clústeres de base de datos

Si ha comprado instancias reservadas, se facturarán según el contrato que haya aceptado al comprar la instancia. Para obtener más información, consulte Instancias de base de datos reservadas para Amazon RDS. Puede obtener la información de facturación de todos sus recursos de AWS mediante AWS Cost Explorer. Para obtener más información, consulte Analyzing your costs with AWS Cost Explorer (Análisis de los costes con AWS Cost Explorer).

- Si elimina una instancia de base de datos que tenga réplicas de lectura en la misma Región de AWS, cada réplica de lectura se promocionará automáticamente a una instancia de base de datos independiente. Para obtener más información, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente. Si su instancia de base de datos tiene réplicas de lectura en diferentes Regiones de AWS, consulte Consideraciones relativas a la replicación entre regiones para obtener información relacionada con la eliminación de la instancia de base de datos de origen para una réplica de lectura entre regiones.
- Cuando el estado de una instancia de base de datos es `deleting`, su valor de certificado de entidad de certificación no aparece en la consola de RDS ni en la salida de comandos de la AWS CLI ni en las operaciones de la API de RDS. Para obtener más información acerca de los certificados de entidad de certificación, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
- El tiempo necesario para eliminar una instancia de base de datos varía en función del periodo de retención de copia de seguridad (es decir, cuántas copias de seguridad se eliminarán), la cantidad de datos que se eliminan y si se crea una instantánea final.

Eliminación de una instancia de base de datos

Puede eliminar una instancia de base de datos mediante la consola de AWS Management Console, la AWS CLI o la API de RDS. Debe hacer lo siguiente:

- Proporcione el nombre de la instancia de base de datos
- Habilitar o deshabilitar la opción de tomar una instantánea de base de datos final de la instancia
- Habilitar o deshabilitar la opción de conservar copias de seguridad automatizadas

> **Note**
>
> No se puede eliminar una instancia de base de datos si está activada la protección contra eliminación. Para obtener más información, consulte Requisitos previos para eliminar una instancia de base de datos.

Consola

Para eliminar una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee eliminar.
3. En Actions (Acciones), elija Delete (Eliminar).
4. Para crear una instantánea de base de datos final para la instancia de base de datos, elija Create final snapshot? (¿Crear una instantánea final?).
5. Si elige crear una instantánea final, introduzca el nombre de instantánea final.
6. Para conservar las copias de seguridad automatizadas, seleccione Retain automated backups (Conservar copias de seguridad automatizadas).
7. En el cuadro, escriba **`delete me`**.
8. Elija Eliminar (Delete).

AWS CLI

Para encontrar los ID de instancia de las instancias de base de datos de su cuenta, llame al comando describe-db-instances:

```
aws rds describe-db-instances --query 'DBInstances[*].[DBInstanceIdentifier]' --output
 text
```

Para eliminar una instancia de base de datos con la AWS CLI, llame al comando delete-db-instance con las siguientes opciones:

- `--db-instance-identifier`

- `--final-db-snapshot-identifier` o `--skip-final-snapshot`

Example Con una instantánea final y sin copias de seguridad automatizadas conservadas

Para Linux, macOS o:Unix

```
aws rds delete-db-instance \
    --db-instance-identifier mydbinstance \
    --final-db-snapshot-identifier mydbinstancefinalsnapshot \
    --delete-automated-backups
```

En:Windows

```
aws rds delete-db-instance ^
    --db-instance-identifier mydbinstance ^
    --final-db-snapshot-identifier mydbinstancefinalsnapshot ^
    --delete-automated-backups
```

Example Con copias de seguridad automatizadas conservadas y sin instantánea final

Para Linux, macOS o:Unix

```
aws rds delete-db-instance \
    --db-instance-identifier mydbinstance \
    --skip-final-snapshot \
    --no-delete-automated-backups
```

En:Windows

```
aws rds delete-db-instance ^
    --db-instance-identifier mydbinstance ^
    --skip-final-snapshot ^
    --no-delete-automated-backups
```

API de RDS

Para eliminar una instancia de base de datos con la API de Amazon RDS, llame a la operación `DeleteDBInstance` con los siguientes parámetros:

- `DBInstanceIdentifier`

- `FinalDBSnapshotIdentifier` o `SkipFinalSnapshot`

Tutorial: Administración de un entorno de instancias de base de datos de MySQL desde el desarrollo hasta la producción

Introducción

Un escenario habitual a la hora de administrar una instancia de base de datos de Amazon RDS implica la supervisión de su ciclo de vida, desde el desarrollo inicial hasta la implementación en producción. Este tutorial ofrece orientación para administrar las tareas clave, de modo que su base de datos funcione de forma óptima y se adapte a unas necesidades operativas en constante evolución. Además, describe las opciones para sincronizar los cambios realizados entre los entornos de desarrollo y producción a fin de garantizar la uniformidad y la fiabilidad.

Al completar estos pasos, aprenderá lo siguiente:

- Cómo realizar tareas específicas con instancias de base de datos de MySQL, como añadir y actualizar etiquetas de Amazon RDS, ampliar el almacenamiento, crear réplicas de lectura y eliminar recursos.
- Cómo sincronizar las actualizaciones de un entorno de producción a un entorno de desarrollo para realizar pruebas y validaciones exhaustivas.

Para completar este tutorial, lleve a cabo las siguientes tareas:

1. Cree una instancia de base de datos de MySQL.
2. Añada etiquetas de Amazon RDS para clasificar su instancia de base de datos como entorno de desarrollo.
3. Aumente la capacidad de almacenamiento de su instancia de base de datos para adaptarse al aumento de las cargas de trabajo.
4. Cree réplicas de lectura para mejorar la resiliencia y la disponibilidad de su instancia de base de datos.
5. Actualice etiquetas de Amazon RDS para clasificar su instancia de base de datos como entorno de producción.
6. Elimine la instancia de base de datos que ya no necesite para que no incurra en costos adicionales.
7. Próximos pasos: sincronice su instancia de desarrollo con la de producción para lograr uniformidad en todos los entornos

Requisitos previos

Antes de empezar, complete los pasos de las siguientes secciones:

- Cómo crear una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Adición de etiquetas para clasificar su instancia de base de datos como entorno de desarrollo

Para clasificar la instancia de base de datos como un entorno de desarrollo, añada una etiqueta Amazon RDS a la instancia que ha creado. Las etiquetas de Amazon RDS son pares clave-valor que usted define y asocia a su instancia de RDS. Etiquetar los recursos de AWS contribuye a distinguir entre los recursos de AWS de desarrollo y los de producción. Para obtener más información acerca de las etiquetas de Amazon RDS, consulte Etiquetado de los recursos de y Amazon RDS.

1. En la consola de Amazon RDS, seleccione Databases (Bases de datos).
2. Seleccione la instancia de base de datos que desea etiquetar.
3. En la sección de detalles, desplácese hasta la sección Etiquetas.
4. Elija Administrar etiquetas y seleccione Agregar nueva etiqueta.
5. Escriba un valor para Tag key (Clave de etiqueta) y Value (Valor). Por ejemplo, puede usar la etiqueta key environment con el valor dev para especificar que la instancia de base de datos forma parte del entorno de desarrollo.
6. Seleccione Agregar nueva etiqueta y Guardar cambios.

Su instancia de base de datos está ahora etiquetada como entorno de desarrollo. Esto hace que sea más fácil identificar la instancia de base de datos y administrar costos asociados a este recurso.

Aumente la capacidad de almacenamiento de una instancia de base de datos para adaptarse a las crecientes necesidades de datos

A continuación, modifique la capacidad de almacenamiento de la instancia de base de datos de MySQL para alojar datos adicionales. Al principio, la capacidad de almacenamiento de la instancia de base de datos está configurada para satisfacer las necesidades inmediatas de la aplicación. Sin embargo, a medida que aumentan los volúmenes de datos, quizá sea necesario ajustar la

configuración de almacenamiento para garantizar el rendimiento y la estabilidad de la base de datos a largo plazo. Este proceso implica aumentar el almacenamiento asignado a la instancia de base de datos. Para obtener más información sobre cómo modificar la capacidad de almacenamiento de la instancia de base de datos, consulte Uso de almacenamiento para instancias de base de datos de Amazon RDS.

1. En la consola de Amazon RDS, seleccione Databases (Bases de datos).
2. Seleccione la instancia de base de datos que desea modificar.
3. Elija Modificar.
4. En Almacenamiento, aumente el almacenamiento asignado. El valor de almacenamiento modificado debe ser mayor que el actual.
5. Elija Continuar.
6. En Programación de modificaciones, puede seleccionar Aplicar inmediatamente, para aplicar los cambios de almacenamiento a la instancia de base de datos de forma inmediata, o bien Aplicar durante el siguiente período de mantenimiento programado, para aplicar los cambios durante el siguiente período de mantenimiento.
7. Cuando los ajustes sean los deseados, elija Modify DB instance (Modificar instancia de base de datos).

Ahora, la capacidad de almacenamiento de su instancia de base de datos habrá aumentado. Esto le permite administrar con eficacia volúmenes de datos más grandes y garantiza un nivel constante de rendimiento y estabilidad a medida que aumentan las necesidades de datos de su aplicación.

Creación de réplicas de lectura para mejorar la resiliencia y la disponibilidad de su instancia de base de datos

Cree una réplica de lectura para la instancia de base de datos de MySQL. Las réplicas de lectura mejoran la resiliencia y la disponibilidad de su instancia de base de datos. Para reducir el tráfico de lectura en la instancia de base de datos principal, cree una réplica de lectura de la instancia de base de datos. Esto redirige las consultas a la réplica de lectura, lo que puede ayudar a distribuir la carga y mejorar el rendimiento general de la base de datos. Para obtener más información sobre las réplicas de lectura de instancias de base de datos, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Para que una instancia de base de datos de MySQL pueda servir como origen para la replicación, debe habilitar las copias de seguridad automáticas en la instancia de base de datos de origen. Para

ello, debe establecer el período de retención de copia de seguridad en un valor distinto de 0. Para obtener más información acerca de las réplicas de lectura de MySQL, consulte Uso de réplicas de lectura de MySQL.

1. En la consola de Amazon RDS, seleccione Databases (Bases de datos).
2. Seleccione la instancia de base de datos que desea usar como origen para la réplica de lectura.
3. En Acciones, elija Crear réplica de lectura.
4. En Identificador de instancias de bases de datos, escriba un nombre para la réplica de lectura en letras minúsculas.
5. Elija la configuración de la instancia. Es recomendable usar la misma clase de instancia de base de datos y el mismo tipo de almacenamiento o mayores que la instancia de base de datos de origen para la réplica de lectura.
6. Para la Región de AWS, especifique la región de destino de la réplica de lectura.
7. Deje la configuración predeterminada o modifíquela según sea necesario.
8. Elija Create read replica (Crear réplica de lectura).

La réplica de lectura aparece debajo de la instancia de base de datos de origen, en la página Bases de datos de la consola de RDS. Muestra Réplica en la columna Rol.

Actualización de etiquetas para clasificar su instancia de base de datos como entorno de producción.

Cuando la instancia de base de datos esté lista para pasar de la fase de desarrollo a la de producción, es importante actualizar sus etiquetas para reflejar la transición. Para alinear su instancia de base de datos con sus estrategias operativas y de supervisión, actualice las etiquetas iniciales para indicar que la instancia de base de datos ahora forma parte del entorno de producción. Esto garantiza una mejor visibilidad y administración de la base de datos.

1. En la consola de Amazon RDS, seleccione Databases (Bases de datos).
2. Elija la instancia de base de datos que desea actualizar.
3. En la sección de detalles, desplácese hasta la sección Etiquetas.
4. Seleccione Administrar etiquetas.
5. Elimine la etiqueta inicial, que indica un entorno de desarrollo.
6. Seleccione Agregar nueva etiqueta.

7. Escriba un valor nuevo para Clave de etiqueta y Valor. Por ejemplo, puede usar la etiqueta key environment con el valor prod para especificar que la instancia de base de datos forma parte del entorno de producción.
8. Seleccione Agregar nueva etiqueta y Guardar cambios.

La etiqueta de la instancia de base de datos se actualiza para indicar la transición de la base de datos a un entorno de producción.

Eliminación de una instancia de base de datos cuando ya no se necesite para evitar incurrir en costos adicionales

Antes de finalizar este tutorial, es fundamental abordar la administración de sus recursos. Si tiene algún recurso que ya no necesite, debe eliminarlo para evitar incurrir en costos adicionales y optimizar su entorno de nube.

1. En la consola de Amazon RDS, seleccione Databases (Bases de datos).
2. Elija la instancia de base de datos que desea eliminar
3. En Acciones, seleccione Eliminar. Al eliminar una instancia de base de datos, se eliminará permanentemente la instancia, con todo su contenido y los recursos relacionados.
4. Confirme la eliminación de la instancia de base de datos y seleccione Eliminar.

También puede seguir administrando la instancia de base de datos como parte de su entorno de producción si decide mantenerla para usarla en el futuro. Esto implica mantener un entorno de desarrollo sincronizado para lograr un nivel exhaustivo de pruebas y validación. Para obtener más información, consulte Próximos pasos: sincronice su instancia de desarrollo con la de producción para lograr uniformidad en todos los entornos.

Próximos pasos: sincronice su instancia de desarrollo con la de producción para lograr uniformidad en todos los entornos

Creación de un entorno de desarrollo

Para administrar un entorno de producción, es importante mantener un entorno de desarrollo sincronizado para realizar pruebas y validaciones exhaustivas. Para crear un nuevo entorno de desarrollo, cree primero una instantánea de base de datos de la instancia de base de datos de producción actual. Una instantánea de base de datos captura toda la instancia de base de datos mediante la creación de una instantánea del volumen de almacenamiento. Para obtener

instrucciones sobre cómo crear una instantánea de base de datos en la consola de Amazon RDS, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Tras crear la instantánea de base de datos de su entorno de producción, cree una nueva instancia de base de datos para su entorno de desarrollo restaurando una instantánea de base de datos. Las instancias de base de datos restauradas se asocian automáticamente con los grupos de opciones y parámetros de base de datos predeterminados. Sin embargo, puede aplicar un grupo de parámetros y opciones personalizados especificándolos durante una restauración. Para obtener instrucciones sobre la restauración de una instantánea de base de datos, consulte Tutorial: restauración de una instancia de base de datos de Amazon RDS a partir de una instantánea de base de datos.

Por último, designe la nueva instancia de base de datos como su nuevo entorno de desarrollo actualizando sus etiquetas de Amazon RDS. Para obtener información sobre cómo actualizar las etiquetas de Amazon RDS para reflejar este cambio, consulte la sección Actualización de etiquetas para clasificar su instancia de base de datos como entorno de producción. anterior.

Ahora dispone de un nuevo entorno de desarrollo que refleja la configuración de la base de datos de su entorno de producción.

Sincronización de un entorno de desarrollo con un entorno de producción

Tras establecer el nuevo entorno de desarrollo, es necesario mantenerlo sincronizado con cualquier cambio que se produzca en el entorno de producción. Esto garantiza que el entorno de desarrollo refleje con precisión el estado actual de la producción, algo esencial para que las pruebas, la validación y la resolución de problemas sean eficaces. Amazon RDS ofrece diversas formas de mantener el entorno de desarrollo actualizado con el entorno de producción. Para obtener más información sobre estas opciones, consulte Orchestrating database refreshes for Amazon RDS and Amazon Aurora.

Una de las principales formas de sincronizar los entornos de desarrollo y producción es crear y restaurar instantáneas de bases de datos. Una instantánea de base de datos le permite crear un entorno de desarrollo que refleje la configuración de base de datos del entorno de producción durante el momento en el que se creó la instantánea. Para obtener más información sobre las instantáneas de bases de datos, consulte Administración de copias de seguridad manuales. Para obtener más información sobre la restauración de una instancia de base de datos, consulte Restauración a una instancia de base de datos.

Las instantáneas de bases de datos son especialmente valiosas para los siguientes casos de uso.

- Configuración inicial de un entorno de desarrollo: las instantáneas de bases de datos son útiles para crear el entorno de desarrollo inicial para las pruebas, ya que proporcionan una referencia uniforme que refleja el estado exacto del entorno de producción en el momento de la instantánea.
- Aplicaciones de alto tráfico: en entornos de producción donde el funcionamiento continuo es fundamental, el uso de implementaciones multi-AZ para las instantáneas evita la suspensión de las E/S en la base de datos principal, lo que garantiza un rendimiento ininterrumpido y una alta disponibilidad.
- Compartir datos entre distintas cuentas de RDS: las instantáneas de bases de datos se pueden compartir entre distintas Cuentas de AWS, lo que facilita la transferencia de datos entre cuentas o regiones. Esto resulta útil para proyectos colaborativos o escenarios en los que los datos deban compartirse con diversos fines. Para obtener más información, consulte Uso compartido de una instantánea manual de base de datos de Amazon RDS.

En este tutorial, hemos analizado las tareas esenciales para administrar una instancia de base de datos a lo largo del ciclo de vida. Ha visto cómo crear una instancia de base de datos, añadir y actualizar etiquetas de Amazon RDS, ampliar el almacenamiento y crear réplicas de lectura. También hemos visto formas de aprovechar estas operaciones fundamentales y de administrar su entorno de producción eficazmente. Esto incluye establecer un entorno de desarrollo para las pruebas y sincronizarlo con el entorno de producción a fin de garantizar la uniformidad. Estas tareas contribuyen a mantener una infraestructura de base de datos flexible y escalable, lo que garantiza que su entorno de Amazon RDS funcione de manera eficiente.

Configuración y administración de una implementación multi-AZ para Amazon RDS

Las implementaciones Multi-AZ pueden tener una o dos instancias de base de datos en espera. Cuando la implementación tiene una instancia de base de datos en espera, se denomina implementación de instancia de base de datos Multi-AZ. Una implementación de instancia de base de datos Multi-AZ tiene una instancia de base de datos en espera que proporciona compatibilidad con la conmutación por error, pero no sirve tráfico de lectura. Cuando la implementación tiene dos instancias de base de datos en espera, se denomina implementación de clúster de base de datos Multi-AZ. La implementación de un clúster de base de datos Multi-AZ tiene instancias de base de datos en espera que proporcionan compatibilidad con la conmutación por error y también pueden servir tráfico de lectura.

Puede utilizar la AWS Management Console para determinar si una implementación Multi-AZ es una implementación de instancia de base de datos Multi-AZ o una implementación de clúster de base de datos Multi-AZ. En el panel de navegación, elija Databases (Bases de datos) y luego, elija un DB identifier (Identificador de base de datos).

- Una implementación de instancia de base de datos Multi-AZ tiene las siguientes características:
  - Solo hay una fila para la instancia de base de datos.
  - El valor de Role (Rol) es Instance (Instancia) o Primary (Principal).
  - El valor de Multi-AZ es Yes (Sí).
- Una implementación de clúster de base de datos Multi-AZ tiene las siguientes características:
  - Hay una fila de nivel de clúster con tres filas de instancias de base de datos debajo.
  - Para la fila de nivel de clúster, el valor de Role (Rol) es Multi-AZ DB cluster (Clúster de base de datos Multi-AZ).
  - Para cada fila de nivel de instancia, el valor de Role (Rol) es Writer instance (Instancia de escritor) o Reader instance (Instancia de lector).
  - Para cada fila de nivel de instancia, el valor de Multi-AZ es 3 Zones (3 zonas).

Temas

- Habilitación de implementaciones de instancias de bases de datos multi-AZ para Amazon RDS
- Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS

Además, los siguientes temas se aplican tanto a las instancias de base de datos como a los clústeres de bases de datos multi-AZ.

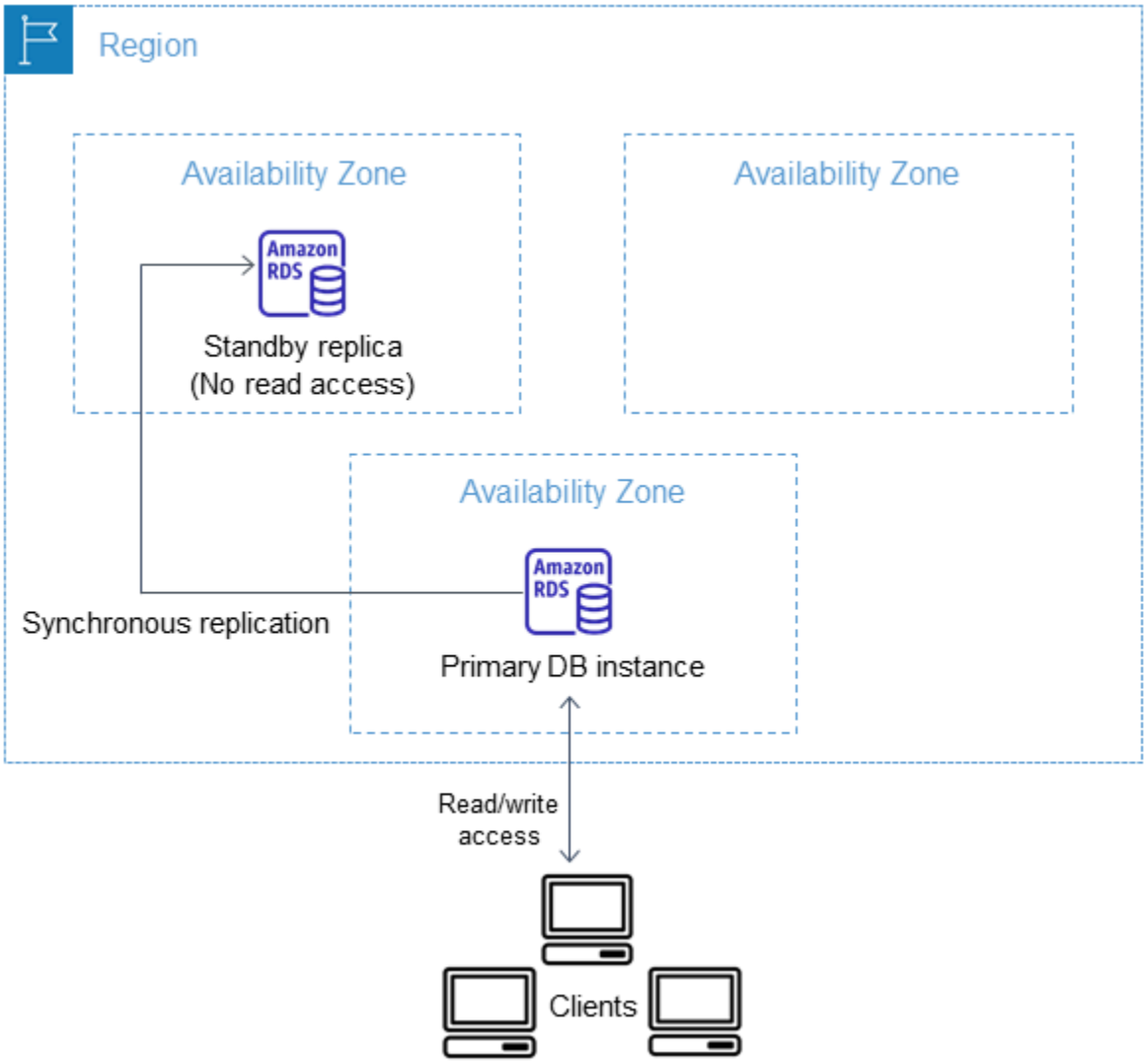
- the section called “Etiquetado de los recursos de RDS”
- the section called “ARN en Amazon RDS”
- the section called “Uso de almacenamiento”
- the section called “Mantenimiento de una instancia de base de datos”
- the section called “Actualización de la versión del motor”

Habilitación de implementaciones de instancias de bases de datos multi-AZ para Amazon RDS

Amazon RDS proporciona alta disponibilidad y compatibilidad con la conmutación por error para las instancias de base de datos mediante implementaciones Multi-AZ con una instancia de base de datos única en espera. Este tipo de implementación se denomina Implementación de instancia de base de datos Multi-AZ. Amazon RDS usa varias tecnologías diferentes para proporcionar esta compatibilidad con la conmutación por error. Las implementaciones multi-AZ de instancias de base de datos de MariaDB, MySQL, Oracle, PostgreSQL y RDS Custom para SQL Server usan la tecnología de conmutación por error de Amazon. Las instancias de base de datos de Microsoft SQL Server utilizan la creación de reflejo de la base de datos (DMB) o grupos de disponibilidad (AG) Always On de SQL Server. Para obtener información sobre la compatibilidad con la versión de SQL Server para multi-AZ, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server. Para obtener información sobre el uso de RDS Custom para SQL Server para multi-AZ, consulte Administración de una implementación multi-AZ de RDS Custom para SQL Server.

En una implementación de instancia de base de datos Multi-AZ, Amazon RDS aprovisiona y mantiene automáticamente una réplica síncrona en espera dentro de una zona de disponibilidad diferente. La instancia de base de datos principal se replica de forma síncrona en distintas zonas de disponibilidad en una réplica en espera para proporcionar redundancia de datos y minimizar los picos de latencia durante las copias de seguridad del sistema. La ejecución de una instancia de base de datos con alta disponibilidad puede mejorar la disponibilidad durante el mantenimiento de sistema planificado. También ayuda a proteger las bases de datos contra los errores de las instancias de base de datos y las interrupciones de las zonas de disponibilidad. Para obtener más información acerca de las zonas de disponibilidad, consulte Regiones, zonas de disponibilidad y Local Zones.

> **Note**
>
> La opción de alta disponibilidad no es una solución de escalado para escenarios de solo lectura. No puede usar una réplica en espera para servir tráfico de lectura. Para servir tráfico de solo lectura, utilice un clúster de base de datos Multi-AZ o una réplica de lectura en su lugar. Para obtener más información acerca de los clústeres de base de datos Multi-AZ, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS. Para obtener más información acerca de las réplicas de lectura, consulte Trabajo con réplicas de lectura de instancias de base de datos.



Con la consola de RDS, puede crear una implementación de instancia de base de datos Multi-AZ si especifica la opción Multi-AZ al crear una instancia de base de datos. Puede usar la consola para convertir las instancias de base de datos existentes en implementaciones de instancia de base de datos Multi-AZ mediante la modificación de la instancia de base de datos y la especificación de la opción Multi-AZ. También puede especificar una implementación de instancia de base de datos Multi-AZ con la AWS CLI o la API de Amazon RDS. Utilice el comando de la CLI create-db-instance o modify-db-instance o la operación de la API CreateDBInstance o ModifyDBInstance.

La consola de RDS muestra la zona de disponibilidad de la réplica en espera (denominada zona de disponibilidad secundaria). También puede utilizar el comando de la CLI describe-db-instances o la operación de la API DescribeDBInstances para buscar la AZ secundaria.

Las instancias de base de datos que usan implementaciones de bases de datos Multi-AZ pueden tener una latencia de escritura y confirmación superior a la de una implementación Single-AZ. Esto

puede ocurrir debido a la replicación de datos síncrona que se produce. Puede detectar un cambio en la latencia si la implementación conmuta a la réplica en espera, aunque AWS se ha diseñado con una conectividad de red de baja latencia entre zonas de disponibilidad. Para cargas de trabajo de producción, recomendamos que utilice IOPS aprovisionadas (operaciones de entrada/salida por segundo) para un rendimiento rápido y consistente. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

Conversión de una instancia de base de datos en una implementación multi-AZ para Amazon RDS

La modificación de una instancia de base de datos en una implementación multi-AZ mejora la disponibilidad al añadir una instancia en espera en otra zona de disponibilidad. El proceso implica un tiempo de inactividad mínimo y requiere una planificación cuidadosa en función de cómo afecte al almacenamiento y al rendimiento. Este cambio mejora la tolerancia a errores y reduce el tiempo de recuperación en caso de errores, lo que lo hace ideal para entornos de alta disponibilidad.

Si tiene una instancia de base de datos en una implementación single-AZ y la modifica para convertirla en una implementación de instancia de base de datos multi-AZ, Amazon RDS realiza las siguientes acciones:

1. Toma una instantánea de los volúmenes de Amazon Elastic Block Store (EBS) de la instancia de base de datos principal.
2. Crea nuevos volúmenes para la réplica en espera a partir de la instantánea. Estos volúmenes se inicializan en segundo plano y se alcanza el máximo rendimiento del volumen cuando los datos se han inicializado por completo.
3. Activa la replicación sincrónica a nivel de bloque entre los volúmenes de las réplicas principal y en espera.

> **Important**
>
> La creación de una instancia de base de datos en espera a partir de una instantánea durante una conversión de single-AZ a multi-AZ evita el tiempo de inactividad, pero podría afectar al rendimiento, especialmente en el caso de las cargas de trabajo que distinguen la escritura. La replicación sincrónica puede aumentar la latencia de E/S y afectar al rendimiento de la base de datos. Como práctica recomendada, evite convertir una instancia de base de datos de producción en una instancia de base de datos multi-AZ.

En cambio, cree una réplica de lectura, habilite copias de seguridad en ella, conviértala en multi-AZ, cargue los datos en sus volúmenes y, a continuación, promociónela a la instancia de base de datos principal. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Una instancia de base de datos se puede modificar de dos maneras para convertirla en una implementación de base de datos Multi-AZ:

Temas

- Convertirla en una implementación de instancia de base de datos Multi-AZ con la consola de RDS
- Modificación de una instancia de base de datos para convertirla en una implementación de base de datos Multi-AZ

Convertirla en una implementación de instancia de base de datos Multi-AZ con la consola de RDS

Puede utilizar la consola de RDS para convertir una instancia de base de datos en una implementación de instancia de base de datos multi-AZ.

Solo puede utilizar la consola para utilizar para completar la conversión. Para usar la AWS CLI o la API de RDS, siga las instrucciones que se indican en Modificación de una instancia de base de datos para convertirla en una implementación de base de datos Multi-AZ.

Para convertirla en una implementación de instancia de base de datos Multi-AZ con la consola de RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. En Actions (Acciones), elija Convert to Multi-AZ deployment (Convertir en implementación multi-AZ).
4. Para aplicar los cambios de forma inmediata, seleccione la opción Apply Immediately (Aplicar inmediatamente) en la página de confirmación. La elección de esta opción no provoca tiempo de inactividad, pero existe un posible impacto en el rendimiento. De forma alternativa, también

puede aplicar la actualización durante la siguiente ventana de mantenimiento. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

5. Elija Convert to Multi-AZ (Convertir a Multi-AZ).

Modificación de una instancia de base de datos para convertirla en una implementación de base de datos Multi-AZ

Puede modificar una instancia de base de datos para convertirla en una implementación de instancia de base de datos multi-AZ de las siguientes maneras:

- Mediante la consola de RDS, modifique la instancia de base de datos y defina la Multi-AZ deployment (Implementación multi-AZ) en Yes (Sí).
- Con la AWS CLI, ejecute el comando modify-db-instance y defina la opción `--multi-az`.
- Con la API de RDS, llame a la operación ModifyDBInstance y establezca el parámetro `MultiAZ` en `true`.

Para obtener más información sobre la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS. Una vez que la modificación se ha completado, Amazon RDS desencadena un evento (RDS-EVENT-0025) que indica que el proceso se ha completado. Puede monitorear los eventos de Amazon RDS. Para obtener más información sobre los eventos, consulte Uso de notificaciones de eventos de Amazon RDS.

Conmutación por error de una instancia de base de datos multi-AZ para Amazon RDS

Si se produce una interrupción planificada o no planificada de la instancia de base de datos a causa de un defecto de la infraestructura, Amazon RDS cambia automáticamente a una réplica en espera de otra zona de disponibilidad.

El tiempo requerido para completar la conmutación por error dependerá de la actividad de la base de datos y de otras condiciones existentes cuando la instancia de base de datos principal dejó de estar disponible. Los tiempos de conmutación por error suelen estar entre 60–120 segundos. Sin embargo, las transacciones grandes o un proceso de recuperación largo pueden aumentar el tiempo de conmutación por error. Cuando la conmutación por error se haya completado, puede hacer falta más tiempo para que la consola de RDS refleje la nueva zona de disponibilidad.

> **Note**
>
> Puede forzar una conmutación por error manualmente cuando reinicie una instancia de base de datos multi-AZ. Para obtener más información, consulte Reinicio de una instancia de base de datos.

Amazon RDS gestiona las conmutaciones por error automáticamente para que sea posible reanudar las operaciones de la base de datos lo antes posible sin intervención administrativa. La instancia de base de datos principal conmuta automáticamente a la réplica en espera si se da cualquiera de las condiciones descritas en la siguiente tabla. Puede ver los motivos de la conmutación por error en el registro de eventos.

Motivo de la conmutación por error	Descripción
Se le aplican parches al sistema operativo subyacente a la instancia de base de datos de RDS en una operación sin conexión.	Se ha desencadenado una conmutación por error durante la ventana de mantenimiento para un parche del sistema operativo o una actualización de seguridad. Para obtener más información, consulte Mantenimiento de una instancia de base de datos.
El host principal de la instancia multi-AZ de RDS no está en buen estado.	La implementación de una instancia de base de datos Multi-AZ detectó una instancia de base de datos principal deteriorada y se produjo una conmutación por error.
El host principal de la instancia multi-AZ de RDS es inaccesible debido a la pérdida de conectividad de red.	El monitoreo de RDS detectó un error de accesibilidad de la red a la instancia de base de datos principal y desencadenó una conmutación por error.
El cliente modificó la instancia de RDS.	Una modificación de la instancia de base de datos de RDS desencadenó una conmutación por error.

Motivo de la conmutación por error	Descripción
	Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Motivo de la conmutación por error	Descripción
La instancia principal multi-AZ de RDS está ocupada y no responde.	La instancia de base de datos principal no responde. Le recomendamos que realice las siguientes acciones: • Examine los registros de eventos y de CloudWatch en busca de uso excesivo de CPU, memoria o espacio de intercambio. Para obtener más información, consulte Uso de notificaciones de eventos de Amazon RDS y Creación de una regla que se desencadena en función de un evento Amazon RDS. • Evalúe su carga de trabajo para determina r si está utilizando la clase de instancia de base de datos adecuada. Para obtener más información, consulte Clases de instancia de base de datos de . • Utilice el monitoreo mejorado para las métricas del sistema operativo en tiempo real. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada. • Utilice la información sobre rendimiento para ayudar a analizar cualquier problema que afecte al rendimiento de la instancia de base de datos. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.

Motivo de la conmutación por error	Descripción
	Para obtener más información sobre estas recomendaciones, consulte Supervisión de herramientas de Amazon RDS y Prácticas recomendadas para Amazon RDS.
El volumen de almacenamiento subyacente al host principal de la instancia multi-AZ de RDS tuvo un error.	La implementación de una instancia de base de datos Multi-AZ detectó un problema de almacenamiento en la instancia de base de datos principal y se produjo una conmutación por error.
El usuario solicitó una conmutación por error de la instancia de base de datos.	Reinició la instancia de base de datos y eligió Reboot with failover (Reiniciar con conmutación por error). Para obtener más información, consulte Reinicio de una instancia de base de datos.

Para determinar si se produjo una conmutación por error en la instancia de base de datos Multi-AZ, puede hacer lo siguiente:

- Configure suscripciones de eventos de base de datos para notificar por correo electrónico o por SMS que se ha iniciado una conmutación por error. Para obtener más información sobre los eventos, consulte Uso de notificaciones de eventos de Amazon RDS.
- Visualice sus eventos de base de datos mediante la consola de RDS o las operaciones de la API.
- Puede ver el estado actual de la implementación de una instancia de base de datos Multi-AZ mediante la consola de RDS o las operaciones de la API.

Para obtener información acerca de la forma de responder a las conmutaciones por error, reducir el tiempo de recuperación y otras prácticas recomendadas para Amazon RDS, consulte Prácticas recomendadas para Amazon RDS.

Configuración del TTL de JVM para las búsquedas de nombres DNS

El mecanismo de conmutación por error cambia automáticamente el registro del Sistema de nombres de dominio (DNS) de la instancia de base de datos para que apunte a la instancia de base de datos en espera. Como consecuencia, necesita restablecer las conexiones existentes a la instancia de base de datos. En un entorno de máquina virtual Java (JVM), debido al funcionamiento del mecanismo de almacenamiento en caché de DNS, puede ser necesario reconfigurar los ajustes de JVM.

La JVM almacena en caché las búsquedas de nombres DNS. Cuando la JVM resuelve un nombre de host en una dirección IP, almacena en caché la dirección IP durante un periodo de tiempo especificado, conocido como periodo de vida (TTL).

Como los recursos de AWS utilizan entradas de nombres de DNS que cambian de vez en cuando, recomendamos que configure su JVM con un valor de TTL no superior a 60 segundos. Al hacer esto se asegurará de que cuando cambie la dirección IP de un recurso, su aplicación pueda recibir y utilizar la nueva dirección IP del recurso volviendo a consultar el DNS.

En algunas configuraciones de Java, el TTL predeterminado de JVM está establecido de forma que nunca se actualicen las entradas DNS hasta que se reinicie la JVM. Por lo tanto, si la dirección IP de un recurso de AWS cambia mientras la aplicación sigue en ejecución, no podrá utilizar dicho recurso hasta que reinicie manualmente la JVM y se actualice la información de la dirección IP almacenada en caché. En este caso, es fundamental establecer el TTL de la JVM de forma que actualice periódicamente la información de las direcciones IP almacenada en caché.

Para obtener el TTL predeterminado de JVM, recupere el valor de la propiedad `networkaddress.cache.ttl`:

```
String ttl = java.security.Security.getProperty("networkaddress.cache.ttl");
```

> **Note**
>
> El TTL predeterminado puede variar en función de la versión de su JVM y de si está instalado un administrador de seguridad. Muchas JVM proporcionan un TTL predeterminado inferior a 60 segundos. Si utiliza una de estas JVM y no usa un administrador de seguridad, puede omitir el resto de este tema. Para obtener más información sobre los administradores de seguridad en Oracle, consulte The Security Manager en la documentación de Oracle.

Para modificar el TTL de la JVM, establezca el valor de la propiedad `networkaddress.cache.ttl`. Utilice uno de los siguientes métodos, en función de sus necesidades:

- Para establecer globalmente el valor de la propiedad para todas las aplicaciones que utilizan la JVM, establezca `networkaddress.cache.ttl` en el archivo `$JAVA_HOME/jre/lib/security/java.security`.

```
networkaddress.cache.ttl=60
```

- Para establecer la propiedad localmente sólo para la aplicación, establezca `networkaddress.cache.ttl` en el código de inicialización de la aplicación antes de establecer las conexiones de red.

```
java.security.Security.setProperty("networkaddress.cache.ttl" , "60");
```

Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS

La implementación de un clúster de base de datos multi-AZ es un modo de implementación de alta disponibilidad semisíncrono de Amazon RDS con dos instancias de base de datos de réplica legibles. Un clúster de base de datos Multi-AZ tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas de disponibilidad diferentes en la misma Región de AWS. Los clústeres de base de datos Multi-AZ proporcionan alta disponibilidad, mayor capacidad para cargas de trabajo de lectura y menor latencia de escritura en comparación con las implementaciones de las instancias de base de datos Multi-AZ.

Puede importar datos de una base de datos en las instalaciones a un clúster de base de datos Multi-AZ siguiendo las instrucciones de Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido.

Puede comprar instancias de base de datos reservadas para un clúster de base de datos multi-AZ. Para obtener más información, consulte Instancias de base de datos reservadas para un clúster de base de datos multi-AZ.

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de Amazon RDS con clústeres de base de datos Multi-AZ, consulte Regiones y motores de base de datos admitidos para clústeres de bases de datos Multi-AZ en Amazon RDS.

Temas

- Disponibilidad de clase de instancia para los clústeres de base de datos multi-AZ
- Arquitectura de clúster de base de datos multi-AZ
- Grupos de parámetros para clústeres de base de datos multi-AZ
- RDS Proxy con clústeres de bases de datos multi-AZ
- Retraso de réplica y clústeres de base de datos Multi-AZ
- Instantáneas de clúster de base de datos multi-AZ
- Creación de un clúster de base de datos multi-AZ para Amazon RDS
- Conexión a un clúster de base de datos multi-AZ para Amazon RDS
- Conexión automática de un recurso de computación de AWS y un clúster de base de datos multi-AZ para Amazon RDS

- Modificación de un clúster de base de datos multi-AZ para Amazon RDS.
- Actualización de la versión del motor de un clúster de base de datos multi-AZ para Amazon RDS
- Cambio de nombre de un clúster de base de datos multi-AZ para Amazon RDS
- Reinicio de un clúster de base de datos multi-AZ e instancias de base de datos de lector para Amazon RDS
- Conmutación por error de un clúster de base de datos multi-AZ para Amazon RDS
- Configuración de la replicación lógica de PostgreSQL con clústeres de base de datos multi-AZ para Amazon RDS
- Uso de réplicas de lectura de clústeres de base de datos multi-AZ para Amazon RDS
- Configuración de la replicación externa a partir de los clústeres de bases de datos multi-AZ para Amazon RDS
- Eliminación de un clúster de base de datos multi-AZ para Amazon RDS
- Limitaciones de clústeres de base de datos multi-AZ para Amazon RDS

> **Important**
>
> Los clústeres de base de datos multi-AZ no son los mismos que los clústeres de base de datos de Aurora. Para obtener información acerca de los clústeres de base de datos de Amazon Aurora, consulte la Guía del usuario de Amazon Aurora.

Disponibilidad de clase de instancia para los clústeres de base de datos multi-AZ

Las implementaciones de clústeres de bases de datos multi-AZ son compatibles con las siguientes clases de instancias de base de datos: `db.m5d`, `db.m6gd`, `db.m6id`, `db.m6idn`, `db.r5d`, `db.r6gd`, `db.x2iedn`, `db.r6id`, `db.r6idn` y `db.c6gd`.

> **Note**
>
> Las clases de instancias c6gd son las únicas que admiten el tamaño de la instancia `medium`.

Para obtener más información sobre las clases de instancias de bases de datos, consulte the section called “Clases de instancia de base de datos”.

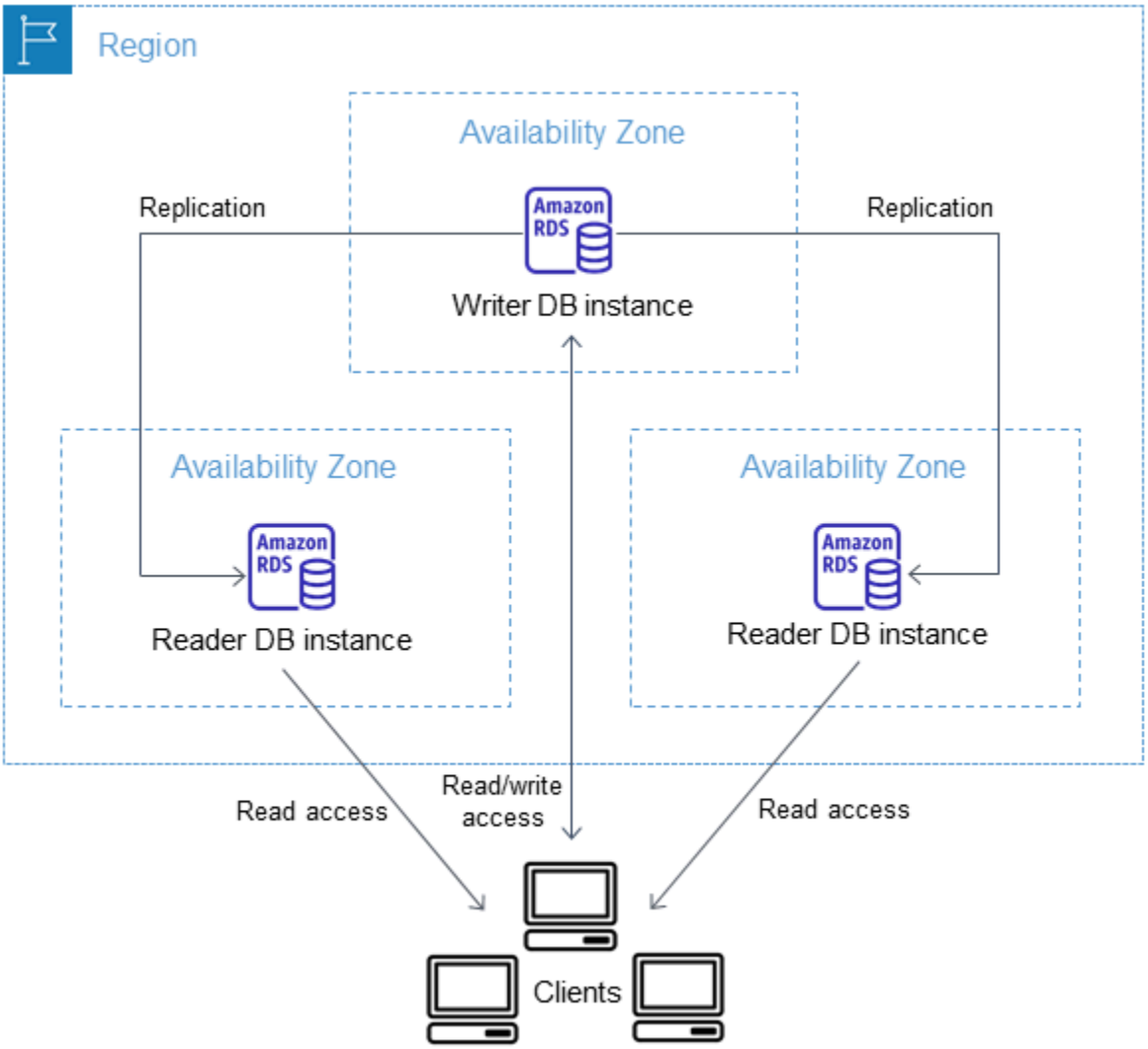
Arquitectura de clúster de base de datos multi-AZ

Con un clúster de base de datos Multi-AZ, Amazon RDS replica los datos de la instancia de base de datos del escritor en las dos instancias de base de datos del lector mediante las capacidades de replicación nativa del motor de base de datos. Cuando se realiza un cambio en la instancia de base de datos del escritor, se envía a cada instancia de base de datos del lector.

Las implementaciones de clústeres de base de datos multi-AZ utilizan la replicación semisíncrona, que requiere el reconocimiento de al menos una instancia de base de datos del lector para confirmar un cambio. No es necesario que se reconozca que los eventos se han ejecutado y confirmado en su totalidad en todas las réplicas.

Las instancias de base de datos del lector actúan como destinos de la conmutación por error automática y también proporcionan tráfico de lectura para aumentar el rendimiento de lectura de las aplicaciones. Si se produce una interrupción en la instancia de base de datos de escritor, RDS administra la conmutación por error a una de las instancias de base de datos de lector. RDS hace esto en función de qué instancia de base de datos del lector tiene el registro de cambios más reciente.

El siguiente diagrama muestra un clúster de base de datos Multi-AZ.



Los clústeres de base de datos Multi-AZ suelen tener menor latencia de escritura en comparación con las implementaciones de instancias de base de datos Multi-AZ. También permiten que las cargas de trabajo de solo lectura se ejecuten en instancias de base de datos del lector. La consola de RDS muestra la zona de disponibilidad de la instancia de base de datos del escritor y las zonas de disponibilidad de las instancias de base de datos del lector. También puede utilizar el comando de la CLI describe-db-clusters o la operación de la API DescribeDBClusters para encontrar esta información.

> **Important**
>
> Para evitar errores de réplica en clústeres de base de datos Multi-AZ de RDS para MySQL, recomendamos encarecidamente que todas las tablas tengan una clave principal.

Grupos de parámetros para clústeres de base de datos multi-AZ

En un clúster de base de datos Multi-AZ, un grupo de parámetros del clúster de base de datos funciona como un contenedor de los valores de configuración del motor que se aplican a cada instancia de base de datos en un clúster de base de datos Multi-AZ.

En un clúster de base de datos Multi-AZ, un grupo de parámetros de base de datos se establece en el grupo de parámetros de base de datos predeterminado para el motor de base de datos y la versión del motor de base de datos. La configuración del grupo de parámetros del clúster de base de datos se utiliza para todas las instancias de base de datos del clúster.

Para obtener información acerca de los grupos de parámetros, consulte the section called “Grupos de parámetros de clúster de bases de datos”.

RDS Proxy con clústeres de bases de datos multi-AZ

Puede utilizar Amazon RDS Proxy para crear un proxy para sus clústeres de base de datos multi-AZ. Con RDS Proxy, las aplicaciones pueden agrupar y compartir conexiones de base de datos para mejorar su capacidad de escala. Todos los proxy hacen multiplexación de conexión, algo conocido también como reutilización de la conexión. Con la multiplexación, el proxy de RDS realiza todas las operaciones de una transacción mediante una conexión de base de datos subyacente. RDS Proxy también puede reducir el tiempo de inactividad de una actualización de una versión secundaria de un clúster de base de datos multi-AZ a un segundo o menos. Para obtener más información sobre las ventajas de RDS Proxy, consulte Amazon RDS Proxy.

Para configurar un proxy para un clúster de base de datos Multi-AZ, seleccione Creación de un proxy de RDS al crear el clúster. Para obtener instrucciones sobre cómo crear y administrar los puntos de conexión del proxy de RDS, consulte the section called “Trabajo con puntos de enlace del proxy de RDS”.

Retraso de réplica y clústeres de base de datos Multi-AZ

El retraso de réplica es la diferencia de tiempo entre la última transacción en la instancia de base de datos del escritor y la última transacción aplicada en una instancia de base de datos del lector. La métrica `ReplicaLag` de Amazon CloudWatch representa esta diferencia de tiempo. Para obtener más información acerca de las métricas de CloudWatch, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.

Aunque los clústeres de bases de datos Multi-AZ permiten un alto rendimiento de escritura, puede producirse un retraso de réplica debido a la naturaleza de la replicación basada en motor. Dado que

cualquier conmutación por error debe resolver el retraso de réplica antes de promover una nueva instancia de base de datos de escritor, la supervisión y administración de este retraso de réplica es una consideración.

Para clústeres de base de datos RDS para MySQL Multi-AZ, el tiempo de conmutación por error depende del retraso de réplica de las dos instancias de base de datos de lectores restantes. Ambas instancias de base de datos de lectura deben aplicar transacciones no aplicadas antes de que una de ellas se promueva a la nueva instancia de base de datos de escritor.

Para clústeres de base de datos RDS para PostgreSQL Multi-AZ, el tiempo de conmutación por error depende del retraso de réplica más bajo de las dos instancias de base de datos de lector restantes. La instancia de base de datos del lector con el retraso de réplica más bajo debe aplicar transacciones no aplicadas antes de que se promueva a la nueva instancia de base de datos del escritor.

Para ver un tutorial que le muestra cómo crear una alarma de CloudWatch cuando el retraso de la réplica supera una cantidad de tiempo establecida, consulte Tutorial: creación de una alarma de Amazon CloudWatch para el retardo de réplica del clúster de base de datos multi-AZ para Amazon RDS.

Causas comunes del retraso de réplica

En general, el retraso de réplica se produce cuando la carga de trabajo de escritura es demasiado alta para que las instancias de base de datos del lector apliquen las transacciones de manera eficiente. Varias cargas de trabajo pueden provocar un retraso de réplica temporal o continuo. Ejemplos de causas comunes:

- Alta simultaneidad de escritura o actualización por lotes pesados en la instancia de base de datos del escritor, lo que hace que el proceso de aplicación en las instancias de base de datos del lector se demore.
- Carga de trabajo de lectura pesada que utiliza recursos en una o más instancias de base de datos del lector. La ejecución de consultas lentas o grandes puede afectar al proceso de aplicación y provocar un retraso de réplica.
- Las transacciones que modifican grandes cantidades de datos o instrucciones DDL a veces pueden provocar un aumento temporal del retraso de réplica porque la base de datos debe conservar el orden de confirmación.

Mitigación del retraso de réplica

En el caso de los clústeres de bases de datos Multi-AZ para RDS para MySQL y RDS para PostgreSQL, puede reducir la carga de la instancia de base de datos del escritor para mitigar el retraso de réplica. También puede usar el control de flujo para reducir el retraso de la réplica. El control de flujo funciona limitando las escrituras en la instancia de base de datos del escritor, lo que garantiza que el retraso de réplica no siga creciendo de forma ilimitada. La limitación de escritura se logra añadiendo un retardo al final de una transacción, lo que reduce el rendimiento de escritura en la instancia de base de datos del escritor. Aunque el control de flujo no garantiza la eliminación del retraso, puede ayudar a reducir el retraso general en muchas cargas de trabajo. Las siguientes secciones brindan información sobre el uso del control de flujo con RDS para MySQL y RDS para PostgreSQL.

Mitigación del retraso de la réplica con control de flujo para RDS para MySQL

Cuando utiliza RDS para clústeres de base de datos MySQL Multi-AZ, el control de flujo se activa de forma predeterminada mediante el parámetro dinámico `rpl_semi_sync_master_target_apply_lag`. Este parámetro especifica el límite superior que desea para el retraso de la réplica. A medida que el retardo de la réplica se acerca a este límite configurado, el control de flujo acelera las transacciones de escritura en la instancia de la base de datos del escritor para intentar contener el retardo de la réplica por debajo del valor especificado. En algunos casos, el retraso de réplica supera el límite especificado. De forma predeterminada, este parámetro se establece en 120 segundos. Para desactivar el control de flujo, establezca este parámetro en su valor máximo de 86 400 segundos (un día).

Para ver el retraso actual inyectado por el control de flujo, muestre el parámetro `Rpl_semi_sync_master_flow_control_current_delay` al ejecturar la siguiente consulta.

```
SHOW GLOBAL STATUS like '%flow_control%';
```

El resultado debería tener un aspecto similar al siguiente.

```
+-----------------------------------------------+-------+
| Variable_name                                 | Value |
+-----------------------------------------------+-------+
| Rpl_semi_sync_master_flow_control_current_delay | 2010  |
+-----------------------------------------------+-------+
1 row in set (0.00 sec)
```

> **Note**
>
> El retraso se muestra en microsegundos.

Cuando tiene Información sobre rendimiento activado para un clúster de base de datos RDS para MySQL Multi-AZ, puede supervisar el evento de espera correspondiente a una instrucción SQL que indica que las consultas se retrasaron por un control de flujo. Cuando un control de flujo introdujo un retraso, puede ver el evento de espera `/wait/synch/cond/semisync/semi_sync_flow_control_delay_cond` correspondiente a la instrucción SQL del panel de Performance Insights (Información sobre rendimiento). Para ver estas métricas, asegúrese de que el esquema de rendimiento esté activado. Para obtener más información acerca de Información sobre rendimiento, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.

Mitigación del retraso de la réplica con control de flujo para RDS para PostgreSQL

Cuando utiliza RDS para clústeres de base de datos Multi-AZ de PostgreSQL, el control de flujo se implementa como una extensión. Activa un empleado en segundo plano para todas las instancias de base de datos en el clúster de base de datos. De forma predeterminada, los empleados en segundo plano de las instancias de base de datos del lector comunican el retraso de réplica actual al empleado en segundo plano de la instancia de base de datos del escritor. Si el retardo supera los dos minutos en cualquier instancia de base de datos del lector, el empleado en segundo plano de la instancia de base de datos del escritor agrega un retraso al final de una transacción. Para controlar el umbral de retraso, utilice el parámetro `flow_control.target_standby_apply_lag`.

Cuando un control de flujo limita un proceso de PostgreSQL, el evento de espera `Extension` en `pg_stat_activity` e Información sobre rendimiento lo indican. La función `get_flow_control_stats` muestra detalles sobre cuánto retardo se está agregando actualmente.

El control de flujo puede beneficiar a la mayoría de las cargas de trabajo de procesamiento de transacciones en línea (OLTP) que tienen transacciones cortas, pero muy simultáneas. Si el retraso se debe a transacciones de larga duración, como operaciones por lotes, el control de flujo no proporciona tanto beneficio.

Para desactivar el control de flujo, elimine la extensión de `shared_preload_libraries` y reinicie la instancia de base de datos.

Instantáneas de clúster de base de datos multi-AZ

Amazon RDS crea y guarda copias de seguridad automatizadas del clúster de base de datos multi-AZ durante el periodo de copia de seguridad configurado. RDS crea una instantánea del volumen de almacenamiento del clúster de base de datos y realiza una copia de seguridad de todo el clúster y no solo de las instancias individuales.

También puede realizar copias de seguridad manuales del clúster de base de datos multi-AZ. Para copias de seguridad a largo plazo, plantéese exportar datos de instantáneas a Amazon S3. Para obtener más información, consulte the section called “Creación de una instantánea de un clúster de base de datos Multi-AZ”.

Para restaurar un clúster de base de datos Multi-AZ a un momento específico, cree un nuevo clúster de base de datos Multi-AZ. Para obtener instrucciones, consulte the section called “Restauración de un clúster de base de datos Multi-AZ a un momento indicado”.

De forma alternativa, puede restaurar una instantánea de clúster de base de datos multi-AZ a una implementación single-AZ o a una implementación de instancia de base de datos multi-AZ. Para obtener instrucciones, consulte the section called “Restauración desde una instantánea de clúster de base de datos Multi-AZ a una instancia de base de datos”.

Creación de un clúster de base de datos multi-AZ para Amazon RDS

Un clúster de base de datos Multi-AZ tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas de disponibilidad diferentes. Los clústeres de base de datos Multi-AZ proporcionan alta disponibilidad, mayor capacidad para cargas de trabajo de lectura y menor latencia en comparación con las implementaciones Multi-AZ. Para obtener más información acerca de los clústeres de base de datos Multi-AZ, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

> **Note**
>
> Los clústeres de base de datos Multi-AZ solo son compatibles con los motores de base de datos MySQL y PostgreSQL.

Requisitos previos de clúster de base de datos

> **Important**
>
> Para poder crear un clúster de base de datos Multi-AZ, debe completar las tareas de Configuración del entorno para Amazon RDS.

A continuación se describen los requisitos previos para crear un clúster de base de datos Multi-AZ.

Temas

- Configurar la red para el clúster de base de datos
- Requisitos previos adicionales

Configurar la red para el clúster de base de datos

Solo puede crear una instancia de base de datos en una Virtual Private Cloud (VPC) en función del servicio de Amazon VPC. Debe estar en una Región de AWS que tenga al menos tres zonas de disponibilidad. El grupo de subred de base de datos que elija para el clúster de base de datos debe abarcar al menos tres zonas de disponibilidad. Esta configuración garantiza que cada instancia de base de datos del clúster de base de datos se encuentre en una zona de disponibilidad diferente.

Para configurar la conectividad entre su nuevo clúster de base de datos y una instancia de Amazon EC2 en la misma VPC, hágalo cuando cree el clúster de base de datos. Para conectarse a su clúster de base de datos desde recursos que no sean instancias de EC2 en la misma VPC, configure las conexiones de red manualmente.

Temas

- Configurar la conectividad de red automática con una instancia de EC2
- Configurar la red manualmente

Configurar la conectividad de red automática con una instancia de EC2

Cuando se crea un clúster de base de datos Multi-AZ, se puede utilizar la AWS Management Console para configurar la conectividad entre una instancia de EC2 y el nuevo clúster de base de datos. Al hacerlo, RDS configura automáticamente los ajustes de red y VPC. El clúster de base de datos se crea en la misma VPC que la instancia de EC2 para que la instancia de EC2 pueda acceder al clúster de base de datos.

Estos son los requisitos para conectar una instancia de EC2 al clúster de base de datos:

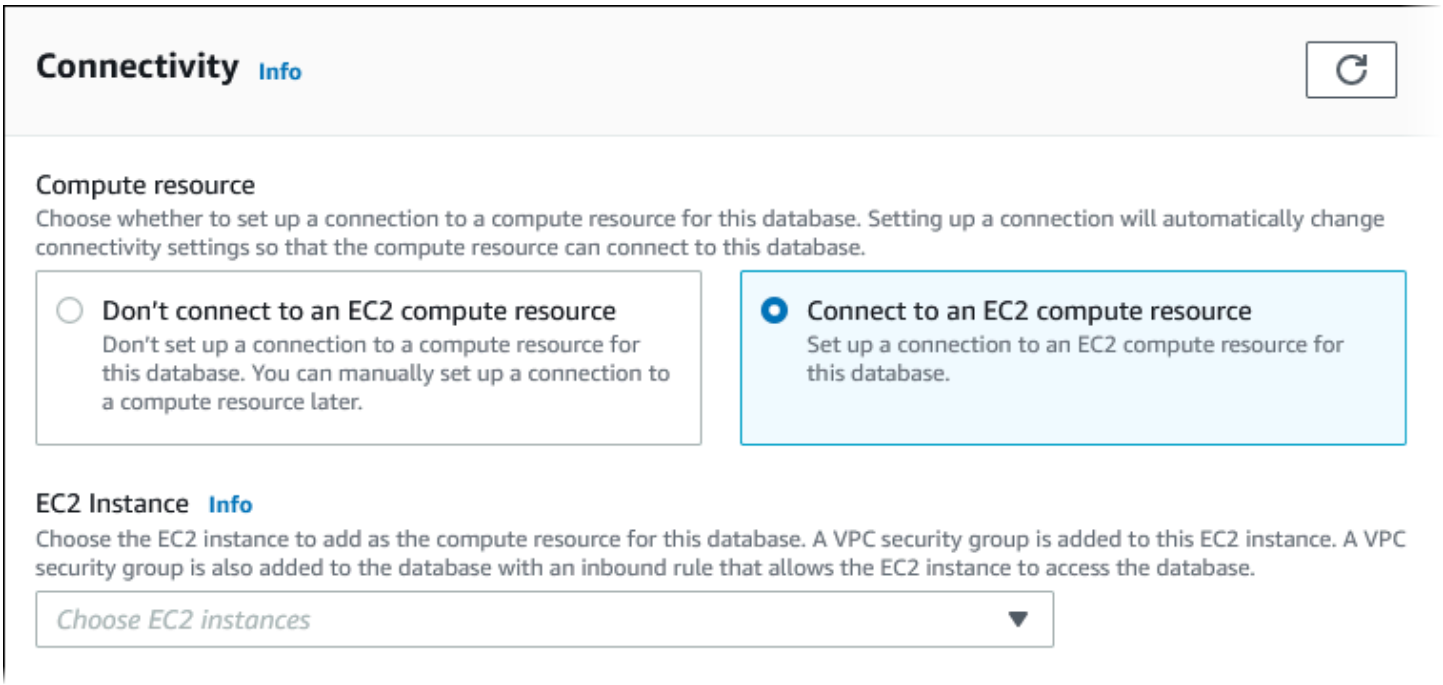
- La instancia de EC2 debe existir en la Región de AWS antes de crear el clúster de base de datos.

  Si no existen instancias de EC2 en la Región de AWS, la consola proporciona un enlace para crear una.
- El usuario que crea el clúster de base de datos debe tener permisos para realizar las siguientes operaciones:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSubnet`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`

- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Esta opción permite crear un clúster de base de datos privado. El clúster de base de datos usa un grupo de subredes de base de datos con solo subredes privadas para restringir el acceso a los recursos dentro de la VPC.

Para conectar una instancia de EC2 al clúster de base de datos, seleccione Connect to an EC2 compute resource (Conectarse a un recurso de computación de EC2) en la sección Connectivity (Conectividad) de la página Create database (Crear base de datos).



Cuando elige Connect to an EC2 compute resource (Conectarse a un recurso de computación de EC2), RDS establece las siguientes opciones automáticamente. No puede cambiar esta configuración a menos que decida no configurar la conectividad con una instancia de EC2 seleccionando Don't connect to an EC2 compute resource (No conectarse a un recurso de computación de EC2).

Opción de la consola	Configuración automática
	RDS establece la VPC en la asociada a la instancia de EC2.

Opción de la consola	Configuración automática
Virtual Private Cloud (VPC) (Nube virtual privada)	
Grupo de subredes de base de datos	RDS necesita un grupo de subredes de base de datos con una subred privada en la misma zona de disponibilidad que la instancia de EC2. Si existe un grupo de subredes de base de datos que cumpla este requisito, RDS utiliza el grupo de subredes de base de datos existente. De forma predeterminada, esta opción está configurada en Automatic setup (Configuración automática). Si selecciona Automatic setup (Configuración automática) y no hay ningún grupo de subredes de base de datos que cumpla este requisito, se produce lo siguiente. RDS usa tres subredes privadas disponibles en tres zonas de disponibilidad, donde una de las zonas de disponibilidad es la misma que la instancia de EC2. Si una subred privada no está disponible en una zona de disponibilidad, RDS crea una subred privada en la zona de disponibilidad. Luego RDS crea el grupo de subredes de base de datos. Cuando hay una subred privada disponible, RDS usa la tabla de enrutamiento asociada a ella y añade cualquier subred que cree a esta tabla de enrutamiento. Cuando no hay ninguna subred privada disponible, RDS crea una tabla de enrutamiento sin acceso a la puerta de enlace de Internet y añade las subredes que crea a la tabla de enrutamiento. RDS también permite utilizar los grupos de subredes de base de datos existentes. Seleccione Choose existing (Elegir existente) si desea utilizar un grupo de subredes de base de datos existente de su elección.

Opción de la consola	Configuración automática
Acceso público	RDS elige No para que no se pueda acceder al clúster de base de datos de forma pública. Por motivos de seguridad, se recomienda mantener la base de datos privada y asegurarse de que no se pueda acceder a ella desde Internet.
Grupo de seguridad de VPC (firewall)	RDS crea un nuevo grupo de seguridad que se asocia al clúster de base de datos. El grupo de seguridad se denomina `rds-ec2-`*n*, donde *n* es un número. Este grupo de seguridad incluye una regla de entrada con el grupo de seguridad de VPC de EC2 (firewall) como origen. Este grupo de seguridad que está asociado al clúster de base de datos permite que la instancia de EC2 acceda al clúster de base de datos. RDS también crea un nuevo grupo de seguridad que se asocia a la instancia de EC2. El grupo de seguridad se denomina `ec2-rds-`*n*, donde *n* es un número. Este grupo de seguridad incluye una regla de salida con el grupo de seguridad de VPC del clúster de base de datos como origen. Este grupo de seguridad permite que la instancia de EC2 envíe tráfico al clúster de base de datos. Para agregar otro grupo de seguridad nuevo, elija Create new (Crear nuevo) y escriba el nombre del nuevo grupo de seguridad . Para añadir grupos de seguridad existentes, elija Choose existing (Elegir existentes) y seleccione los grupos de seguridad que desea añadir.

Opción de la consola	Configuración automática
Zona de disponibilidad	RDS elige la zona de disponibilidad de la instancia de EC2 para una instancia de base de datos en la implementación del clúster de base de datos Multi-AZ. RDS elige aleatoriamente una zona de disponibilidad diferente para las otras dos instancias de base de datos. La instancia de base de datos del escritor se crea en la misma zona de disponibilidad que la instancia de EC2. Existe la posibilidad de incurrir en costos entre zonas de disponibilidad si se produce una conmutación por error y la instancia de base de datos del escritor se encuentra en una zona de disponibilidad diferente.

Para obtener más información sobre estas opciones, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.

Si cambia esta configuración después de crear el clúster de base de datos, los cambios pueden afectar a la conexión entre la instancia de EC2 y el clúster de base de datos.

Configurar la red manualmente

Para conectarse a su clúster de base de datos desde recursos que no sean instancias de EC2 en la misma VPC, configure las conexiones de red manualmente. Si usa la AWS Management Console para crear un clúster de base de datos Multi-AZ, puede hacer que Amazon RDS cree automáticamente una VPC. O puede usar una VPC ya existente o crear una nueva VPC para su clúster de base de datos Multi-AZ. La VPC debe tener como mínimo una subred en al menos tres de las zonas de disponibilidad para que la use con un clúster de base de datos Multi-AZ. Para obtener información acerca de las VPC, consulte VPC de Amazon y Amazon RDS.

Si no tiene una VPC predeterminada, no ha creado una VPC o no tiene previsto usar la consola, haga lo siguiente:

- Cree una VPC que tenga como mínimo una subred en al menos tres de las zonas de disponibilidad de la región de AWS en la que desea implementar su clúster de base de datos. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.
- Especifique un grupo de seguridad de VPC que autorice las conexiones con su clúster de base de datos de . Para obtener más información, consulte Proporcionar acceso a la instancia de base de

datos en la VPC mediante la creación de un grupo de seguridad y Control de acceso con grupos de seguridad.

- Especifique un grupo de subredes de base de datos de RDS que defina al menos tres subredes de la VPC que pueda usar el clúster de base de datos Multi-AZ. Para obtener más información, consulte Uso de los grupos de subredes de base de datos.

Para obtener información sobre las limitaciones que se aplican a los clústeres de base de datos Multi-AZ, consulte Limitaciones de clústeres de base de datos multi-AZ para Amazon RDS.

Si desea conectarse a un recurso que no está en la misma VPC que el clúster de base de datos Multi-AZ, consulte los escenarios adecuados en Escenarios de acceso a una instancia de base de datos en una VPC.

Requisitos previos adicionales

Antes de crear el clúster de base de datos Multi-AZ, tenga en cuenta los siguientes requisitos previos adicionales:

- para adaptar los parámetros de configuración para su clúster de base de datos, especifique un grupo de parámetros de clúster de base de datos con la configuración de parámetros requerida. Para obtener más información acerca de cómo crear un grupo de parámetros de clúster de base de datos, consulte Grupos de parámetros para clústeres de base de datos multi-AZ.
- Determine el número de puerto de TCP/IP que quiera especificar para el clúster de base de datos. Los firewalls de algunas compañías bloquean las conexiones a los puertos predeterminados. Si el firewall de su compañía bloquea el puerto predeterminado, elija otro puerto para el clúster de base de datos. Todas las instancias de base de datos de un clúster de base de datos usan el mismo puerto.
- Si la versión principal del motor de su base de datos ha alcanzado la fecha de finalización del soporte estándar de RDS, deberá utilizar la opción CLI de soporte extendido o el parámetro API de RDS. Para obtener más información, consulte el uso del soporte extendido de RDS en Configuración para la creación de clústeres de base de datos Multi-AZ.

Creación de un clúster de base de datos

Puede crear un clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Puede crear un clúster de base de datos Multi-AZ al elegir Multi-AZ DB cluster (Clúster de base de datos Multi-AZ) en la sección Availability and durability (Disponibilidad y durabilidad).

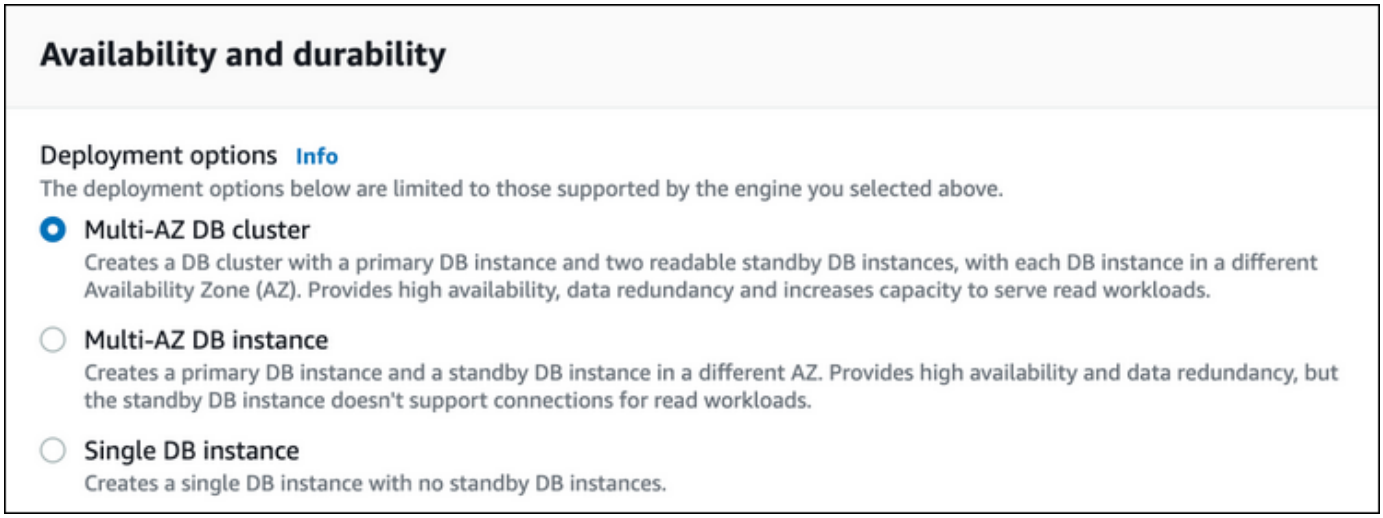
Para crear un clúster de base de datos Multi-AZ con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la AWS Management Console, elija la Región de AWS en la que desea crear el clúster de base de datos.

   Para obtener más información acerca de las Regiones de AWS que admiten clústeres de base de datos Multi-AZ, consulte Limitaciones de clústeres de base de datos multi-AZ para Amazon RDS.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija Create database (Creación de base de datos).

   Para crear un clúster de base de datos Multi-AZ, asegúrese de que la opción Standard Create (Creación estándar) esté seleccionada y Easy Create (Creación fácil) no.
5. En Engine type (Tipo de motor), elija MySQL o PostgreSQL.
6. En Versión (Versión), elija la versión del motor de base de datos.

   Para obtener más información sobre las versiones del motor de base de datos que admiten clústeres de base de datos Multi-AZ, consulte Limitaciones de clústeres de base de datos multi-AZ para Amazon RDS.
7. En Templates (Plantillas), elija la plantilla adecuada para su implementación.
8. En Availability and durability (Disponibilidad y durabilidad), elija Multi-AZ DB cluster (Clúster de base de datos Multi-AZ).



9. En DB cluster identifier (Identificador del clúster de base de datos), ingrese el identificador del clúster de base de datos.
10. En Master username (Nombre de usuario maestro), ingrese su nombre de usuario maestro o mantenga la configuración predeterminada.
11. Ingrese su contraseña maestra:
    a. En la sección Settings (Configuración), abra Credential Settings (Configuración de credenciales).
    b. Si desea especificar una contraseña, desactive la casilla Auto generate a password (Generar una contraseña de forma automática) si está seleccionada.
    c. (Opcional) Cambie el valor Master username (Nombre de usuario maestro).
    d. Ingrese la misma contraseña en Master password (Contraseña maestra) y elija Confirm password (Confirmar contraseña).
12. En Clase de instancia de base de datos, elija la clase de instancia de base de datos. Para obtener una lista de clases de instancias de base de datos compatibles, consulte the section called “Disponibilidad de clase de instancia para los clústeres de base de datos multi-AZ”.
13. (Opcional) Configure una conexión a un recurso de computación para este clúster de base de datos.

    Puede configurar la conectividad entre una instancia de Amazon EC2 y el nuevo clúster de base de datos durante la creación del clúster de base de datos. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2.

14. En la sección Conectividad del Grupo de seguridad de VPC (firewall), si selecciona Crear nuevo, se crea un grupo de seguridad de VPC con una regla de entrada que permite que la dirección IP del equipo local acceda a la base de datos.
15. En el resto de secciones, especifique los ajustes de configuración del clúster de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.
16. Elija Create database (Crear base de datos).

    Si decide utilizar una contraseña generada automáticamente, el botón View credential details (Ver detalles de credenciales) aparece en la página Databases (Bases de datos).

    Para consultar la contraseña y el nombre de usuario maestros del clúster de base de datos, seleccione View credential details (Ver detalles de credenciales).

    Para conectarse al clúster de base de datos como usuario maestro, utilice el nombre de usuario y la contraseña que aparecen.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo.

17. En Databases (Bases de datos), elija el nombre del nuevo clúster de base de datos.

Los detalles del nuevo clúster de base de datos aparecen en la consola de RDS. El clúster de base de datos tendrá el estado Creating (En creación) hasta que se cree y esté listo para el uso. Cuando el estado cambie a Available (Disponible), podrá conectarse al clúster de base de datos. Dependiendo de la clase de instancia clúster y del almacenamiento asignado, es posible que el nuevo clúster de base de datos tarde varios minutos en estar disponible.

AWS CLI

Antes de crear un clúster de base de datos Multi-AZ a través de la AWS CLI, asegúrese de cumplir los requisitos previos. Esto incluye la creación de una VPC y un grupo de subredes de base de datos de RDS Para obtener más información, consulte Requisitos previos de clúster de base de datos.

Para crear un clúster de base de datos Multi-AZ mediante la AWS CLI, llama al comando create-db-cluster. Especifique el `--db-cluster-identifier`. Para la opción del `--engine`, especifique `mysql` o `postgres`.

Para obtener más información acerca de cada opción, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.

Para obtener más información sobre las Regiones de AWS, motores de base de datos y versiones de motores de base de datos compatibles con clústeres de base de datos Multi-AZ, consulte Limitaciones de clústeres de base de datos multi-AZ para Amazon RDS.

El comando `create-db-cluster` crea la instancia de base de datos del escritor de su clúster de base de datos y dos instancias de base de datos del lector. Cada instancia de base de datos se encuentra en una zona de disponibilidad diferente.

Por ejemplo, el siguiente comando crea un clúster de base de datos Multi-AZ compatible con MySQL 8.0 llamado `mysql-multi-az-db-cluster`.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-cluster \
   --db-cluster-identifier mysql-multi-az-db-cluster \
   --engine mysql \
   --engine-version 8.0.32  \
   --master-username admin \
   --manage-master-user-password  \
   --port 3306 \
   --backup-retention-period 1  \
   --db-subnet-group-name default \
   --allocated-storage 4000 \
   --storage-type io1 \
   --iops 10000 \
   --db-cluster-instance-class db.m5d.xlarge
```

Para Windows:

```
aws rds create-db-cluster ^
   --db-cluster-identifier mysql-multi-az-db-cluster ^
   --engine mysql ^
   --engine-version 8.0.32 ^
   --manage-master-user-password ^
   --master-username admin ^
   --port 3306 ^
   --backup-retention-period 1 ^
```

```
    --db-subnet-group-name default ^
    --allocated-storage 4000 ^
    --storage-type io1 ^
    --iops 10000 ^
    --db-cluster-instance-class db.m5d.xlarge
```

El comando siguiente crea un clúster de base de datos Multi-AZ de PostgreSQL 13.4 llamado `postgresql-multi-az-db-cluster`.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-cluster \
    --db-cluster-identifier postgresql-multi-az-db-cluster \
    --engine postgres \
    --engine-version 13.4 \
    --manage-master-user-password \
    --master-username postgres \
    --port 5432 \
    --backup-retention-period 1  \
    --db-subnet-group-name default \
    --allocated-storage 4000 \
    --storage-type io1 \
    --iops 10000 \
    --db-cluster-instance-class db.m5d.xlarge
```

Para Windows:

```
aws rds create-db-cluster ^
    --db-cluster-identifier postgresql-multi-az-db-cluster ^
    --engine postgres ^
    --engine-version 13.4 ^
    --manage-master-user-password ^
    --master-username postgres ^
    --port 5432 ^
    --backup-retention-period 1 ^
    --db-subnet-group-name default ^
    --allocated-storage 4000 ^
    --storage-type io1 ^
    --iops 10000 ^
    --db-cluster-instance-class db.m5d.xlarge
```

API de RDS

Antes de poder crear un clúster de base de datos Multi-AZ a través de la API de RDS, asegúrese de cumplir los requisitos previos, como crear una VPC y un grupo de subred de base de datos de RDS. Para obtener más información, consulte Requisitos previos de clúster de base de datos.

Para crear un clúster Multi-AZ con la API de RDS, llame a la operación CreateDBCluster. Especifique el `DBClusterIdentifier`. En el parámetro `Engine`, especifique `mysql` o `postgresql`.

Para obtener más información acerca de cada opción, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.

La operación `CreateDBCluster` crea la instancia de base de datos del escritor de su clúster de base de datos y dos instancias de base de datos del lector. Cada instancia de base de datos se encuentra en una zona de disponibilidad diferente.

Configuración para la creación de clústeres de base de datos Multi-AZ

Para detalles sobre los ajustes de configuración que se eligen al crear un clúster de base de datos Multi-AZ, consulte la siguiente tabla. Para obtener más información acerca de las opciones de la AWS CLI, consulte create-db-cluster. Para obtener más información sobre los parámetros de la API de RDS, consulte CreateDBCluster.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Allocated storage (Almacenamiento asignado)	La cantidad de almacenamiento que se tiene que asignar a la instancia de base de datos en el clúster de base de datos (en gibibytes). Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.	Opción de la CLI:
		`--allocated-storage`
		Parámetro de la API:
		`AllocatedStorage`

Auto minor version upgrade (Actualización automática	Habilite la actualización automática de versiones secundarias para que el clúster de base de datos reciba actualizaciones preferida	Opción de la CLI: `--auto-minor-version-upgrade`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

de versiones secundarias)	s de la versión secundaria del motor de base de datos automátic amente cuando estén disponibl es. Amazon RDS realiza actualiza ciones automáticas de versiones secundarias en el periodo de mantenimiento.	`--no-auto-minor-version-upg rade`
		
		Parámetro de la API:
		
		`AutoMinorVersionUpgrade`

Backup retention period (Periodo de retención de copia de seguridad)	Número de días que tiene que retener las copias de seguridad automáticas del clúster de base de datos. Para un clúster de base de datos Multi-AZ, este valor debe establecerse en **1** o más.
	
	Para obtener más información, consulte Introducción a las copias de seguridad.
		Opción de la CLI:
		
		`--backup-retention-period`
		
		Parámetro de la API:
		
		`BackupRetentionPeriod`

Backup target (Intervalo de copia de seguridad)	Periodo de tiempo durante el cual Amazon RDS lleva a cabo automáticamente una copia de seguridad del clúster de base de datos. A menos que desee hacer una copia de seguridad de la base de datos a una hora determinada, utilice el valor predeterminado No Preference (Sin preferencia).
	
	Para obtener más información, consulte Introducción a las copias de seguridad.
		Opción de la CLI:
		
		`--preferred-backup-window`
		
		Parámetro de la API:
		
		`PreferredBackupWindow`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Certificate authority (Autoridad de certificado)	Entidad de certificación (CA) del certificado de servidor que utiliza el clúster de base de datos.
	
	Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
		Opción de la CLI:
		
		`--ca-certificate-identifier`
		
		Parámetro de la API de RDS:
		
		`CACertificateIdentifier`

Copy tags to snapshots (Copiar etiquetas en instantáneas)	Esta opción copia las etiquetas de los clústeres de base de datos en una instantánea de base de datos cuando se crea una instantánea.
	
	Para obtener más información, consulte Etiquetado de los recursos de y Amazon RDS.
		Opción de la CLI:
		
		`-copy-tags-to-snapshot`
		
		`-no-copy-tags-to-snapshot`
		
		Parámetro de la API de RDS:
		
		`CopyTagsToSnapshot`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Database authentication (Autenticación de bases de datos)	La opción de autenticación de la base de datos que desea usar.
	
	Elija Password authentication (Autenticación de contraseña) para autenticar solo a los usuarios de la base de datos con contraseñas de base de datos.
	
	Elija Password and IAM DB authentication (Contraseña y autenticación de base de datos de IAM) para autenticar a los usuarios de la base de datos con contraseñas y credenciales de usuario a través de usuarios y roles. Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.
		Opción de la CLI:
		
		`--enable-iam-database-authentication`
		
		`--no-enable-iam-database-authentication`
		
		Parámetro de la API de RDS:
		
		`EnableIAMDatabaseAuthentication`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Database port (Puerto de base de datos)	Puerto que desea utilizar para obtener acceso al clúster de base de datos. Se muestra el puerto predeterminado.
	
	El puerto no se puede cambiar una vez creado el clúster de base de datos.
	
	Los firewalls de algunas compañías bloquean las conexiones a los puertos predeterminados. Si el firewall de su compañía bloquea el puerto predeterminado, ingrese otro puerto para el clúster de base de datos.
		Opción de la CLI:
		
		`--port`
		
		Parámetro de la API de RDS:
		
		`Port`

DB clúster identifier (Identificador de clúster de base de datos)	El nombre del clúster de base de datos. Asigne a sus clústeres de base de datos el mismo nombre que a sus servidores en las instalaciones. El identificador del clúster de bases de datos puede contener un máximo de 63 caracteres alfanuméricos y debe ser único para su cuenta en la región de AWS que elija.	Opción de la CLI:
		
		`--db-cluster-identifier`
		
		Parámetro de la API de RDS:
		
		`DBClusterIdentifier`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

DB instance class (Clase de instancia de base de datos)	La capacidad de memoria y computación de cada instancia de base de datos en el clúster de base de datos Multi-AZ, por ejemplo, `db.m5d.xlarge` .
	
	Si es posible, elija una clase de instancia de base de datos lo bastante grande como para albergar en la memoria el conjunto de trabajo de una consulta típica. Cuando los conjuntos de trabajo se albergan en la memoria, el sistema puede evitar escribir en el disco, lo que mejora su rendimiento.
	
	Para obtener una lista de clases de instancias de base de datos compatibles, consulte the section called “Disponibilidad de clase de instancia para los clústeres de base de datos multi-AZ”.
		Opción de la CLI:
		
		`--db-cluster-instance-class`
		
		Parámetro de la API de RDS:
		
		`DBClusterInstanceClass`

Grupo de parámetros de clúster de base de datos	El grupo de parámetros de clúster de base de datos que desea asociar al clúster de base de datos.
	
	Para obtener más información, consulte Grupos de parámetros para clústeres de base de datos multi-AZ.
		Opción de la CLI:
		
		`--db-cluster-parameter-group-name`
		
		Parámetro de la API de RDS:
		
		`DBClusterParameterGroupName`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

DB engine version (Versión del motor de base de datos)	La versión del motor de base de datos que se desea utilizar.	Opción de la CLI:
		`--engine-version`
		Parámetro de la API de RDS:
		`EngineVersion`

Grupo de parámetros de clúster de base de datos	Grupo de parámetros de la instancia de base de datos a asociar con el clúster de base de datos. Para obtener más información, consulte Grupos de parámetros para clústeres de base de datos multi-AZ.	Opción de la CLI: `--db-cluster-parameter-group-name` Parámetro de la API de RDS: **`DBClusterParameterGroupName`**

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Grupo de subredes de base de datos	El grupo de subredes de base de datos que desea utilizar para el clúster de base de datos. Seleccione Choose existing (Elegir existente) para utilizar un grupo de subredes de base de datos existente. A continuación, elija el grupo de subredes requerido en la lista desplegable Existing DB subnet groups (Grupos de subredes de base de datos existentes).
	
	Elija Automatic setup (Configuración automática) para permitir que RDS seleccione un grupo de subredes de base de datos compatible. Si no existe ninguno, RDS crea un nuevo grupo de subredes para el clúster.
	
	Para obtener más información, consulte Uso de los grupos de subredes de base de datos.
		Opción de la CLI:
		
		`--db-subnet-group-name`
		
		Parámetro de la API de RDS:
		
		`DBSubnetGroupName`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Deletion protection (Protección contra eliminación)	Seleccione Enable deletion protection (Habilitar la protección contra la eliminación) para evitar que se elimine el clúster de base de datos. Si crea un clúster de base de datos de producción con la consola, se activa de forma predeterminada la protección contra la eliminación.
	
	Para obtener más información, consulte Eliminación de una instancia de base de datos.
		Opción de la CLI:
		
		`--deletion-protection`
		
		`--no-deletion-protection`
		
		Parámetro de la API de RDS:
		
		`DeletionProtection`

Cifrado	Enable Encryption (Habilitar cifrado) para activar el cifrado en reposo para este clúster de base de datos.
	
	El cifrado está activado de forma predeterminada para los clústeres de base de datos Multi-AZ.
	
	Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
		Opciones de CLI:
		
		`--kms-key-id`
		
		`--storage-encrypted`
		
		`--no-storage-encrypted`
		
		Parámetros de la API de RDS:
		
		`KmsKeyId`
		
		`StorageEncrypted`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Supervisión mejorada	Enable enhanced monitoring (Habilitar monitoreo mejorado) a fin de activar la recopilación de métricas en tiempo real para el sistema operativo en el que se ejecute el clúster de base de datos.
	
	Para obtener más informaci ón, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.
		Opciones de CLI:
		
		`--monitoring-interval`
		
		`--monitoring-role-arn`
		
		Parámetros de la API de RDS:
		
		`MonitoringInterval`
		
		`MonitoringRoleArn`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Initial database name (Nombre inicial de la base de datos)	Nombre de la base de datos del clúster de base de datos. Si no se proporciona un nombre para un clúster de base de datos Aurora MySQL. Sin embargo, crea una base de datos en el clúster de base de datos para PostgreSQL. El nombre no puede ser una palabra reservada por el motor de base de datos. Tiene otras restricciones según el motor de base de datos.
	
	MySQL:
	
	• Debe tener entre 1 y 64 caracteres alfanuméricos.
	
	PostgreSQL:
	
	• Debe tener entre 1 y 63 caracteres alfanuméricos.
	• Debe comenzar por una letra o un guion bajo. Los caracteres subsiguientes pueden ser letras, guiones bajos o dígitos (0-9).
	• El nombre inicial de la base de datos es `postgres`.
		Opción de la CLI:
		
		`--database-name`
		
		Parámetro de la API de RDS:
		
		`DatabaseName`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Log exports (Exportaciones de registros)	Los tipos de archivos de registro de base de datos que se publicarán en Amazon CloudWatch Logs.
	
	Para obtener más información, consulte Publicación de registros de base de datos en registros de Amazon Cloudwatch.
		Opción de la CLI:
		
		`-enable-cloudwatch-logs-exports`
		
		Parámetro de la API de RDS:
		
		`EnableCloudwatchLogsExports`

Periodo de mantenimiento	Periodo de 30 minutos durante el cual se aplican las modificaciones pendientes en el clúster de base de datos. Si el periodo de tiempo no es importante, elija No Preference (Sin preferencia).
	
	Para obtener más información, consulte La ventana de mantenimiento de Amazon RDS.
		Opción de la CLI:
		
		`--preferred-maintenance-window`
		
		Parámetro de la API de RDS:
		
		`PreferredMaintenanceWindow`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Gestionar las credenciales maestras en AWS Secrets Manager	Seleccione Manage master credentials in AWS Secrets Manager (Administrar credencia les maestras en AWS Secrets Manager) para administrar la contraseña del usuario maestro en un secreto en Secrets Manager.
	
	De forma opcional, elija la clave KMS para proteger el secreto. Elija entre las claves de KMS de su cuenta o bien introduzca la clave de otra cuenta.
	
	Para obtener más informaci ón, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.
		Opción de la CLI:
		
		`--manage-master-user-passwo rd | --no-manage-master- user-password`
		
		`--master-user-secret-kms-ke y-id`
		
		Parámetro de la API de RDS:
		
		`ManageMasterUserPassword`
		
		`MasterUserSecretKmsKeyId`

Master password (Contraseña maestra)	Contraseña de la cuenta del usuario maestro.	Opción de la CLI:
		
		`--master-user-password`
		
		Parámetro de la API de RDS:
		
		`MasterUserPassword`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Master Username (Nombre de usuario maestro)	El nombre que utiliza como nombre de usuario maestro para iniciar sesión en el clúster de base de datos con todos los privilegios de la base de datos.
	• Puede contener 1–16 caracteres alfanuméricos y guiones bajos.
	• El primer carácter debe ser una letra.
	• No puede ser una palabra reservada por el motor de base de datos.
	
	Después de crear el clúster de base de datos Multi-AZ, no se puede cambiar el nombre de usuario maestro.
	
	Para obtener más información sobre los privilegios concedidos al usuario maestro, consulte Privilegios de la cuenta de usuario maestro.
		Opción de la CLI:
		
		`--master-username`
		
		Parámetro de la API de RDS:
		
		`MasterUsername`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Performance Insights	Enable Performance Insights (Habilitar Información sobre rendimiento) para monitorear la carga del clúster de base de datos para poder analizar y solucionar los problemas de rendimiento de la base de datos.
	
	Elija un periodo de retención para determinar durante cuánto tiempo conservar el historial de datos de Performance Insights. La configuración de retención en la capa gratuita es Default (7 days) (Predeterminado [7 días]). Para retener los datos de rendimiento durante más tiempo, especifique de 1 a 24 meses. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.
	
	Elija la clave de KMS que se utilizará para proteger la clave que se utiliza para cifrar el volumen de esta base de datos. Elija entre las claves de KMS de su cuenta o bien introduzca la clave de otra cuenta.
	
	Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.
		Opciones de CLI:
		
		`--enable-performance-insights`
		
		`--no-enable-performance-insights`
		
		`--performance-insights-retention-period`
		
		`--performance-insights-kms-key-id`
		
		Parámetros de la API de RDS:
		
		`EnablePerformanceInsights`
		
		`PerformanceInsightsRetentionPeriod`
		
		`PerformanceInsightsKMSKeyId`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Provisioned IOPS (IOPS aprovisionadas)	La cantidad de IOPS aprovisionadas (operaciones de entrada/salida por segundo) asignada inicialmente para el clúster de base de datos.	Opción de la CLI:
		`--iops`
		Parámetro de la API de RDS:
		`Iops`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Acceso público	Publicly accesible (Accesible públicamente) para proporcionar una dirección IP pública al clúster de base de datos, lo que significa que es accesible desde fuera de la VPC. Para que sea accesible públicamente, el clúster de base de datos también debe estar en una subred pública de la VPC.
	
	Not publicly accesible (No es accesible públicamente) para que el clúster de base de datos sea accesible solo desde dentro de la VPC.
	
	Para obtener más informaci ón, consulte Cómo ocultar una instancia de base de datos en una VPC desde Internet..
	
	Para conectarse a un clúster de base de datos desde afuera de su VPC, el clúster de base de datos debe ser accesible públicamente. Además, el acceso debe concederse mediante las reglas entrantes del grupo de seguridad del clúster de base de datos y deben cumplirse otros requisitos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.
		Opción de la CLI:
		
		`--publicly-accessible`
		
		`--no-publicly-accessible`
		
		Parámetro de la API de RDS:
		
		`PubliclyAccessible`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS
	Si su clúster de base de datos no es accesible públicamente, también puede usar una conexión de AWS Site-to-site VPN o una conexión de AWS Direct Connect para acceder a ella desde una red privada. Para obtener más información, consulte Privacidad del tráfico entre redes.	

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Soporte extendido de RDS	Seleccione Habilitar el Soporte extendio de RDS para permitir que las versiones principales de los motores compatibles sigan funcionando una vez pasada la fecha de finalización del soporte estándar de RDS.
	
	Al crear un clúster de base de datos, Amazon RDS utiliza el Soporte extendido de RDS de forma predeterminada. Para evitar la creación de un nuevo clúster de base de datos después de la fecha de finalización del soporte estándar de RDS y evitar cargos por el Soporte extendido de RDS, deshabilite esta configuración. Sus clústeres de bases de datos existentes no incurrirán en cargos hasta la fecha de inicio de los precios del Soporte extendido de RDS.
	
	Para obtener más información, consulte Soporte extendido de Amazon RDS con Amazon RDS.
		Opción de la CLI:
		
		`--engine-lifecycle-support`
		
		Parámetro de la API de RDS:
		
		`EngineLifecycleSupport`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS
Rendimiento de almacenamiento	El valor de rendimiento de almacenamiento para el clúster de base de datos. Esta configuración solo es visible si selecciona SSD de uso general (gp3) como tipo de almacenamiento. Este ajuste no se puede configurar y se establece automáticamente en función de las IOPS que especifiq ue. Para obtener más información, consulte Almacenamiento gp3 (recomendado).	Este valor se calcula automáticamente y no tiene una opción CLI.
RDS Proxy	Elija Create an RDS Proxy (Crear un RDS Proxy) para crear un proxy para el clúster de base de datos. Amazon RDS crea automátic amente un rol de IAM y un secreto de Secrets Manager para el proxy.	No está disponible al crear un clúster de base de datos.

Storage type (Tipo de almacenam iento)	Tipo de almacenamiento de su clúster de base de datos.
	
	Solo se admite el almacenamiento de uso general (gp3), de IOPS aprovisionadas (io1) y de SSD de IOPS aprovisionadas (io2).
	
	Para obtener más información, consulte Tipos de almacenamiento de Amazon RDS.
		Opción de la CLI:
		
		`--storage-type`
		
		Parámetro de la API de RDS:
		
		`StorageType`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS
Virtual Private Cloud (VPC) (Nube virtual privada)	Una VPC basada en el servicio de Amazon VPC para asociar con este clúster de base de datos. Para obtener más informaci ón, consulte VPC de Amazon y Amazon RDS.	Para la CLI y la API, especifique los ID de grupo de seguridad de la VPC.

Grupo de seguridad de VPC (firewall)	Los grupos de seguridad para asociar al clúster de base de datos.
	
	Para obtener más información, consulte Información general de los grupos de seguridad de VPC.
		Opción de la CLI:
		
		`--vpc-security-group-ids`
		
		Parámetro de la API de RDS:
		
		`VpcSecurityGroupIds`

Configuración que no se aplica al crear clústeres de base de datos Multi-AZ

La siguiente configuración del comando `create-db-cluster` de la AWS CLI y la operación de la API de RDS `CreateDBCluster` no se aplica a clústeres de base de datos Multi-AZ.

Tampoco puede especificar esta configuración para clústeres de base de datos Multi-AZ en la consola.

Configuración de la AWS CLI	Configuración de la API de RDS
`--availability-zones`	`AvailabilityZones`
`--backtrack-window`	`BacktrackWindow`
`--character-set-name`	`CharacterSetName`
`--domain`	`Domain`
`--domain-iam-role-name`	`DomainIAMRoleName`

Configuración de la AWS CLI	Configuración de la API de RDS
`--enable-global-write-forwarding | --no-enable-global-write-forwarding`	`EnableGlobalWriteForwarding`
`--enable-http-endpoint | --no-enable-http-endpoint`	`EnableHttpEndpoint`
`--global-cluster-identifier`	`GlobalClusterIdentifier`
`--option-group-name`	`OptionGroupName`
`--pre-signed-url`	`PreSignedUrl`
`--replication-source-identifier`	`ReplicationSourceIdentifier`
`--scaling-configuration`	`ScalingConfiguration`

Conexión a un clúster de base de datos multi-AZ para Amazon RDS

Un clúster de base de datos Multi-AZ tiene tres instancias de base de datos en vez de solo una. Una instancia de base de datos específica gestiona cada conexión. Cuando se conecta a un clúster de base de datos Multi-AZ, el nombre de host y el puerto que especifica apuntan a un nombre de dominio completo llamado punto de conexión. El clúster de base de datos Multi-AZ utiliza el mecanismo de punto de conexión para abstraer estas conexiones, de modo que no es necesario especificar exactamente a qué instancia de base de datos del clúster de base de datos se va a conectar. Por lo tanto, no tiene que codificar todos los nombres de host ni escribir su propia lógica para redirigir las conexiones cuando algunas instancias de base de datos no están disponibles.

El punto de conexión del escritor se conecta a la instancia de la base de datos del escritor del clúster de la base de datos, que admite operaciones de lectura y escritura. El punto de conexión del lector se conecta a cualquiera de las dos instancias de base de datos del lector, que solo admiten operaciones de lectura.

Al usar puntos de conexión puede asignar cada conexión a la instancia de base de datos o grupo de instancias de base de datos adecuados en función de su caso de uso. Por ejemplo, para desempeñar instrucciones DDL y DML puede conectarse a la instancia de base de datos que sea la instancia de base de datos del escritor. Para realizar consultas, puede conectarse al extremo del lector, con el clúster de base de datos Multi-AZ al administrar automáticamente las conexiones entre las instancias de base de datos del lector. En el caso de diagnóstico o ajuste, puede conectarse a un punto de conexión de instancia de base de datos específico para examinar los detalles de una instancia de base de datos específica.

Para obtener más información acerca de la conexión a una instancia de base de datos, consulte Conexión a una instancia de base de datos de Amazon RDS.

Para obtener más información sobre la conexión a clústeres de base de datos multi-AZ, consulte los temas siguientes.

Temas

- Puntos de conexión de clúster
- Puntos de enlace del lector
- Puntos de conexión de instancia
- Conexiones de alta disponibilidad

- Conexión a clústeres de bases de datos multi-AZ con los controladores de AWS para Amazon RDS

Tipos de puntos de conexión del clúster de base de datos Multi-AZ

Un punto de conexión se representa mediante un identificador único que contiene una dirección de host. Los siguientes tipos de puntos de conexión están disponibles en un clúster de base de datos Multi-AZ:

Punto de conexión de clúster

El punto de conexión de clúster o (punto de conexión del escritor) de un clúster de base de datos Multi-AZ se conecta a la instancia de base de datos del escritor actual de ese clúster de base de datos. Este punto de conexión es el único que puede llevar a cabo operaciones de escritura como instrucciones DDL y DML. Este punto de conexión también puede llevar a cabo operaciones de lectura.

Cada clúster de base de datos Multi-AZ tiene un punto de conexión de clúster y una instancia de base de datos del escritor.

Utilice el punto de conexión del clúster para todas las operaciones de escritura en el clúster de la base de datos, incluidos inserciones, actualizaciones, eliminaciones y cambios de DDL. También puede usar el punto de conexión del clúster para operaciones de lectura, como por ejemplo consultas.

Si se produce un error en la instancia de base de datos del escritor actual de un clúster de base de datos, el clúster de base de datos Multi-AZ conmuta por error automáticamente a una nueva instancia de base de datos del escritor. Durante una conmutación por error, el clúster de base de datos todavía atiende solicitudes de conexión al punto de conexión del clúster de la nueva instancia de base de datos del escritor, con una interrupción del servicio mínima.

En el siguiente ejemplo se ilustra el punto de conexión del clúster de un clúster de base de datos Multi-AZ.

```
mydbcluster.cluster-123456789012.us-east-1.rds.amazonaws.com
```

Para obtener más información sobre la conexión a los puntos de conexión de clúster, consulte Puntos de conexión de clúster.

Punto de conexión del lector

El punto de conexión del lector para un clúster de base de datos Multi-AZ proporciona soporte para conexiones de solo lectura al clúster de base de datos. Utilice el punto de conexión del lector para operaciones de lectura, como por ejemplo consultas `SELECT`. Al procesar esas instrucciones en las instancias de base de datos del lector, este punto de conexión reduce la sobrecarga de la instancia de base de datos del escritor. También ayuda al clúster a escalar la capacidad de manejo simultáneo de consultas `SELECT`. Cada clúster de base de datos Multi-AZ tiene un punto de conexión del lector.

El punto de conexión del lector envía cada solicitud de conexión a una de las instancias de base de datos del lector. Cuando se utiliza el punto de conexión del lector para una sesión, solo se pueden ejecutar instrucciones de solo lectura como `SELECT` en esa sesión.

En el siguiente ejemplo se ilustra un punto de conexión del lector de un clúster de base de datos Multi-AZ. La intención de solo lectura de un punto de conexión de lector se indica mediante `-ro` en el punto de conexión del clúster.

```
mydbcluster.cluster-ro-123456789012.us-east-1.rds.amazonaws.com
```

Para obtener más información sobre los puntos de conexión de lector, consulte Puntos de enlace del lector.

Punto de conexión de instancia

Un punto de conexión de instancia se conecta a una instancia de base de datos específica de un clúster de base de datos Multi-AZ. Cada instancia de base de datos de un clúster de bases de datos tiene su propio punto de conexión de instancia único. Así que hay un punto de conexión de instancia para la actual instancia de base de datos del escritor del clúster de base de datos y un punto de conexión de instancia para cada una de las instancias de base de datos del lector en el clúster de la base de datos.

El punto de conexión de instancia proporciona control directo sobre las conexiones al clúster de base de datos. Este control puede ayudarle a abordar situaciones en las que el uso del punto de conexión del clúster o del lector puede no ser adecuado. Por ejemplo, su aplicación cliente podría necesitar un balanceo de carga más detallado en función del tipo de carga de trabajo. En este caso, puede configurar varios clientes para que se conecten a distintas instancias de base de datos del lector en un clúster de base de datos con el fin de distribuir las cargas de trabajo de lectura.

En el siguiente ejemplo se ilustra un punto de conexión de instancia de una instancia de base de datos de un clúster de base de datos Multi-AZ.

```
mydbinstance.123456789012.us-east-1.rds.amazonaws.com
```

Para obtener más información sobre la conexión a los puntos de conexión de instancia, consulte Puntos de conexión de instancia.

Visualización de puntos de enlace

Utilice la consola, la AWS CLI o la API de Amazon RDS para ver los puntos de conexión de clúster, lector e instancia.

Console

En la AWS Management Console, verá el punto de conexión del clúster y el punto de conexión del lector en la página de detalles de cada clúster de base de datos Multi-AZ. Verá el punto de conexión de instancia en la página de detalles de cada instancia de base de datos.

AWS CLI

Con la AWS CLI, verá el escritor y cualquier punto de conexión del lector personalizado en la salida del comando describe-db-clusters. Por ejemplo, el siguiente comando muestra los atributos de punto de conexión de todos los clústeres en la región de AWS actual.

```
aws rds describe-db-cluster-endpoints
```

Amazon RDS API

Con la API de Amazon RDS, recuperará los puntos de conexión llamando a la acción DescribeDBClusterEndpoints. El resultado también muestra los puntos de conexión del clúster de base de datos de Amazon Aurora, si existen.

Puntos de conexión de clúster

Cada clúster de base de datos Multi-AZ tiene un solo punto de conexión integrado, cuyo nombre y otros atributos administra Amazon RDS. No puede crear, eliminar o modificar este tipo de punto de conexión.

Use el punto de conexión del clúster al administrar su clúster de base de datos, extraer, transformar, cargar (ETL) o desarrollar y probar aplicaciones. El punto de conexión del clúster se conecta a la

instancia de base de datos del escritor del clúster. La instancia de base de datos del escritor es la única instancia de base de datos donde puede crear tablas e índices, ejecutar instrucciones `INSERT` y realizar otras operaciones de DDL y DML.

La dirección IP física a la que apunta el punto de conexión del clúster cambia cuando el mecanismo de conmutación por error promueve una nueva instancia de base de datos para que sea la instancia de base de datos del escritor del clúster. Si usa cualquier forma de grupos de conexiones u otros multiplexados, prepárese para vaciar o reducir el tiempo de vida de cualquier información de DNS almacenada en caché. De esta forma se garantiza que no intente establecer una conexión de lectura/escritura en una instancia de base de datos que deje de estar disponible o sea ahora de solo lectura tras una conmutación por error.

Puntos de enlace del lector

Use el punto de conexión del lector para conexiones de solo lectura al clúster de base de datos Multi-AZ. Dicho punto de conexión ayuda a su clúster de base de datos a manejar una carga de trabajo de consultas intensivas. El punto de conexión del lector es el punto de conexión que proporciona a las aplicaciones que realizan informes u otras operaciones de solo lectura en el clúster. El extremo del lector envía conexiones a las instancias de base de datos de lector disponibles en un clúster de base de datos Multi-AZ.

Cada clúster Multi-AZ tiene un solo punto de conexión del lector integrado, cuyo nombre y otros atributos se administran mediante Amazon RDS. No puede crear, eliminar o modificar este tipo de punto de conexión.

Puntos de conexión de instancia

Cada instancia de base de datos en un clúster de base de datos Multi-AZ tiene su propio punto de conexión de instancia integrado, cuyo nombre y otros atributos administra Amazon RDS. No puede crear, eliminar o modificar este tipo de punto de conexión. Normalmente, con un clúster de base de datos Multi-AZ se utilizan los puntos de conexión del lector y del escritor con más frecuencia que los puntos de conexión de instancia.

En las operaciones diarias, la forma principal de uso de los puntos de conexión de instancia consiste en diagnosticar los problemas de rendimiento o capacidad que afectan a una instancia de base de datos específica de un clúster de base de datos Multi-AZ. Mientras se conecta a una instancia de base de datos específica, puede examinar sus variables de estado, métricas, etc. Hacer esto puede ayudarlo a determinar qué sucede con esa instancia de base de datos que es distinto de lo que ocurre con otras instancias de base de datos del clúster.

Conexiones de alta disponibilidad

Para clústeres de base de datos Multi-AZ en los que la alta disponibilidad es importante, utilice el punto de conexión del escritor para conexiones de lectura y escritura o de uso general, y el punto de conexión del lector para conexiones de solo lectura. Los puntos de enlace del escritor y del lector administran la conmutación por error de instancias de base de datos mejor que los puntos de enlace de instancia. A diferencia de los puntos de enlace de instancia, los puntos de enlace del escritor y del lector cambian automáticamente a qué instancia de base de datos se conectan si una instancia de base de datos del clúster deja de estar disponible.

Si se produce un error en la instancia de base de datos del escritor de un clúster de base de datos, Amazon RDS conmuta por error automáticamente a una nueva instancia de base de datos del escritor. Lo hace al convertir una instancia de base de datos del lector en una nueva instancia de base de datos del escritor. Si se produce una conmutación por error, puede usar el punto de conexión del escritor para volver a conectarse a la instancia de base de datos recién promovida. O bien puede usar el punto de conexión del lector para volver a conectarse a una de las instancias de base de datos en el lector del clúster de base de datos. Durante una conmutación por error, el punto de conexión del lector podría dirigir las conexiones a la nueva instancia de base de datos del escritor de un clúster de base de datos durante un breve periodo, tras convertir una instancia de base de datos del lector en la nueva instancia de base de datos del escritor. Si diseña su propia lógica de aplicación para administrar conexiones a puntos de conexión de instancia, puede, manualmente o mediante programación, encontrar el conjunto resultante de instancias de base de datos disponibles en el clúster de base de datos.

Conexión a clústeres de bases de datos multi-AZ con los controladores de AWS para Amazon RDS

El conjunto de controladores de AWS se ha diseñado para permitir tiempos de transición y conmutación por error más rápidos y autenticarse con AWS Secrets Manager, AWS Identity and Access Management (IAM) e identidad federada. Los controladores de AWS se basan en la supervisión del estado del clúster de base de datos y en el conocimiento de la topología del clúster para determinar quién es el nuevo escritor. Este enfoque reduce los tiempos de transición y conmutación por error a segundos de un solo dígito, en comparación con las decenas de segundos de los controladores de código abierto.

A medida que se introducen nuevas características de servicio, el objetivo del conjunto de controladores de AWS es contar con soporte integrado para estas características de servicio.

Conexión a clústeres de bases de datos Multi-AZ con el controlador JDBC de Amazon Web Services (AWS)

El controlador JDBC de Amazon Web Services (AWS) se ha diseñado como un contenedor JDBC avanzado para ayudar a las aplicaciones a aprovechar las características de las bases de datos agrupadas en clústeres. Este contenedor complementa y amplía la funcionalidad del controlador JDBC existente. El controlador se admite con los siguientes controladores de la comunidad:

- MySQL Connector/J
- MariaDB Connector/J
- pgJDBC

Para instalar el controlador JDBC de AWS, añada el archivo .jar del controlador JDBC de AWS (ubicado en la aplicación `CLASSPATH`) y conserve las referencias al controlador de la comunidad correspondiente. Actualice el prefijo de la URL de conexión correspondiente de la siguiente manera:

- De `jdbc:mysql://` a `jdbc:aws-wrapper:mysql://`
- De `jdbc:mariadb://` a `jdbc:aws-wrapper:mariadb://`
- De `jdbc:postgresql://` a `jdbc:aws-wrapper:postgresql://`

Para obtener más información sobre el controlador JDBC de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador JDBC de Amazon Web Services (AWS).

Conexión a clústeres de bases de datos Multi-AZ con el controlador de Python de Amazon Web Services (AWS)

El controlador de Python de Amazon Web Services (AWS) se ha diseñado como un contenedor de Python avanzado. Este contenedor complementa y amplía la funcionalidad del controlador de Psycopg de código abierto. El controlador de Python de AWS se admite con las versiones 3.8 y posteriores de Python. Puede instalar el paquete de `aws-advanced-python-wrapper` mediante el comando `pip`, junto con los paquetes de código abierto de `psycopg`.

Para obtener más información sobre el controlador de Python de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador de Python de Amazon Web Services (AWS).

Conexión automática de un recurso de computación de AWS y un clúster de base de datos multi-AZ para Amazon RDS

Puede conectar automáticamente un clúster de base de datos Multi-AZ y recursos de computación de AWS, como instancias de Amazon Elastic Compute Cloud (Amazon EC2) y funciones de AWS Lambda.

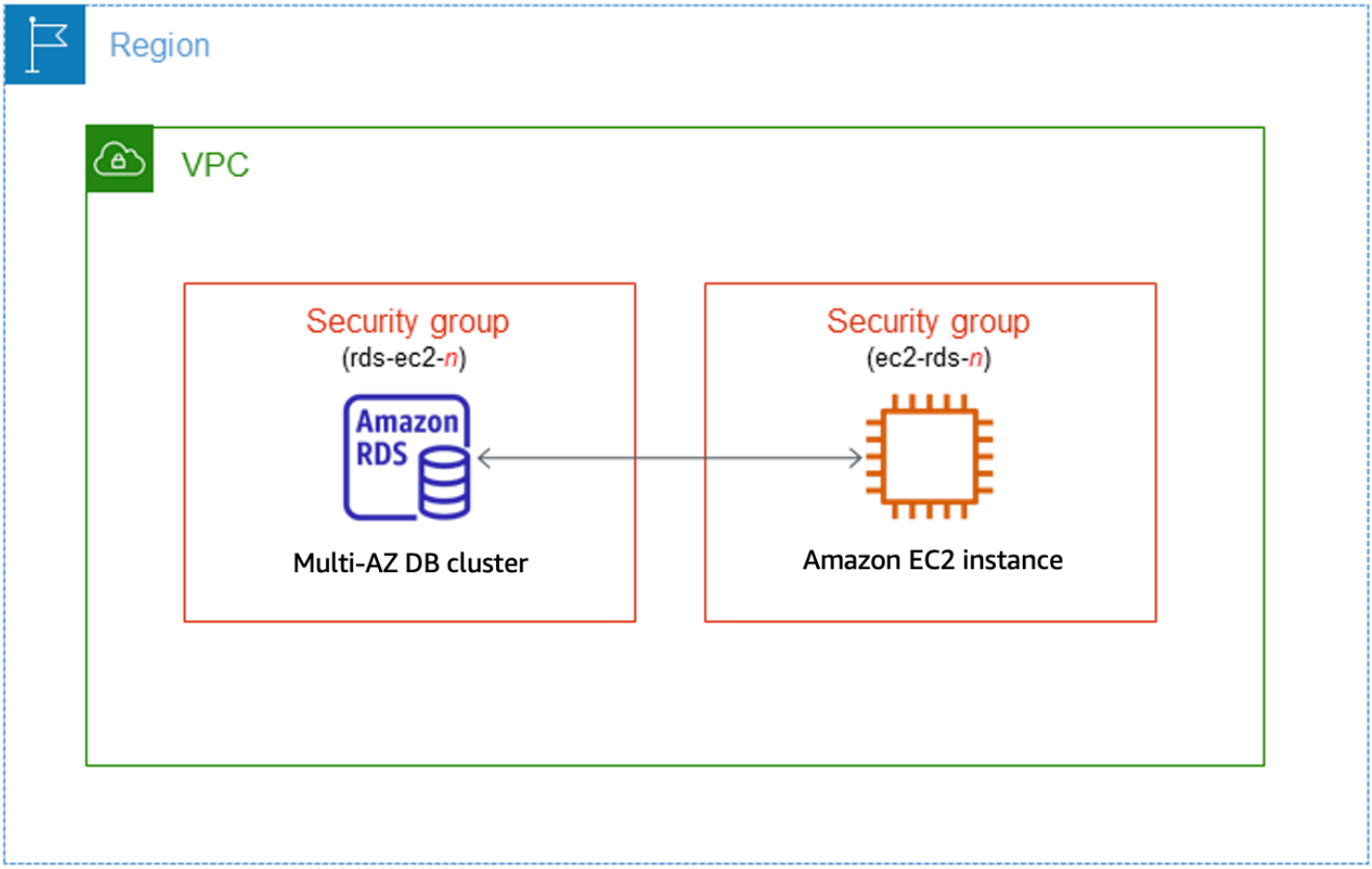
En los temas siguientes, se proporcionan instrucciones detalladas para configurar los ajustes de red, los grupos de seguridad y los parámetros de conexión con el fin de establecer conexiones fiables con las instancias de base de datos de Amazon RDS dentro de una implementación de clúster de base de datos multi-AZ. Se centran en optimizar la conectividad y el rendimiento de la red para las aplicaciones que interactúan con un clúster de base de datos multi-AZ, lo que garantiza operaciones de datos seguras y eficaces.

Temas

- Conexión automática de una instancia de EC2 con un clúster de base de datos Multi-AZ
- Conexión automática de una función de Lambda y un clúster de base de datos Multi-AZ

Conexión automática de una instancia de EC2 con un clúster de base de datos Multi-AZ

Puede utilizar la consola de Amazon RDS para simplificar la configuración de una conexión entre una instancia de Amazon Elastic Compute Cloud (Amazon EC2) y un clúster de base de datos Multi-AZ. Con frecuencia, el clúster de base de datos multi-AZ se encuentra en una subred privada y la instancia de EC2 en una subred pública dentro de una VPC. Puede usar un cliente SQL en su instancia de EC2 para conectarse al clúster de base de datos multi-AZ. La instancia de EC2 también puede ejecutar servidores web o aplicaciones que accedan al clúster de base de datos multi-AZ privado.



Si desea conectarse a una instancia de EC2 que no está en la misma VPC que el clúster de base de datos Multi-AZ, consulte los escenarios en the section called “Escenarios de acceso a una instancia de base de datos en una VPC”.

Temas

- Descripción general de la conectividad automática con una instancia de EC2
- Conexión de una instancia de EC2 con un clúster de base de datos Multi-AZ de forma automática
- Visualización de los recursos de computación conectados

Descripción general de la conectividad automática con una instancia de EC2

Cuando se configura una conexión entre una instancia de EC2 y un clúster de base de datos Multi-AZ automáticamente, Amazon RDS configura el grupo de seguridad de la VPC para su instancia de EC2 y su clúster de base de datos.

Estos son los requisitos para conectar una instancia de EC2 al clúster de base de datos Multi-AZ:

- La instancia de EC2 debe existir en la misma VPC que el clúster de base de datos Multi-AZ.

  Si no existen instancias de EC2 en la misma VPC, la consola proporciona un enlace para crear una.

- El usuario que configura la conectividad debe tener permisos para realizar las siguientes operaciones de EC2:
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeSecurityGroups`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Cuando se establece una conexión con una instancia de EC2, Amazon RDS realiza una acción basada en la configuración actual de los grupos de seguridad asociados al clúster de base de datos Multi-AZ y la instancia de EC2, como se describe en la siguiente tabla.

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n* (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo	Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `rds-ec2-`*n* (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de la VPC del	Amazon RDS no realiza ninguna acción. Ya se configuró automátic amente una conexión entre la instancia de EC2 y el clúster de base de datos Multi-AZ. Como ya existe una conexión entre la instancia de EC2 y la base de datos de RDS, los grupos de seguridad no se modifican.

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
de seguridad de VPC de la instancia de EC2 como origen.	clúster de base de datos Multi-AZ como origen.	

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Se aplica alguna de las siguientes condiciones: • Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n*. • Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n*. Sin embargo, ninguno de estos grupos de seguridad se puede usar para la conexión con la instancia de EC2. Un grupo de seguridad no se puede usar si no tiene una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen. Tampoco se puede usar un grupo de seguridad si se ha modificado. Los ejemplos de modificaciones incluyen agregar una regla o cambiar el puerto de una regla existente.	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la instancia de EC2 con un nombre que coincida con el patrón `ec2-rds-`*n*. • Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `ec2-rds-`*n*. Sin embargo, ninguno de estos grupos de seguridad se puede usar para la conexión con el clúster de base de datos Multi-AZ. Un grupo de seguridad no se puede usar si no tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ como origen. Tampoco se puede usar un grupo de seguridad si se ha modificado.	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen.	Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `ec2-rds-`*n*. Sin embargo, ninguno de estos grupos de seguridad se puede usar para la conexión con el clúster de base de datos Multi-AZ. Un grupo de seguridad no se puede usar si no tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ como origen. Tampoco se puede usar un grupo de seguridad si se ha modificado.	RDS action: create new security groups
Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen.	Existe un grupo de seguridad de EC2 válido para la conexión, pero no está asociado a la instancia de EC2. Este grupo de seguridad tiene un nombre que coincide con el patrón `rds-ec2-`*n*. No se ha modificado. Solo tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ como origen.	RDS action: associate EC2 security group

Configuración del grupo de seguridad de RDS actual	Configuración del grupo de seguridad de EC2 actual	Acción de RDS
Se aplica alguna de las siguientes condiciones: • Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n*. • Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-ec2-`*n*. Sin embargo, ninguno de estos grupos de seguridad se puede usar para la conexión con la instancia de EC2. Un grupo de seguridad no se puede usar si no tiene una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen. Tampoco se puede usar un grupo de seguridad si se ha modificado.	Hay uno o más grupos de seguridad asociados a la instancia de EC2 con un nombre que coincide con el patrón `rds-ec2-`*n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ como origen.	RDS action: create new security groups

Acción de RDS de: crear nuevos grupos de seguridad

Amazon RDS realiza las siguientes acciones:

- Crea un nuevo grupo de seguridad que coincide con el patrón `rds-ec2-`*n*. Este grupo de seguridad tiene una regla de entrada con el grupo de seguridad de VPC de la instancia de EC2 como origen. Este grupo de seguridad está asociado al clúster de base de datos Multi-AZ y permite que la instancia de EC2 acceda al clúster de base de datos Multi-AZ.
- Crea un nuevo grupo de seguridad que coincide con el patrón `ec2-rds-`*n*. Este grupo de seguridad tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ como origen. Este grupo de seguridad está asociado a la instancia de EC2 y permite que la instancia de EC2 envíe tráfico al clúster de base de datos Multi-AZ.

Acción de RDS de: asociar un grupo de seguridad EC2

Amazon RDS asocia el grupo de seguridad de EC2 válido y existente con la instancia de EC2. Este grupo de seguridad permite que la instancia de EC2 envíe tráfico al clúster de base de datos Multi-AZ.

Conexión de una instancia de EC2 con un clúster de base de datos Multi-AZ de forma automática

Antes de configurar una conexión entre una instancia de EC2 y una base de datos de RDS, asegúrese de cumplir con los requisitos descritos en Descripción general de la conectividad automática con una instancia de EC2.

Si realiza cambios en los grupos de seguridad después de configurar la conectividad, los cambios pueden afectar a la conexión entre la instancia de EC2 y la base de datos RDS.

> **Note**
>
> Solo puede configurar automáticamente una conexión entre una instancia de EC2 y una base de datos de RDS automáticamente utilizando la AWS Management Console. No puede configurar una conexión automáticamente con la AWS CLI o la API de RDS.

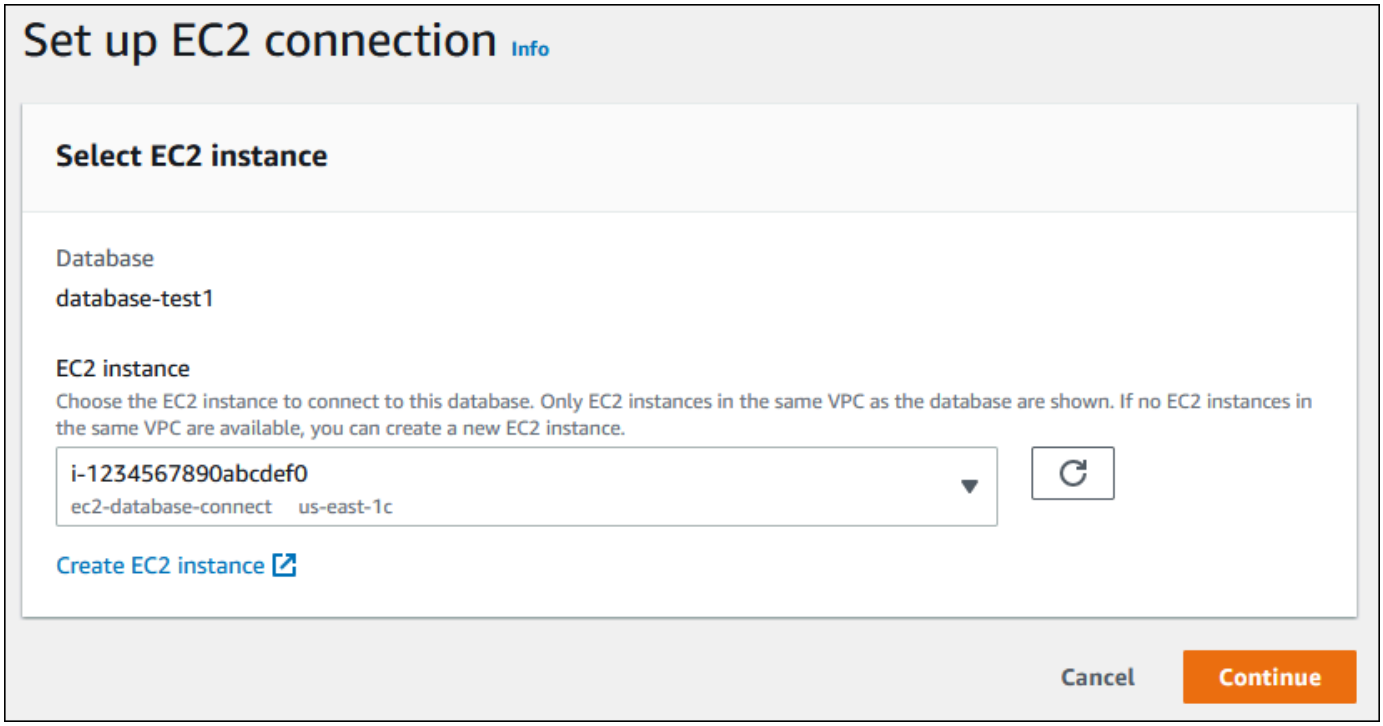
Para conectar automáticamente de una instancia de EC2 y una base de datos de RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, luego, la instancia de base de datos.

3. En Acciones, elija Configurar conexión de EC2.

   Aparece la página Set up EC2 connection Configurar conexión de EC2).

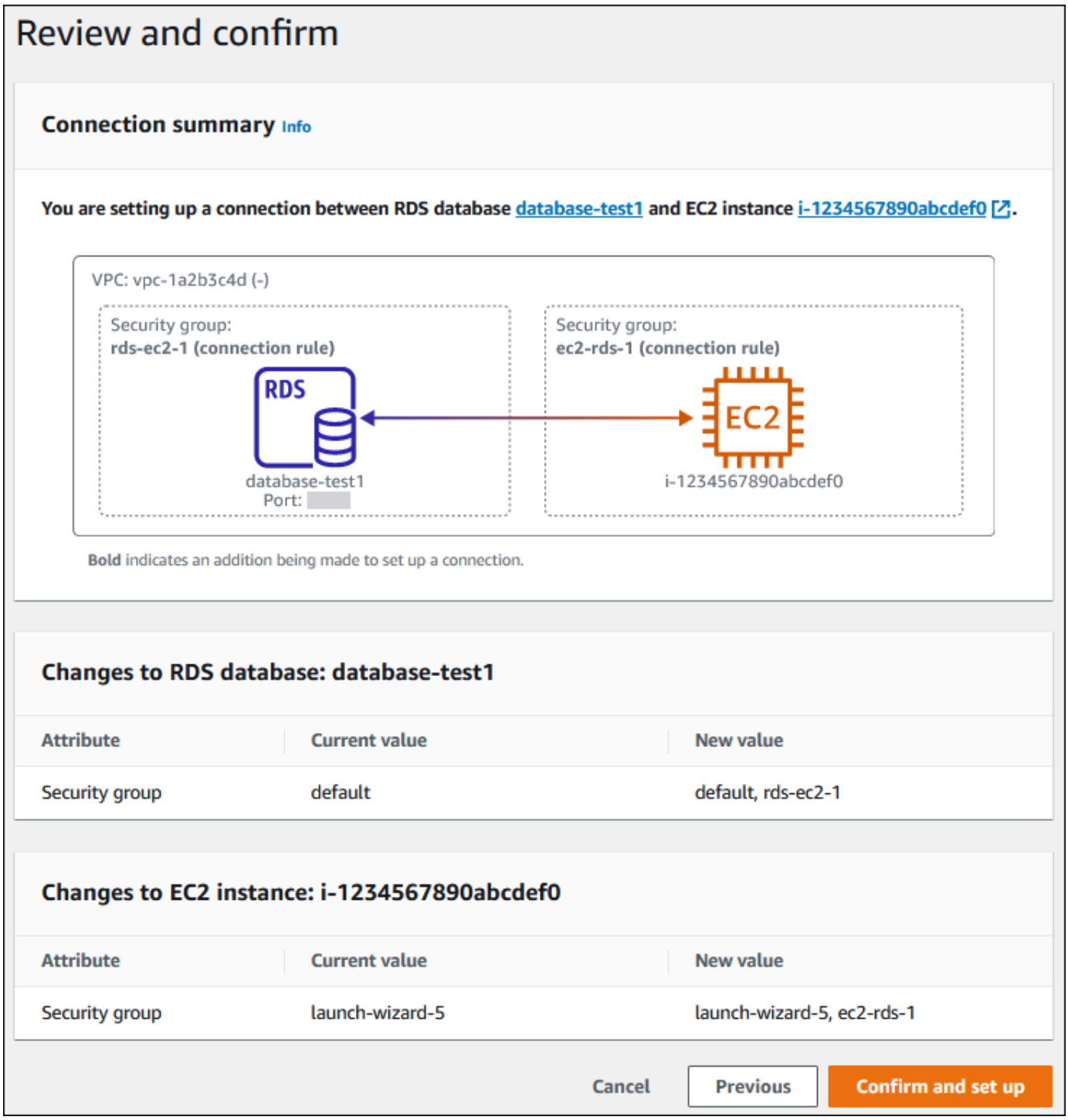
4. En la página Set up EC2 connection (Configurar conexión de EC2), elija la instancia de EC2.



   Si no existen instancias de EC2 en la misma VPC, elija Create EC2 instance (Crear instancia de EC2) para crear una. En este caso, asegúrese de que la nueva instancia de EC2 esté en la misma VPC que la base de datos de RDS.

5. Elija Continuar.

   Aparece la página Review and confirm (Revisar y confirmar).



6. En la página Review and confirm (Revisar y confirmar), revise los cambios que realizará RDS para configurar la conectividad con la instancia de EC2.

   Si los cambios son correctos, seleccione Confirmar y configurar.

   Si los cambios no son correctos, seleccione Previous (Anterior) o Cancel (Cancelar).

Visualización de los recursos de computación conectados

Puede utilizar la AWS Management Console para ver los recursos de computación que están conectados a una base de datos RDS. Los recursos que se muestran incluyen conexiones de recursos informáticos que se configuraron automáticamente. Puede definir la conectividad con los recursos informáticos de manera automática de las siguientes maneras:

- Puede seleccionar el recurso informático al crear la base de datos.

  Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS y Creación de un clúster de base de datos multi-AZ para Amazon RDS.
- Puede configurar la conectividad entre una base de datos existente y un recurso informático.

  Para obtener más información, consulte Conexión automática de una instancia de EC2 y una base de datos de RDS.

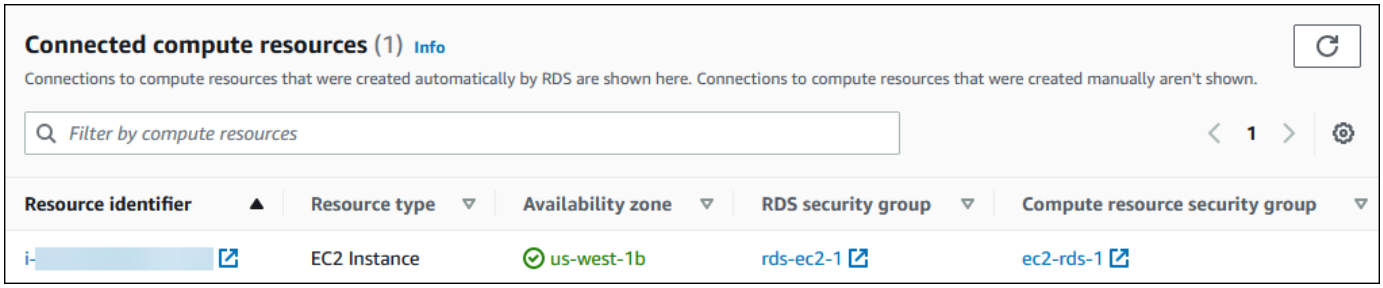
Los recursos informáticos de la lista no incluyen los que se conectaron a la base de datos manualmente. Por ejemplo, puede permitir que un recurso informático acceda a una base de datos manualmente añadiendo una regla al grupo de seguridad de la VPC asociado a la base de datos.

Para que un recurso informático coincida, se deben cumplir las siguientes condiciones:

- El nombre del grupo de seguridad asociado al recurso informático coincide con el patrón `ec2-rds-`*n* (donde *n* es un número).
- El grupo de seguridad asociado al recurso de computación tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por la base de datos RDS.
- El grupo de seguridad asociado al recurso informático tiene una regla de salida en la que el origen está establecido en un grupo de seguridad asociado a la base de datos RDS.
- El nombre del grupo de seguridad asociados a la base de datos de RDS coincide con el patrón `rds-ec2-`*n* (donde *n* es un número).
- El grupo de seguridad asociado a la base de datos de RDS tiene una regla de entrada con el rango de puertos establecido en el puerto utilizado por la base de datos de RDS.
- El grupo de seguridad asociado a la base de datos de RDS tiene una regla de entrada con el origen establecido en un grupo de seguridad asociado al recurso informático.

Para ver los recursos de computación conectados a una base de datos de RDS

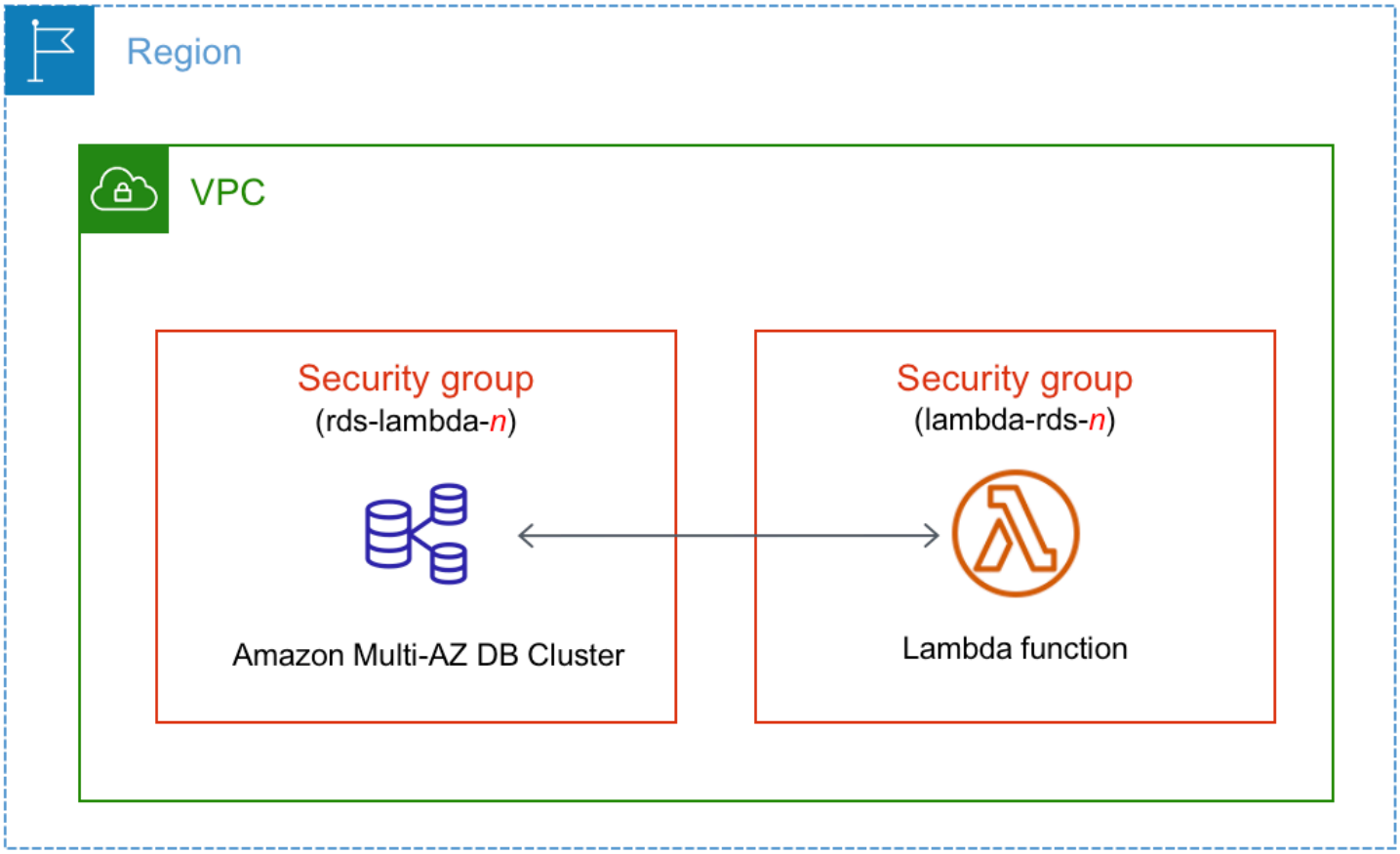
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, luego, el nombre de la instancia de base de datos.
3. En la pestaña Connectivity & security (Conectividad y seguridad), consulte los recursos informáticos en Connected compute resources (Recursos informáticos conectados).



Conexión automática de una función de Lambda y un clúster de base de datos Multi-AZ

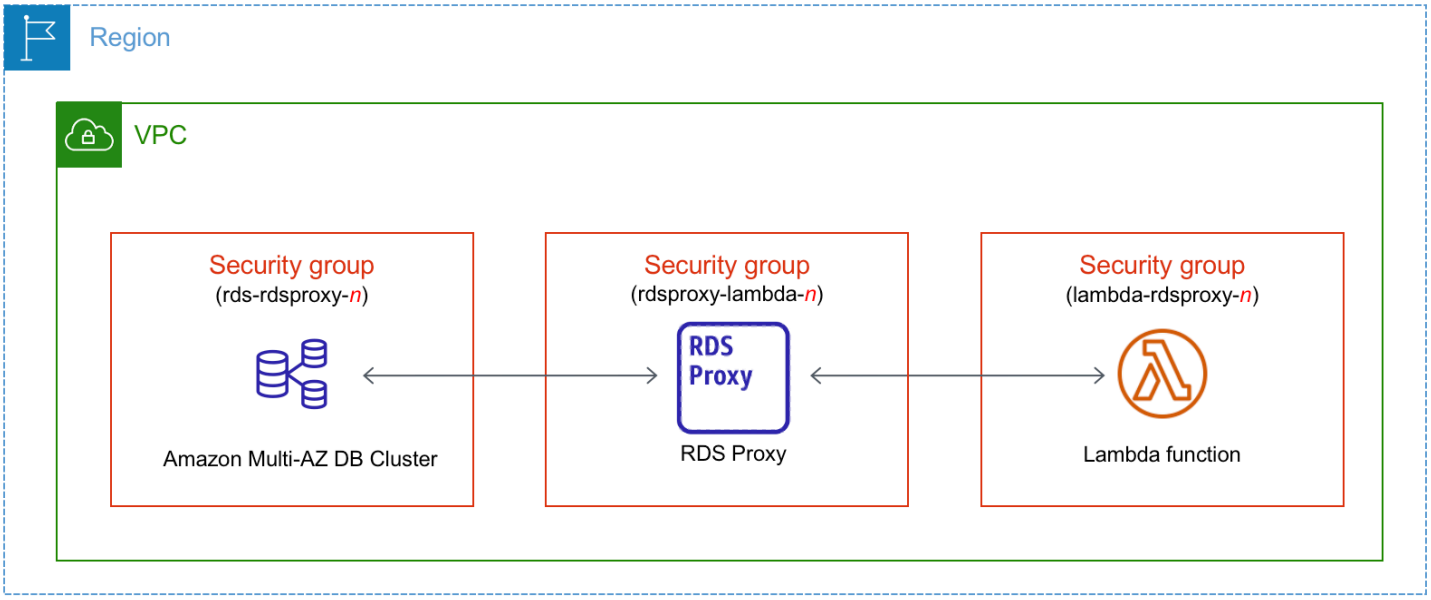
Puede utilizar la consola de RDS para simplificar la configuración de una conexión entre una función de Lambda y un clúster de base de datos Multi-AZ. Puede utilizar la consola de RDS para simplificar la configuración de una conexión entre una función de Lambda y un clúster de base de datos Multi-AZ. A menudo, el clúster de base de datos Multi-AZ se encuentra en una subred privada dentro de una VPC. Las aplicaciones pueden utilizar la función de Lambda para acceder a su clúster de base de datos Multi-AZ privado.

La siguiente imagen muestra una conexión directa entre su clúster de base de datos Multi-AZ y su función de Lambda.



Puede configurar la conexión entre la función de Lambda y su base de datos a través de RDS Proxy para mejorar el rendimiento y la resiliencia de la base de datos. A menudo, las funciones de Lambda hacen frecuentes conexiones cortas a la base de datos que aprovechan el grupo de conexiones que ofrece RDS Proxy. Puede aprovechar cualquier autenticación de IAM que ya tenga para las funciones de Lambda, en lugar de administrar las credenciales de la base de datos en el código de la aplicación de Lambda. Para obtener más información, consulte Amazon RDS Proxy .

Puede utilizar la consola para crear automáticamente un proxy para su conexión. También puede seleccionar los proxies existentes. La consola actualiza el grupo de seguridad del proxy para permitir las conexiones entre la base de datos y la función de Lambda. Puede introducir las credenciales de la base de datos o seleccionar el secreto de Secrets Manager que necesita para acceder a la base de datos.



Temas

- Información general de la conectividad automática con una función de Lambda
- Conexión automática de una función de Lambda y un clúster de base de datos Multi-AZ
- Visualización de los recursos de computación conectados

Información general de la conectividad automática con una función de Lambda

Cuando se configura una conexión entre una función de Lambda y un clúster de base de datos Multi-AZ automáticamente, Amazon RDS configura el grupo de seguridad de la VPC para su función de Lambda y su clúster de base de datos.

Estos son los requisitos para conectar una función de Lambda a un clúster de base de datos Multi-AZ:

- La función de Lambda debe encontrarse en la misma VPC que el clúster de base de datos Multi-AZ.

  Si no existen funciones de Lambda en la misma VPC, la consola proporciona un enlace para crear una.
- El usuario que configure la conectividad debe tener permisos para realizar las siguientes operaciones de Amazon RDS, Amazon EC2, Lambda, Secrets Manager e IAM:
  - Amazon RDS
    - `rds:CreateDBProxies`

  - `rds:DescribeDBInstances`
  - `rds:DescribeDBProxies`
  - `rds:ModifyDBInstance`
  - `rds:ModifyDBProxy`
  - `rds:RegisterProxyTargets`
- Amazon EC2
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:AuthorizeSecurityGroupIngress`
  - `ec2:CreateSecurityGroup`
  - `ec2:DeleteSecurityGroup`
  - `ec2:DescribeSecurityGroups`
  - `ec2:RevokeSecurityGroupEgress`
  - `ec2:RevokeSecurityGroupIngress`
- Lambda
  - `lambda:CreateFunctions`
  - `lambda:ListFunctions`
  - `lambda:UpdateFunctionConfiguration`
- Secrets Manager
  - `sercetsmanager:CreateSecret`
  - `secretsmanager:DescribeSecret`
- IAM
  - `iam:AttachPolicy`
  - `iam:CreateRole`
  - `iam:CreatePolicy`
- AWS KMS
  - `kms:describeKey`

Cuando se configura una conexión entre una función de Lambda y un clúster de base de datos Multi-AZ, Amazon RDS configura el grupo de seguridad de la VPC para su función y su clúster de base de datos Multi-AZ. Si usa RDS Proxy, Amazon RDS también configura el grupo de seguridad de la VPC para el proxy. Amazon RDS realiza una acción de acuerdo con la configuración actual de los grupos

de seguridad asociados al clúster de base de datos Multi-AZ, la función de Lambda y el proxy, tal como se describe en la siguiente tabla.

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Amazon RDS no toma ninguna medida porque los grupos de seguridad de todos los recursos siguen el patrón de nomenclatura correcto y tienen las reglas de entrada y salida correctas.	Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-lambda-` *n* (donde *n* es un número) o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen.	Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n* (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida bien con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como destino.	Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con el patrón `rdsproxy-lambda-` *n* (donde *n* es un número). No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene reglas de entrada y salida con los grupos de seguridad de la VPC de la función de Lambda y el clúster de base de datos Multi-AZ.
		Se aplica alguna de las siguientes condiciones:	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado al clúster de base de datos Multi-AZ con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. • Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la función de Lambda con un nombre que coincida con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. • Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con el clúster de base de datos Multi-AZ.	• No hay ningún grupo de seguridad asociado al proxy con un nombre que coincida con el patrón `rdsproxy-lambda-` *n*. • Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con `rdsproxy-lambda-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con el clúster de base de datos Multi-AZ o la función de Lambda. Amazon RDS no puede utilizar un grupo de seguridad	

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la función de Lambda. Amazon RDS no puede usar un grupo de seguridad que no tengan una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificad o. Los ejemplos de modificaciones incluyen agregar una regla o cambiar el puerto de una regla existente.	Amazon RDS no puede usar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	que no tenga reglas de entrada y salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ y la función de Lambda. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE` . No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen.	Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con el clúster de base de datos Multi-AZ. Amazon RDS no puede utilizar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como destino. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con el patrón `rdsproxy-lambda-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con el clúster de base de datos Multi-AZ o la función de Lambda. Amazon RDS no puede utilizar un grupo de seguridad que no tenga reglas de entrada y salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ y la función de Lambda. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene solo una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen.	Existe un grupo de seguridad de Lambda válido para la conexión, pero no está asociado a la función de Lambda. Este grupo de seguridad tiene un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. No se ha modificado. Solo tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como destino.	Existe un grupo de seguridad del proxy válido para la conexión, pero no está asociado al proxy. Este grupo de seguridad tiene un nombre que coincide con el patrón `rdsproxy-lambda-` *n*. No se ha modificado. Este grupo de seguridad tiene reglas de entrada y salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ y la función de Lambda.	RDS action: associate Lambda security group

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado al clúster de base de datos Multi-AZ con un nombre que coincida con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado es `AVAILABLE`. • Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-lambda-` *n* o si el valor de `TargetHealth` de un proxy asociado	Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad solo tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como destino.	Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con el patrón `rdsproxy-lambda-` *n*. No se ha modificado ningún grupo de seguridad que coincida con el patrón. Este grupo de seguridad tiene reglas de entrada y salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ y la función de Lambda.	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
es `AVAILABLE`. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con la función de Lambda o el proxy. Amazon RDS no puede usar un grupo de seguridad que no tengan una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.			

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
Hay uno o más grupos de seguridad asociados al clúster de base de datos Multi-AZ con un nombre que coincide con el patrón `rds-rdsproxy-` *n* (donde *n* es un número).	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado a la función de Lambda con un nombre que coincida con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. • Hay uno o más grupos de seguridad asociados a la función de Lambda con un nombre que coincide con el patrón `lambda-rds-` *n* o `lambda-rdsproxy-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con el clúster de base de datos Multi-AZ.	Se aplica alguna de las siguientes condiciones: • No hay ningún grupo de seguridad asociado al proxy con un nombre que coincida con el patrón `rdsproxy-lambda-` *n*. • Hay uno o más grupos de seguridad asociados al proxy con un nombre que coincide con `rdsproxy-lambda-` *n*. Sin embargo, Amazon RDS no puede usar ninguno de estos grupos de seguridad para la conexión con el clúster de base de datos Multi-AZ o la función de Lambda. Amazon RDS no puede utilizar un	RDS action: create new security groups

Configuración del grupo de seguridad de RDS actual	Configuración actual del grupo de seguridad de Lambda	Configuración actual del grupo de seguridad del proxy	Acción de RDS
	Amazon RDS no puede utilizar un grupo de seguridad que no tenga una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como destino. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	grupo de seguridad que no tenga reglas de entrada y salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ y la función de Lambda. Amazon RDS tampoco puede usar un grupo de seguridad que se haya modificado.	

Acción de RDS de: crear nuevos grupos de seguridad

Amazon RDS realiza las siguientes acciones:

- Crea un nuevo grupo de seguridad que coincide con el patrón `rds-lambda-`*n*. Este grupo de seguridad tiene una regla de entrada con el grupo de seguridad de la VPC de la función de Lambda o el proxy como origen. Este grupo de seguridad está asociado al clúster de base de datos Multi-AZ y permite que la función o el proxy acceda al clúster de base de datos Multi-AZ.
- Crea un nuevo grupo de seguridad que coincide con el patrón `lambda-rds-`*n*. Este grupo de seguridad tiene una regla de salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ o el proxy como destino. Este grupo de seguridad está asociado a la función de Lambda y permite que la función de Lambda envíe tráfico al clúster de base de datos Multi-AZ o que envíe tráfico a través de un proxy.
- Crea un nuevo grupo de seguridad que coincide con el patrón `rdsproxy-lambda-`*n*. Este grupo de seguridad tiene reglas de entrada y salida con el grupo de seguridad de la VPC del clúster de base de datos Multi-AZ y la función de Lambda.

Acción de RDS de : asociar un grupo de seguridad de Lambda

Amazon RDS asocia el grupo de seguridad de Lambda válido y existente a la función de Lambda. Este grupo de seguridad permite que la función envíe tráfico al clúster de base de datos Multi-AZ o que envíe tráfico a través de un proxy.

Conexión automática de una función de Lambda y un clúster de base de datos Multi-AZ

Puede utilizar la consola de Amazon RDS para conectar automáticamente una función de Lambda a su clúster de base de datos Multi-AZ. Esto simplifica el proceso de establecer una conexión entre estos recursos.

También puede usar RDS Proxy para incluir un proxy en la conexión. Las funciones de Lambda hacen frecuentes conexiones cortas a la base de datos que aprovechan el grupo de conexiones que ofrece RDS Proxy. Puede aprovechar cualquier autenticación de IAM que ya tenga para sus funciones de Lambda, en lugar de administrar las credenciales de la base de datos en el código de la aplicación de Lambda.

Puede conectar un clúster de base de datos Multi-AZ existente a funciones de Lambda nuevas y existentes mediante la página Configurar la conexión de Lambda. El proceso de configuración configura automáticamente los grupos de seguridad necesarios en su nombre.

Antes de configurar una conexión entre una función de Lambda y un clúster de base de datos Multi-AZ, asegúrese de que:

- Su función de Lambda y el clúster de base de datos Multi-AZ estén en la misma VPC.
- Tiene los permisos adecuados para su cuenta de usuario. Para obtener más información acerca de los requisitos, consulte Información general de la conectividad automática con una función de Lambda.

Si realiza cambios en los grupos de seguridad después de configurar la conectividad, los cambios podrían afectar a la conexión entre la función de Lambda y el clúster de base de datos Multi-AZ.

> **Note**
>
> Puede configurar automáticamente una conexión entre el clúster de base de datos Multi-AZ y una función de Lambda solo en la AWS Management Console. Para conectar una función de Lambda, todas las instancias del clúster de base de datos Multi-AZ deben estar en estado Disponible.

Para conectar automáticamente una función de Lambda y un clúster de base de datos Multi-AZ

<result>

Tras confirmar la configuración, Amazon RDS inicia el proceso de conexión de su función de Lambda, RDS Proxy (si ha utilizado un proxy) y clúster de base de datos Multi-AZ. La consola muestra el cuadro de diálogo Detalles de la conexión, que muestra los cambios del grupo de seguridad que permiten las conexiones entre los recursos.
</result>

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, seleccione el clúster de base de datos Multi-AZ que desea conectar a una función de Lambda.
3. En Acciones, elija Configurar la conexión de Lambda.
4. En la página Configurar la conexión de Lambda, en Seleccionar la función de Lambda, realice una de las siguientes acciones:
   - Si ya tiene una función de Lambda en la misma VPC que su clúster de base de datos Multi-AZ, elija Elegir una función existente y, a continuación, seleccione la función.
   - Si no tiene una función de Lambda en la misma VPC, elija Crear función nueva y, a continuación, introduzca un Nombre de la función. El tiempo de ejecución predeterminado está establecido en Nodejs.18. Puede modificar la configuración de la nueva función de Lambda en la consola de Lambda después de completar la configuración de la conexión.
5. (Opcional) En RDS Proxy, seleccione Conexión mediante RDS Proxy y, a continuación, realice una de las siguientes acciones:
   - Si ya tiene un proxy que quiere usar, elija Elegir un proxy existente y, a continuación, elija el proxy.
   - Si no dispone de un proxy y desea que Amazon RDS lo cree automáticamente, elija Crear un proxy nuevo. A continuación, para Credenciales de la base de datos, realice una de las siguientes acciones:

     a. Elija Nombre de usuario y contraseña de la base de datos y, a continuación, introduzca el Nombre de usuario y la Contraseña para su clúster de base de datos Multi-AZ.

     b. Elija Secreto de Secrets Manager. A continuación, para Seleccionar secreto, elija un secreto de AWS Secrets Manager. Si no tiene ningún secreto de Secrets Manager, elija Crear un nuevo secreto de Secrets Manager para crear un nuevo secreto. Después de crear el secreto, en Seleccionar secreto, elija el nuevo secreto.

Después de crear el nuevo proxy, elija Elegir un proxy existente y, a continuación, elija el proxy. Tenga en cuenta que el proxy puede tardar algún tiempo en estar disponible para la conexión.

6. (Opcional) Amplíe Resumen de conexión y verifique las actualizaciones destacadas de sus recursos.
7. Elija Set up (Configurar).

Visualización de los recursos de computación conectados

Puede utilizar la AWS Management Console para ver los recursos de computación que están conectados a su clúster de base de datos Multi-AZ. Los recursos que se muestran incluyen las conexiones de los recursos de computación que Amazon RDS configuró automáticamente.

Los recursos de computación de la lista no incluyen los que se conectan manualmente al clúster de base de datos Multi-AZ. Por ejemplo, para permitir que un recurso de computación acceda manualmente a su clúster de base de datos Multi-AZ puede añadir una regla al grupo de seguridad de la VPC asociado al clúster.

Para que la consola muestre una función de Lambda, se deben cumplir las siguientes condiciones:

- El nombre del grupo de seguridad asociado al recurso de computación coincide con el patrón `lambda-rds-`*n* o `lambda-rdsproxy-`*n* (donde *n* es un número).
- El grupo de seguridad asociado al recurso de computación tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por el clúster de base de datos Multi-AZ o un proxy asociado. El destino de la regla de salida debe establecerse en un grupo de seguridad asociado al clúster de base de datos Multi-AZ o un proxy asociado.
- El nombre del grupo de seguridad adjunto al proxy asociado a la base de datos coincide con el patrón `rds-rdsproxy-`*n* (donde *n* es un número).
- El grupo de seguridad asociado a la función tiene una regla de salida con el rango de puertos establecido en el puerto utilizado por el clúster de base de datos Multi-AZ o un proxy asociado. El destino debe establecerse en un grupo de seguridad asociado al clúster de base de datos Multi-AZ o un proxy asociado.

Para ver los recursos de computación conectados automáticamente un clúster de base de datos Multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija el clúster de base de datos Multi-AZ.
3. En la pestaña Conectividad y seguridad, consulte los recursos de computación en Recursos de computación conectados.

Modificación de un clúster de base de datos multi-AZ para Amazon RDS.

Un clúster de base de datos Multi-AZ tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas de disponibilidad diferentes. Los clústeres de base de datos Multi-AZ proporcionan alta disponibilidad, mayor capacidad para cargas de trabajo de lectura y menor latencia en comparación con las implementaciones Multi-AZ. Para obtener más información acerca de los clústeres de base de datos Multi-AZ, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

Puede modificar un clúster de base de datos Multi-AZ para cambiar su configuración. También puede realizar operaciones en un clúster de base de datos Multi-AZ, como tomar una instantánea del mismo.

> **Important**
>
> No se pueden modificar las instancias de base de datos de un clúster de base de datos multi-AZ. Todas las modificaciones deben realizarse en el clúster de base de datos. La única operación que se puede realizar en una instancia de base de datos de un clúster de base de datos multi-AZ es reiniciarla.

Puede modificar un clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para modificar un clúster de base de datos Multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, elija el clúster de base de datos Multi-AZ que desea modificar.
3. Elija Modify (Modificar). Aparece la página Modify DB clúster (Modificar clúster de base de datos).
4. Cambie los parámetros que desee. Para obtener más información acerca de cada ajuste, consulte Configuración para modificarlos clústeres de base de datos Multi-AZ.
5. Cuando haya realizado todos los cambios que desee, elija Continue y compruebe el resumen de las modificaciones.

6. (Opcional) Seleccione Apply immediately (Aplicar inmediatamente) para aplicar los cambios inmediatamente. Si se selecciona esta opción, puede producirse un tiempo de inactividad en algunos casos. Para obtener más información, consulte Aplicación inmediata de los cambios.
7. En la página de confirmación, revise los cambios. Si son correctos, elija Modify DB cluster (Modificar clúster de base de datos) para guardarlos.

   O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para modificar un clúster de base de datos Multi-AZ mediante la AWS CLI, llame al comando modify-db-cluster. Especifique el identificador del clúster de base de datos y los valores de las opciones que desea modificar. Para obtener más información acerca de cada opción, consulte Configuración para modificarlos clústeres de base de datos Multi-AZ.

Example

El siguiente código modifica `my-multi-az-dbcluster` configurando el período de retención de copia de seguridad en 1 semana (7 días). El código activa la protección de eliminación mediante el uso de `--deletion-protection`. Para desactivar la protección contra la eliminación, utilice `--no-deletion-protection`. Los cambios se aplican durante el siguiente periodo de mantenimiento si se utiliza el parámetro `--no-apply-immediately`. Utilice `--apply-immediately` para aplicar los cambios inmediatamente. Para obtener más información, consulte Aplicación inmediata de los cambios.

Para Linux, macOS o Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier my-multi-az-dbcluster \
    --backup-retention-period 7 \
    --deletion-protection \
    --no-apply-immediately
```

Para Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier my-multi-az-dbcluster ^
    --backup-retention-period 7 ^
    --deletion-protection ^
```

```
    --no-apply-immediately
```

API de RDS

Para modificar un clúster de base de datos Multi-AZ mediante la API de Amazon RDS, llame a la operación ModifyDBCluster. Especifique el identificador del clúster de base de datos y los parámetros de la configuración que desea modificar. Para obtener información acerca de cada parámetro, consulte Configuración para modificarlos clústeres de base de datos Multi-AZ.

Aplicación inmediata de los cambios

Al modificar un clúster de base de datos Multi-AZ, puede aplicar los cambios inmediatamente. Para aplicar los cambios de forma inmediata, seleccione la opción Apply Immediately (Aplicar inmediatamente) en la AWS Management Console. O utilice la opción `--apply-immediately` al llamar a la AWS CLI o establezca el parámetro `ApplyImmediately` en `true` al usar la API de Amazon RDS.

Si decide no aplicar los cambios inmediatamente, estos se colocan en la cola de modificaciones pendientes. Los cambios pendientes en la cola se aplican durante el siguiente periodo de mantenimiento. Si opta por aplicar los cambios inmediatamente, se aplican los nuevos cambios y cualquier cambio de la cola de modificaciones pendientes.

> **Important**
>
> Si alguna de las modificaciones pendientes requiere que clúster de base de datos no esté disponible temporalmente (tiempo de inactividad), la elección de la opción aplicar inmediatamente puede provocar un tiempo de inactividad inesperado.
> Al elegir aplicar un cambio inmediatamente, cualquier modificación pendiente se aplica también inmediatamente, en lugar de durante el siguiente periodo de mantenimiento.
> Si no desea que se aplique un cambio pendiente en el siguiente periodo de mantenimiento, puede modificar la instancia de base de datos para revertir el cambio. Para ello, utilice la AWS CLI y especifique la opción `--apply-immediately`.

Los cambios en algunos ajustes de la base de datos se aplican de inmediato, incluso si elige aplazarlos. Para ver cómo interactúan los distintos ajustes de la base de datos con la configuración de aplicación inmediata, consulte Configuración para modificarlos clústeres de base de datos Multi-AZ.

Configuración para modificarlos clústeres de base de datos Multi-AZ

Para detalles sobre los ajustes de configuración que puede elegir para modificar un clúster de base de datos Multi-AZ, consulte la siguiente tabla. Para obtener más información acerca de las opciones de la AWS CLI, consulte modify-db-cluster. Para obtener más información sobre los parámetros de la API de RDS, consulte ModifyDBCluster.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Allocated storage (Almacenamiento asignado	La cantidad de almacenamiento que se tiene que asignar a la instancia de base de datos en el clúster de base de datos (en gibibytes). Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.	Opción de la CLI:
		`--allocated-storage`
		Parámetro de la API de RDS:
		`AllocatedStorage`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				No se produce un tiempo de inactividad durante este cambio.

Auto minor version upgrade (Actualización automática de	Habilite la actualización automática de versiones secundarias para que el clúster de base de datos reciba actualiza	Opción de la CLI: `--auto-minor-version-upgrade`	El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	Se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

versiones secundarias)	ciones preferidas de la versión secundaria del motor de base de datos automáticamente cuando estén disponibles. Amazon RDS realiza actualizaciones automáticas de versiones secundarias en el periodo de mantenimiento.	`--no-auto-minor-version-upgrade`
		
		Parámetro de la API de RDS:
		
		`AutoMinorVersionUpgrade`		

Backup retention period (Periodo de retención de copia de seguridad)	El número de días que se retienen las copias de seguridad automáticas del clúster de base de datos. El valor debe ser mayor que cero.
	
	Para obtener más información, consulte Introducción a las copias de seguridad.
		Opción de la CLI:
		
		`--backup-retention-period`
		
		Parámetro de la API de RDS:
		
		`BackupRetentionPeriod`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Backup target (Intervalo de copia de seguridad)	Periodo de tiempo durante el cual Amazon RDS lleva a cabo automáticamente una copia de seguridad del clúster de base de datos. A menos que desee hacer una copia de seguridad de la base de datos a una hora determinada, utilice el valor predeterminado No Preference (Sin preferencia).
	
	Para obtener más información, consulte Introducción a las copias de seguridad.
		Opción de la CLI:
		
		`--preferred-backup-window`
		
		Parámetro de la API de RDS:
		
		`PreferredBackupWindow`
			El cambio se aplica de forma asíncrona, tan pronto como sea posible.	No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Certificate authority (Autoridad de certificado)	Entidad de certificación (CA) del certificado de servidor que utiliza el clúster de base de datos.
	
	Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
		Opción de la CLI:
		
		`--ca-certificate-identifier`
		
		Parámetro de la API de RDS:
		
		`CACertificateIdentifier`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				Solo se produce una interrupción si el motor de base de datos no admite la rotación sin reinicio. Puede utilizar el comando de la AWS CLI describe-db-engine-versions para determinar si el motor de base de datos admite la rotación sin reinicio.

Copy tags to snapshot (Copiar etiquetas en instantáneas)	Esta opción copia las etiquetas de los clústeres de base de datos en una instantánea de base de datos cuando se crea una instantánea.
	
	Para obtener más información, consulte Etiquetado de los recursos de y Amazon RDS.
		Opción de la CLI:
		
		`-copy-tags-to-snapshot`
		
		`-no-copy-tags-to-snapshot`
		
		Parámetro de la API de RDS:
		
		`CopyTagsToSnapshot`
			El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
Database authentication (Autenticación de bases de datos)	Para clústeres de base de datos Multi-AZ, solo se admite Password authentication (Autenticación de contraseña).	Ninguna porque la autenticación de contraseña es la predeterminada.	Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente. Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.	No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

DB clúster identifier (Identificador de clúster de base de datos)	Identificador de clúster de base de datos. Este valor se almacena como una cadena en minúsculas.
	
	Al cambiar el identificador del clúster de base de datos, cambia el punto de conexión del clúster de base de datos. Los identificadores y los puntos de conexión de las instancias de base de datos del clúster de base de datos también cambian. El nuevo nombre del clúster de base de datos debe ser único. La longitud máxima es de 63 caracteres.
		Opción de la CLI:
		
		`--new-db-cluster-identifier`
		
		Parámetro de la API de RDS:
		
		`NewDBClusterIdentifier`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
	Los nombres de las instancias de base de datos del clúster de base de datos se cambian para que se correspondan con el nombre nuevo del clúster de base de datos. El nuevo nombre de una instancia de base de datos no puede ser el mismo que el nombre de una instancia de base de datos existente. Por ejemplo, si cambia el nombre del clúster de base de datos a `maz`, puede cambiarse el nombre de una instancia de base de datos a `maz-instance-1`. En este caso, no puede existir ninguna			

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
	instancia de base de datos con el nombre`maz-instance-1` . Para obtener más información, consulte Cambio de nombre de un clúster de base de datos multi-AZ para Amazon RDS.			

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Clase de instancia de clúster	La capacidad de memoria y computación de cada instancia de base de datos en el clúster de base de datos Multi-AZ, por ejemplo, `db.r6gd.xlarge` .
	
	Si es posible, elija una clase de instancia de base de datos lo bastante grande como para albergar en la memoria el conjunto de trabajo de una consulta típica. Cuando los conjuntos de trabajo se albergan en la memoria, el sistema puede evitar escribir en el disco, lo que mejora su rendimiento.
		Opción de la CLI:
		
		`--db-cluster-instance-class`
		
		Parámetro de la API de RDS:
		
		`DBClusterInstanceClass`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				Se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
	Para obtener más información, consulte the section called "Disponibilidad de clase de instancia para los clústeres de base de datos multi-AZ".			

Grupo de parámetros de clúster de base de datos	El grupo de parámetros de clúster de base de datos que desea asociar al clúster de base de datos.
	
	Para obtener más información, consulte Grupos de parámetros para clústeres de base de datos multi-AZ.
		Opción de la CLI:
		
		`--db-cluster-parameter-group-name`
		
		Parámetro de la API de RDS:
		
		`DBClusterParameterGroupName`
			El cambio de grupo de parámetros se produce inmediatamente.	No se produce un tiempo de inactividad durante este cambio. Cuando cambia el grupo de parámetros, los cambios en algunos parámetros se aplican a las instancias de base de datos en el clúster de base de datos Multi-AZ inmediatamente, sin reinicio. Los cambios en otros parámetros se aplican únicamente después de reiniciar las instancias de base de datos.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

DB engine version (Versión del motor de base de datos)	La versión del motor de base de datos que se desea utilizar.	Opción de la CLI:
		`--engine-version`
		Parámetro de la API de RDS:
		`EngineVersion`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				Se produce un tiempo de inactividad durante este cambio.

Deletion protection (Protección contra eliminación)	Seleccione Enable deletion protection (Habilitar la protección contra la eliminación) para evitar que se elimine el clúster de base de datos.
	Para obtener más información, consulte Eliminación de una instancia de base de datos.
		Opción de la CLI:
		`--deletion-protection`
		`--no-deletion-protection`
		Parámetro de la API de RDS:
		`DeletionProtection`
			El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Periodo de mantenimiento	Periodo de 30 minutos durante el cual se aplican las modificaciones pendientes en el clúster de base de datos. Si el periodo de tiempo no es importante, elija No Preference (Sin preferencia).
	
	Para obtener más información, consulte La ventana de mantenimiento de Amazon RDS.
		Opción de la CLI:
		
		`--preferred-maintenance-window`
		
		Parámetro de la API de RDS:
		
		`PreferredMaintenanceWindow`
			El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	Si hay una o varias acciones pendientes que provocan un tiempo de inactividad y el periodo de mantenimiento se cambia para incluir la hora actual, las acciones pendientes se aplican inmediatamente y se produce un tiempo de inactividad.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Gestiona las credenciales maestras en AWS Secrets Manager	Seleccione Manage master credentials in AWS Secrets Manager (Administrar credenciales maestras en AWS Secrets Manager) para administrar la contraseña del usuario maestro en un secreto en Secrets Manager.
	
	De forma opcional, elija la clave KMS para proteger el secreto. Elija entre las claves de KMS de su cuenta o bien introduzca la clave de otra cuenta.
	
	Si Aurora ya administra la contraseña de usuario maestra del clúster de
		Opción de la CLI:
		
		`--manage-master-user-password | --no-manage-master-user-password`
		
		`--master-user-secret-kms-key-id`
		
		`--rotate-master-user-password | --no-rotate-master-user-password`
		
		Parámetro de la API de RDS:
		
		`ManageMasterUserPassword`
		
		`MasterUserSecretKmsKeyId`
		
		`RotateMasterUserPassword`
			Si activa o desactiva la administración automática de contraseñas de usuario maestro, el cambio se produce inmediatamente. Este cambio omite la configuración de aplicación inmediata.
			
			Si va a rotar la contraseña del usuario maestro, debe especificar que el cambio se aplique inmediatamente.
				No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
	base de datos, puede rotar la contraseña del usuario maestro seleccionando Rotate secret immediately (Rotar el secreto inmediatamente). Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.			

New master password (Nueva contraseña maestra)	Contraseña de la cuenta del usuario maestro.	Opción de la CLI:
		
		`--master-user-password`
		
		Parámetro de la API de RDS:
		
		`MasterUserPassword`
			El cambio se aplica de forma asíncrona, tan pronto como sea posible. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Provisioned IOPS (IOPS aprovisionadas)	La cantidad de IOPS aprovisionadas (operaciones de entrada/salida por segundo) asignada inicialmente para el clúster de base de datos.	Opción de la CLI:
		`--iops`
		Parámetro de la API de RDS:
		`Iops`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
Acceso público	Publicly accesible (Accesible públicamente) para proporcionar una dirección IP pública al clúster de base de datos, lo que significa que es accesible desde fuera de su nube virtual privada (VPC). Para que sea accesible públicamente, el clúster de base de datos también debe estar en una subred pública de la VPC. Not publicly accesible (No es accesible públicamente) para que el clúster de base de datos sea accesible solo desde dentro de la VPC.	No está disponible al modificar un clúster de bases de datos.	El cambio se produce inmediatamente. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
	Para obtener más información, consulte Cómo ocultar una instancia de base de datos en una VPC desde Internet.. Para conectarse a un clúster de base de datos desde afuera de su VPC, el clúster de base de datos debe ser accesible públicamente. Además, el acceso debe concederse mediante las reglas entrantes del grupo de seguridad del clúster de base de datos y deben cumplirse otros requisitos. Para obtener más información, consulte No			

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad
	puede conectarse a la instancia de base de datos de Amazon RDS. Si su clúster de base de datos no es accesible públicamente, también puede usar una conexión de AWS Site-to-site VPN o una conexión de AWS Direct Connect para acceder a ella desde una red privada. Para obtener más información, consulte Privacidad del tráfico entre redes.			

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

Storage type (Tipo de almacenamiento)	Tipo de almacenamiento de su clúster de base de datos.
	
	Solo se admite el almacenamiento de uso general (gp3), de IOPS aprovisionadas (io1) y de SSD de IOPS aprovisionadas (io2).
	
	Para obtener más información, consulte Tipos de almacenamiento de Amazon RDS.
		Opción de la CLI:
		
		`--storage-type`
		
		Parámetro de la API de RDS:
		
		`StorageType`
			Si decide aplicar el cambio inmediatamente, surte efecto inmediatamente.
			
			Si no decide aplicar el cambio inmediatamente, surtirá efecto durante la siguiente ventana de mantenimiento.
				No se produce un tiempo de inactividad durante este cambio.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS	Cuándo se produce el cambio	Notas acerca del tiempo de inactividad

VPC security group (Grupo de seguridad de VPC)	Los grupos de seguridad para asociar al clúster de base de datos.
	
	Para obtener más información, consulte Información general de los grupos de seguridad de VPC.
		Opción de la CLI:
		
		`--vpc-security-group-ids`
		
		Parámetro de la API de RDS:
		
		`VpcSecurityGroupIds`
			El cambio se aplica de forma asíncrona, tan pronto como sea posible. Este ajuste omite la configuración de aplicación inmediata.	No se produce un tiempo de inactividad durante este cambio.

Configuración que no se aplica al modificar clústeres de base de datos Multi-AZ

La siguiente configuración del comando AWS CLIde la modify-db-cluster y la operación de la API de RDS ModifyDBCluster no se aplica a clústeres de base de datos Multi-AZ.

Tampoco puede modificar esta configuración para clústeres de base de datos Multi-AZ en la consola.

Configuración de la AWS CLI	Configuración de la API de RDS
`--backtrack-window`	`BacktrackWindow`
`--cloudwatch-logs-export-configuration`	`CloudwatchLogsExportConfiguration`
`--copy-tags-to-snapshot | --no-copy-tags-to-snapshot`	`CopyTagsToSnapshot`
`--db-instance-parameter-group-name`	`DBInstanceParameterGroupName`

Configuración de la AWS CLI	Configuración de la API de RDS
`--domain`	`Domain`
`--domain-iam-role-name`	`DomainIAMRoleName`
`--enable-global-write-forwarding | --no-enable-global-write-forwarding`	`EnableGlobalWriteForwarding`
`--enable-http-endpoint | --no-enable-http-endpoint`	`EnableHttpEndpoint`
`--option-group-name`	`OptionGroupName`
`--port`	`Port`
`--scaling-configuration`	`ScalingConfiguration`
`--storage-type`	`StorageType`

Actualización de la versión del motor de un clúster de base de datos multi-AZ para Amazon RDS

Amazon RDS proporciona versiones más recientes de cada motor de base de datos admitido para que pueda mantener actualizado su clúster de base de datos multi-AZ. En este tema se explica el proceso de actualización de un clúster de base de datos multi-AZ a versiones más recientes.

La actualización de un clúster de base de datos multi-AZ implica seleccionar una nueva versión de motor compatible y planificar un posible tiempo de inactividad. El proceso garantiza una interrupción mínima al utilizar las capacidades de conmutación por error de la arquitectura multi-AZ. Durante la actualización, primero se actualiza la instancia principal y, a continuación, se realiza una conmutación por error en la instancia en espera para mantener la disponibilidad. Entre las prácticas recomendadas, se incluyen realizar actualizaciones durante los períodos de poco tráfico, realizar pruebas en entornos que no son de producción y verificar la compatibilidad de las aplicaciones con la nueva versión.

Temas

- Actualizaciones de la versión secundaria
- Actualizaciones de la versión principal
- Actualización de un clúster de base de datos multi-AZ
- Actualización de réplicas de lectura de clústeres de base de datos Multi-AZ

Actualizaciones de la versión secundaria

Una actualización de una versión secundaria solo incluye cambios compatibles con las versiones anteriores de las aplicaciones existentes. Cuando se inicia una actualización de una versión secundaria, Amazon RDS actualiza primero las instancias de base de datos del lector de una en una. A continuación, una de las instancias de base de datos de lector pasa a ser la nueva instancia de base de datos de escritor. Amazon RDS actualiza luego la antigua instancia de escritor (que ahora es una instancia de lector).

El tiempo de inactividad durante la actualización se limita al tiempo que tarda una de las instancias de base de datos de lector en convertirse en la nueva instancia de base de datos de escritor. Este tiempo de inactividad actúa como una conmutación por error automática. Para obtener más información, consulte the section called “Conmutación por error de un clúster de base de datos multi-AZ”. Tenga en cuenta que el retardo de la réplica de su clúster de base de datos multi-AZ puede

afectar al tiempo de inactividad. Para obtener más información, consulte the section called “Retraso de réplica y clústeres de base de datos Multi-AZ”.

En las réplicas de lectura del clúster de base de datos multi-AZ de RDS para PostgreSQL, Amazon RDS actualiza las instancias miembros del clúster de una en una. Los roles del clúster de lector y escritor no cambian durante la actualización. Por lo tanto, es posible que su clúster de base de datos experimente un tiempo de inactividad mientras Amazon RDS actualiza la instancia de escritor del clúster.

> **Note**
>
> El tiempo de inactividad de una actualización de la versión secundaria de un clúster de base de datos multi-AZ suele ser de 35 segundos. Cuando se utilizan con RDS Proxy, se puede reducir aún más el tiempo de inactividad a un segundo o menos. Para obtener más información, consulte Amazon RDS Proxy. Otra opción, puede utilizar un proxy de base de datos de código abierto como ProxySQL, PgBouncer o el controlador de contenedor JDBC avanzado de AWS.

Actualizaciones de la versión principal

Una actualización de versión principal puede introducir cambios que no sean compatibles con las aplicaciones existentes.

Cuando se inicia una actualización de la versión principal de un clúster de bases de datos Multi-AZ de RDS for PostgreSQL, Amazon RDS actualiza simultáneamente las instancias de lector y escritor. Por lo tanto, es posible que su clúster de bases de datos no esté disponible hasta que se complete la actualización.

Cuando se actualiza la versión principal de un clúster de base de datos multi-AZ de RDS para MySQL, Amazon RDS actualiza las instancias miembros del clúster una por una, de modo que la replicación se produce de una versión de motor inferior a una superior. Es importante asegurarse de que la carga de trabajo sea compatible con las versiones del motor de origen y de destino durante la actualización de una versión principal, ya que las versiones del motor pueden diferir en cuanto a la sintaxis y las características.

> **Note**
>
> Al igual que las actualizaciones de las versiones secundarias, el tiempo de inactividad de una actualización de la versión principal de RDS para MySQL suele ser de 35 segundos. Cuando se utilizan con RDS Proxy, se puede reducir aún más el tiempo de inactividad a un segundo o menos. Para obtener más información, consulte Amazon RDS Proxy.

Actualización de un clúster de base de datos multi-AZ

El proceso de actualización de la versión del motor de un clúster de base de datos Multi-AZ es el mismo que el proceso de actualización de una versión del motor de instancia de base de datos. Para obtener instrucciones, consulte the section called “Actualización de la versión del motor”. La única diferencia es que cuando se utiliza la AWS Command Line Interface (AWS CLI), se usa el comando modify-db-cluster y se especifica el parámetro `--db-cluster-identifier` (así como el parámetro `--allow-major-version-upgrade`).

Para obtener más información acerca de las actualizaciones de las versiones principales y secundarias, consulte la documentación del motor de base de datos que se indica a continuación:

- the section called “Actualizaciones del motor de base de datos de PostgreSQL”
- the section called “Actualizaciones del motor de base de datos de MySQL”

Actualización de réplicas de lectura de clústeres de base de datos Multi-AZ

Amazon RDS no actualiza réplicas de lectura de clústeres de base de datos Multi-AZ. En el caso de actualizaciones de versiones secundarias, primero debe actualizar manualmente todas las réplicas de lectura y, a continuación, actualizar el clúster. De lo contrario, la actualización se bloquea. Al actualizar la versión principal de un clúster, el estado de replicación de las réplicas de lectura cambia a terminado. Debe eliminar y volver a crear manualmente las réplicas de lectura una vez finalizada la actualización. Para obtener más información, consulte the section called “Monitoreo de la replicación de lectura”.

Cambio de nombre de un clúster de base de datos multi-AZ para Amazon RDS

Puede cambiar el nombre de un clúster de base de datos Multi-AZ mediante la AWS Management Console, el comando `modify-db-cluster` de la AWS CLI o la operación `ModifyDBCluster` de la API de Amazon RDS. El cambio de nombre de un clúster de base de datos Multi-AZ puede tener efectos significativos. A continuación, se muestra una lista de consideraciones a tener en cuenta antes de cambiar el nombre de un clúster de base de datos Multi-AZ.

- Al cambiar el nombre de un clúster de base de datos Multi-AZ, también cambian los puntos de conexión del clúster de base de datos Multi-AZ. Estos puntos de conexión cambian porque incluyen el nombre asignado al clúster de base de datos Multi-AZ. Puede redirigir el tráfico de un punto de conexión antiguo a uno nuevo. Para obtener más información acerca de los punto de conexión de los clústeres de base de datos Multi-AZ, consulte Conexión a un clúster de base de datos multi-AZ para Amazon RDS.
- Si cambia el nombre de un clúster de base de datos Multi-AZ, el nombre de DNS anterior que utilizaba el clúster se elimina, si bien puede quedar almacenado en la caché durante varios minutos. El nuevo nombre de DNS del clúster de base de datos Multi-AZ renombrado se hace efectivo, aproximadamente, a los dos minutos. El clúster de base de datos Multi-AZ renombrado estará disponible una vez que se haga efectivo el nombre nuevo.
- No puede usar un nombre de clúster de base de datos Multi-AZ existente al cambiar el nombre de un clúster.
- Las métricas y los eventos asociados con el nombre de un clúster de base de datos se mantienen si reutiliza un nombre de clúster de base de datos.
- Las etiquetas de clúster de base de datos Multi-AZ permanecen en el clúster de base de datos Multi-AZ, independientemente del cambio de nombre.
- Las instantáneas del clúster de base de datos se conservan para un clúster de base de datos Multi-AZ renombrado.

> **Note**
>
> Un clúster de base de datos Multi-AZ es un entorno de base de datos aislado que se ejecuta en la nube. Un clúster de base de datos Multi-AZ puede alojar varias bases de datos. Para obtener información sobre cómo cambiar el nombre de una base de datos, consulte la documentación de su motor de base de datos.

Cambio de nombre para sustituir un clúster de base de datos Multi-AZ existente

Los escenarios más habituales por los que se cambia el nombre de un clúster de base de datos Multi-AZ incluyen la restauración de datos a partir de una instantánea de un clúster de base de datos o realizar una restauración en un momento dado (PITR, por sus siglas en inglés). Al cambiar el nombre del clúster de base de datos Multi-AZ, puede reemplazar el clúster de base de datos Multi-AZ sin cambiar ningún código de aplicación que haga referencia al clúster de base de datos Multi-AZ. En estos casos, complete los siguientes pasos:

1. Detenga todo el tráfico que va hacia el clúster de base de datos Multi-AZ. Puede redireccionar el tráfico para evitar que tenga acceso a las bases de datos del clúster de base de datos Multi-AZ o elegir otro método para evitar que acceda a las bases de datos del clúster de base de datos Multi-AZ.
2. Cambie el nombre del clúster de base de datos Multi-AZ existente.
3. Cree un nuevo clúster de base de datos Multi-AZ mediante la restauración de una instantánea de un clúster de base de datos o la restauración en un momento dado. A continuación, asigne al nuevo clúster de base de datos Multi-AZ el nombre del clúster de base de datos Multi-AZ anterior.

Si elimina el antiguo clúster de base de datos Multi-AZ, deberá eliminar también todas las instantáneas del clúster de base de datos Multi-AZ antiguo no deseadas.

Consola

Para cambiar el nombre de un clúster de base de datos Multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el clúster de base de datos Multi-AZ que quiere renombrar.
4. Elija Modificar.
5. En Settings (Configuración), escriba un nuevo nombre para DB instance identifier (Identificador de instancia de base de datos).
6. Elija Continue.
7. Para aplicar los cambios inmediatamente, elija Apply immediately. Si se selecciona esta opción, puede producirse una interrupción en algunos casos. Para obtener más información, consulte Aplicación inmediata de los cambios.

8. En la página de confirmación, revise los cambios. Si son correctos, elija Modify clúster (Modificar clúster) para guardarlos.

   O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para cambiar el nombre de un clúster de base de datos Multi-AZ, utilice el comando modify-db-cluster de la AWS CLI. Proporcione el nombre nuevo del clúster de base de datos Multi-AZ al valor `--db-cluster-identifier` y al parámetro `--new-db-cluster-identifier` actuales.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-cluster \
    --db-cluster-identifier DBClusterIdentifier \
    --new-db-cluster-identifier NewDBClusterIdentifier
```

En:Windows

```
aws rds modify-db-cluster ^
    --db-cluster-identifier DBClusterIdentifier ^
    --new-db-cluster-identifier NewDBClusterIdentifier
```

API de RDS

Para renombrar un clúster de bases de datos Multi-AZ, llame a la operación ModifyDBCluster de la API de Amazon RDS con los siguientes parámetros:

- `DBClusterIdentifier`: nombre existente del clúster de bases de datos.
- `NewDBClusterIdentifier`: nombre nuevo del clúster de bases de datos.

Reinicio de un clúster de base de datos multi-AZ e instancias de base de datos de lector para Amazon RDS

Es posible que necesite reiniciar su clúster de base de datos Multi-AZ, normalmente por razones de mantenimiento. Por ejemplo, si lleva a cabo determinadas modificaciones o cambia el grupo de parámetros del clúster de base de datos asociado con un clúster de base de datos, se reinicia el clúster de base de datos. Al hacerlo, los cambios surtirán efecto.

Por ejemplo, si el clúster de base de datos no utiliza los cambios más recientes del grupo de parámetros del clúster de base de datos asociado, la AWS Management Console muestra el grupo de parámetros de base de datos con el estado pending-reboot. El estado de los grupos de parámetros pending-reboot no genera un reinicio automático durante la siguiente ventana de mantenimiento. Para aplicar los cambios de parámetros más recientes en ese clúster de base de datos, reinícielo manualmente. Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para clústeres de base de datos multi-AZ.

Cuando se reinicia un clúster de base de datos, se reinicia el servicio del motor de base de datos. Al reiniciar un clúster de base de datos, se produce una interrupción momentánea, durante la cual su estado se establece en rebooting.

No puede reiniciar su clúster de base de datos si no tiene el estado Available (Disponible). Su base de datos puede no estar disponible por varias razones, como una copia de seguridad en curso, una modificación solicitada anteriormente o una acción durante un periodo de mantenimiento.

El tiempo necesario para reiniciar el clúster de base de datos depende del proceso de recuperación de fallos, la actividad de la base de datos en el momento del reinicio y el comportamiento del clúster de base de datos específico. Para mejorar el tiempo de reinicio, recomendamos reducir la actividad de la base de datos tanto como sea posible durante el proceso de reinicio. Al reducirse la actividad de la base de datos, se reduce la actividad de restauración para las transacciones en tránsito.

> **Important**
>
> Los clústeres de base de datos Multi-AZ no admiten el reinicio con una conmutación por error. Cuando reinicia la instancia de escritor de un clúster de base de datos Multi-AZ, no afecta a las instancias de base de datos de lector de ese clúster de base de datos y no se produce ninguna conmutación por error. Al reiniciar una instancia de base de datos del lector, no se produce ninguna conmutación por error. Para conmutar por error un clúster de base de

datos Multi-AZ, elija Failover (Conmutación por error) en la consola, llame al comando de la AWS CLI `failover-db-cluster` o llame a la operación de la API `FailoverDBCluster`.

Consola

Pasos para reiniciar un clúster de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, elija el clúster de base de datos Multi-AZ que desea reiniciar.
3. Para Actions (Acciones), elija Reboot (Reiniciar).

   Aparece la página Restore DB cluster (Restaurar clúster de base de datos).
4. Para reiniciar el clúster, elija Reboot (Reiniciar).

   O elija Cancel (Cancelar).

AWS CLI

Para reiniciar un clúster de base de datos Multi-AZ mediante la AWS CLI, llame al comando create-db-cluster.

```
aws rds reboot-db-cluster --db-cluster-identifier mymultiazdbcluster
```

API de RDS

Para reiniciar un clúster de base de datos Multi-AZ mediante la API de Amazon RDS, llame a la operación RebootDBCluster.

Conmutación por error de un clúster de base de datos multi-AZ para Amazon RDS

Si hay una interrupción planificada o no planificada de su instancia de base de datos de escritor en un clúster de base de datos Multi-AZ, Amazon RDS conmuta por error automáticamente a una instancia de base de datos de lector en una zona de disponibilidad diferente. Esto garantiza una alta disponibilidad con una interrupción mínima. Las conmutaciones por error pueden producirse durante errores de hardware, problemas de red o solicitudes manuales. En este tema, se describen la detección automática de errores, la secuencia de eventos durante la conmutación por error y su impacto en las operaciones de lectura y escritura. También se indican prácticas recomendadas para supervisar y minimizar los tiempos de conmutación por error.

El tiempo requerido para completar la conmutación por error dependerá de la actividad de la base de datos y de otras condiciones existentes cuando la instancia de base de datos del escritor dejó de estar disponible. Los tiempos de conmutación por error suelen ser inferiores a 35 segundos. La conmutación por error se completa cuando ambas instancias de base de datos del lector han aplicado transacciones pendientes del escritor con errores. Cuando la conmutación por error se haya completado, puede hacer falta más tiempo para que la consola de RDS refleje la nueva zona de disponibilidad.

Temas

- Conmutaciones por error automáticas
- Conmutación por error manual de un clúster de base de datos Multi-AZ
- Determinar si se ha llevado a cabo una conmutación por error en un clúster de base de datos Multi-AZ
- Configuración del TTL de JVM para las búsquedas de nombres DNS

Conmutaciones por error automáticas

Amazon RDS gestiona las conmutaciones por error automáticamente para que sea posible reanudar las operaciones de la base de datos lo antes posible sin intervención administrativa. Para llevar a cabo la conmutación por error, la instancia de base de datos del escritor cambia automáticamente a una instancia de base de datos del lector.

Conmutación por error manual de un clúster de base de datos Multi-AZ

Si lleva a cabo una conmutación por error manual de un clúster de base de datos multi-AZ, RDS primero termina la instancia de base de datos principal. Luego, el sistema de monitorización interna detecta que la instancia de base de datos principal no se encuentra en buen estado y promueve una instancia de base de datos de réplica legible. Los tiempos de conmutación por error suelen ser inferiores a 35 segundos.

Puede llevar a cabo una conmutación por error manual de un clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para llevar a cabo una conmutación por error manual de un clúster de base de datos Multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el clúster de base de datos Multi-AZ que quiere conmutar por error.
4. En Actions (Acciones), elija Failover (conmutación por error).

   Aparece la página Conmutar por error el clúster de base de datos.
5. Elija Failover (Conmutación por error) para confirmar la conmutación por error manual.

AWS CLI

Para llevar a cabo una conmutación por error manual de un clúster de base de datos Multi-AZ, utilice el comando de la AWS CLI failover-db-cluster.

Example

```
aws rds failover-db-cluster --db-cluster-identifier mymultiazdbcluster
```

API de RDS

Para llevar a cabo manualmente la conmutación por error de un clúster de base de datos Multi-AZ, llame a la API de Amazon RDS FailoverDBCluster y especifique la `DBClusterIdentifier`.

Determinar si se ha llevado a cabo una conmutación por error en un clúster de base de datos Multi-AZ

Para determinar si se produjo una conmutación por error en el clúster de base de datos Multi-AZ, puede hacer lo siguiente:

- Configure suscripciones de eventos de base de datos para notificar por correo electrónico o por SMS que se ha iniciado una conmutación por error. Para obtener más información sobre los eventos, consulte Uso de notificaciones de eventos de Amazon RDS.
- Vea sus eventos de base de datos mediante la consola de Amazon RDS o las operaciones de la API.
- Vea el estado actual del clúster de base de datos Multi-AZ mediante la consola de Amazon RDS, la AWS CLIy la API de RDS.

Para obtener información acerca de la forma de responder a las conmutaciones por error, reducir el tiempo de recuperación y otras prácticas recomendadas para Amazon RDS, consulte Prácticas recomendadas para Amazon RDS.

Configuración del TTL de JVM para las búsquedas de nombres DNS

El mecanismo de conmutación por error cambia automáticamente el registro del Sistema de nombres de dominio (DNS) de la instancia de base de datos para que apunte a la instancia de base de datos del lector. Como consecuencia, necesita restablecer las conexiones existentes a la instancia de base de datos. En un entorno de máquina virtual Java (JVM), debido al funcionamiento del mecanismo de almacenamiento en caché de DNS, puede ser necesario reconfigurar los ajustes de JVM.

La JVM almacena en caché las búsquedas de nombres DNS. Cuando la JVM resuelve un nombre de host en una dirección IP, almacena en caché la dirección IP durante un periodo de tiempo especificado, conocido como periodo de vida (TTL).

Como los recursos de AWS utilizan entradas de nombres de DNS que cambian de vez en cuando, recomendamos que configure su JVM con un valor de TTL no superior a 60 segundos. Al hacer esto se asegurará de que cuando cambie la dirección IP de un recurso, su aplicación pueda recibir y utilizar la nueva dirección IP del recurso volviendo a consultar el DNS.

En algunas configuraciones de Java, el TTL predeterminado de JVM está establecido de forma que nunca se actualicen las entradas DNS hasta que se reinicie la JVM. Por lo tanto, si la dirección IP de un recurso de AWS cambia mientras la aplicación sigue en ejecución, no podrá utilizar dicho

recurso hasta que reinicie manualmente la JVM y se actualice la información de la dirección IP almacenada en caché. En este caso, es fundamental establecer el TTL de la JVM de forma que actualice periódicamente la información de las direcciones IP almacenada en caché.

> **Note**
>
> El TTL predeterminado puede variar en función de la versión de su JVM y de si está instalado un administrador de seguridad. Muchas JVM proporcionan un TTL predeterminado inferior a 60 segundos. Si utiliza una de estas JVM y no usa un administrador de seguridad, puede omitir el resto de este tema. Para obtener más información sobre los administradores de seguridad en Oracle, consulte The Security Manager en la documentación de Oracle.

Para modificar el TTL de la JVM, establezca el valor de la propiedad `networkaddress.cache.ttl`. Utilice uno de los siguientes métodos, en función de sus necesidades:

- Para establecer globalmente el valor de la propiedad para todas las aplicaciones que utilizan la JVM, establezca `networkaddress.cache.ttl` en el archivo `$JAVA_HOME/jre/lib/security/java.security`.

  ```
  networkaddress.cache.ttl=60
  ```

- Para establecer la propiedad localmente sólo para la aplicación, establezca `networkaddress.cache.ttl` en el código de inicialización de la aplicación antes de establecer las conexiones de red.

  ```
  java.security.Security.setProperty("networkaddress.cache.ttl" , "60");
  ```

Configuración de la replicación lógica de PostgreSQL con clústeres de base de datos multi-AZ para Amazon RDS

Al utilizar la replicación lógica de PostgreSQL con su clúster de base de datos multi-AZ, puede replicar y sincronizar tablas individuales en lugar de toda la instancia de base de datos. La replicación lógica usa un modelo de publicación y suscripción para replicar los cambios de una fuente a uno o más destinatarios. Para ello, usa registros de cambios del registro de escritura anticipada (WAL) de PostgreSQL. Para obtener más información, consulte the section called "Realización de la replicación lógica".

Al crear una nueva ranura de replicación lógica en la instancia de base de datos de escritor de un clúster de base de datos multi-AZ, la ranura se copia de forma asincrónica en cada instancia de base de datos de lector del clúster. Las ranuras de las instancias de base de datos de lector se sincronizan continuamente con las de la instancia de base de datos de escritor.

Se admite la replicación lógica para los clústeres de bases de datos multi-AZ que ejecutan RDS para PostgreSQL versión 14.8-R2 y versiones posteriores, y 15.3-R2 y versiones posteriores.

> **Note**
>
> Además de la característica de replicación lógica nativa de PostgreSQL, los clústeres de base de datos multi-AZ de RDS para PostgreSQL también admiten la extensión `pglogical`.

Para obtener información adicional sobre la replicación lógica de PostgreSQL, consulte Logical replication en la documentacion de PostgreSQL.

Temas

- Requisitos previos
- Configuración de la replicación lógica
- Limitaciones y recomendaciones

Requisitos previos

Para configurar la replicación lógica de PostgreSQL para clústeres de bases de datos multi-AZ, debe cumplir los siguientes requisitos previos.

- La cuenta de usuario debe ser miembro del grupo `rds_superuser` y tener privilegios de `rds_superuser`. Para obtener más información, consulte the section called “Descripción de los roles y permisos de PostgreSQL”.
- El clúster de base de datos multi-AZ debe estar asociado a un grupo de parámetros de clúster de base de datos personalizado de modo que pueda configurar los valores de los parámetros que se describen en el siguiente procedimiento. Para obtener más información, consulte the section called “Grupos de parámetros de clúster de bases de datos”.

Configuración de la replicación lógica

Para configurar la replicación lógica para un clúster de base de datos multi-AZ, habilite parámetros específicos dentro del grupo de parámetros del clúster de base de datos asociado y, a continuación, cree ranuras de replicación lógica.

> **Note**
>
> A partir de la versión 16 de PostgreSQL, puede utilizar instancias de base de datos de lector del clúster de base de datos multi-AZ para la replicación lógica.

Para configurar la replicación lógica para un clúster de base de datos multi-AZ de RDS para PostgreSQL

1. Abra el grupo de parámetros de clúster de base de datos personalizado asociado a su clúster de base de datos multi-AZ de RDS para PostgreSQL.
2. En el campo búsqueda Parámetros, busque el `rds.logical_replication`parámetro estático y establezca su valor en 1. Este cambio de parámetro puede aumentar la generación de WAL, por lo que debe habilitarlo solo cuando utilice ranuras lógicas.
3. Como parte de este cambio, configure los siguientes parámetros del clúster de base de datos.
   - `max_wal_senders`
   - `max_replication_slots`
   - `max_connections`

En función del uso previsto, es posible que también tenga que cambiar los valores de los siguientes parámetros. Sin embargo, en muchos casos, los valores predeterminados son suficientes.

- `max_logical_replication_workers`
- `max_sync_workers_per_subscription`

4. Reinicie el clúster de base de datos multi-AZ para que los valores de los parámetros surtan efecto. Para obtener instrucciones, consulte the section called “Reinicio de un clúster de base de datos Multi-AZ”.
5. Cree una ranura de replicación lógica en la instancia de base de datos de escritor del clúster de base de datos multi-AZ, como se explica en the section called “Trabajo con ranuras de replicación lógica”. Este proceso necesita que especifique un complemento de descodificación. Actualmente, RDS para PostgreSQL admite los complementos `test_decoding`, `wal2json` y `pgoutput` que se incluyen con PostgreSQL.

   La ranura se copia de forma asincrónica en cada instancia de base de datos de lector del clúster.
6. Verifique el estado de la ranura en todas las instancias de base de datos de lector del clúster de base de datos multi-AZ. Para ello, inspeccione la vista `pg_replication_slots` de todas las instancias de base de datos de lector y asegúrese de que el estado `confirmed_flush_lsn` avanza a medida que la aplicación consume activamente los cambios lógicos.

   Los siguientes comandos muestran cómo inspeccionar el estado de replicación en las instancias de base de datos de lector.

```
% psql -h test-postgres-instance-2.abcdefabcdef.us-west-2.rds.amazonaws.com

postgres=> select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;
  slot_name   | slot_type | confirmed_flush_lsn
--------------+-----------+---------------------
 logical_slot | logical   | 32/D0001700
(1 row)

postgres=> select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;
```

```
  slot_name   | slot_type | confirmed_flush_lsn
--------------+-----------+---------------------
 logical_slot | logical   | 32/D8003628
(1 row)

% psql -h test-postgres-instance-3.abcdefabcdef.us-west-2.rds.amazonaws.com

postgres=> select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;
  slot_name   | slot_type | confirmed_flush_lsn
--------------+-----------+---------------------
 logical_slot | logical   | 32/D0001700
(1 row)

postgres=> select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;
  slot_name   | slot_type | confirmed_flush_lsn
--------------+-----------+---------------------
 logical_slot | logical   | 32/D8003628
(1 row)
```

Tras completar las tareas de replicación, detenga el proceso de replicación, elimine las ranuras de replicación y desactive la replicación lógica. Para desactivar la replicación lógica, modifique el grupo de parámetros del clúster de base de datos y establezca el valor `rds.logical_replication` de nuevo en `0`. Reinicie el clúster para que el cambio de parámetro surta efecto.

Limitaciones y recomendaciones

Estas son las limitaciones y recomendaciones que se aplican a la replicación lógica con los clústeres de base de datos multi-AZ que ejecutan PostgreSQL 16:

- Solo puede usar instancias de base de datos de escritura para crear o eliminar ranuras de replicación lógica. Por ejemplo, el comando `CREATE SUBSCRIPTION` debe usar el punto de conexión del escritor del clúster en la cadena de conexión del host.
- Debe utilizar el punto de conexión del escritor del clúster durante cualquier sincronización o resincronización de tablas. Por ejemplo, puede utilizar los siguientes comandos para volver a sincronizar una tabla recién agregada.

```
Postgres=>ALTER SUBSCRIPTION subscription-name CONNECTION host=writer-endpoint
Postgres=>ALTER SUBSCRIPTION subscription-name REFRESH PUBLICATION
```

- Debe esperar a que se complete la sincronización de las tablas antes de utilizar las instancias de base de datos de lector para la replicación lógica. Puede utilizar la tabla de catálogo `pg_subscription_rel` para supervisar la sincronización de la tabla. La sincronización de tablas finaliza cuando la columna `srsubstate` se establece en lista (`r`).
- Recomendamos utilizar puntos de conexión de instancia para la conexión de replicación lógica una vez completada la sincronización inicial de las tablas. El siguiente comando reduce la carga en la instancia de base de datos de escritor al descargar la replicación a una de las instancias de base de datos de lector:

  ```
  Postgres=>ALTER SUBSCRIPTION subscription-name CONNECTION host=reader-instance-endpoint
  ```

  No puede utilizar la misma ranura en más de una instancia de base de datos a la vez. Cuando dos o más aplicaciones replican los cambios lógicos de distintas instancias de base de datos en el clúster, es posible que algunos cambios se pierdan debido a una conmutación por error del clúster o a un problema de red. En estas situaciones, puede usar los puntos de conexión de la instancia para la replicación lógica en la cadena de conexión del host. En la otra aplicación que utiliza la misma configuración, se mostrará el siguiente mensaje de error:

  ```
  replication slot slot_name is already active for PID x providing immediate feedback.
  ```

- Al usar la extensión `pglogical`, solo puede usar el punto de conexión del escritor de clústeres. La extensión tiene limitaciones conocidas que pueden crear ranuras de replicación lógica no utilizadas durante la sincronización de tablas. Las ranuras de replicación obsoletas reservan archivos de registro de escritura anticipada (WAL) y pueden provocar problemas de espacio en disco.

Uso de réplicas de lectura de clústeres de base de datos multi-AZ para Amazon RDS

Una réplica de lectura de clúster de base de datos es un tipo especial de clúster que se crea a partir de una instancia de base de datos de origen. Después de crear una réplica de lectura, cualquier actualización realizada en la instancia de base de datos principal se copia de forma asíncrona en la réplica de lectura del clúster de base de datos multi-AZ. Puede reducir la carga de la instancia de la base de datos principal enrutando las consultas de lectura de sus aplicaciones a la réplica de lectura. Las réplicas de lectura le permiten ajustar la escala de manera elástica por encima de las restricciones de capacidad de una instancia de base de datos para las cargas de trabajo de las bases de datos con operaciones intensivas de lectura.

También puede crear una o varias réplicas de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ. Las réplicas de lectura de instancia de base de datos permiten escalar por encima de la capacidad de computación o de E/S del clúster de base de datos multi-AZ de origen al dirigir el exceso de tráfico de lectura a las réplicas leídas. Actualmente, no puede crear una réplica de lectura de clúster de base de datos multi-AZ a partir de un clúster de base de datos multi-AZ existente.

Al elegir entre migrar a un clúster de base de datos multi-AZ mediante una réplica de lectura o crear una réplica de lectura de instancia de base de datos a partir de un clúster de base de datos multi-AZ, tenga en cuenta su caso de uso específico y los requisitos de rendimiento.

Migración a un clúster de base de datos Multi-AZ mediante una réplica de lectura

> Este enfoque es ideal cuando necesita mejorar la disponibilidad y la durabilidad de la base de datos y, al mismo tiempo, minimizar el tiempo de inactividad. Al utilizar una réplica de lectura para realizar la transición a un clúster de base de datos multi-AZ, puede garantizar un funcionamiento continuo y la coherencia de los datos. Este método resulta especialmente útil para los entornos de producción en los que es fundamental mantener la disponibilidad y reducir el impacto en las cargas de trabajo activas.

Creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ

> Este método es adecuado si desea escalar las operaciones de lectura o reducir el tráfico de lectura de la instancia de base de datos principal. Al crear una réplica de lectura desde un clúster existente de base de datos multi-AZ, puede distribuir cargas de trabajo con operaciones intensivas de lectura y mejorar el rendimiento sin afectar a la estabilidad de la instancia principal.

La elección del enfoque correcto depende de si su prioridad es garantizar una alta disponibilidad y durabilidad o escalar el rendimiento de lectura. Evalúe las características de la carga de trabajo y los requisitos operativos para tomar una decisión fundamentada.

Temas

- Migración a un clúster de base de datos Multi-AZ mediante una réplica de lectura
- Creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ

Migración a un clúster de base de datos Multi-AZ mediante una réplica de lectura

Para migrar una implementación Single-AZ o una implementación de instancia de base de datos Multi-AZ a una implementación de clúster de base de datos Multi-AZ con un tiempo de inactividad reducido, puede crear una réplica de lectura de clúster de base de datos Multi-AZ. Para el origen, especifique la instancia de base de datos en la implementación Single-AZ o la instancia de base de datos principal en la implementación de instancia de base de datos Multi-AZ. La instancia de base de datos puede procesar transacciones de escritura durante la migración a un clúster de base de datos Multi-AZ.

Tenga en cuenta lo siguiente antes de crear una réplica de lectura de clúster de base de datos Multi-AZ:

- La instancia de base de datos de origen debe estar en una versión que sea compatible con clústeres de base de datos Multi-AZ. Para obtener más información, consulte Regiones y motores de base de datos admitidos para clústeres de bases de datos Multi-AZ en Amazon RDS.
- La réplica de lectura del clúster de base de datos Multi-AZ debe estar en la misma versión principal que su origen y en la misma versión secundaria o una posterior.
- Debe habilitar las copias de seguridad automáticas en la instancia de base de datos de origen estableciendo el periodo de retención de copia de seguridad en un valor distinto de 0.
- El almacenamiento asignado a la instancia de base de datos de origen debe ser de 100 GiB o más.
- En el caso de RDS para MySQL, los parámetros`gtid-mode` y `enforce_gtid_consistency` se deben definir como `ON` para la instancia de base de datos de origen. Debe usar un grupo de parámetros personalizado, no el grupo de parámetros predeterminado. Para obtener más información, consulte the section called “Grupos de parámetros de base de datos”.

- Una transacción activa de ejecución prolongada puede ralentizar el proceso de creación de la réplica de lectura. Le recomendamos que espere a que se completen las transacciones de ejecución prolongada antes de crear una réplica de lectura.
- Si elimina la instancia de base de datos de origen de una réplica de lectura de clúster de base de datos Multi-AZ, la réplica de lectura se promociona a un clúster de base de datos Multi-AZ independiente.

Creación y promoción de la réplica de lectura de clúster de base de datos Multi-AZ

Puede crear y promocionar una réplica de lectura de clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> Recomendamos encarecidamente crear todas las réplicas de lectura en la misma nube privada virtual (VPC) basándose en la Amazon VPC de la instancia de base de datos de origen.
> Si crea una réplica de lectura en una VPC que no sea la instancia de base de datos de origen, los rangos de enrutamiento entre dominios sin clases (CIDR) pueden superponerse entre la réplica y el sistema de Amazon RDS. La superposición de CIDR hace que la réplica sea inestable, lo que puede afectar negativamente a las aplicaciones que se conectan a ella.
> Si obtiene un error al crear la réplica de lectura, elija un grupo de subred de base de datos de destino diferente. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.

Consola

Para migrar una implementación Single-AZ o una implementación de instancia de base de datos Multi-AZ a un clúster de base de datos Multi-AZ mediante una réplica de lectura, siga estos pasos con la AWS Management Console.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Cree la réplica de lectura de clúster de base de datos Multi-AZ.

    a. En el panel de navegación, seleccione Databases (Bases de datos).

b. Seleccione la instancia de base de datos que desea usar como origen de una réplica de lectura

c. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).

d. En Availability and durability (Disponibilidad y durabilidad), elija Multi-AZ DB cluster (Clúster de base de datos Multi-AZ).

e. En DB instance identifier (Identificador de instancias de bases de datos), escriba un nombre para la réplica de lectura.

f. En el resto de secciones, especifique los ajustes de configuración del clúster de base de datos. Para obtener más información acerca de una configuración, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.

g. Elija Create read replica (Crear réplica de lectura).

3. Cuando haya terminado, promocione la réplica de lectura para que sea un clúster de base de datos Multi-AZ independiente:

a. Detenga la escritura de transacciones en la instancia de base de datos de origen y, a continuación, espere hasta que se hayan realizado todas las actualizaciones en la réplica de lectura.

Las actualizaciones de la base de datos se producen en la réplica de lectura después de haberse producido en la instancia de la base de datos principal. Este retardo en la replicación puede variar considerablemente. Utilice la métrica `ReplicaLag` para determinar cuándo se han completado todas las actualizaciones en la réplica de lectura. Para obtener más información acerca del retardo de replicación, consulte Monitoreo de la replicación de lectura.

b. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

c. En la consola de Amazon RDS, seleccione Databases (Bases de datos).

Aparece el panel Databases (Bases de datos). Cada réplica de lectura muestra Replica (Réplica) en la columna Role (Rol).

d. Elija la réplica de lectura del clúster de base de datos Multi-AZ que desea promocionar.

e. En Actions (Acciones), seleccione Promote (Promover).

f. En la página Promote Read Replica (Promocionar réplica de lectura), escriba el periodo de retención de copia de seguridad y el periodo de copia de seguridad para el clúster de base de datos Multi-AZ que acaba de promocionar.

g. Cuando la configuración sea la deseada, elija Promote read replica (Promocionar réplica de lectura).

h. Espere a que el estado del clúster de base de datos Multi-AZ promocionado sea `Available`.

i. Indique a sus aplicaciones que utilicen el clúster de base de datos Multi-AZ promocionado.

Si lo desea, elimine la implementación Single-AZ o la implementación de instancia de base de datos Multi-AZ si ya no es necesaria. Para obtener instrucciones, consulte Eliminación de una instancia de base de datos.

AWS CLI

Para migrar una implementación Single-AZ o una implementación de instancia de base de datos Multi-AZ a un clúster de base de datos Multi-AZ mediante una réplica de lectura, siga estos pasos con la AWS CLI.

1. Cree la réplica de lectura de clúster de base de datos Multi-AZ.

   Para crear una réplica de lectura a partir de una instancia de base de datos de origen, utilice el comando de AWS CLI `create-db-cluster`. Para `--replication-source-identifier`, especifique el nombre de recurso de Amazon (ARN) de la instancia de base de datos de origen.

   Para Linux, macOS o:Unix

```
aws rds create-db-cluster \
  --db-cluster-identifier mymultiazdbcluster \
  --replication-source-identifier arn:aws:rds:us-
east-2:123456789012:db:mydbinstance
  --engine postgres \
  --db-cluster-instance-class db.m5d.large \
  --storage-type io1 \
  --iops 1000 \
  --db-subnet-group-name defaultvpc \
  --backup-retention-period 1
```

   En:Windows

```
aws rds create-db-cluster ^
```

```
  --db-cluster-identifier mymultiazdbcluster ^
  --replication-source-identifier arn:aws:rds:us-
east-2:123456789012:db:mydbinstance
  --engine postgres ^
  --db-cluster-instance-class db.m5d.large ^
  --storage-type io1 ^
  --iops 1000 ^
  --db-subnet-group-name defaultvpc ^
  --backup-retention-period 1
```

2. Detenga la escritura de transacciones en la instancia de base de datos de origen y, a continuación, espere hasta que se hayan realizado todas las actualizaciones en la réplica de lectura.

   Las actualizaciones de la base de datos se producen en la réplica de lectura después de haberse producido en la instancia de la base de datos principal. Este retardo en la replicación puede variar considerablemente. Utilice la métrica `Replica Lag` para determinar cuándo se han completado todas las actualizaciones en la réplica de lectura. Para obtener más información acerca del retardo de replicación, consulte Monitoreo de la replicación de lectura.

3. Cuando esté listo, promocione la réplica de lectura para que sea un clúster de base de datos Multi-AZ independiente:

   Para promocionar una réplica de lectura de clúster de base de datos Multi-AZ, utilice el comando de la AWS CLI `promote-read-replica-db-cluster`. En `--db-cluster-identifier`, especifique el identificador de la réplica de lectura del clúster de base de datos Multi-AZ.

   ```
   aws rds promote-read-replica-db-cluster --db-cluster-identifier mymultiazdbcluster
   ```

4. Espere a que el estado del clúster de base de datos Multi-AZ promocionado sea `Available`.
5. Indique a sus aplicaciones que utilicen el clúster de base de datos Multi-AZ promocionado.

Si lo desea, elimine la implementación Single-AZ o la implementación de instancia de base de datos Multi-AZ si ya no es necesaria. Para obtener instrucciones, consulte Eliminación de una instancia de base de datos.

API de RDS

Para migrar una implementación Single-AZ o una implementación de instancia de base de datos Multi-AZ a un clúster de base de datos Multi-AZ mediante una réplica de lectura, siga estos pasos con la API de EDS.

1. Cree la réplica de lectura de clúster de base de datos Multi-AZ.

   Para crear una réplica de lectura de clúster de base de datos Multi-AZ, utilice la operación `CreateDBCluster` con el parámetro requerido `DBClusterIdentifier`. Para `ReplicationSourceIdentifier`, especifique el nombre de recurso de Amazon (ARN) de la instancia de base de datos de origen.

2. Detenga la escritura de transacciones en la instancia de base de datos de origen y, a continuación, espere hasta que se hayan realizado todas las actualizaciones en la réplica de lectura.

   Las actualizaciones de la base de datos se producen en la réplica de lectura después de haberse producido en la instancia de la base de datos principal. Este retardo en la replicación puede variar considerablemente. Utilice la métrica `Replica Lag` para determinar cuándo se han completado todas las actualizaciones en la réplica de lectura. Para obtener más información acerca del retardo de replicación, consulte Monitoreo de la replicación de lectura.

3. Cuando esté listo, promocione la réplica de lectura para que sea un clúster de base de datos Multi-AZ independiente.

   Para promocionar una réplica de lectura de clúster de base de datos Multi-AZ, utilice la operación `PromoteReadReplicaDBCluster` con el parámetro requerido `DBClusterIdentifier`. Especifique el identificador de la réplica de lectura del clúster de base de datos Multi-AZ.

4. Espere a que el estado del clúster de base de datos Multi-AZ promocionado sea `Available`.

5. Indique a sus aplicaciones que utilicen el clúster de base de datos Multi-AZ promocionado.

Si lo desea, elimine la implementación Single-AZ o la implementación de instancia de base de datos Multi-AZ si ya no es necesaria. Para obtener instrucciones, consulte Eliminación de una instancia de base de datos.

Limitaciones para crear una réplica de lectura del clúster de base de datos Multi-AZ

Las siguientes limitaciones se aplican a la creación de una réplica de lectura del clúster de base de datos Multi-AZ a partir de una implementación Single-AZ o una implementación de instancia de base de datos Multi-AZ.

- No puede crear una réplica de lectura del clúster de base de datos multi-AZ en una Cuenta de AWS que no sea la Cuenta de AWS que posee la instancia de base de datos de origen.

- No puede crear una réplica de lectura del clúster de base de datos Multi-AZ en una cuenta de Región de AWS diferente de la instancia de base de datos de origen.
- No se puede recuperar una réplica de lectura del clúster de base de datos Multi-AZ en un punto en el tiempo.
- El cifrado de almacenamiento debe tener la misma configuración en la instancia de base de datos de origen y en el clúster de base de datos Multi-AZ.
- Si la instancia de base de datos de origen está cifrada, la réplica de lectura del clúster de base de datos Multi-AZ debe cifrarse con la misma clave de KMS.
- Si la instancia de base de datos de origen utiliza almacenamiento SSD de uso general (gp3) y tiene menos de 400 GiB de almacenamiento asignado, no puede modificar las IOPS aprovisionadas para la réplica de lectura del clúster de base de datos multi-AZ.
- Para realizar una actualización de la versión secundaria en la instancia de base de datos de origen, primero debe realizarla en la réplica de lectura del clúster de base de datos Multi-AZ.
- Al realizar una actualización de la versión secundaria en una réplica de lector de un clúster de base de datos multi-AZ de RDS para PostgreSQL, la instancia de base de datos del lector no cambia a la instancia de base de datos del escritor después de la actualización. Por lo tanto, es posible que su clúster de base de datos experimente un tiempo de inactividad mientras Amazon RDS actualiza la instancia de escritor.
- No se puede realizar una actualización de la versión principal en una réplica de lectura de un clúster de base de datos multi-AZ.
- Puede realizar una actualización de la versión principal en la instancia de base de datos de origen de una réplica de lectura del clúster de base de datos Multi-AZ, pero la replicación en la réplica de lectura se detiene y no se puede reiniciar.
- La réplica de lectura del clúster de base de datos Multi-AZ no admite réplicas de lectura en cascada.
- En el caso de RDS para PostgreSQL, las réplicas de lectura del clúster de base de datos Multi-AZ no pueden realizar una conmutación por error.

Creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ

Puede crear una réplica de lectura de instancia de base de datos a partir de un clúster de base de datos multi-AZ para escalar por encima de la capacidad de computación o E/S del clúster para cargas de trabajo de las bases de datos con operaciones intensivas de lectura. Puede dirigir este

exceso del tráfico de lectura a una o varias réplicas de lectura de instancia de base de datos. También puede usar réplicas de lectura para migrar desde un clúster de base de datos multi-AZ a una instancia de base de datos.

Para crear una réplica de lectura, especifique un clúster de base de datos multi-AZ como origen de la replicación. Una de las instancias de lector del clúster de base de datos multi-AZ es siempre el origen de la replicación, no la instancia del escritor. Esto garantiza que la réplica esté siempre sincronizada con el clúster de origen, incluso en casos de conmutación por error.

Temas

- Comparación de instancias de base de datos del lector con réplicas de lectura de instancia de base de datos
- Consideraciones
- Creación de una réplica de lectura de instancia de base de datos
- Promoción de la réplica de lectura de instancia de base de datos
- Limitaciones en la creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ

Comparación de instancias de base de datos del lector con réplicas de lectura de instancia de base de datos

Una réplica de lectura de instancia de base de datos de un clúster de base de datos multi-AZ se diferencia de las instancias de base de datos de lector del clúster de base de datos multi-AZ en los siguientes aspectos:

- Las instancias de base de datos del lector actúan como destinos de la conmutación por error automática, mientras que las réplicas de lectura de instancia de base de datos no.
- Las instancias de base de datos del lector deben reconocer un cambio en la instancia de base de datos del escritor antes de poder confirmarlo. Sin embargo, en las réplicas de lectura de instancia de base de datos, las actualizaciones se copian de forma asíncrona en la réplica de lectura sin necesidad de que se reconozcan.
- Las instancias de base de datos del lector siempre comparten la misma clase de instancia, tipo de almacenamiento y versión de motor que la instancia de base de datos del escritor del clúster de base de datos multi-AZ. Sin embargo, las réplicas de lectura de instancia de base de datos no tienen que compartir necesariamente las mismas configuraciones que el clúster de origen.

- Puede promocionar una réplica de lectura de instancia de base de datos a una instancia de base de datos independiente. No puede promocionar una instancia de base de datos de lector de un clúster de base de datos multi-AZ a una instancia independiente.
- El punto de conexión del lector solo enruta las solicitudes a las instancias de base de datos del lector del clúster de base de datos multi-AZ. Nunca las enruta a una réplica de lectura de una instancia de base de datos.

Para obtener más información acerca de las instancias de base de datos de lector y escritor, consulte the section called “Arquitectura de clúster de base de datos multi-AZ”.

Consideraciones

Tenga en cuenta lo siguiente antes de crear una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ:

- Cuando cree la réplica de lectura de la instancia de base de datos, esta debe tener la misma versión principal que su clúster de origen y la misma versión secundaria o una posterior. Después de crearla, tiene la opción de actualizar la réplica de lectura a una versión secundaria posterior a la del clúster de origen.
- Al crear la réplica de lectura de la instancia de base de datos, el almacenamiento asignado debe ser el mismo que el del clúster de base de datos multi-AZ de origen. Puede cambiar el almacenamiento asignado después de crear la réplica de lectura.
- El parámetro `gtid-mode` debe establecerse en `ON` para el clúster de base de datos Multi-AZ de origen. Para obtener más información, consulte the section called “Grupos de parámetros de clúster de bases de datos”.
- Una transacción activa de ejecución prolongada puede ralentizar el proceso de creación de la réplica de lectura. Le recomendamos que espere a que se completen las transacciones de ejecución prolongada antes de crear una réplica de lectura.
- Si elimina el clúster de base de datos multi-AZ de origen de una réplica de lectura de instancia de base de datos, todas las réplicas de lectura en las que esté escribiendo se promocionan a instancias de base de datos independientes.

Creación de una réplica de lectura de instancia de base de datos

Puede crear una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> Recomendamos encarecidamente crear todas las réplicas de lectura en la misma nube privada virtual (VPC) basándose en la Amazon VPC del clúster de base de datos multi-AZ de origen.
> Si crea una réplica de lectura en una VPC diferente del clúster de base de datos multi-AZ de origen, los rangos de enrutamiento entre dominios sin clases (CIDR) pueden superponerse entre la réplica y el sistema RDS. La superposición de CIDR hace que la réplica sea inestable, lo que puede afectar negativamente a las aplicaciones que se conectan a ella. Si obtiene un error al crear la réplica de lectura, elija un grupo de subred de base de datos de destino diferente. Para obtener más información, consulte the section called “Uso de una instancia de base de datos en una VPC”.

Consola

Para crear una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ, siga estos pasos con la AWS Management Console.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el clúster de base de datos multi-AZ que desea usar como origen de una réplica de lectura.
4. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).
5. En Origen de réplica, asegúrese de seleccionar el clúster de base de datos multi-AZ correcto.
6. En Identificador de base de datos, escriba un nombre para la réplica de lectura.
7. En el resto de secciones, especifique los ajustes de configuración de la instancia de base de datos. Para obtener más información acerca de una configuración, consulte the section called “Opciones disponibles”.

   > **Note**
   >
   > El almacenamiento asignado para la réplica de lectura de la instancia de base de datos debe ser el mismo que el del clúster de base de datos multi-AZ de origen.

8. Elija Create read replica (Crear réplica de lectura).

AWS CLI

Para crear una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ, utilice el comando de la AWS CLI `create-db-instance-read-replica`. En `--source-db-cluster-identifier`, especifique el identificador del clúster de base de datos multi-AZ.

Para Linux, macOS o:Unix

```
aws rds create-db-instance-read-replica \
  --db-instance-identifier myreadreplica \
  --source-db-cluster-identifier mymultiazdbcluster
```

En:Windows

```
aws rds create-db-instance-read-replica ^
  --db-instance-identifier myreadreplica ^
  --source-db-cluster-identifier mymultiazdbcluster
```

API de RDS

Para crear una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ, utilice la operación `CreateDBInstanceReadReplica`.

Promoción de la réplica de lectura de instancia de base de datos

Si ya no necesita la réplica de lectura de instancia de base de datos, puede promocionarla a una instancia de base de datos independiente. Cuando se promociona una réplica de lectura, la instancia de base de datos se reinicia antes de que esté disponible. Para obtener instrucciones, consulte the section called “Promoción de una réplica de lectura”.

Si utiliza la réplica de lectura para migrar una implementación de clúster de base de datos multi-AZ a una implementación de instancia de base de datos single-AZ o multi-AZ, asegúrese de detener cualquier transacción que se esté escribiendo en el clúster de base de datos de origen. A continuación, espere hasta que se hayan realizado todas las actualizaciones en la réplica de lectura. Las actualizaciones de la base de datos se realizan en la réplica de lectura después de haberse realizado en una de las instancias de base de datos del lector del clúster de base de datos multi-AZ. Este retardo en la replicación puede variar considerablemente. Utilice la métrica `ReplicaLag` para determinar cuándo se han completado todas las actualizaciones en la réplica de lectura. Para

obtener más información acerca del retardo de replicación, consulte the section called “Monitoreo de la replicación de lectura”.

Tras promocionar la réplica de lectura, espere a que el estado de la instancia de base de datos promocionada sea `Available` antes de indicar a las aplicaciones que utilicen la instancia de base de datos promocionada. Si lo desea, elimine la implementación del clúster de base de datos multi-AZ si ya no la necesita. Para obtener instrucciones, consulte the section called “Eliminación de un clúster de base de datos Multi-AZ”.

Limitaciones en la creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ

Las siguientes limitaciones se aplican a la creación de una réplica de lectura de instancia de base de datos desde una implementación de clúster de base de datos multi-AZ.

- No puede crear una réplica de lectura de instancia de base de datos en una Cuenta de AWS que no sea la Cuenta de AWS que posee el clúster de base de datos multi-AZ de origen.
- No puede crear una réplica de lectura de instancia de base de datos en una Región de AWS diferente a la del clúster de base de datos multi-AZ de origen.
- No se puede recuperar una réplica de lectura de instancia de base de datos en un punto en el tiempo.
- El cifrado de almacenamiento debe tener la misma configuración en el clúster de base de datos multi-AZ de origen y en la réplica de lectura de instancia de base de datos.
- Si el clúster de base de datos multi-AZ de origen está cifrado, la réplica de lectura de instancia de base de datos debe cifrarse con la misma clave de KMS.
- Para realizar una actualización de la versión secundaria en el clúster de base de datos multi-AZ de origen, primero debe realizarla en la réplica de lectura de instancia de base de datos.
- La réplica de lectura de instancia de base de datos no admite réplicas de lectura en cascada.
- Para RDS para PostgreSQL, el clúster de base de datos Multi-AZ de origen debe ejecutar la versión 13.11, 14.8, 15.2.R2 o posterior de PostgreSQL para poder crear una réplica de lectura de instancia de base de datos.
- Puede realizar una actualización de la versión principal en el clúster de base de datos multi-AZ de origen de una réplica de lectura de la instancia de base de datos, pero la replicación en la réplica de lectura se detiene y no se puede reiniciar.

Configuración de la replicación externa a partir de los clústeres de bases de datos multi-AZ para Amazon RDS

Puede configurar la replicación entre un clúster de base de datos multi-AZ y una base de datos externa a Amazon RDS.

La replicación externa permite que los clústeres de bases de datos multi-AZ repliquen datos entre una instancia de base de datos de RDS y una base de datos externa, ya sea en las instalaciones o en otro entorno de nube. Es útil para la recuperación ante desastres, la migración de datos y el mantenimiento de la coherencia entre los sistemas en diferentes ubicaciones. En esta sección, se describen los requisitos previos para configurar la replicación, cómo configurar el proceso y aspectos clave, como, por ejemplo, la latencia de la replicación, el ancho de banda y la compatibilidad con diferentes motores de bases de datos.

RDS para MySQL

Para configurar la replicación externa de un clúster de base de datos multi-AZ de RDS para MySQL, debe retener los archivos de registro binarios en las instancias de base de datos dentro del clúster durante el tiempo suficiente para garantizar que los cambios se apliquen a la réplica antes de que Amazon RDS elimine el archivo binlog. Para ello, configure la retención de registros binarios llamando al procedimiento `mysql.rds_set_configuration` almacenado y especificando el parámetro `binlog retention hours`. Para obtener más información, consulte the section called “binlog retention hours”.

El valor predeterminado de `binlog retention hours` es `NULL`, lo que significa que los registros binarios no se retienen (0 horas). Si desea configurar la replicación externa para un clúster de base de datos multi-AZ, debe establecer el parámetro en un valor distinto de `NULL`.

Solo puede configurar la retención de registros binarios desde la instancia de base de datos de escritor del clúster de base de datos multi-AZ, y la configuración se propaga a todas las instancias de base de datos de lector de forma asíncrona.

Además, le recomendamos encarecidamente que habilite la replicación basada en GTID en su réplica externa. A continuación, si una de las instancias de base de datos falla, puede reanudar la replicación desde otra instancia de base de datos en buen estado dentro del clúster. Para obtener más información, consulte Replication with Global Transaction Identifiers en la documentación de MySQL.

RDS para PostgreSQL

Para configurar la replicación lógica para un clúster de base de datos multi-AZ de RDS para PostgreSQL, debe habilitar la replicación lógica. Para obtener instrucciones, consulte the section called “Replicación lógica de PostgreSQL con clústeres de base de datos multi-AZ”.

Eliminación de un clúster de base de datos multi-AZ para Amazon RDS

Puede eliminar un clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

El tiempo necesario para eliminar un clúster de base de datos multi-AZ puede variar en función de los siguientes factores:

- El periodo de retención de copia de seguridad (es decir, cuántas copias de seguridad se eliminarán).
- Cuántos datos se eliminan.
- Si se toma una instantánea final.

La protección de eliminación debe estar deshabilitada en el clúster de base de datos multi-AZ antes de poder eliminarla. Para obtener más información, consulte the section called “Requisitos previos para eliminar una instancia de base de datos”. Puede deshabilitar la protección contra eliminación modificando el clúster de base de datos multi-AZ. Para obtener más información, consulte the section called “Modificación de un clúster de base de datos Multi-AZ”.

Consola

Para eliminar un clúster de base de datos Multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, elija el clúster de base de datos Multi-AZ que desea eliminar.
3. En Actions (Acciones), seleccione Delete (Eliminar).
4. Para crear una instantánea de base de datos final del clúster de base de datos Multi-AZ, elija Create final snapshot? (¿Crear una instantánea final?).

   Si crea una instantánea final, ingrese el nombre en Final snapshot name (Nombre de instantánea final).
5. Para retener las copias de seguridad automatizadas, elija Retain automated backups (Retener copias de seguridad automatizadas).
6. En el cuadro, escriba **`delete me`**.
7. Elija Eliminar (Delete).

AWS CLI

Para eliminar un clúster de base de datos Multi-AZ con la AWS CLI, llame al comando delete-db-cluster con las siguientes opciones:

- `--db-cluster-identifier`
- `--final-db-snapshot-identifier` o `--skip-final-snapshot`

Example Con una instantánea final

Para Linux, macOS o:Unix

```
aws rds delete-db-cluster \
    --db-cluster-identifier mymultiazdbcluster \
    --final-db-snapshot-identifier mymultiazdbclusterfinalsnapshot
```

En:Windows

```
aws rds delete-db-cluster ^
    --db-cluster-identifier mymultiazdbcluster ^
    --final-db-snapshot-identifier mymultiazdbclusterfinalsnapshot
```

Example Sin instantánea final

Para Linux, macOS o:Unix

```
aws rds delete-db-cluster \
    --db-cluster-identifier mymultiazdbcluster \
    --skip-final-snapshot
```

En:Windows

```
aws rds delete-db-cluster ^
    --db-cluster-identifier mymultiazdbcluster ^
    --skip-final-snapshot
```

API de RDS

Para eliminar un clúster de base de datos Multi-AZ con la API de Amazon RDS, llame a la operación DeleteDBCluster con los siguientes parámetros:

- `DBClusterIdentifier`
- `FinalDBSnapshotIdentifier` o `SkipFinalSnapshot`

Limitaciones de clústeres de base de datos multi-AZ para Amazon RDS

Un clúster de base de datos Multi-AZ tiene una instancia de base de datos del escritor y dos instancias de base de datos del lector en tres zonas de disponibilidad diferentes. Los clústeres de base de datos Multi-AZ proporcionan alta disponibilidad, mayor capacidad para cargas de trabajo de lectura y menor latencia en comparación con las implementaciones Multi-AZ. Para obtener más información acerca de los clústeres de base de datos Multi-AZ, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

Las siguientes limitaciones se aplican a los clústeres de base de datos multi-AZ.

- Los clústeres de base de datos Multi-AZ no admiten las siguientes características:
  - Conexiones IPv6 (modo de pila doble)
  - Copias de seguridad automatizadas entre regiones
  - Autenticación de Kerberos
  - Modificación del puerto. Como alternativa, puede restaurar un clúster de base de datos Multi-AZ a un momento determinado y especificar un puerto diferente.
  - Grupos de opciones
  - Recuperación en un momento dado (PITR) para clústeres eliminados
  - Escalado automático del almacenamiento mediante la configuración del almacenamiento máximo asignado. Como alternativa, puede escalar manualmente el almacenamiento.
  - Detención e inicio del clúster de base de datos multi-AZ
  - Copia de una instantánea de un clúster de base de datos Multi-AZ
  - Cifrado de un clúster de base de datos Multi-AZ sin cifrar
- Los clústeres de base de datos RDS para MySQL Multi-AZ solo admiten los siguientes procedimientos almacenados del sistema:
  - `mysql.rds_rotate_general_log`
  - `mysql.rds_rotate_slow_log`
  - `mysql.rds_show_configuration`
  - `mysql.rds_set_external_master_with_auto_position`
  - `mysql.rds_set_configuration`
- Los clústeres de base de datos Multi-AZ de RDS para PostgreSQL no admiten las siguientes extensiones: `aws_s3` y `pg_transport`.

- Los clústeres de base de datos Multi-AZ de RDS para PostgreSQL no admiten el uso de un servidor DNS personalizado para el acceso a red saliente.

Soporte extendido de Amazon RDS con Amazon RDS

El soporte extendido de RDS le permite seguir ejecutando una base de datos en una versión principal del motor después de la fecha de finalización del soporte estándar de RDS por un costo adicional.

Solo puede inscribir una base de datos en el soporte extendido de RDS si habilita el soporte extendido de RDS al crear o restaurar una instancia de base de datos por primera vez. No puede actualizar el estado de inscripción de soporte extendido de RDS en las instancias de base de datos existentes a menos que las restaure.

Si ha habilitado el soporte extendido de RDS durante la creación o la restauración de una instancia de base de datos, después del final de RDS de la fecha de soporte estándar, Amazon RDS inscribirán automáticamente la instancia de base de datos en el soporte extendido de RDS. La inscripción automática en el soporte extendido de RDS no cambia el motor de la base de datos ni afecta al tiempo de actividad ni al rendimiento de la instancia de base de datos.

Soporte extendido de RDS ofrece las siguientes actualizaciones y soporte técnico:

- Actualizaciones de seguridad para las CVE críticas y altas para la instancia de base de datos o clúster de base de datos, incluido el motor de base de datos
- Correcciones de errores y parches para problemas críticos
- La posibilidad de abrir casos de soporte y recibir ayuda para la solución de problemas según el Acuerdo de nivel de servicio de Amazon RDS

Esta oferta de pago le da más tiempo para llevar a cabo la actualización a una versión principal del motor compatible. Por ejemplo, la fecha de finalización del soporte estándar de RDS para MySQL 5.7 es el 29 de febrero de 2024. Sin embargo, no está preparado para llevar a cabo la actualización manual a la versión 8.0 de RDS para MySQL antes de esa fecha. En este caso, Amazon RDS inscribe automáticamente sus bases de datos en el Soporte extendido de RDS el 29 de febrero de 2024 y puede seguir ejecutando la versión 5.7 de RDS para MySQL. A partir del 1 de marzo de 2024, Amazon RDS le cobrará automáticamente por el Soporte extendido de RDS.

El soporte extendido de RDS está disponible durante un máximo de 3 años después de la fecha de fin de soporte estándar de RDS para una versión principal del motor. Transcurrido este tiempo, si no ha actualizado la versión principal del motor a una versión compatible, Amazon RDS actualizará

automáticamente la versión principal del motor. Se recomienda que lleva a cabo la actualización a una versión principal del motor compatible lo antes posible.

Para obtener más información sobre las fechas de finalización del soporte estándar de RDS y las fechas de finalización del soporte extendido de RDS, consulte Versiones principales de MySQL compatibles en Amazon RDS y Release calendar for Amazon RDS for PostgreSQL.

Temas

- Información general del Soporte extendido de Amazon RDS
- Precios del Soporte extendido de Amazon RDS
- Versiones con el Soporte extendido de Amazon RDS
- Amazon RDS y las responsabilidades del cliente con el Soporte extendido de Amazon RDS
- Creación de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS
- Visualización de la inscripción de sus instancias de base de datos o clústeres de base de datos multi-AZ en el Soporte extendido de Amazon RDS
- Visualización de las fechas de soporte de las versiones del motor en soporte extendido de Amazon RDS
- Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS

Información general del Soporte extendido de Amazon RDS

Tras la fecha de finalización del soporte estándar de RDS, si no ha deshabilitado el soporte extendido de RDS durante la creación o restauración de las instancias de base de datos, Amazon RDS las inscribirá automáticamente en el soporte extendido de RDS. Amazon RDS actualiza automáticamente su instancia de base de datos a la versión secundaria más reciente publicada antes de la fecha de fin del soporte estándar de RDS, si aún no está ejecutando esa versión. Amazon RDS no actualizará la versión secundaria hasta después de la fecha de finalización del soporte estándar de RDS para su versión principal del motor.

Puede crear nuevas bases de datos con las versiones principales del motor que hayan alcanzado la fecha de finalización del soporte estándar de RDS. RDS inscribe automáticamente estas nuevas bases de datos en el Soporte extendido de RDS y le cobra por esta oferta.

Si realiza una actualización a un motor para el que sigue vigente el soporte estándar de RDS antes de la fecha de finalización del soporte estándar de RDS, Amazon RDS no inscribirá el motor en el Soporte extendido de RDS.

Si intenta restaurar una instantánea de una base de datos compatible con un motor cuya fecha de finalización del soporte estándar de RDS haya pasado, pero que no está inscrito en el Soporte extendido de RDS, Amazon RDS intentará actualizar la instantánea para que sea compatible con la última versión del motor cuyo soporte estándar de RDS sigue vigente. Si se produce un error en la restauración, Amazon RDS inscribirá automáticamente el motor en el Soporte extendido de RDS con una versión que sea compatible con la instantánea.

Puede finalizar la inscripción en el Soporte extendido de RDS en cualquier momento. Para finalizar la inscripción, actualice cada motor inscrito a una versión más reciente cuyo soporte estándar de RDS siga vigente. La finalización de la inscripción en el Soporte extendido de RDS entrará en vigor el día en que complete una actualización a una versión más reciente del motor cuyo soporte estándar de RDS siga vigente.

Para obtener más información sobre las fechas de finalización del soporte estándar de RDS y las fechas de finalización del soporte extendido de RDS, consulte Versiones principales de MySQL compatibles en Amazon RDS y Release calendar for Amazon RDS for PostgreSQL.

Precios del Soporte extendido de Amazon RDS

Se incurrirá en cargos por todos los motores inscritos en el Soporte extendido de RDS a partir del día siguiente a la fecha de finalización del soporte estándar de RDS. Para conocer la fecha de finalización del soporte estándar de RDS, consulte Versiones principales compatibles en MySQL y Release calendar for Amazon RDS for PostgreSQL. Los cargos del Soporte extendido de RDS se aplican a instancias en espera en implementaciones multi-AZ.

El cargo adicional del Soporte extendido de RDS se detiene automáticamente cuando realiza una de las siguientes acciones:

- Actualizar a una versión de motor incluida en el soporte estándar.
- Eliminar la base de datos en la que se ejecuta una versión principal pasada la fecha de finalización del soporte estándar de RDS.

Los cargos se reiniciarán si la versión del motor de destino se incluye en el Soporte extendido de RDS en el futuro.

Por ejemplo, RDS para PostgreSQL 11 entra en el Soporte extendido el 1 de marzo de 2024, pero los cargos no empiezan a cobrarse hasta el 1 de abril de 2024. Actualiza la base de datos RDS para PostgreSQL 11 a RDS para PostgreSQL 12 el 30 de abril de 2024. Solo se le cobrarán 30 días de soporte extendido en RDS para PostgreSQL 11. Seguirá ejecutando RDS para PostgreSQL 12 en esta instancia de base de datos después de la fecha de finalización del soporte estándar de RDS, el 28 de febrero de 2025. Su base de datos volverá a incurrir en cargos de Soporte extendido de RDS a partir del 1 de marzo de 2025.

Para obtener más información, consulte Precios de Amazon RDS para MySQL y Precios de Amazon RDS para PostgreSQL.

Prevención de cargos del Soporte extendido de Amazon RDS

Puede evitar que se le cobre por el Soporte extendido de RDS impidiendo que RDS cree o restaure una instancia de base de datos o un clúster de base de datos multi-AZ después de la fecha de finalización del soporte estándar de RDS. Para ello, utilice la AWS CLI o la API de RDS.

En la AWS CLI, especifique `open-source-rds-extended-support-disabled` para la opción `--engine-lifecycle-support`. En la API de RDS, especifique `open-source-rds-extended-support-disabled` para el parámetro `LifeCycleSupport`. Para obtener más información, consulte Creación de una instancia de base de datos o un clúster de base de datos multi-AZ o Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ.

Versiones con el Soporte extendido de Amazon RDS

El Soporte extendido de RDS solo está disponible para las versiones principales. No está disponible para versiones secundarias.

El soporte extendido de RDS está disponible para RDS para MySQL y para RDS para PostgreSQL. Para obtener más información, consulte Versiones principales compatibles en MySQL y Release calendar for Amazon RDS for PostgreSQL en Amazon RDS for PostgreSQL Release Notes.

También puede ver información sobre las fechas de soporte de las versiones del motor mediante la AWS CLI o la API de RDS. Para obtener más información, consulte Visualización de las fechas de soporte de las versiones del motor en soporte extendido de Amazon RDS.

Nombre de versiones con el Soporte extendido de Amazon RDS

Amazon RDS lanzará nuevas versiones secundarias con correcciones y parches de CVE para los motores con el Soporte extendido de RDS. Para obtener más información, consulte Versiones

de soporte extendido de Amazon RDS para RDS para MySQL y Amazon RDS Extended Support updates for RDS for PostgreSQL en Amazon RDS for PostgreSQL Release Notes.

Los nombres de estas versiones secundarias tendrán el formato major.minor-RDS.YYYYMMDD.patch.YYYYMMDD; por ejemplo, 5.7.44-RDS.20240208.R2.20240210 (para RDS para MySQL) o 11.22-RDS.20240208.R2.20240210 (para RDS para PostgreSQL).

principal

Para MySQL. el número de versión principal es tanto el entero como la primera parte fraccional del número de versión (por ejemplo, 8.0). Una actualización de versión principal aumenta la parte principal del número de versión. Por ejemplo, una actualización de 5.7.44 a 8.0.33 es una actualización de versión principal, donde 5.7 y 8.0 son los números de la versión principal.

Para PostgreSQL, el número de versión principal es el entero; por ejemplo, 11.

minor-RDS.YYYYMMDD

Para MySQL, el número de versión secundaria es la tercera parte del número de versión (por ejemplo, el 44-RDS.20240208 en 5.7.44-RDS.20240208).

Para PostgeSQL, el número de versión secundaria es la segunda parte del número de versión (por ejemplo, el 22-RDS.20240208 en 11.22-RDS.20240208).

La fecha es cuando Amazon RDS creó la versión secundaria de Amazon RDS.

parche

La versión del parche es la que sigue a la fecha en que Amazon RDS creó la versión secundaria de Amazon RDS; por ejemplo, R2 en 5.7.44-RDS.20240208.R2 o 11.22-RDS.20240208.R2.

Una versión de parche de Amazon RDS incluye correcciones de errores importantes que se agregaron a una versión secundaria de Amazon RDS después de su lanzamiento.

AAAAMMDD

La fecha es aquella en la que Amazon RDS creó la versión del parche; por ejemplo, 20240210 en 5.7.44-RDS.20240208.R2.20240210 o 11.22-RDS.20240208.R2.20240210.

Una versión de fecha de Amazon RDS es un parche de seguridad que incluye correcciones de seguridad importantes que se agregan a una versión secundaria después de su lanzamiento. No incluye ninguna corrección que pueda cambiar el comportamiento de un motor.

Amazon RDS y las responsabilidades del cliente con el Soporte extendido de Amazon RDS

El siguiente contenido describe las responsabilidades de Amazon RDS y sus responsabilidades con el Soporte extendido de RDS.

Temas

- Responsabilidades de Amazon RDS
- Sus responsabilidades

Responsabilidades de Amazon RDS

Tras la fecha de finalización del soporte estándar de RDS, Amazon RDS proporcionará parches, correcciones de errores y actualizaciones para los motores inscritos en el Soporte extendido de RDS. Esto ocurrirá durante un máximo de 3 años o hasta que deje de utilizar los motores, lo que ocurra primero.

Los parches serán para las CVE críticas y altas, según se definen en las puntuaciones de gravedad de CVSS de la National Vulnerability Database (NVD). Para obtener más información, consulte las métricas de vulnerabilidad.

Sus responsabilidades

Usted es responsable de aplicar los parches, las correcciones de errores y las actualizaciones proporcionadas para las instancias de bases de datos o los clústeres de bases de datos multi-AZ inscritos en el Soporte extendido de RDS. Amazon RDS se reserva el derecho de cambiar, sustituir o retirar dichos parches, correcciones de errores y actualizaciones en cualquier momento. Si se necesita un parche para solucionar problemas de seguridad o estabilidad críticos, Amazon RDS se reserva el derecho de actualizar sus instancias de bases de datos o clústeres de bases de datos multi-AZ con el parche, o bien de solicitarle que instale el parche.

También es responsable de actualizar el motor a una versión más reciente antes de la fecha de finalización del Soporte extendido de RDS. La fecha de finalización del Soporte extendido de RDS suele ser 3 años después de la fecha de finalización del soporte estándar de RDS. Para conocer la fecha de fin del Soporte extendido de RDS para la versión principal del motor de bases de datos, consulte Versiones principales compatibles en MySQL y Release calendar for Amazon RDS for PostgreSQL.

Si no actualiza el motor, después de la fecha de finalización del soporte extendido de RDS, Amazon RDS intentará actualizar el motor a una versión más reciente del motor que admita el soporte estándar RDS. Si se produce un fallo de actualización, Amazon RDS se reserva el derecho a eliminar la instancia de bases de datos o el clúster de bases de datos multi-AZ que ejecuta el motor una vez pasada la fecha de finalización del soporte estándar de RDS. Sin embargo, antes de hacerlo, Amazon RDS conservará los datos de ese motor.

Creación de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS

Al crear una instancia de base de datos o un clúster de base de datos multi-AZ, seleccione Habilitar el Soporte extendido de RDS en la consola, o utilice la opción Soporte extendido en la AWS CLI o el parámetro de API de RDS. Al inscribir una instancia de base de datos o un clúster de base de datos multi-AZ en el Soporte extendido de Amazon RDS, se inscribe permanentemente en el Soporte extendido de RDS durante toda la vida de la instancia de base de datos o el clúster de base de datos multi-AZ.

Si usa la consola, debe seleccionar Activar el soporte extendido de RDS. La opción no está seleccionada de forma predeterminada.

Si utiliza la AWS CLI o la API de RDS y no especifica la opción del Soporte extendido de RDS, Amazon RDS usará de manera predeterminada el Soporte extendido de RDS. Al automatizar usando AWS CloudFormation u otros servicios, este comportamiento predeterminado mantiene la disponibilidad de la base de datos después de la fecha del fin del soporte estándar de RDS.

Puede evitar la inscripción en el Soporte extendido de RDS mediante la AWS CLI o la API de RDS para crear una instancia de base de datos o un clúster de base de datos multi-AZ.

Temas

- Comportamiento del Soporte extendido de RDS
- Observaciones sobre el Soporte extendido de RDS
- Creación de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de RDS

Comportamiento del Soporte extendido de RDS

En la siguiente tabla se resume lo que ocurre cuando una versión principal del motor llega al final del soporte estándar de RDS.

Estado del Soporte extendido de RDS*	Comportamiento
Habilitado	Amazon RDS le cobra por el Soporte extendido de RDS.
Deshabilitado	Amazon RDS actualiza su instancia de base de datos o clúster de base de datos multi-AZ a una versión del motor compatible. Esta actualización se lleva a cabo en la fecha de fin del soporte estándar de RDS o poco después.

* En la consola de RDS, el estado del Soporte extendido de RDS aparece como Sí o No. En la AWS CLI o en la API de RDS, el estado del Soporte extendido de RDS aparece como `open-source-rds-extended-support` o `open-source-rds-extended-support-disabled`.

Observaciones sobre el Soporte extendido de RDS

Antes de crear una instancia de base de datos o un clúster de base de datos multi-AZ, tenga en cuenta lo siguiente:

- Una vez pasada la fecha del fin del soporte estándar de RDS, puede impedir que se cree una nueva instancia de base de datos o un nuevo clúster de base de datos multi-AZ y evitar los cargos del Soporte extendido de RDS. Para ello, utilice la AWS CLI o la API de RDS. En la AWS CLI, especifique `open-source-rds-extended-support-disabled` para la opción `--engine-lifecycle-support`. En la API de RDS, especifique `open-source-rds-extended-support-disabled` para el parámetro `LifeCycleSupport`. Si especifica `open-source-rds-extended-support-disabled` y ha pasado la fecha del fin del soporte estándar de RDS, siempre se producirá un error al crear una instancia de base de datos o un clúster de base de datos multi-AZ.
- El Soporte extendido de RDS se establece en el nivel de clúster. Los miembros de un clúster siempre tendrán la misma configuración para el Soporte extendido de RDS en la consola de RDS, `--engine-lifecycle-support` en la AWS CLI y `EngineLifecycleSupport` en la API de RDS.

Para obtener más información, consulte Versiones de MySQL y el Calendario de versiones de Amazon RDS para PostgreSQL.

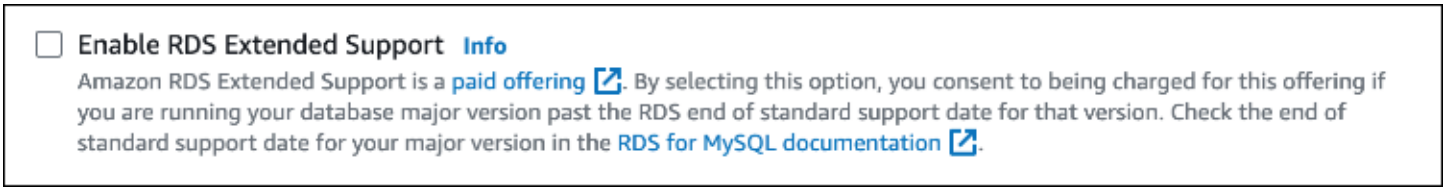
Creación de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de RDS

Puede crear una instancia de base de datos o un clúster de base de datos multi-AZ con una versión del Soporte extendido de RDS que utilice la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Al crear una instancia de base de datos o un clúster de base de datos multi-AZ, seleccione Habilitar el Soporte extendido de RDS en la sección Opciones del motor. Esta configuración no está seleccionada de forma predeterminada.

La siguiente imagen muestra la configuración Habilitar el Soporte extendido de RDS:



AWS CLI

Cuando ejecute el comando create-db-instance o create-db-cluster (clúster de base de datos multi-AZ) de la AWS CLI, seleccione el Soporte extendido de RDS especificando `open-source-rds-extended-support` para la opción `--engine-lifecycle-support`. Esta opción está configurada en `open-source-rds-extended-support` de forma predeterminada.

Para evitar la creación de una nueva instancia de base de datos o un clúster de base de datos multi-AZ después de la fecha del fin del soporte estándar de RDS, especifique `open-source-rds-extended-support-disabled` para la opción `--engine-lifecycle-support`. De este modo, evitará los cargos del Soporte extendido de RDS asociados.

API de RDS

Cuando utilice la operación API CreateDBInstance o CreateDBCluster (clúster de base de datos multi-AZ) de Amazon RDS, seleccione el Soporte extendido de RDS poniendo el parámetro

`EngineLifecycleSupport` en `open-source-rds-extended-support`. Este parámetro está establecido en `open-source-rds-extended-support` de forma predeterminada.

Para evitar la creación de una nueva instancia de base de datos o un clúster de base de datos multi-AZ después de la fecha del fin del soporte estándar de RDS, especifique `open-source-rds-extended-support-disabled` para el parámetro `EngineLifecycleSupport`. De este modo, evitará los cargos del Soporte extendido de RDS asociados.

Para obtener más información, consulte los temas siguientes:

- Para crear una instancia de base de datos, siga las instrucciones del motor de base de datos específico que se indican en Creación de una instancia de base de datos de Amazon RDS.
- Para crear un clúster de bases de datos Multi-AZ, siga las instrucciones para su motor de base de datos en Creación de un clúster de base de datos multi-AZ para Amazon RDS.

Visualización de la inscripción de sus instancias de base de datos o clústeres de base de datos multi-AZ en el Soporte extendido de Amazon RDS

Puede ver la inscripción de sus instancias de base de datos o clústeres de base de datos multi-AZ en el Soporte extendido de RDS usando la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> La columna Soporte extendido de RDS de la consola, la opción `-engine-lifecycle-support` en la AWS CLI y el parámetro `EngineLifecycleSupport` de la API de RDS solo indican la inscripción en el Soporte extendido de RDS. Los cargos por el Soporte extendido de RDS solo comienzan cuando la versión de su motor de base de datos ha alcanzado el final del soporte estándar de RDS. Para obtener más información, consulte Versiones principales compatibles en MySQL y Release calendar for Amazon RDS for PostgreSQL en Amazon RDS for PostgreSQL Release Notes.
>
> Por ejemplo, tiene una base de datos de RDS para MySQL 5.7 que está inscrita en el Soporte extendido de RDS. El 1 de marzo de 2024, Amazon RDS comenzó a cobrarle por el Soporte extendido de RDS para esta base de datos. El 31 de julio de 2024, actualizó esta base de datos a RDS para MySQL 8.0. El estado del Soporte extendido de RDS para esta base de datos permanece habilitado. Sin embargo, los cargos del Soporte extendido de RDS para esta base de datos se suspendieron porque RDS para MySQL 8.0 aún no había

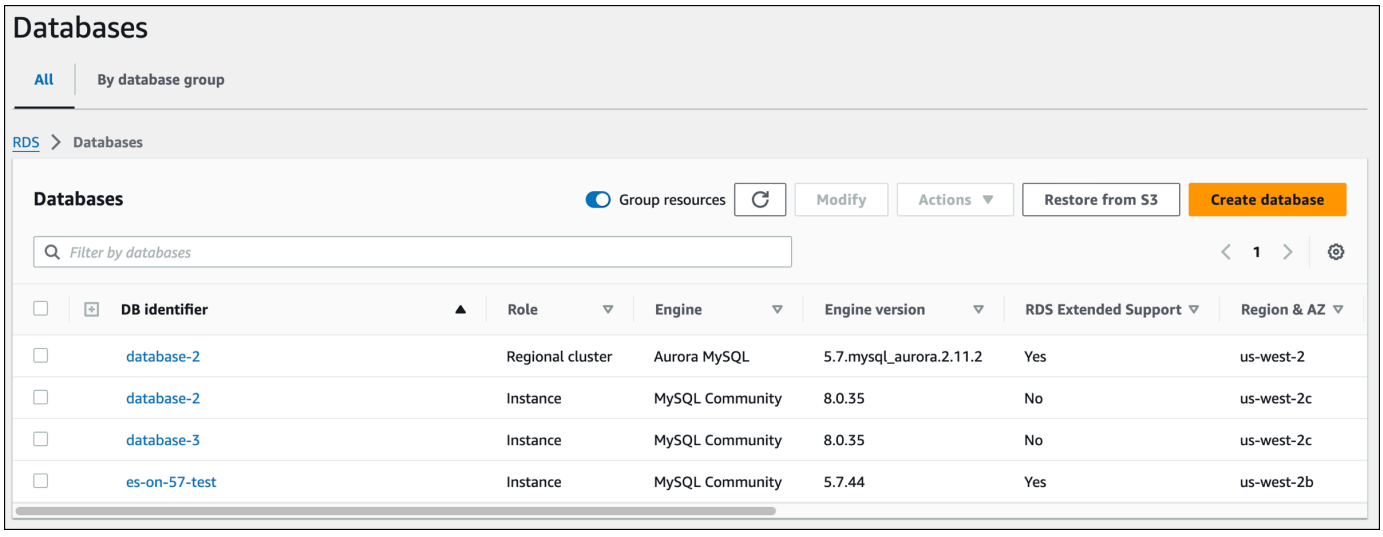
alcanzado el final del soporte estándar de RDS. Amazon RDS no le cobrará por el Soporte extendido de RDS para esta base de datos hasta el 1 de agosto de 2026, fecha en la que finaliza el soporte estándar de RDS para MySQL 8.0.

Consola

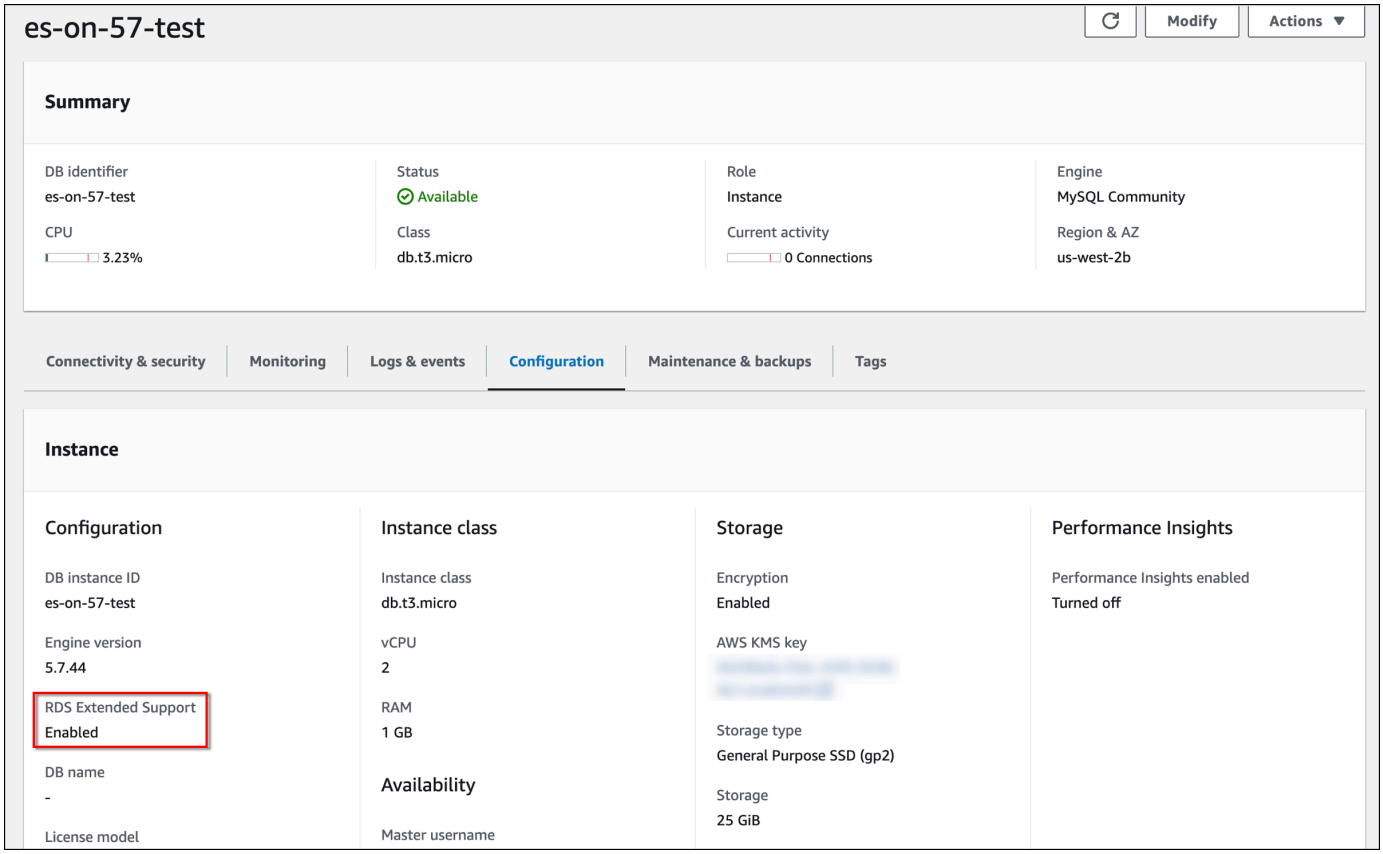
Para ver la inscripción de sus instancias de base de datos o clústeres de base de datos multi-AZ en el Soporte extendido de RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos). El valor en Soporte extendido de RDS indica si una instancia de base de datos o un clúster de base de datos multi-AZ están inscritos en el Soporte extendido de RDS. Si no aparece ningún valor, eso significa que el Soporte extendido de RDS no está disponible para su base de datos.

> **Tip**
>
> Si la columna Soporte extendido de RDS no aparece, seleccione el icono Preferencias y, a continuación, active Soporte extendido de RDS.



3. También puede ver la inscripción en la pestaña Configuración de de cada base de datos. Elija una base de datos en el Identificador de la base de datos. En la pestaña Configuración, consulte Soporte extendido para ver si la base de datos está inscrita o no.



AWS CLI

Para ver la inscripción de sus bases de datos en el Soporte extendido de RDS mediante la AWS CLI, ejecute el comando describe-db-instances o describe-db-clusters (clústeres de base de datos multi-AZ).

Si el Soporte extendido de RDS está disponible para una base de datos, la respuesta incluye el parámetro `EngineLifecycleSupport`. El valor `open-source-rds-extended-support` indica que una instancia de base de datos o clúster de base de datos multi-AZ están inscritos en el Soporte extendido de RDS. El valor `open-source-rds-extended-support-disabled` indica que se ha deshabilitado la inscripción de la instancia de base de datos o clúster de base de datos multi-AZ en el Soporte extendido de RDS.

Ejemplo

El siguiente comando devuelve la información de todas las instancias de base de datos:

```
aws rds describe-db-instances
```

La siguiente respuesta muestra que un motor PostgreSQL que se ejecuta en la instancia de base de datos `database-1` está inscrito en el Soporte extendido de RDS:

```
{
    "DBInstanceIdentifier": "database-1",
    "DBInstanceClass": "db.t3.large",
    "Engine": "postgres",
    ...
    "EngineLifecycleSupport": "open-source-rds-extended-support"
}
```

API de RDS

Para ver la inscripción de sus bases de datos en el Soporte extendido de RDS mediante la API de Amazon RDS, utilice la operación DescribeDBInstances o DescribeDBClusters.

Si el Soporte extendido de RDS está disponible para una base de datos, la respuesta incluye el parámetro `EngineLifecycleSupport`. El valor `open-source-rds-extended-support` indica que una instancia de base de datos o clúster de base de datos multi-AZ están inscritos en el Soporte extendido de RDS. El valor `open-source-rds-extended-support-disabled` indica que se ha deshabilitado la inscripción de la instancia de base de datos o clúster de base de datos multi-AZ en el Soporte extendido de RDS.

Visualización de las fechas de soporte de las versiones del motor en soporte extendido de Amazon RDS

Puede ver la información sobre las fechas de soporte de las versiones de motor para las instancias de base de datos o los clústeres de base de datos de Multi-AZ en el soporte extendido de Amazon RDS mediante la AWS CLI o la API de RDS. Esta información puede ayudarle a planificar las actualizaciones.

Los comandos de la AWS CLI y las operaciones de la API de RDS devuelven las fechas de inicio y finalización del soporte estándar de RDS y del soporte extendido de RDS. Estas fechas también se pueden encontrar en las tablas de versiones principales del motor. Para obtener más información, consulte Versiones principales de MySQL compatibles en Amazon RDS y Calendario de publicación de versiones de Amazon RDS para PostgreSQL en Notas de la versión de Amazon RDS para PostgreSQL.

AWS CLI

Para ver las fechas de inicio y finalización del soporte estándar de RDS y del soporte extendido de RDS para las versiones principales del motor mediante la AWS CLI, ejecute el comando describe-db-major-engine-versions.

Este comando devuelve los siguientes parámetros relevantes para los motores de código abierto (MariaDB, MySQL y PostgreSQL). No devuelve estos parámetros para los motores comerciales (Db2, SQL Server y Oracle).

- `SupportedEngineLifecycles`: este parámetro es una matriz de objetos que incluye `LifecycleSupportName`, `LifecycleSupportStartDate` y `LifecycleSupportEndDate`.
- `LifecycleSupportName`: este parámetro indica el tipo de soporte en el que se encuentra la versión del motor: soporte estándar para RDS (`open-source-rds-standard-support`) o soporte extendido de RDS (`open-source-rds-extended-support`). Para MariaDB, este parámetro solo devuelve el soporte estándar de RDS (`open-source-rds-standard-support`).
- `LifecycleSupportStartDate`: este parámetro muestra la fecha de inicio del soporte estándar de RDS o del soporte extendido de RDS para la versión principal del motor, según el valor de `LifecycleSupportName`.
- `LifecycleSupportEndDate`: este parámetro muestra la fecha de finalización del soporte estándar de RDS o del soporte extendido de RDS para la versión principal del motor, según el valor de `LifecycleSupportName`.

Ejemplo

El ejemplo de respuesta muestra la siguiente información:

- Las fechas de inicio y finalización de los ciclos de vida de los motores compatibles `open-source-rds-standard-support` y `open-source-rds-extended-support` para MySQL 5.7. El soporte extendido de RDS está disponible para MySQL 5.7.
- Las fechas de inicio y finalización del ciclo de vida del motor compatible `open-source-rds-standard-support` para MariaDB 10.6. El soporte extendido de RDS no está disponible para MariaDB 10.6.
- No hay información sobre los ciclos de vida de los motores compatibles para SQL Server Enterprise Edition 13 porque SQL Server es un motor comercial.

```
{
    "DBMajorEngineVersions": [
        {
            "Engine": "mysql",
            "MajorEngineVersion": "5.7",
            "SupportedEngineLifecycles": [
                {
                    "LifecycleSupportName": "open-source-rds-standard-support",
                    "LifecycleSupportStartDate": "2016-02-22T00:00:00+00:00",
                    "LifecycleSupportEndDate": "2024-02-29T23:59:59.999000+00:00"
                },
                {
                    "LifecycleSupportName": "open-source-rds-extended-support",
                    "LifecycleSupportStartDate": "2024-03-01T00:00:00+00:00",
                    "LifecycleSupportEndDate": "2027-02-28T23:59:59.999000+00:00"
                }
            ]
        },
        {
            "Engine": "mariadb",
            "MajorEngineVersion": "10.6",
            "SupportedEngineLifecycles": [
                {
                    "LifecycleSupportName": "open-source-rds-standard-support",
                    "LifecycleSupportStartDate": "2022-02-03T00:00:00+00:00",
                    "LifecycleSupportEndDate": "2026-07-31T23:59:59.999000+00:00"
                }
            ]
        },
        {
            "Engine": "sqlserver-ee",
            "MajorEngineVersion": "13.00"
        },
        ...
    ]
}
```

API de RDS

Para ver las fechas de inicio y finalización del soporte estándar de RDS y del soporte extendido de RDS para las versiones principales del motor mediante la API de RDS, utilice la operación DescribeDBMajorEngineVersions.

Si el soporte extendido de RDS está disponible para una versión del motor, la respuesta incluye el parámetro `SupportedEngineLifeCycles` como una matriz con dos objetos. Un objeto incluye las fechas de inicio y finalización del soporte estándar de RDS. El segundo objeto incluye las fechas de inicio y finalización del soporte extendido de RDS.

Si el soporte extendido de RDS no está disponible para una versión de motor de código abierto (MariaDB, MySQL y PostgreSQL), la respuesta solo incluye el parámetro `SupportedEngineLifeCycles` como una matriz con un único objeto. Este objeto incluye las fechas de inicio y finalización del soporte estándar de RDS.

Si la versión del motor es para un motor comercial (Db2, SQL Server y Oracle), la respuesta no incluye el parámetro `SupportedEngineLifeCycles`.

Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS

Al restaurar una instancia de base de datos o un clúster de base de datos multi-AZ, seleccione Habilitar el Soporte extendido de RDS en la consola, o utilice la opción Soporte extendido en la AWS CLI o el parámetro de API de RDS. Al inscribir una instancia de base de datos o un clúster de base de datos multi-AZ en el Soporte extendido de Amazon RDS, se inscribe permanentemente en el Soporte extendido de RDS durante toda la vida de la instancia de base de datos o el clúster de base de datos multi-AZ.

El valor predeterminado de la configuración del Soporte extendido de RDS depende de si utiliza la consola, la AWS CLI o la API de RDS para restaurar la base de datos. Si utiliza la consola, no selecciona Habilitar el Soporte extendido de RDS y la versión principal del motor que va a restaurar ha superado la fecha de finalización del soporte estándar para RDS, Amazon RDS actualiza automáticamente la instancia de base de datos a una versión de motor más reciente. Si utiliza la AWS CLI o la API de RDS y no especifica la configuración del Soporte extendido de RDS, entonces Amazon RDS usará de manera predeterminada el Soporte extendido de RDS. Al automatizar usando AWS CloudFormation u otros servicios, este comportamiento predeterminado mantiene la disponibilidad de la base de datos después de la fecha del fin del soporte estándar de RDS. Puede deshabilitar el Soporte extendido de RDS mediante la AWS CLI o la API de RDS.

Temas

- Comportamiento del Soporte extendido de RDS
- Observaciones sobre el Soporte extendido de RDS

- Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de RDS

Comportamiento del Soporte extendido de RDS

En la siguiente tabla se resume lo que ocurre cuando una versión del motor principal de una instancia de base de datos o un clúster de base de datos multi-AZ que está restaurando ha alcanzado el final del soporte estándar de RDS.

Estado del Soporte extendido de RDS*	Comportamiento
Habilitado	Amazon RDS le cobra por el Soporte extendido de RDS.
Deshabilitado**	Una vez finalizada la restauración, Amazon RDS actualiza automáticamente la instancia de base de datos o el clúster de base de datos multi-AZ a una versión de motor más reciente (en un futuro periodo de mantenimiento).

* En la consola de RDS, el estado del Soporte extendido de RDS aparece como Sí o No. En la AWS CLI o en la API de RDS, el estado del Soporte extendido de RDS aparece como `open-source-rds-extended-support` o `open-source-rds-extended-support-disabled`.

** Esta opción solo está disponible al restaurar una instancia de base de datos o un clúster de base de datos multi-AZ que ejecute PostgreSQL 12 y versiones posteriores o MySQL 8 y versiones posteriores.

Observaciones sobre el Soporte extendido de RDS

Antes de restaurar una instancia de base de datos o un clúster de base de datos multi-AZ, tenga en cuenta lo siguiente:

- Tras la fecha de finalización del soporte estándar de RDS, si desea restaurar una instancia de base de datos o un clúster de base de datos multi-AZ desde Amazon S3, solo podrá hacerlo con la AWS CLI o la API de RDS. Utilice la opción `--engine-lifecycle-support` en el comando restore-db-cluster-from-s3 de la AWS CLI o el parámetro `EngineLifecycleSupport` en la operación API RestoreDBClusterFromS3 de RDS.

- Si desea evitar que RDS restaure sus bases de datos a las versiones del Soporte extendido de RDS, especifique `open-source-rds-extended-support-disabled` en la AWS CLI o en la API de RDS. De este modo, evitará los cargos del Soporte extendido de RDS asociados.

  Si especifica esta configuración, Amazon RDS actualizará automáticamente la base de datos restaurada a una versión principal compatible más reciente. Si la actualización no pasa las comprobaciones previas, Amazon RDS volverá de forma segura a la versión del motor del Soporte extendido de RDS. Esta base de datos permanecerá en el modo de Soporte extendido de RDS y Amazon RDS le cobrará por el Soporte extendido de RDS hasta que actualice manualmente la base de datos.

  Por ejemplo, si restaura una instantánea de MySQL 5.7 sin utilizar el Soporte extendido de RDS, Amazon RDS intentará actualizar automáticamente la base de datos a MySQL 8.0. Si esta actualización falla debido a un problema que debe resolverse, Amazon RDS revertirá la base de datos a MySQL 5.7. Amazon RDS mantendrá la base de datos en el Soporte extendido de RDS hasta que pueda solucionar el problema. Por ejemplo, es posible que se produzca un error en una actualización debido a la falta de espacio de almacenamiento. Tras solucionar el problema, debe iniciar la actualización. Tras el primer intento de actualización de la base de datos, Amazon RDS no intentará volver a actualizarla.
- El Soporte extendido de RDS se establece en el nivel de clúster. Los miembros de un clúster siempre tendrán la misma configuración para el Soporte extendido de RDS en la consola de RDS, `--engine-lifecycle-support` en la AWS CLI y `EngineLifecycleSupport` en la API de RDS.

Para obtener más información, consulte Versiones de MySQL y el Calendario de versiones de Amazon RDS para PostgreSQL.

Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de RDS

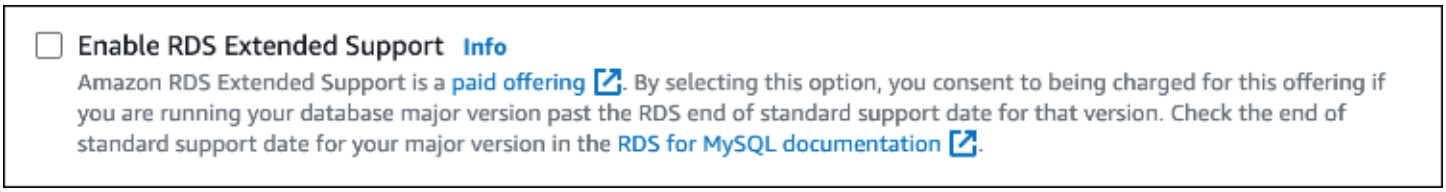
Puede restaurar una instancia de base de datos o un clúster de base de datos multi-AZ con una versión del Soporte extendido de RDS que utilice la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Al restaurar una instancia de base de datos o un clúster de base de datos multi-AZ, seleccione Habilitar el Soporte extendido de RDS en la sección Opciones del motor. Si no selecciona esta

configuración y la versión principal del motor que va a restaurar ha superado la fecha de finalización del soporte estándar de RDS, Amazon RDS actualiza automáticamente su instancia de base de datos o clúster de base de datos multi-AZ a una versión cuyo soporte estándar de RDS esté vigente.

La siguiente imagen muestra la configuración Habilitar el Soporte extendido de RDS:



AWS CLI

Cuando ejecute el comando restore-db-instance-from-db-snapshot o restore-db-cluster-from-snapshot de la AWS CLI, seleccione el Soporte extendido de RDS especificando `open-source-rds-extended-support` para la opción `--engine-lifecycle-support`.

Si quiere evitar los cargos asociados con el Soporte extendido de RDS, defina la opción `--engine-lifecycle-support` en `open-source-rds-extended-support-disabled`. Esta opción está configurada en `open-source-rds-extended-support` de forma predeterminada.

También puede especificar este valor con los siguientes comandos de la AWS CLI:

- restore-db-cluster-from-s3
- restore-db-clúster-to-point-in-time
- restore-db-instance-from-s3
- restore-db-instance-to-point-in-time

API de RDS

Cuando utilice la operación API RestoreDBInstanceFromDBSnapshot o RestoreDBClusterFromSnapshot de Amazon RDS, seleccione el Soporte extendido de RDS ajustando el parámetro `EngineLifecycleSupport` en `open-source-rds-extended-support`.

Si quiere evitar los cargos asociados con el Soporte extendido de RDS, defina el parámetro `EngineLifecycleSupport` en `open-source-rds-extended-support-disabled`. Este parámetro está establecido en `open-source-rds-extended-support` de forma predeterminada.

También puede especificar este valor utilizando las siguientes operaciones API de RDS:

- RestoreDBClusterFromS3
- RestoreDBclústerToPointInTime
- RestoreDBInstanceFromS3
- RestoreDBInstanceToPointInTime

Para obtener más información sobre cómo restaurar una instancia de base de datos o un clúster de base de datos multi-AZ, siga las instrucciones en Restauración a una instancia de base de datos para su motor de base de datos.

Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos

Una implementación azul/verde copia un entorno de base de datos de producción en un entorno de almacenamiento provisional sincronizado e independiente. Con las implementaciones azul/verde de Amazon RDS, puede realizar cambios en la base de datos en el entorno de almacenamiento provisional sin que eso afecte al entorno de producción. Por ejemplo, puede actualizar la versión principal o secundaria del motor de base de datos o cambiar los parámetros de la base de datos en el entorno de ensayo. Cuando esté listo, puede promocionar el entorno de almacenamiento provisional para que sea el nuevo entorno de la base de datos de producción, con un tiempo de inactividad normalmente inferior a un minuto.

> **Note**
>
> Actualmente, las implementaciones azul/verde solo son compatibles en RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL. Para conocer la disponibilidad de Amazon Aurora, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos en la Guía del usuario de Amazon Aurora.

Temas

- Descripción general de las implementaciones azul/verde de Amazon RDS
- Creación de una implementación azul/verde en Amazon RDS
- Visualización de una implementación azul/verde en Amazon RDS
- Cambio de una implementación azul/verde en Amazon RDS
- Eliminación de una implementación azul/verde en Amazon RDS

Descripción general de las implementaciones azul/verde de Amazon RDS

Con las implementaciones azul/verde de Amazon RDS, puede realizar y probar cambios en las bases de datos antes de implementarlas en un entorno de producción. Una implementación azul/verde crea un área de almacenamiento provisional que copia el entorno de producción. En una implementación azul/verde, el entorno azul es el entorno de producción actual. El entorno verde es el entorno de almacenamiento provisional. El entorno de almacenamiento provisional permanece sincronizado con el entorno de producción actual mediante la replicación lógica.

Puede realizar cambios en las instancias de base de datos de RDS en un entorno verde sin que eso afecte a las cargas de trabajo de producción. Por ejemplo, puede actualizar la versión principal o secundaria del motor de base de datos, actualizar la configuración del sistema de archivos subyacente o cambiar los parámetros de la base de datos en el entorno de almacenamiento provisional. Puede probar exhaustivamente los cambios en el entorno verde. Cuando esté listo, puede conmutar los entornos para hacer que el entorno verde sea el nuevo entorno de producción. La conmutación suele tardar menos de un minuto sin que se produzca una pérdida de datos y sin la necesidad de realizar cambios en la aplicación.

Dado que el entorno verde es una copia de la topología del entorno de producción, el entorno verde incluye las características utilizadas por la instancia de base de datos. Estas características incluyen las réplicas de lectura, la configuración del almacenamiento, las instantáneas de bases de datos, las copias de seguridad automatizadas, Información sobre rendimiento y la monitorización mejorada. Si la instancia de base de datos azul/verde es una implementación de instancia de base de datos Multi-AZ, la instancia de base de datos verde es también una implementación de la instancia de base de datos Multi-AZ.

> **Note**
>
> Actualmente, las implementaciones azul/verde solo son compatibles en RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL. Para conocer la disponibilidad de Amazon Aurora, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos en la Guía del usuario de Amazon Aurora.

Temas

- Disponibilidad en regiones y versiones

- Ventajas de utilizar las implementaciones azul/verde de Amazon RDS
- Flujo de trabajo de una implementación azul/verde
- Autorización del acceso a las operaciones de la implementación azul/verde de Amazon RDS
- Limitaciones y consideraciones para implementaciones azul/verde de Amazon RDS
- Prácticas recomendadas para las implementaciones azul/verde de Amazon RDS

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información, consulte the section called “Implementaciones azul/verde”.

Ventajas de utilizar las implementaciones azul/verde de Amazon RDS

Al utilizar las implementaciones azul/verde de Amazon RDS, puede mantenerse al día con los parches de seguridad, mejorar el rendimiento de las bases de datos y adoptar nuevas características de bases de datos con un tiempo de inactividad breve y predecible. Las implementaciones azules y verdes reducen los riesgos y el tiempo de inactividad de las actualizaciones de las bases de datos, como las actualizaciones principales o secundarias de las versiones del motor.

Las implementaciones azul/verde ofrecen los siguientes beneficios:

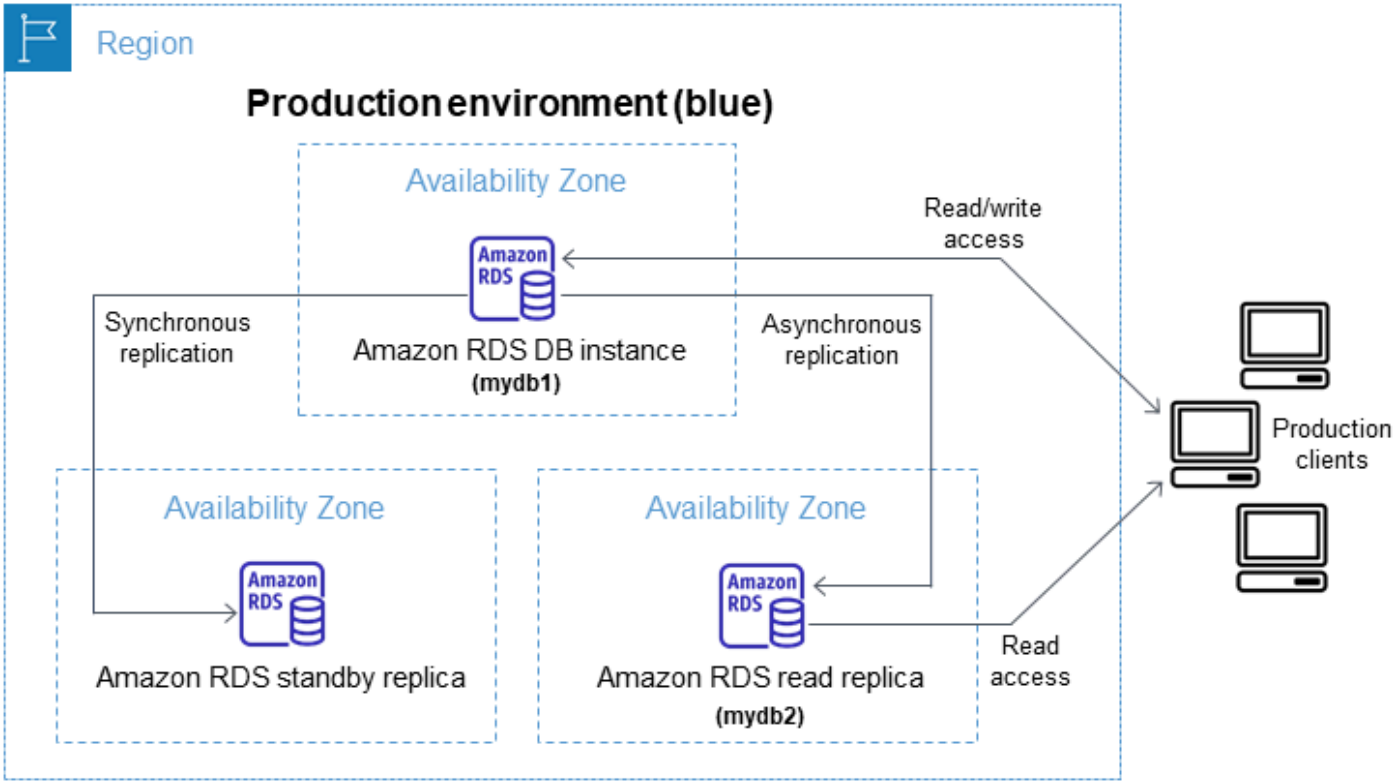
- Cree fácilmente un entorno de almacenamiento provisional listo para la producción.
- Replique automáticamente los cambios de la base de datos del entorno de producción al entorno de almacenamiento provisional.
- Pruebe los cambios en la base de datos en un entorno de almacenamiento provisional seguro sin que eso afecte al entorno de producción.
- Manténgase al día con los parches de las bases de datos y las actualizaciones del sistema.
- Implemente y pruebe las características más recientes de las bases de datos.
- Conmute su entorno de almacenamiento provisional para convertirlo en el nuevo entorno de producción sin cambios en la aplicación.
- Cambie de forma segura mediante el uso de barreras de protección de conmutaciones integradas.
- Elimine la pérdida de datos durante la conmutación.
- Conmutar rápidamente, normalmente en menos de un minuto, según su carga de trabajo.

Flujo de trabajo de una implementación azul/verde

Realice los siguientes pasos principales cuando utilice una implementación azul/verde para las actualizaciones de la base de datos.

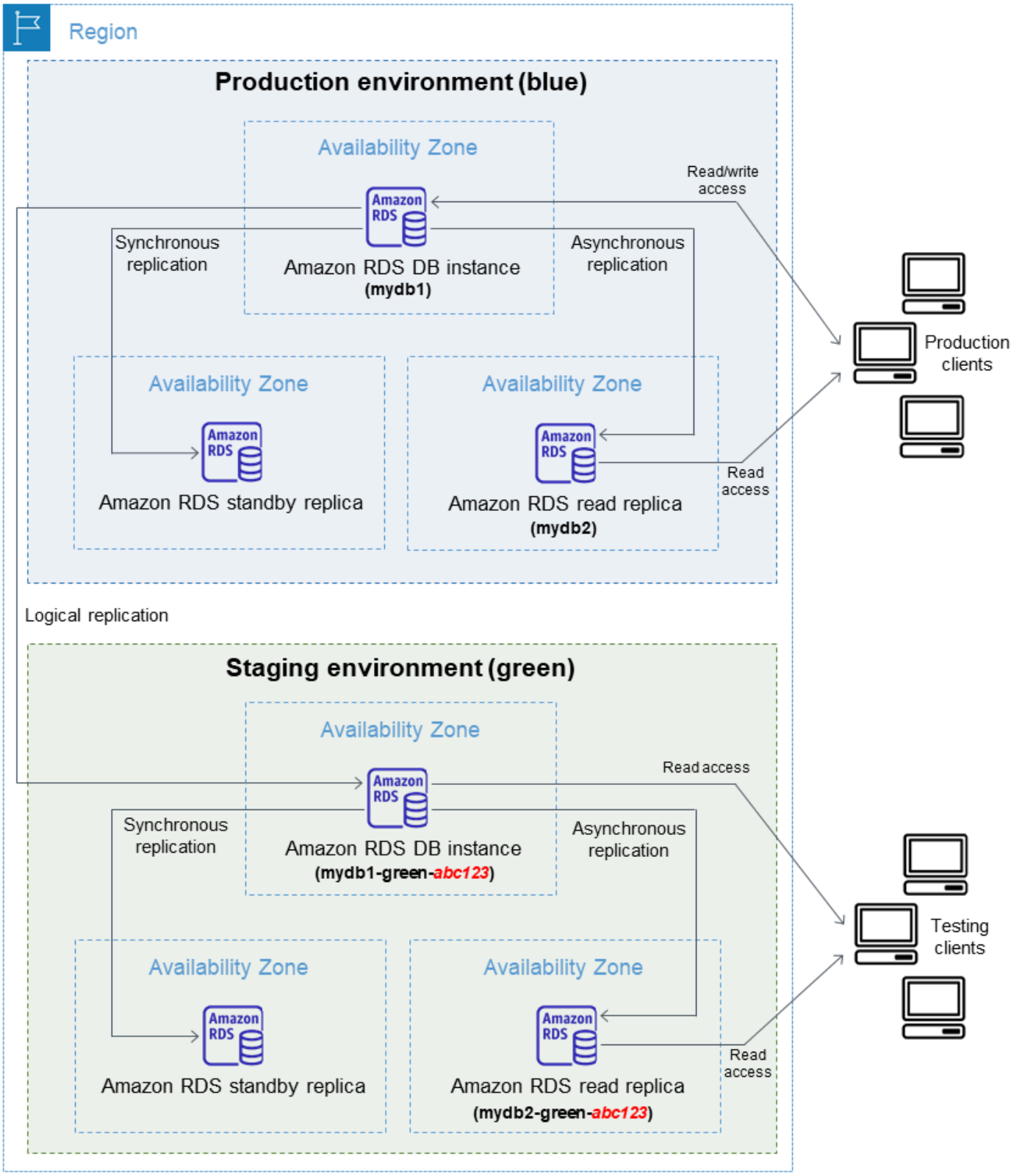
1. Identifique un entorno de producción que requiera actualizaciones.

   Por ejemplo, el entorno de producción de esta imagen tiene una implementación de instancias de base de datos Multi-AZ (mydb1) y una réplica de lectura (mydb2).



2. Cree la implementación azul/verde. Para obtener instrucciones, consulte Creación de una implementación azul/verde en Amazon RDS.

   La siguiente imagen muestra un ejemplo de una implementación azul/verde del entorno de producción del paso 1. Al crear la implementación azul/verde, RDS copia la topología y la configuración completas de la instancia de base de datos principal para crear el entorno verde. Los nombres de las instancias de base de datos copiadas se adjuntan con `-green-`*`random-characters`*. El entorno de almacenamiento provisional de la imagen contiene una implementación de instancias de base de datos Multi-AZ (mydb1-green- *`abc123`*) y una réplica de lectura (mydb2-green- *`abc123`*).



Al crear la implementación azul/verde, puede actualizar la versión del motor de base de datos y especificar un grupo de parámetros de base de datos diferente para las instancias de base de

datos del entorno verde. RDS también configura la replicación lógica desde la instancia de base de datos principal en el entorno azul hasta la instancia de base de datos principal en el entorno verde.

Tras crear la implementación azul/verde, la instancia de base de datos del entorno verde es de solo lectura de forma predeterminada.

3. Realice cambios adicionales en el entorno de almacenamiento provisional, si es necesario.

   Por ejemplo, puede realizar cambios de esquema en la base de datos o cambiar la clase de instancia de base de datos que utilizan una o más instancias de base de datos en el entorno verde.

   Para obtener más información sobre la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

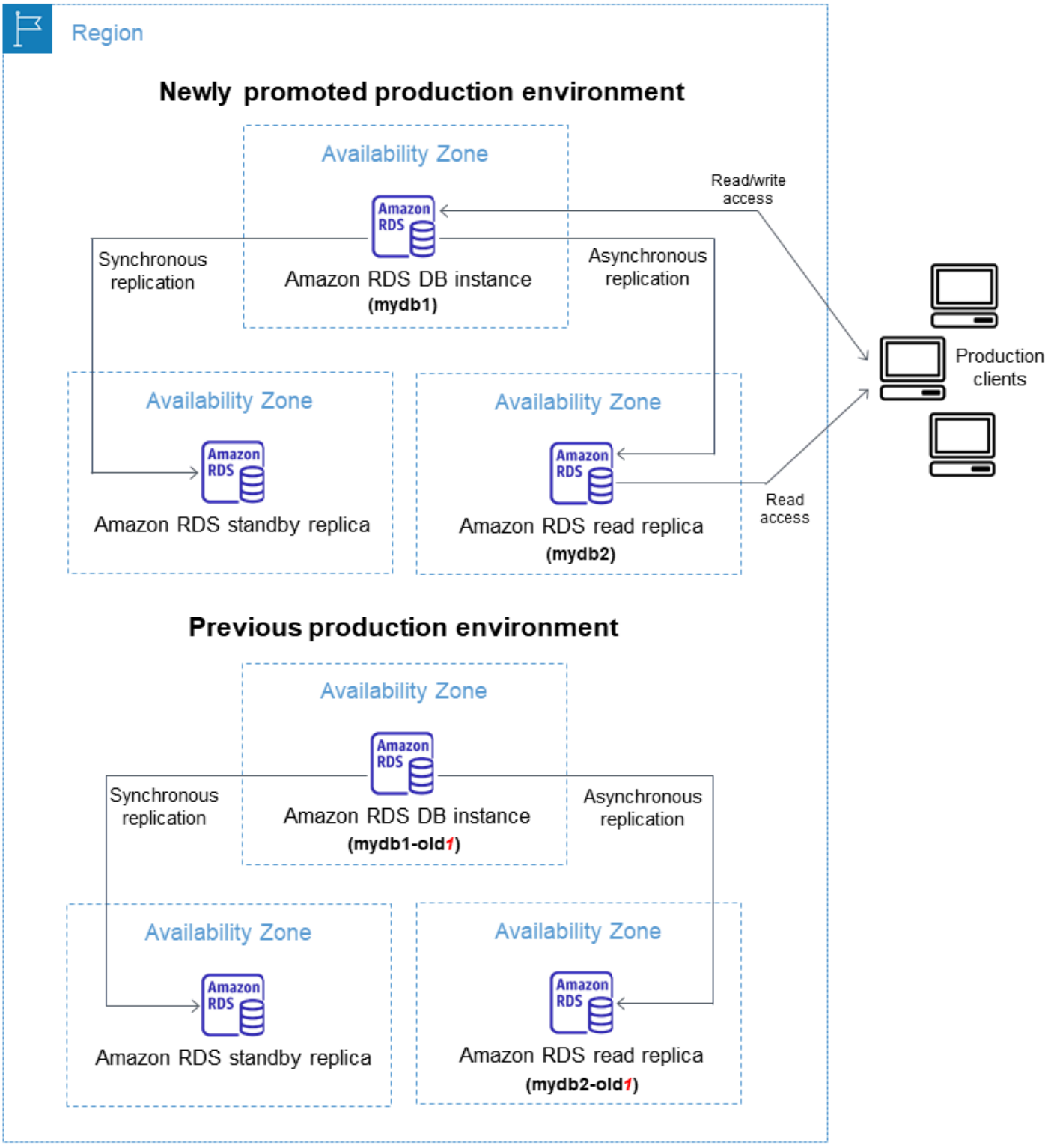
4. Ponga a prueba su entorno de almacenamiento temporal.

   Durante las pruebas, le recomendamos que mantenga como solo lectura las bases de datos de un entorno verde. Habilite las operaciones de escritura en el entorno verde con precaución, ya que pueden provocar conflictos de replicación. También pueden generar datos no deseados en las bases de datos de producción después de la conmutación. Para habilitar las operaciones de escritura para RDS para MySQL, ponga el parámetro `read_only` en `0` y reinicie la instancia de base de datos. En el caso de RDS para PostgreSQL, ponga el parámetro `default_transaction_read_only` en `off` en el nivel de sesión.

5. Cuando esté listo, conmútelo para hacer que el entorno de almacenamiento provisional sea el nuevo entorno de producción. Para obtener instrucciones, consulte Cambio de una implementación azul/verde en Amazon RDS.

   La conmutación provoca un tiempo de inactividad. El tiempo de inactividad suele ser inferior a un minuto, pero puede prolongarse en función de la carga de trabajo.

   En la imagen siguiente, se muestran las instancias de base de datos tras la conmutación.



Tras la conmutación, las instancias de base de datos que estaban en el entorno verde se convierten en las nuevas instancias de base de datos de producción. Los nombres y puntos de conexión del entorno de producción actual se asignan al entorno de producción que se acaba

de promocionar, por lo que no es necesario realizar cambios en la aplicación. Como resultado, el tráfico de producción ahora fluye al nuevo entorno de producción. Las instancias de base de datos del entorno azul anterior se cambian de nombre al añadirles `-old`*n* al nombre actual, donde *n* es un número. Por ejemplo, suponga que el nombre de la instancia de base de datos en el entorno azul es `mydb1`. Tras la conmutación, el nombre de la instancia de base de datos puede ser `mydb1-old1`.

En el ejemplo de la imagen, se producen los siguientes cambios durante la conmutación:

- La implementación de la instancia de base de datos Multi-AZ del entorno verde denominada `mydb1-green-abc123` se convierte en la implementación de la instancia de base de datos Multi-AZ de producción denominada`mydb1`
- La réplica de lectura del entorno verde denominada `mydb2-green-abc123` se convierte en la réplica de lectura de producción `mydb2`.
- La implementación de la instancia de base de datos Multi-AZ del entorno azul denominada `mydb1` se convierte en `mydb1-old1`.
- La réplica de lectura del entorno azul denominada `mydb2` se convierte en `mydb2-old1`.

6. Si ya no necesita una implementación azul/verde, puede eliminarla. Para obtener instrucciones, consulte Eliminación de una implementación azul/verde en Amazon RDS.

   Tras la conmutación, el entorno de producción anterior no se elimina, por lo que puede usarlo para realizar pruebas de regresión, si es necesario.

Autorización del acceso a las operaciones de la implementación azul/verde de Amazon RDS

Los usuarios deben tener los permisos necesarios para realizar operaciones relacionadas con las implementaciones azul/verde. Puede crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. A continuación, puede asociar esas políticas a los roles o conjuntos de permisos de IAM que necesiten esos permisos. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.

El usuario que crea una implementación azul/verde debe tener permisos para realizar las siguientes operaciones de RDS:

- `rds:CreateBlueGreenDeployment`

- `rds:AddTagsToResource`
- `rds:CreateDBInstanceReadReplica`

El usuario que cambia a una implementación azul/verde debe tener permisos para realizar las siguientes operaciones de RDS:

- `rds:SwitchoverBlueGreenDeployment`
- `rds:ModifyDBInstance`
- `rds:PromoteReadReplica`

El usuario que elimina una implementación azul/verde debe tener permisos para realizar las siguientes operacione de RDS:

- `rds:DeleteBlueGreenDeployment`
- `rds:DeleteDBInstance`

Amazon RDS aprovisiona y modifica los recursos en el entorno de almacenamiento provisional en su nombre. Estos recursos incluyen instancias de base de datos que utilizan una convención de nomenclatura definida internamente. Por lo tanto, las políticas de IAM asociadas no pueden contener patrones de nombres de recursos parciales, como `my-db-prefix-*`. Solo se admite el uso de comodines (*). En general, se recomienda utilizar etiquetas de recursos y otros atributos compatibles para controlar el acceso a estos recursos, en lugar de utilizar comodines. Para obtener más información, consulte Acciones, recursos y claves de condición de Amazon .

Limitaciones y consideraciones para implementaciones azul/verde de Amazon RDS

Las implementaciones azul/verde en Amazon RDS requieren una consideración cuidadosa de factores como las ranuras de replicación, la administración de recursos, el tamaño de las instancias y los posibles impactos en el rendimiento de la base de datos. Las siguientes secciones proporcionan orientación para ayudarle a optimizar su estrategia de implementación a fin de garantizar un tiempo de inactividad mínimo, transiciones fluidas y una administración eficaz del entorno de su base de datos.

Temas

- Limitaciones de las implementaciones azul/verde

- Consideraciones acerca de las implementaciones azul/verde

Limitaciones de las implementaciones azul/verde

Las siguientes limitaciones se aplican a las implementaciones azul/verde.

Temas

- Limitaciones generales de las implementaciones azul/verde
- Limitaciones de RDS para MySQL en implementaciones azul/verde
- Limitaciones de RDS para PostgreSQL para las implementaciones azul/verde con replicación física
- Limitaciones de RDS para PostgreSQL para implementaciones azul/verde con replicación lógica

Limitaciones generales de las implementaciones azul/verde

Las siguientes limitaciones generales se aplican a las implementaciones azul/verde:

- Las implementaciones azul/verde no admiten la administración de las contraseñas de los usuarios maestros con AWS Secrets Manager
- Si el volumen de registro dedicado (DLV) está habilitado en la base de datos azul, debe estar habilitado en todas las instancias de base de datos, incluidas las réplicas de lectura.
- Durante la conmutación, los entornos azul y verde no pueden tener integración sin ETL con Amazon Redshift. Debe eliminar la integración en primer lugar, realizar la conmutación y, a continuación, volver a crear la integración.
- El programador de eventos (parámetro `event_scheduler`) debe estar deshabilitado en el entorno verde al crear una implementación azul/verde. Esto evita que se generen eventos en el entorno verde que provoquen incoherencias.
- No puede cambiar una instancia de base de datos sin cifrar por una instancia de base de datos con cifrado. Además, no puede cambiar una instancia de base de datos con cifrado por una instancia de base de datos sin cifrar.
- No puede cambiar una instancia de base de datos azul por una versión del motor superior a su instancia de base de datos verde correspondiente.
- Los recursos del entorno azul y el entorno verde deben estar en la misma Cuenta de AWS.
- Las implementaciones azul/verde no son compatibles con las siguientes características:
  - Amazon RDS Proxy

- Réplicas de lectura en cascada
- Réplicas de lectura entre regiones
- AWS CloudFormation
- Implementaciones de clústeres de base de datos Multi-AZ

  Las implementaciones azul/verde son compatibles con las implementaciones de instancias de base de datos Multi-AZ. Para obtener más información sobre las implementaciones multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Limitaciones de RDS para MySQL en implementaciones azul/verde

Las siguientes limitaciones se aplican a las implementaciones azul/verde de RDS para MySQL:

- El clúster de base de datos azul no puede ser una réplica binlog externa.
- Si la base de datos de origen está asociada a un grupo de opciones personalizado, no puede especificar una actualización de la versión principal al crear la implementación azul/verde.

  En este caso, puede crear una implementación azul/verde sin especificar una actualización de la versión principal. A continuación, puede actualizar la base de datos en el entorno verde. Para obtener más información, consulte Actualización de una versión del motor de una instancia de base de datos.
- Las implementaciones azul/verde no admiten el controlador JDBC de AWS para MySQL. Para obtener más información, consulte Known Limitations en GitHub.

Limitaciones de RDS para PostgreSQL para las implementaciones azul/verde con replicación física

Las siguientes limitaciones se aplican a las implementaciones azul/verde de RDS para PostgreSQL que utilizan la replicación física. Para saber en qué momento las implementaciones azul/verde utilizan la replicación física en lugar de la replicación lógica, consulte ???.

- Una vez creado el entorno verde, no se puede realizar una actualización manual a la versión principal.
- Las implementaciones azul/verde que utilizan la replicación física no admiten cambios de esquema en el entorno verde, ya que son estrictamente de solo lectura.
- La instancia de base de datos azul no puede ser un origen lógico (publicador) ni una réplica (suscriptor).

Limitaciones de RDS para PostgreSQL para implementaciones azul/verde con replicación lógica

Las siguientes limitaciones se aplican a las implementaciones azul/verde de RDS para PostgreSQL que utilizan la replicación lógica. Para saber en qué momento las implementaciones azul/verde utilizan la replicación lógica en lugar de la replicación física, consulte ???.

- Las tablas no registradas no se replican en el entorno verde.
- La instancia de base de datos azul no puede ser un origen lógico (publicador) ni una réplica (suscriptor).
- Si la instancia de base de datos está configurado como el servidor externo de un contenedor de datos externo (FDW), debe usar el nombre del punto de conexión de la instancia en lugar de las direcciones IP. Esto permite que la configuración siga funcionando después de la transición.
- En una implementación azul/verde, cada base de datos requiere una ranura de replicación lógica. A medida que aumenta el número de bases de datos, aumenta la sobrecarga de recursos, lo que puede provocar un retardo en la replicación, especialmente si la instancia de base de datos no se ha escalado lo suficiente. El impacto depende de factores como la carga de trabajo de la base de datos y el número de conexiones. Para mitigarlo, valore la posibilidad de escalar verticalmente la clase de instancia de base de datos o de reducir el número de bases de datos en la instancia de origen.
- El proceso de aplicación de replicación lógica en el entorno verde es de un solo subproceso. Si el entorno azul genera un gran volumen de tráfico de escritura, es posible que el entorno verde no pueda seguirle el ritmo. Esto puede provocar un retardo o un error en la replicación, sobre todo en el caso de las cargas de trabajo que producen un alto rendimiento continuo de escritura. Asegúrese de probar a fondo las cargas de trabajo. En los escenarios que requieran actualizaciones de versiones principales y administrar cargas de trabajo de escritura de gran volumen, considere enfoques alternativos como utilizar AWS Database Migration Service (AWS DMS).
- La creación de nuevas particiones en tablas particionadas no es compatible durante las implementaciones azul/verde de RDS para PostgreSQL. La creación de nuevas particiones implica operaciones de lenguaje de definición de datos (DDL)`CREATE TABLE`, que no se replican desde el entorno azul al entorno verde. Sin embargo, las tablas particionadas existentes y sus datos se replicarán en el entorno verde.
- Las siguientes limitaciones se aplican a las extensiones de PostgreSQL:
  - La extensión `pg_partman` debe estar deshabilitada en el entorno azul al crear una implementación azul/verde. La extensión realiza operaciones de DDL, como `CREATE TABLE`, lo que rompe la replicación lógica del entorno azul al entorno verde.

- La extensión `pg_cron` debe permanecer deshabilitada en todas las bases de datos verdes tras crear la implementación azul/verde. La extensión tiene programas de trabajo en segundo plano que se ejecutan como superusuarios y omiten la configuración de solo lectura del entorno verde, lo que podría provocar conflictos de replicación.
- Las extensiones `pglogical` y `pgactive` deben estar deshabilitadas en el entorno azul al crear una implementación azul/verde. Después de realizar una transición del entorno verde para que sea el nuevo entorno de producción, puede volver a habilitar las extensiones. Además, la base de datos azul no puede ser un suscriptor lógico de una instancia externa.
- Si utiliza la extensión `pgAudit`, debe permanecer en las bibliotecas compartidas (`shared_preload_libraries`) de los grupos de parámetros de base de datos personalizados para las instancias de base de datos azules y verdes. Para obtener más información, consulte the section called “Configuración de la extensión pgAudit”.

Limitaciones específicas de la replicación lógica para las implementaciones azul/verde

PostgreSQL tiene ciertas restricciones relacionadas con la replicación lógica, que se traducen en limitaciones a la hora de crear implementaciones azul/verde para instancias de base de datos de RDS para PostgreSQL.

En la siguiente tabla, se describen las limitaciones de replicación lógica que se aplican a las implementaciones azul/verde para RDS para PostgreSQL. Para obtener más información, consulte Restricciones en la documentación de replicación lógica de PostgreSQL.

Limitación	Explicación
Las instrucciones del lenguaje de definición de datos (DDL), como `CREATE TABLE` y `CREATE SCHEMA`, no se replican desde el entorno azul al entorno verde.	Si Amazon RDS detecta un cambio de DDL en el entorno azul, las bases de datos verdes pasan a un estado de Replicación degradada. Debe eliminar la implementación azul/verde y todas las bases de datos verdes y, a continuación, volver a crearla.

Limitación	Explicación
Las instrucciones del lenguaje de control de datos (DCL), como `GRANT` y `REVOKE`, no se replican desde el entorno azul al entorno verde.	Si Amazon RDS PostgreSQL detecta un intento de ejecutar una instrucción de DCL en el entorno azul, aparecerá un mensaje de advertencia. No hay ninguna configuración o API disponible para cambiar este comportamiento, ya que se trata de una limitación del proceso de implementación azul/verde.
Las operaciones `NEXTVAL` en los objetos de secuencia no están sincronizadas entre el entorno azul y el entorno verde.	Durante la transición, Amazon RDS incrementa los valores de secuencia en el entorno verde para que coincidan con los del entorno azul. Si tiene miles de secuencias, esto puede retrasar la transición.
Los objetos grandes en el entorno azul no se replican en el entorno verde. Esto incluye los objetos grandes existentes como cualquier objeto grande recién creado o modificado durante el proceso de implementación azul/verde.	Si Amazon RDS detecta la creación o modificación de objetos grandes en el entorno azul que están almacenados en la tabla de sistema `pg_largeobject` , las bases de datos verdes pasan a un estado de Replicación degradada. Debe eliminar la implementación azul/verde y todas las bases de datos verdes y, a continuación, volver a crearla.

Limitación	Explicación
Las vistas materializadas no se actualizan automáticamente en el entorno verde.	La actualización de las vistas materializadas en el entorno azul no genera una actualización en el entorno verde. Tras la transición, puede actualizarlos manualmente mediante el comando REFRESH MATERIALIZED VIEW o programar una actualización.
Las operaciones UPDATE y DELETE no están permitidas en las tablas que no tengan una clave principal.	Antes de crear una implementación azul/verde, asegúrese de que todas las tablas tengan una clave principal o usen `REPLICA IDENTITY FULL`. Sin embargo, use `REPLICA IDENTITY FULL` solo si no existe una clave principal o única, ya que afecta al rendimiento de la replicación. Para obtener más información, consulte la documentación de PostgreSQL.

Consideraciones acerca de las implementaciones azul/verde

Amazon RDS rastrea los recursos en las implementaciones azul/verde con el `DbiResourceId` de cada recurso. Este identificador de recurso es un identificador inmutable único de la Región de AWS para el recurso.

El ID del recurso es independiente del ID de la instancia de base de datos: Todos aparecen en la configuración de la base de datos de la consola de RDS.

El nombre (ID de instancia) de un recurso cambia cuando conmuta una implementación azul/verde, pero cada recurso conserva el mismo ID de recurso. Por ejemplo, un identificador de instancia de base de datos podría ser `mydb` en el entorno azul. Tras la conmutación, el nombre de la instancia de base de datos podría ser `mydb-old1`. Sin embargo, el identificador del recurso de la instancia de base de datos no cambia durante la conmutación. Por lo tanto, cuando se realiza una transición de los recursos verdes para que sean los nuevos recursos de producción, sus identificadores de recurso no coinciden con los identificadores de recurso azules que estaban en producción anteriormente.

Tras realizar una transición a una implementación azul/verde, valore la posibilidad de actualizar los ID de recursos a los de los recursos de producción que se acaban de promocionar para las características y los servicios integrados que utilizó con los recursos de producción. Específicamente, tenga en cuenta las siguientes actualizaciones:

- Si realiza el filtrado mediante la API de RDS y los identificadores de recursos, ajuste los identificadores de recursos utilizados en el filtrado después de la conmutación.
- Si utiliza CloudTrail para auditar recursos, ajuste los consumidores del CloudTrail para que realicen un seguimiento de los nuevos identificadores de recursos tras la conmutación. Para obtener más información, consulte Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail.
- Si utiliza la API de Información de rendimiento, ajuste los identificadores de los recursos en las llamadas a la API después de la conmutación. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.

  Puede supervisar una base de datos con el mismo nombre después de la conmutación, pero no contiene los datos de antes de la conmutación.
- Si usa identificadores de recursos en las políticas de IAM, asegúrese de agregar los identificadores de los recursos a los que se les acaba de realizar una transición cuando sea necesario. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.
- Si tiene roles de IAM asociados a la instancia de base de datos, asegúrese de volver a asociarlas tras la transición. Los roles asociados no se copian automáticamente en el entorno verde.
- Si se autentica en su instancia de base de datos con la autenticación de base de datos de IAM, asegúrese de que la política de IAM usada para acceder a la base de datos tenga las bases de datos azul y verde enumeradas bajo el elemento `Resource` de la política. Esto es necesario para conectarse a la base de datos verde después del cambio. Para obtener más información, consulte the section called “Creación y uso de una política de IAM para el acceso a bases de datos de IAM”.
- Si utiliza AWS Backup para administrar copias de seguridad automatizadas de los recursos en una implementación azul/verde, ajuste los identificadores de recursos que ha utilizado AWS Backup después de la conmutación. Para obtener más información, consulte Utilización de AWS Backup para administrar copias de seguridad automatizadas para Amazon RDS.
- Si desea restaurar una instantánea de base de datos manual o automática para una instancia de base de datos que formaba parte de una implementación azul/verde, asegúrese de restaurar la instantánea de base de datos correcta examinando la hora en la que se tomó. Para obtener más información, consulte Restauración a una instancia de base de datos.
- Si desea describir una copia de seguridad automática de una instancia de base de datos del entorno azul anterior o restaurarla en un momento determinado, utilice el identificador del recurso para la operación.

  Como el nombre de la instancia de base de datos se modifica durante la conmutación, no puede usar su nombre anterior para las operaciones `DescribeDBInstanceAutomatedBackups` o `RestoreDBInstanceToPointInTime`.

Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

- Al añadir una réplica de lectura a una instancia de base de datos en el entorno verde de una implementación azul/verde, la nueva réplica de lectura no reemplazará a una réplica de lectura en el entorno azul cuando conmute. Sin embargo, la nueva réplica de lectura se conserva en el nuevo entorno de producción tras la conmutación.
- Tras la transición, las tareas de replicación de AWS Database Migration Service (AWS DMS) no se pueden reanudar porque el punto de control del entorno azul no es válido en el entorno verde. Debe volver a crear la tarea de DMS con un nuevo punto de control para continuar con la replicación.
- Al eliminar una instancia de base de datos en el entorno verde de una implementación azul/verde, no puede crear una nueva instancia de base de datos para reemplazarla en la implementación azul/verde.

  Si crea una nueva instancia de base de datos con el mismo nombre y el mismo nombre de recurso de Amazon (ARN) que la instancia de base de datos eliminada, tendrá un `DbiResourceId` diferente, por lo que no forma parte del entorno verde.

  Si se elimina una instancia de base de datos en el entorno verde, se produce el siguiente comportamiento:

  - Si existe la instancia de base de datos del entorno azul con el mismo nombre, no se cambiará a la instancia de base de datos del entorno verde. El nombre de esta instancia de base de datos no se cambiará añadiendo `-old`*n* al nombre de la instancia de base de datos.
  - Cualquier aplicación que apunte a la instancia de base de datos en el entorno azul seguirá utilizando la misma instancia de base de datos después de la conmutación.

  El mismo comportamiento se aplica a las instancias de base de datos y a las réplicas de lectura.

Prácticas recomendadas para las implementaciones azul/verde de Amazon RDS

Estos son los procedimientos recomendados para las implementaciones azul/verde.

Temas

- Prácticas recomendadas generales para las implementaciones azul/verde

- Prácticas recomendadas de RDS para MySQL para las implementaciones azul/verde
- Prácticas recomendadas de RDS para PostgreSQL para las implementaciones azul/verde

Prácticas recomendadas generales para las implementaciones azul/verde

Tenga en cuenta las prácticas recomendadas generales al crear una implementación azul/verde.

- Pruebe minuciosamente las instancias de base de datos en el entorno verde antes de realizar el cambio.
- Mantenga sus bases de datos del entorno verde en modo de solo lectura. Se recomienda habilitar las operaciones de escritura en el entorno verde con precaución, ya que pueden provocar conflictos de replicación. También pueden generar datos no deseados en las bases de datos de producción después de la conmutación.
- Si utiliza una implementación azul/verde para implementar cambios en el esquema, realice solo cambios compatibles con la replicación.

  Por ejemplo, puede añadir nuevas columnas al final de una tabla, sin interrumpir la replicación de la implementación azul a la implementación verde. Sin embargo, los cambios en el esquema, como cambiar el nombre de las columnas o las tablas, interrumpen la replicación en la implementación verde.

  Para obtener más información sobre los cambios compatibles con la replicación, consulte Replication with Differing Table Definitions on Source and Replica en la documentación de MySQL y Restrictions en la documentación de la replicación lógica de PostgreSQL.

  > **Note**
  >
  > Esta limitación no se aplica a las implementaciones azul/verde de RDS para PostgreSQL que utilizan la replicación física. Para obtener más información, consulte the section called “Limitaciones de RDS para PostgreSQL para las implementaciones azul/verde con replicación física”.

- Tras crear la implementación azul/verde, gestione la carga diferida si es necesario. Asegúrese de que la carga de datos esté completa antes de realizar el cambio. Para obtener más información, consulte Carga diferida e inicialización de almacenamiento para implementaciones azul/verde.

- Al cambiar a una implementación azul/verde, siga las prácticas recomendadas de conmutación. Para obtener más información, consulte the section called “Prácticas recomendadas para realizar la conmutación”.

Prácticas recomendadas de RDS para MySQL para las implementaciones azul/verde

Tenga en cuenta las siguientes prácticas recomendadas a la hora de crear una implementación azul/verde a partir de una instancia de base de datos de RDS para MySQL.

- Evite utilizar motores de almacenamiento no transaccionales, como MyISAM, que no estén optimizados para la replicación.
- Optimice las réplicas de lectura y el entorno verde para la replicación de registros binarios. Si lo admite su motor de base de datos, habilite la replicación GTID, paralela y a prueba de fallos para garantizar la coherencia y la durabilidad de los datos antes de crear una implementación azul/verde. Para obtener más información, consulte Uso de la replicación basada en GTID.
- Si el entorno verde presenta un retraso en las réplicas, tenga en cuenta lo siguiente:
  - Establezca temporalmente el parámetro `innodb_flush_log_at_trx_commit` en 2 en el grupo de parámetros de base de datos verde. Una vez que la replicación se ponga al mismo nivel que los valores predeterminados de 1, vuelva a los valores predeterminados antes de la transición. Si se produce un cierre o bloqueo inesperado con el valor de los parámetros temporales, reconstruya el entorno verde para evitar que los datos se corrompan de forma no detectada.
  - Cambie temporalmente las instancias de base de datos Multi-AZ de color verde por instancias de base de datos Single-AZ para reducir la latencia de escritura y mejorar el rendimiento de la replicación. Vuelva a habilitar Multi-AZ justo antes de la transición.

Prácticas recomendadas de RDS para PostgreSQL para las implementaciones azul/verde

Tenga en cuenta las siguientes prácticas recomendadas a la hora de crear una implementación azul/verde a partir de una instancia de base de datos de RDS para PostgreSQL.

Temas

- Prácticas recomendadas generales de RDS para PostgreSQL para las implementaciones azul/verde

- Prácticas recomendadas de RDS para PostgreSQL para las implementaciones azul/verde con replicación física
- Prácticas recomendadas de RDS para PostgreSQL para las implementaciones azul/verde con replicación lógica

Prácticas recomendadas generales de RDS para PostgreSQL para las implementaciones azul/verde

Tenga en cuenta las siguientes prácticas recomendadas generales a la hora de crear una implementación azul/verde a partir de una instancia de base de datos de RDS para PostgreSQL.

- Actualice todas las extensiones de PostgreSQL a la versión más reciente antes de crear una implementación azul/verde. Para obtener más información, consulte the section called "Actualización de las extensiones de PostgreSQL".
- Las transacciones de larga duración pueden provocar un retraso significativo en las réplicas. Para reducir el retraso en las réplicas, realice lo siguiente:
  - Reduzca las transacciones de larga duración que pueden retrasarse hasta que el entorno verde se ponga al mismo nivel que el entorno azul.
  - Reduzca las operaciones masivas en el entorno azul hasta que el entorno verde se ponga al mismo nivel que el entorno azul.
  - Inicie una operación de inmovilización de vacío manual en tablas ocupadas antes de crear la implementación azul/verde.
  - Para la versión 12 y posteriores de PostgreSQL, desactive el parámetro `index_cleanup` en tablas grandes u ocupadas para aumentar la tasa de mantenimiento normal en las bases de datos azules. Para obtener más información, consulte the section called "Vaciado de una tabla lo más rápido posible".

    > **Note**
    >
    > Omitir regularmente la limpieza del índice durante la aspiración puede provocar una sobrecarga del índice, lo que podría degradar el rendimiento del escaneo. Como práctica recomendada, utilice este enfoque únicamente cuando utilice una implementación azul/verde. Una vez finalizada la implementación, se recomienda reanudar el mantenimiento y la limpieza periódicos de los índices.

- La replicación lenta puede provocar que los remitentes y los destinatarios se reinicien con frecuencia, lo que retrasa la sincronización. Para garantizar que permanezcan activos, deshabilite

los tiempos de espera configurando el parámetro `wal_sender_timeout` en `0` en el entorno azul y el parámetro `wal_receiver_timeout` en `0` en el entorno verde.

- Para evitar que los segmentos de registro de escritura anticipada (WAL) se eliminen del entorno azul, establezca el parámetro `wal_keep_segments` en 15625 para PostgreSQL versión 13 y versiones anteriores. Para la versión 14 y posteriores, establezca el parámetro `wal_keep_size` en 1 TiB, si hay suficiente espacio de almacenamiento libre.

Prácticas recomendadas de RDS para PostgreSQL para las implementaciones azul/verde con replicación física

Con la replicación física, Amazon RDS crea una réplica de lectura de la instancia de base de datos de origen. Para obtener información sobre los parámetros relacionados, la supervisión, el ajuste y la solución de problemas, consulte the section called “Uso de réplicas de lectura para RDS para PostgreSQL”.

Para saber en qué momento las implementaciones azul/verde utilizan la replicación física en lugar de la replicación lógica, consulte ???.

Prácticas recomendadas de RDS para PostgreSQL para las implementaciones azul/verde con replicación lógica

Tenga en cuenta las siguientes prácticas recomendadas al crear una implementación azul/verde que utiliza la replicación lógica. Para saber en qué momento las implementaciones azul/verde utilizan la replicación lógica en lugar de la replicación física, consulte ???.

- Si su base de datos tiene suficiente memoria liberable, aumente el valor del parámetro de base de datos `logical_decoding_work_mem` en el entorno azul. De este modo, se reduce la decodificación en el disco y, en su lugar, se utiliza memoria. Para obtener más información, consulte la documentación de PostgreSQL.
  - Puede supervisar el desbordamiento de transacciones que se escribe en el disco mediante la métrica de CloudWatch `ReplicationSlotDiskUsage`. Esta métrica ofrece información sobre el uso del disco en las ranuras de replicación, lo que ayuda a identificar cuándo los datos de las transacciones superan la capacidad de la memoria y se almacenan en el disco. Puede supervisar la memoria liberable con la métrica `FreeableMemory` de CloudWatch. Para obtener más información, consulte the section called “Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS”.
  - En RDS para PostgreSQL versión 14 y posteriores, puede supervisar el tamaño de los archivos de desbordamiento lógico mediante la vista del sistema `pg_stat_replication_slots`.

- Si utiliza la extensión `aws_s3`, otorgue acceso a la instancia de bases de datos verde a Amazon S3 a través de un rol de IAM tras crear el entorno verde. Esto permite que los comandos de importación y exportación sigan funcionando después de la transición. Para obtener instrucciones, consulte the section called “Configuración del acceso a un bucket de Amazon S3”.
- Revise el rendimiento de sus instrucciones UPDATE y DELETE y evalúe si la creación de un índice en la columna utilizada en la cláusula WHERE puede optimizar estas consultas. Esto puede mejorar el rendimiento cuando las operaciones se reproducen en un entorno verde.
- Si se utilizan desencadenadores, asegúrese de que no interfieran con la creación, actualización y eliminación de objetos `pg_catalog.pg_publication`, `pg_catalog.pg_subscription` y `pg_catalog.pg_replication_slots` objetos cuyos nombres comiencen por “rds”.
- Si especifica una versión de motor superior para el entorno verde, ejecute la operación `ANALYZE` en todas las bases de datos para actualizar la tabla de `pg_statistic`. Las estadísticas del optimizador no se transfieren durante una actualización de la versión principal, por lo que debe regenerar todas las estadísticas para evitar problemas de rendimiento. Para conocer prácticas recomendadas adicionales durante las actualizaciones de versiones principales, consulte the section called “Cómo realizar una actualización de versión principal”.
- Evite configurar desencadenadores como `ENABLE REPLICA` o `ENABLE ALWAYS` si el desencadenador se utiliza en el origen para manipular los datos. De lo contrario, el sistema de replicación propaga los cambios y ejecuta el desencadenador, lo que provoca la duplicación.

Creación de una implementación azul/verde en Amazon RDS

Al crear una implementación azul/verde, se especifica la instancia de base de datos de origen que se va a copiar en la implementación. La instancia de base de datos que elija es la instancia de base de datos de producción y se convierte en la instancia de base de datos principal en el entorno azul. Esta instancia de base de datos se copia al entorno verde y RDS configura la replicación desde la instancia de base de datos del entorno azul a la instancia de base de datos del entorno verde.

RDS copia la topología y las características del entorno azul en un área de almacenamiento. Cuando la instancia de base de datos azul tiene réplicas de lectura, estas se copian como réplicas de la instancia verde. El almacenamiento asignado de todas las réplicas verdes coincide con la instancia principal verde, mientras que otros parámetros de almacenamiento se heredan de las réplicas azules.

Si la instancia de base de datos azul/verde es una implementación de instancia de base de datos Multi-AZ, la instancia de base de datos verde se crea como implementación de la instancia de base de datos Multi-AZ.

Temas

- Preparación para una implementación azul/verde
- Especificación de cambios al crear una implementación azul/verde
- Carga diferida e inicialización de almacenamiento para implementaciones azul/verde
- Creación de una implementación azul/verde
- Configuración para la creación de implementaciones azul/verde

Preparación para una implementación azul/verde

Hay ciertos pasos que debe seguir antes de crear una implementación azul/verde, en función del motor que ejecute su instancia de base de datos.

Temas

- Preparación de una instancia de base de datos de RDS para MySQL o RDS para MariaDB para una implementación azul/verde
- Preparación de una instancia de base de datos de RDS para PostgreSQL para una implementación azul/verde con replicación física
- Preparación de una instancia de base de datos de RDS para PostgreSQL para una implementación azul/verde con replicación lógica

Preparación de una instancia de base de datos de RDS para MySQL o RDS para MariaDB para una implementación azul/verde

Antes de crear una implementación azul/verde para una instancia de base de datos de RDS para MySQL o RDS para MariaDB, debe habilitar las copias de seguridad automatizadas. Para obtener instrucciones, consulte the section called “Habilitar las copias de seguridad automatizadas”.

Preparación de una instancia de base de datos de RDS para PostgreSQL para una implementación azul/verde con replicación física

Antes de crear una implementación azul/verde de RDS para PostgreSQL que utiliza una replicación física, haga lo siguiente. Para obtener una lista de las versiones que utilizan la replicación física en lugar de la replicación lógica, consulte ???.

- Habilite las copias de seguridad automáticas en la instancia de base de datos. Para obtener instrucciones, consulte the section called “Habilitar las copias de seguridad automatizadas”.
- Confirme que la instancia de base de datos no sea el origen ni el destino de la replicación externa. Para obtener más información, consulte the section called “Limitaciones generales”.

Preparación de una instancia de base de datos de RDS para PostgreSQL para una implementación azul/verde con replicación lógica

Antes de crear una implementación azul/verde para RDS para PostgreSQL que utiliza una replicación lógica, haga lo siguiente. Para obtener una lista de las versiones que utilizan la replicación lógica en lugar de la replicación física, consulte ???.

- Asocie la instancia a un grupo de parámetros de base de datos personalizado con la replicación lógica (`rds.logical_replication`) activada. La replicación lógica es necesaria para la replicación del entorno azul en el entorno verde. Para obtener instrucciones, consulte the section called “Modificación de parámetros de un grupo de parámetros de base de datos”.

  Dado que las implementaciones azul/verde requieren al menos un trabajo en segundo plano por base de datos, asegúrese de configurar los siguientes ajustes de configuración en función de su carga de trabajo: Para obtener instrucciones sobre cómo ajustar cada configuración, consulte los Ajustes de configuración en la documentación de PostgreSQL.

  - `max_replication_slots`
  - `max_wal_senders`
  - `max_logical_replication_workers`
  - `max_worker_processes`

  Tras habilitar la replicación lógica y configurar todas las opciones de configuración, reinicie la instancia de base de datos para que los cambios entren en vigor. Las implementaciones azul/verde requieren que la instancia de base de datos esté sincronizada con el grupo de parámetros

de base de datos; de lo contrario, habrá un error en la creación. Para obtener más información, consulte the section called “Reinicio de una instancia de base de datos”.

- Confirme que la instancia de base de datos no sea el origen ni el destino de la replicación externa. Para obtener más información, consulte the section called “Limitaciones generales”.
- Asegúrese de que todas las tablas de la instancia de base de datos tengan una clave principal. La replicación lógica de PostgreSQL no permite llevar a cabo operaciones `UPDATE` o `DELETE` en tablas que no tengan una clave principal.
- En RDS para PostgreSQL se utiliza la replicación lógica nativa de PostgreSQL, que almacena segmentos de registros de escritura anticipada (WAL) en la instancia azul hasta que se reproducen en el entorno verde. Antes de crear una implementación azul/verde, compruebe que la instancia azul tenga la capacidad adecuada comprobando las siguientes métricas:
  - `FreeStorageSpace`
  - `TransactionLogsGeneration`
  - `TransactionLogsDiskUsage`
  - `OldestReplicationSlotLag`

  Para calcular el almacenamiento adicional necesario en la instancia azul, supervise la métrica de CloudWatch `TransactionLogsGeneration` durante los períodos de máxima carga de trabajo. Por ejemplo, si su carga de trabajo genera 100 GB de datos de WAL en 24 horas, asegúrese de disponer de al menos 100 GB de almacenamiento adicional para alojar segmentos de WAL de un día. Para obtener más información, consulte Supervisión de métricas en una instancia de base de datos.

Especificación de cambios al crear una implementación azul/verde

Puede realizar los siguientes cambios en la instancia de base de datos en el entorno verde al crear la implementación azul/verde:

Puede realizar otras modificaciones en la instancia en el entorno verde después de su implementación. Por ejemplo, puede especificar una versión superior del motor o un grupo de parámetros diferente.

Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Temas

- Especificación de una versión de motor superior
- Especificación de un grupo de parámetros de base de datos diferente
- Modificación de la configuración de almacenamiento y rendimiento
- Activación de las escrituras optimizadas de RDS
- Actualización de la configuración de almacenamiento

Especificación de una versión de motor superior

Puede especificar una versión superior del motor si desea probar una actualización del motor de base de datos. Tras la transición, la base de datos se actualiza a la versión principal o secundaria del motor de base de datos que especifique.

Especificación de un grupo de parámetros de base de datos diferente

Puede comprobar cómo los cambios de parámetros afectan a las instancias de base de datos en el entorno verde o especificar un grupo de parámetros para una nueva versión principal del motor de base de datos en caso de una actualización.

Si especifica un grupo de parámetros de base de datos diferente, el grupo de parámetros de base de datos especificado se asocia a todas las instancias de base de datos del entorno verde. Si no especifica un grupo de parámetros diferente, cada instancia de base de datos del entorno verde se asocia al grupo de parámetros de su instancia de base de datos azul correspondiente.

Modificación de la configuración de almacenamiento y rendimiento

Ajuste la configuración de almacenamiento y rendimiento en un entorno verde para optimizar la asignación de recursos. Estas configuraciones incluyen el almacenamiento asignado, las IOPS aprovisionadas, el tipo de almacenamiento y el rendimiento del almacenamiento (para el almacenamiento gp3).

Puede cambiar el tipo de almacenamiento de la instancia de base de datos verde a gp2, gp3, io1 o io2. En el caso del almacenamiento gp3, también puede ajustar el rendimiento del almacenamiento para mejorar el rendimiento de la transferencia de datos para cargas de trabajo de alta demanda o para reducir los costos de las aplicaciones menos intensivas. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

También puede optar por aumentar o reducir el almacenamiento asignado al entorno verde. Sin embargo, la reducción del almacenamiento solo se produce si el almacenamiento asignado

al destino es al menos un 20 % superior al uso de almacenamiento actual. Si reduce el almacenamiento asignado, Amazon RDS inicia una actualización de la configuración de almacenamiento. Para obtener más información, consulte the section called “Actualización de la configuración de almacenamiento”.

Si la instancia de base de datos azul utiliza almacenamiento magnético, debe cambiar la instancia de base de datos verde por un tipo de almacenamiento de uso general o de IOPS aprovisionadas para aumentar o reducir el almacenamiento asignado.

Activación de las escrituras optimizadas de RDS

Puede utilizar una implementación azul/verde para actualizar a una clase de instancia de base de datos que admita las escrituras optimizadas de RDS. Solo puede habilitar las escrituras optimizadas de RDS en una base de datos que se haya creado con una clase de instancia de base de datos compatible. Por lo tanto, esta opción crea una base de datos verde que utiliza una clase de instancia de base de datos compatible, lo que le permite activar las escrituras optimizadas de RDS en la instancia de base de datos verde.

Si va a actualizar una clase de instancia de base de datos que no admite las escrituras optimizadas de RDS a una que sí lo hace, también debe actualizar la configuración de almacenamiento de la instancia de base de datos verde. Para obtener más información, consulte the section called “Actualización de la configuración de almacenamiento”.

Solo puede actualizar la clase de instancia de base de datos de la instancia de base de datos verde principal. De forma predeterminada, las réplicas de lectura del entorno verde heredan la configuración de la instancia de base de datos del entorno azul. Una vez que el entorno verde se haya creado correctamente, debe modificar manualmente la clase de instancia de base de datos de las réplicas de lectura en el entorno verde.

Algunas actualizaciones de clases de instancia no se admiten según la versión del motor y la clase de instancia de la instancia de base de datos azul. Para obtener más información sobre las clases de instancias de bases de datos, consulte the section called “Clases de instancia de base de datos”.

Actualización de la configuración de almacenamiento

Si la base de datos azul no tiene la configuración de almacenamiento más reciente, RDS puede migrar la instancia de base de datos verde desde la configuración de almacenamiento anterior (sistema de archivos de 32 bits) hacia la configuración preferida. Puede utilizar las implementaciones azul/verde de RDS para superar las limitaciones de escalado de almacenamiento y tamaño de archivos de los sistemas de archivos de 32 bits más antiguos. Además, esta configuración cambia la

configuración del almacenamiento para que sea compatible con las escrituras optimizadas de RDS si la clase de instancia de base de datos especificada admite las escrituras optimizadas.

> **Note**
>
> La actualización de la configuración de almacenamiento es una operación que requiere un uso intensivo de E/S y prolonga los tiempos de creación en las implementaciones azul/verde. El proceso de actualización del almacenamiento es más rápido si la instancia de base de datos azul utiliza un almacenamiento SSD (io1 o io2 Block Express) de IOPS aprovisionadas y si ha aprovisionado el entorno verde con un tamaño de instancia 4xlarge o superior.
> Las actualizaciones de almacenamiento que implican el almacenamiento de SSD de uso general (gp2) pueden agotar el saldo de créditos de E/S, lo que puede generar retrasos en la actualización. Para obtener más información, consulte the section called “Almacenamiento de instancias de base de datos”.
> Durante la actualización del almacenamiento, la instancia de base de datos verde no está disponible temporalmente, mientras que la instancia de base de datos azul permanece disponible. Durante este intervalo se detiene la replicación. Supervise el almacenamiento de la instancia azul y considere la posibilidad de escalarlo si el almacenamiento alcanza el 90 %, ya que la instancia verde se escala automáticamente un 10 % después de la actualización.

Esta opción solo está disponible si su base de datos azul no tiene la configuración de almacenamiento más reciente o si va a cambiar la clase de instancia de base de datos en la misma solicitud. Solo puede actualizar la configuración de almacenamiento al crear inicialmente una implementación azul/verde.

Carga diferida e inicialización de almacenamiento para implementaciones azul/verde

Al crear una implementación azul/verde, Amazon RDS crea la instancia de base de datos principal en el entorno verde mediante una restauración a partir de una instantánea de base de datos. Una vez creada, la instancia de base de datos verde y sus réplicas de lectura siguen cargando datos en segundo plano, lo que se conoce como carga diferida.

La carga diferida solo carga los bloques de datos cuando las aplicaciones los solicitan. Si intenta acceder a datos que aún no se han cargado, Amazon EBS los recupera inmediatamente de Amazon S3, mientras que los datos restantes continúan cargándose en segundo plano. Para obtener más información, consulte Instantáneas de Amazon EBS.

Para acelerar el rendimiento de todo el volumen, Amazon RDS proporciona la inicialización del almacenamiento, que lee todos los bloques del volumen del entorno verde. Amazon EBS descarga bloques de Amazon S3 de forma proactiva, lo que proporciona el máximo rendimiento de volumen desde el primer uso. La inicialización del almacenamiento se produce completamente en segundo plano, lo que garantiza que no se vea afectada la disponibilidad de la instancia de base de datos ni las actividades en curso, como la aplicación de parches o las actualizaciones.

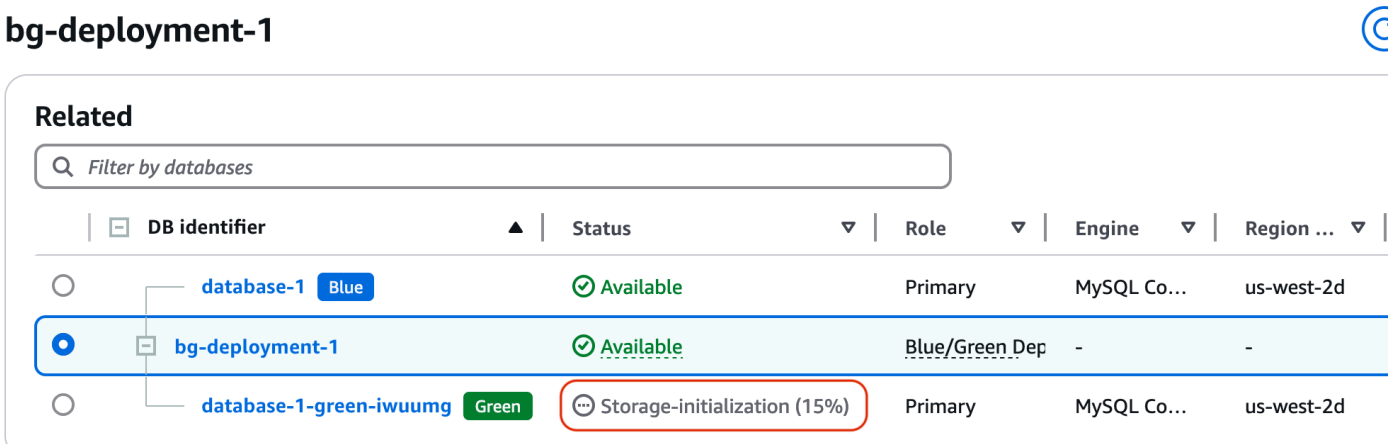
La inicialización del almacenamiento solo está disponible para instancias en implementaciones azul/verde con los tipos de volumen `gp2`, `gp3`, `io1` y `io2`. Es compatible con todas las clases de instancia, excepto las de las familias t3 y t4. Si modifica una instancia de base de datos verde en una implementación Single-AZ por una implementación de instancia de base de datos Multi-AZ, la inicialización del almacenamiento incluye el nodo secundario en la configuración Multi-AZ.

Durante la inicialización del almacenamiento, la instancia permanece totalmente disponible y utilizable para las operaciones de la base de datos, aunque es posible que el almacenamiento no alcance el máximo rendimiento hasta que se complete la inicialización. Mientras se lleva a cabo la inicialización del almacenamiento, el estado general de la instancia cambia a Inicialización del almacenamiento y el indicador de progreso refleja el nivel mínimo de inicialización en todos los volúmenes de la instancia de base de datos.

Utilice la consola, la AWS CLI o la API de Amazon RDS para supervisar la inicialización del almacenamiento.

Console

En la AWS Management Console, verá el progreso de la inicialización del almacenamiento con el estado de la instancia de base de datos.



AWS CLI

Con la AWS CLI, puede supervisar la inicialización del almacenamiento con el comando describe-db-instances. El campo `PercentProgress` de la respuesta muestra el porcentaje de datos que se ha recuperado de Amazon S3.

```
aws rds describe-db-instances --db-instance-identifier my-db-instance

{
    "DBInstances": [
        {
            "DBInstanceIdentifier": "my-db-instance",
            "DBInstanceClass": "db.m5.2xlarge",
            "Engine": "postgres",
            "DBInstanceStatus": "storage-initialization",
            ...
            "PercentProgress": "34"
        }
    ]
}
```

Amazon RDS API

Con la API de Amazon RDS, puede recuperar el estado de la inicialización del almacenamiento llamando a la acción DescribeDBInstances.

El indicador de progreso se actualiza a medida que avanza el trabajo de inicialización en segundo plano, lo que le permite realizar un seguimiento de la disponibilidad del almacenamiento antes de que se complete la inicialización total del almacenamiento. La inicialización del almacenamiento permite optimizar el rendimiento a medida que la instancia de base de datos verde esté a pleno funcionamiento.

Creación de una implementación azul/verde

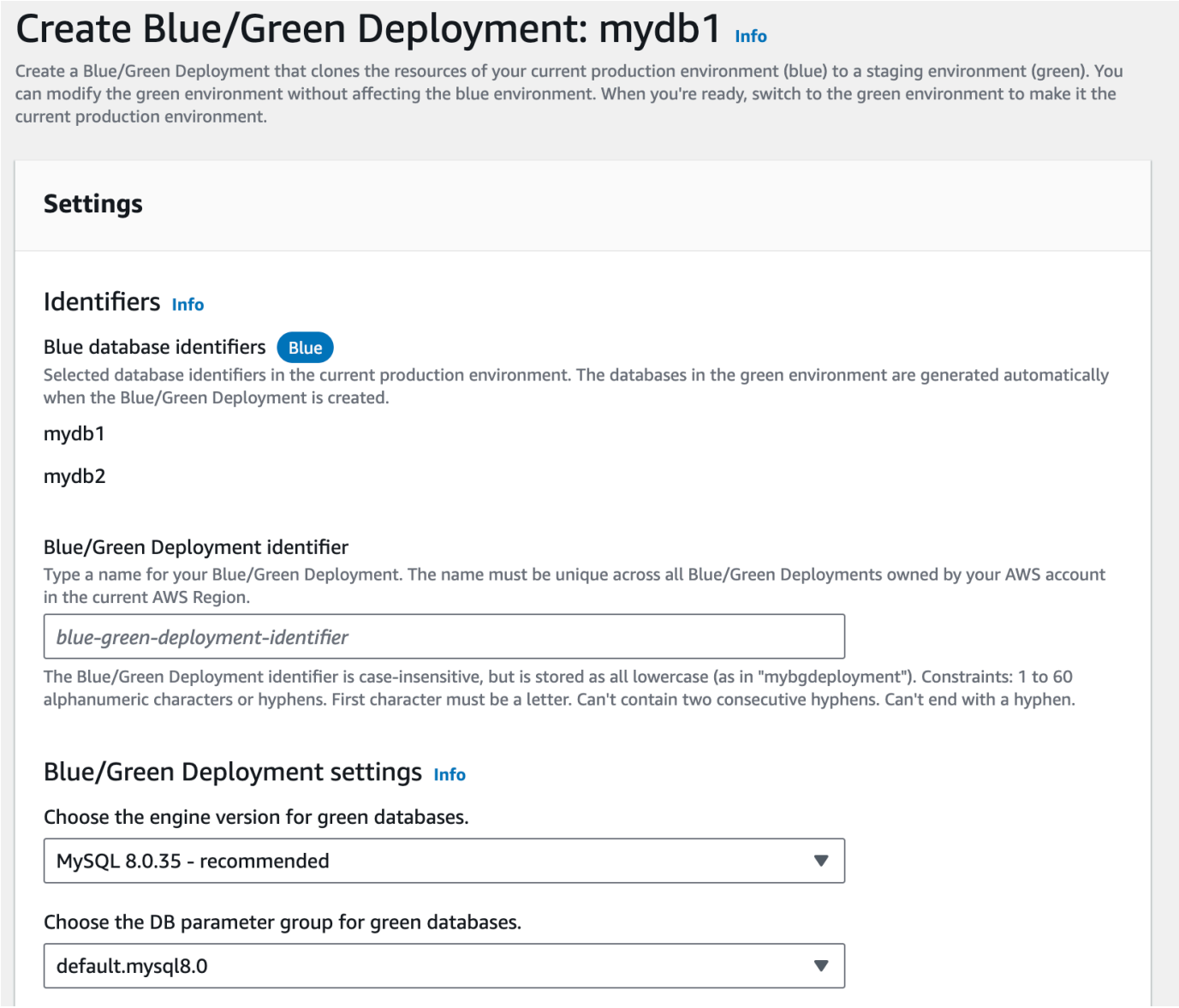
Puede crear una implementación azul/verde mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para crear una implementación azul/verde

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desea copiar a un entorno verde.
3. Elija Acciones y Crear implementación azul/verde.

   Aparece la página Crear implementación azul/verde.



4. Revise los identificadores de la base de datos azul. Asegúrese de que coincidan con las instancias de base de datos esperadas en el entorno azul. Si no es así, seleccione Cancel (Cancelar).
5. En Nombre de implementación azul/verde, ingrese un nombre para la implementación azul/verde.
6. En el resto de secciones, especifique los ajustes de configuración del entorno verde. Para obtener más información acerca de cada configuración, consulte the section called “Opciones disponibles”.

   Puede realizar otras modificaciones en las bases de datos en el entorno verde después de su implementación.
7. Seleccione Crear.

AWS CLI

Para crear una implementación azul/verde mediante la AWS CLI, utilice el comando create-blue-green-deployment. Para obtener información sobre todas las opciones disponibles, consulte the section called “Opciones disponibles”.

Example

Para Linux, macOS o Unix:

```
aws rds create-blue-green-deployment \
    --blue-green-deployment-name my-blue-green-deployment \
    --source arn:aws:rds:us-east-2:123456789012:db:mydb1 \
    --target-engine-version 8.0.31 \
    --target-db-parameter-group-name mydbparametergroup
```

Para Windows:

```
aws rds create-blue-green-deployment ^
    --blue-green-deployment-name my-blue-green-deployment ^
    --source arn:aws:rds:us-east-2:123456789012:db:mydb1 ^
    --target-engine-version 8.0.31 ^
    --target-db-parameter-group-name mydbparametergroup
```

API de RDS

Para crear una implementación azul/verde mediante la API de Amazon RDS, utilice la operación `CreateBlueGreenDeployment`. Para obtener más información acerca de cada opción, consulte the section called “Opciones disponibles”.

Configuración para la creación de implementaciones azul/verde

En la siguiente tabla se explican los ajustes que puede elegir al crear una implementación azul/verde. Para obtener más información sobre las opciones de la AWS CLI, consulte create-blue-green-deployment. Para obtener más información sobre los parámetros de la API de RDS, consulte CreateBlueGreenDeployment.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Allocated storage (Almacenamiento asignado)	Es la cantidad de almacenamiento que debe asignar a la instancia de base de datos verde (en gibibytes). Puede optar por aumentar o reducir el almacenamiento asignado.
	
	Si la instancia de base de datos azul utiliza almacenamiento magnético (`standard`), debe cambiar la instancia de base de datos verde por un tipo de almacenamiento de uso general o de IOPS aprovisionadas para modificar el almacenamiento asignado al entorno verde.
	
	Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.
		Opción de la CLI:
		
		`--target-allocated-storage`
		
		Parámetro de la API:
		
		`TargetAllocatedStorage`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Identificador de implementación azul/verde	Un nombre de la implementación azul/verde.	Opción de la CLI:
		`--blue-green-deployment-name`
		Parámetro de la API:
		`BlueGreenDeploymentName`

Identificador de base de datos azul	El identificador de la instancia que desea copiar al entorno verde. Cuando utilice la CLI o la API, especifique la instancia del nombre de recurso de Amazon (ARN).	Opción de la CLI:
		`--source`
		Parámetro de la API:
		`Source`

Grupo de parámetros de base de datos para bases de datos verdes	Un grupo de parámetros para asociarlo a las bases de datos en el entorno verde.	Opción de la CLI:
		`--target-db-parameter-group-name`
		`--target-db-cluster-parameter-group-name`
		Parámetro de la API:
		`TargetDBParameterGroupName`
		`TargetDBClusterParameterGroupName`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS
Habilite las escrituras optimizadas para una base de datos verde	Habilite las escrituras optimizadas de RDS en la instancia de base de datos principal verde. Para obtener más información, consulte the section called “Activación de las escrituras optimizadas de RDS”. Si va a cambiar una clase de instancia de base de datos no compatible con las escrituras optimizadas por una que sí lo sea, también debe actualizar la configuración de almacenamiento. Para obtener más información, consulte the section called “Actualización de la configuración de almacenamiento”.	Para la CLI y la API, si se especific a una clase de instancia de base de datos de destino que admita las escrituras optimizadas de RDS, se habilita automáticamente en la instancia de base de datos principal verde.

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Versión de motor para bases de datos verdes	Actualice las bases de datos del entorno verde a la versión del motor de base de datos especificada.
	
	Si no se especifica, cada base de datos del entorno verde se crea con la misma versión de motor que la instancia de base de datos correspondiente en el entorno azul.
	
	Si elige una instancia de base de datos de RDS para PostgreSQL que utiliza la replicación lógica, revise y acepte las limitaciones de la replicación lógica. Para obtener más información, consulte the section called “Limitaciones específicas de la replicación lógica para las implementaciones azul/verde”.
		Opción de la CLI:
		
		`--target-engine-version`
		
		Parámetro de la API de RDS:
		
		`TargetEngineVersion`

Clase de instancia de base de datos verde	La capacidad de memoria y de computación de cada instancia de base de datos en el entorno verde, por ejemplo, `db.m5d.xlarge` .
	
	Esta opción solo está visible cuando se habilita la escritura optimizada de RDS para la base de datos verde.
		Opción de la CLI:
		
		`--target-db-instance-class`
		
		Parámetro de la API de RDS:
		
		`TargetDBInstanceClass`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Provisioned IOPS (IOPS aprovisionadas)	Es la cantidad de operaciones de entrada/salida por segundo (IOPS) aprovisionadas asignada inicialmente a la base de datos verde.
	
	Este valor solo se aplica a la instancia de base de datos principal verde, no a las réplicas verdes.
		Opción de la CLI:
		
		`--target-iops`
		
		Parámetro de la API de RDS:
		
		`TargetIops`

Actualización de la configuración del almacenamiento	Seleccione si desea actualizar la configuración del sistema de archivos de almacenamiento. Si habilita este ajuste, RDS migra la base de datos verde desde el sistema de archivos de almacenamiento anterior a la configuración preferida.
	
	Esta opción solo está disponible si su base de datos azul no tiene la configuración de almacenamiento más reciente o si va a habilitar las escrituras optimizadas de RDS en la misma solicitud. Solo puede actualizar la configuración de almacenamiento al crear inicialmente una implementación azul/verde.
	
	Para obtener más información, consulte the section called “Actualización del sistema de archivos de almacenamiento”.
		Opción de la CLI:
		
		`--upgrade-target-storage-config`
		
		Parámetro de la API de RDS:
		
		`UpgradeTargetStorageConfig`

Configuración de la consola	Descripción de la configuración	Opción de la CLI y parámetro de la API de RDS

Rendimiento de almacenamiento	Es el valor de rendimiento de almacenamiento de la base de datos verde. Esta configuración solo es visible si selecciona SSD de uso general (gp3) como tipo de almacenamiento.
	
	Este valor solo se aplica a la instancia de base de datos principal verde, no a las réplicas verdes.
	
	Para obtener más información, consulte Almacenamiento gp3 (recomendado).
		Opción de la CLI:
		
		`--target-storage-throughput`
		
		Parámetro de la API de RDS:
		
		`TargetStorageThroughput`

Storage type (Tipo de almacenamiento)	Es el tipo de almacenamiento de la base de datos verde. Se admiten los siguientes tipos de almacenamiento:
	
	• SSD de uso general (gp2)
	• SSD de uso general (gp3)
	• IOPS aprovisionadas (io1)
	• SSD de IOPS aprovisionadas (io2)
	
	Este valor solo se aplica a la instancia de base de datos principal verde, no a las réplicas verdes.
	
	Para obtener más información, consulte Tipos de almacenamiento de Amazon RDS.
		Opción de la CLI:
		
		`--target-storage-type`
		
		Parámetro de la API de RDS:
		
		`TargetStorageType`

Visualización de una implementación azul/verde en Amazon RDS

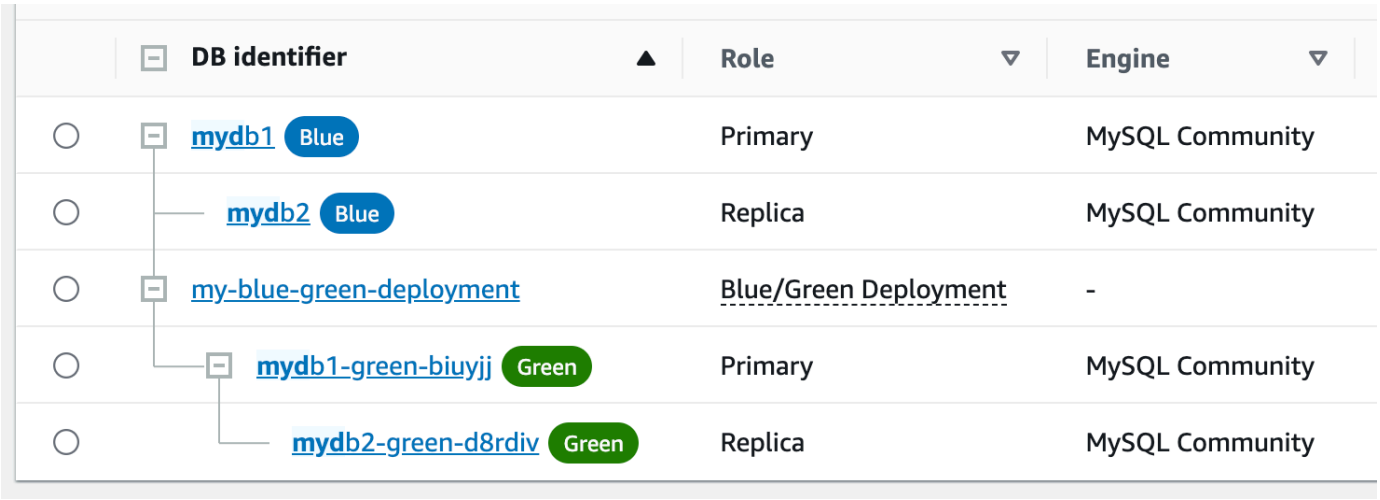
Puede ver los detalles de una implementación azul/verde mediante la AWS Management Console, la AWS CLI o la API de RDS.

También puede ver los eventos y suscribirse a ellos para obtener información sobre una implementación azul/verde. Para obtener más información, consulte Eventos de implementación azul/verde.

Consola

Para ver los detalles de una implementación azul/verde

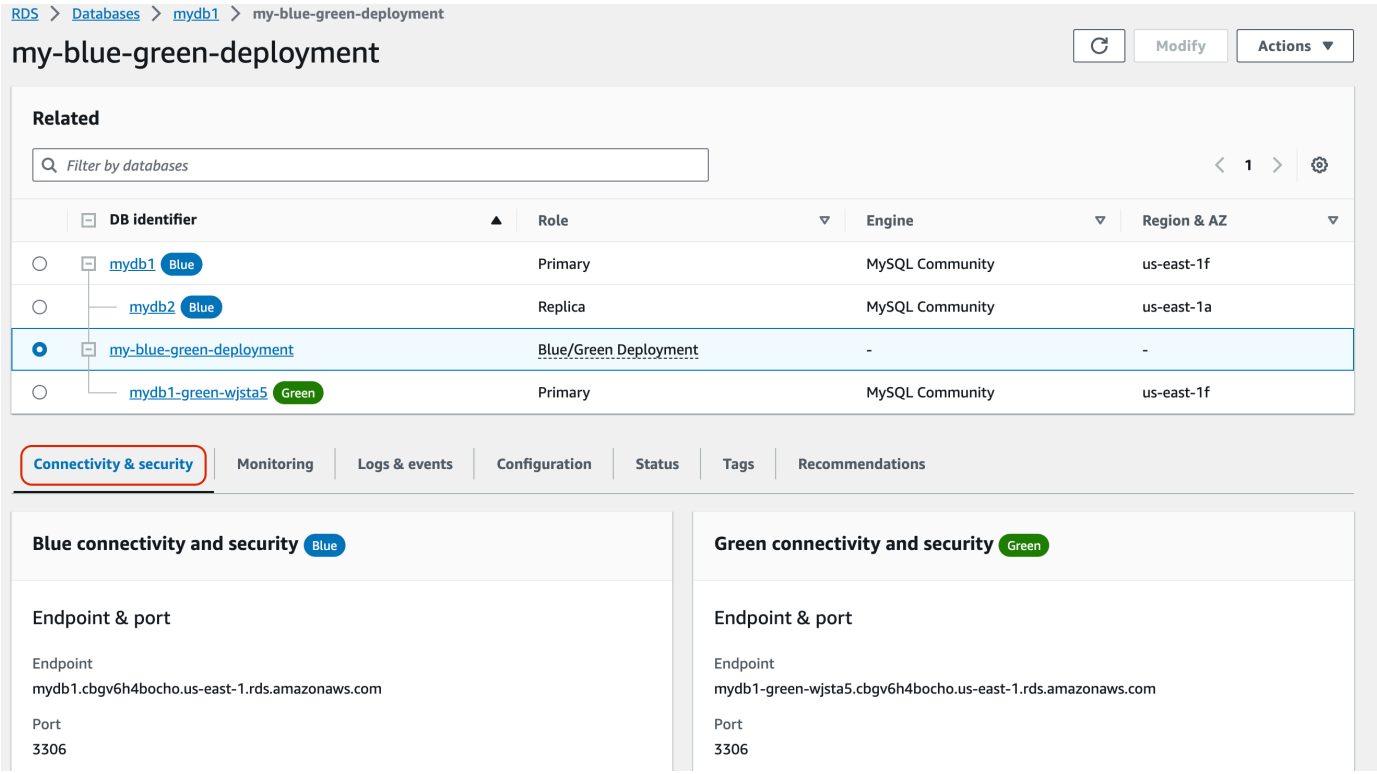
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos) y, a continuación, busque la implementación azul/verde en la lista.



   El valor de Role (Rol) para la implementación azul/verde es Blue/Green Deployment (Implementación azul/verde).
3. Elija el nombre de la implementación azul/verde que desee ver para mostrar sus detalles.

   Cada pestaña tiene una sección para la implementación azul y una sección para la implementación verde. Por ejemplo, en la pestaña Configuración, la versión del motor de base de datos puede ser diferente en el entorno azul y en el entorno verde si está actualizando la versión del motor de base de datos en el entorno verde.

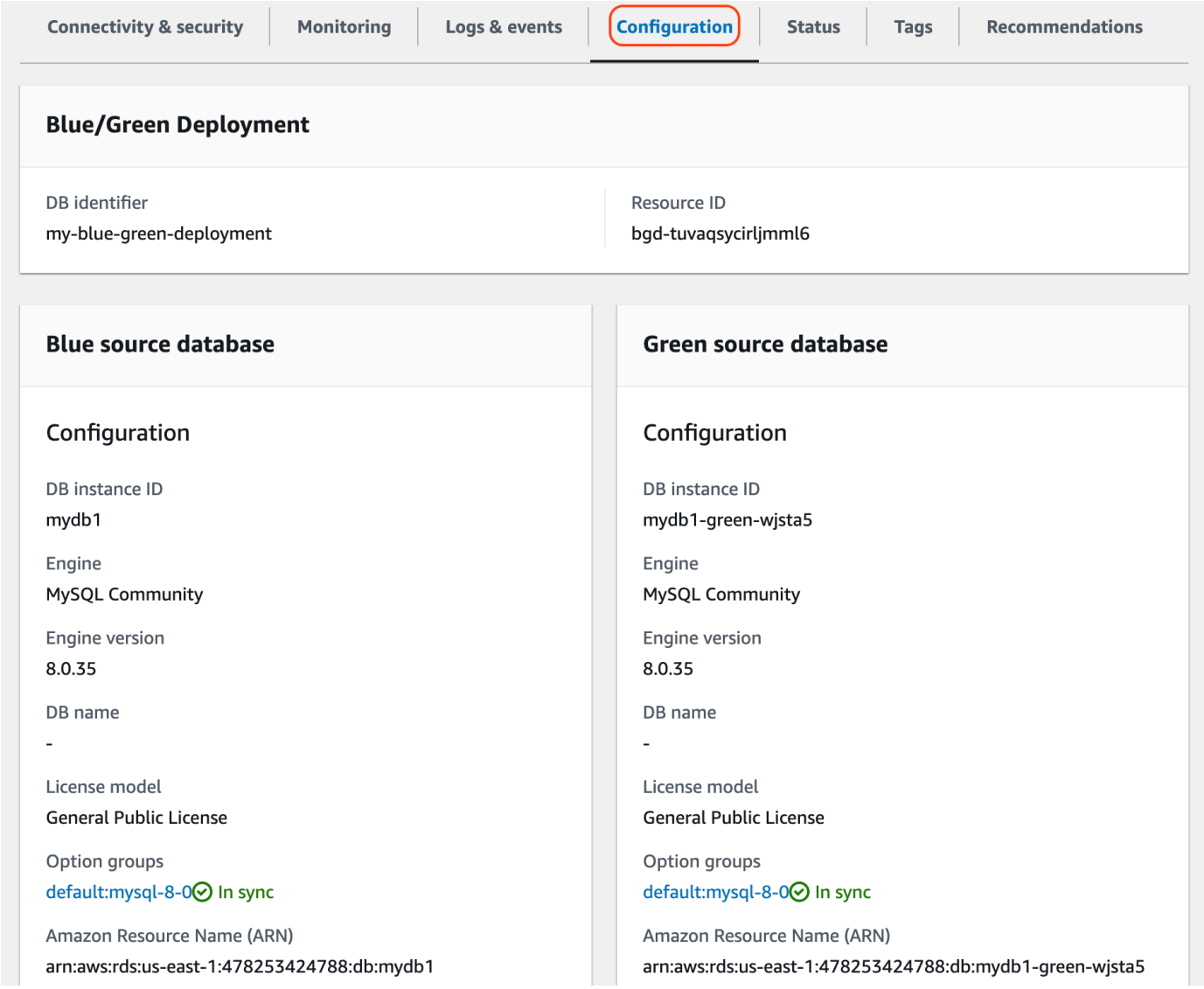
   En la siguiente imagen se muestra un ejemplo de la pestaña Conectividad y seguridad.



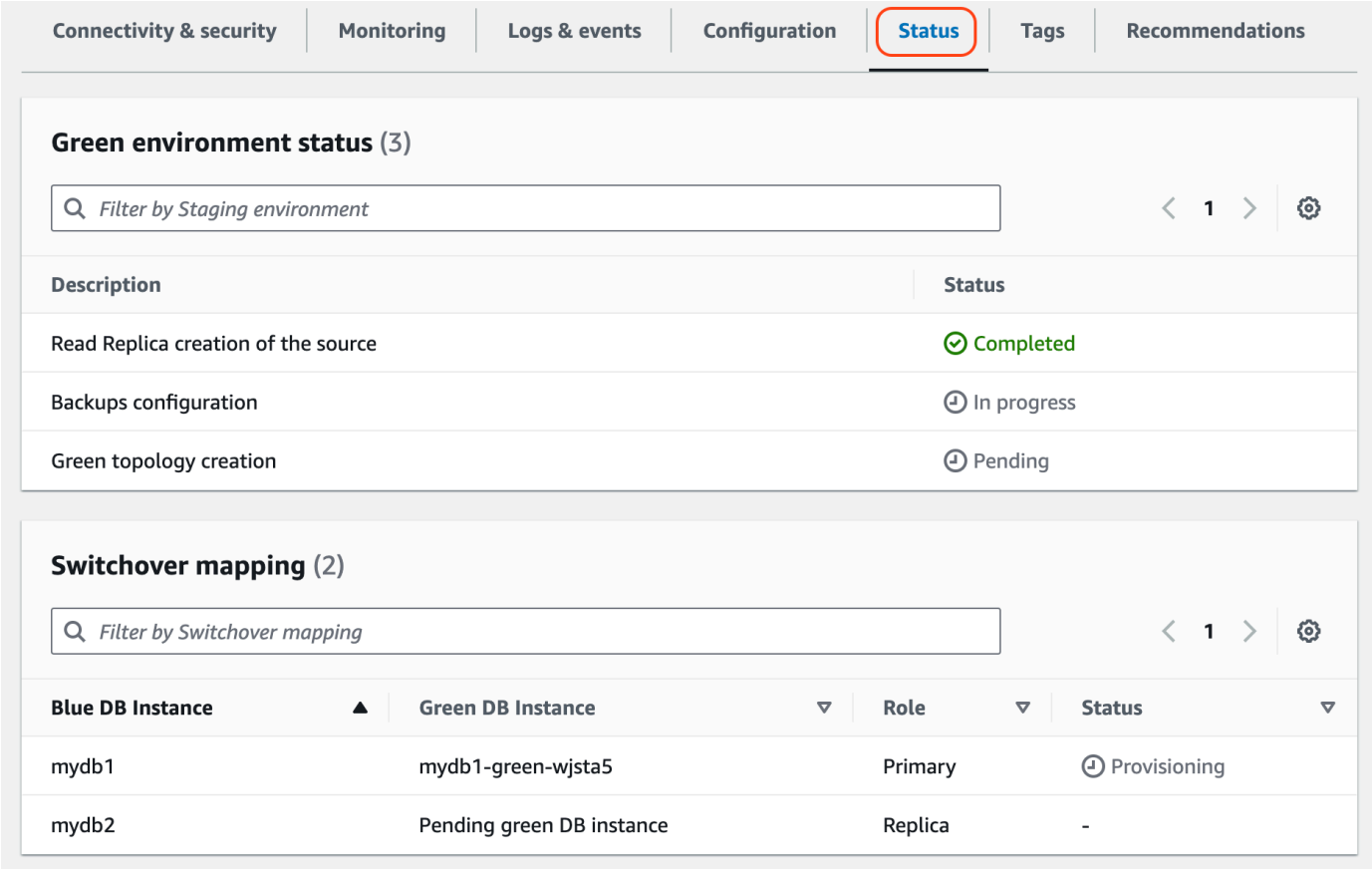
La pestaña Conectividad y seguridad también incluye una sección llamada Replicación, que muestra el estado actual de la replicación y el retraso de réplica entre los entornos azul y verde. Si el estado de replicación es `Replicating`, la implementación azul/verde se está replicando correctamente.

En el caso de las implementaciones azul/verde de RDS para PostgreSQL que utilizan la replicación lógica, el estado de la replicación puede cambiar a `Replication degraded` si realiza cambios en DDL o en objetos grandes no compatibles en el entorno azul. Para obtener más información, consulte the section called “Limitaciones específicas de la replicación lógica para las implementaciones azul/verde”.

En la siguiente imagen se muestra un ejemplo de la pestaña Configuración.



En la siguiente imagen se muestra un ejemplo de la pestaña Estado.



AWS CLI

Para ver los detalles de una implementación azul/verde mediante la AWS CLI, utilice el comando describe-blue-green-deployments.

Example Vea los detalles de una implementación azul/verde filtrando por su nombre

Con el comando describe-blue-green-deployments, puede filtrar por `--blue-green-deployment-name`.

En el siguiente ejemplo, se muestran los detalles de una implementación azul/verde denominada *`my-blue-green-deployment`*.

```
aws rds describe-blue-green-deployments \
  --filters Name=blue-green-deployment-name,Values=my-blue-green-deployment
```

Example Para ver los detalles de una implementación azul/verde, especifique su identificador

Cuando use el comando describe-blue-green-deployments, puede especificar la opción `--blue-green-deployment-identifier`.

En el siguiente ejemplo, se muestran los detalles de una implementación azul/verde con el identificador *bgd-1234567890abcdef*.

```
aws rds describe-blue-green-deployments \
  --blue-green-deployment-identifier bgd-1234567890abcdef
```

API de RDS

Para ver los detalles de una implementación azul/verde mediante la API de Amazon RDS, utilice la opración `DescribeBlueGreenDeployments` y especifique el `BlueGreenDeploymentIdentifier`.

Cambio de una implementación azul/verde en Amazon RDS

Una transición hace que el entorno verde sea el nuevo entorno de producción. Cuando la instancia de base de datos verde tiene réplicas de lectura, a estas también se les realiza la transición. Antes de conmutar, el tráfico de producción se dirige a la instancia de base de datos y las réplicas de lectura en el entorno azul. Tras conmutar, el tráfico de producción se dirige a la instancia de base de datos y las réplicas de lectura en el entorno verde.

Cambiar una implementación azul/verde no es lo mismo que promocionar la instancia de base de datos verde dentro de la implementación azul/verde. Si promociona manualmente la instancia de base de datos seleccionando Promocionar en el menú Acciones, la replicación entre los entornos azul y verde se romperá y la implementación azul/verde entrará en el estado La configuración no es válida.

Temas

- Tiempo de espera de la conmutación
- Barreras de protección de la conmutación
- Acciones de conmutación
- Prácticas recomendadas para realizar la conmutación
- Verificación de las métricas de CloudWatch antes de la conmutación
- Monitoreo del retardo de réplica antes de la transición

- Conmutación de una implementación azul/verde
- Después de la conmutación

Tiempo de espera de la conmutación

Puede especificar un tiempo de espera para la conmutación de entre 30 y 3600 segundos (una hora). Si la conmutación dura más de lo especificado, los cambios se revierten y no se realiza ningún cambio en ninguno de los entornos. El valor predeterminado del tiempo de espera es de 300 segundos (cinco minutos).

Barreras de protección de la conmutación

Al iniciar una conmutación, Amazon RDS realiza algunas comprobaciones básicas para comprobar si los entornos azul y verde están preparados para ella. Estas comprobaciones se conocen como barreras de protección de la conmutación. Estas barreras de protección de la conmutación evitan que este se realice si los entornos no están preparados para ello. Por lo tanto, evitan que haya tiempos de inactividad más prolongados de lo esperado y evitan la pérdida de datos entre los entornos azul y verde que podría producirse si se iniciara la conmutación.

Amazon RDS ejecuta las siguientes comprobaciones de barreras de protección en el entorno verde:

- Estado de la replicación: comprueba si el estado de replicación de la instancia de base de datos principal es correcto. La instancia de base de datos principal verde es una réplica de la instancia de base de datos principal azul.
- Retraso de replicación: comprueba si el retraso de la instancia de base de datos principal verde está dentro de los límites permisibles para la transición. Los límites permitidos se basan en el tiempo de espera especificado. El retardo de la réplica indica qué retardo tiene la instancia de base de datos principal verde con respecto a la instancia de base de datos principal azul. Para obtener más información, consulte the section called “Monitoreo del retardo de réplica antes de la transición”.
- Escrituras activas: asegúrese de que no haya escrituras activas en la instancia de base de datos principal verde.

Amazon RDS ejecuta las siguientes comprobaciones de barreras de protección en el entorno azul:

- Replicación externa: en el caso de RDS para PostgreSQL, se asegura de que el entorno azul no sea un origen lógico autoadministrado (publicador) o una réplica (suscriptor). Si es así, le

recomendamos que elimine las ranuras de replicación autoadministradas y las suscripciones en todas las bases de datos del entorno azul, proceda con la transición y, a continuación, vuelva a crearlos para reanudar la replicación. En el caso de RDS para MySQL y RDS para MariaDB, comprueba si la base de datos azul no es una réplica binlog externa. Si es así, asegúrese de que no se esté replicando activamente.

- Escrituras activas de ejecución prolongada: asegúrese de que no haya escrituras activas de ejecución prolongada en la instancia de base de datos principal azul, ya que pueden aumentar el retardo de la réplica.
- Instrucciones DDL de ejecución prolongada: asegúrese de que no haya instrucciones DDL de ejecución prolongada en la instancia de base de datos principal azul, ya que pueden aumentar el retardo de la réplica.
- Cambios en PostgreSQL no compatibles: en el caso de RDS para PostgreSQL, se asegura de que no haya habido cambios de DDL ni adiciones o modificaciones de objetos grandes en el entorno azul. Para obtener más información, consulte the section called “Limitaciones específicas de la replicación lógica para las implementaciones azul/verde”.

  Si Amazon RDS detecta cambios no compatibles en PostgreSQL, cambia el estado de la replicación a `Replication degraded` y le notifica de que la transición no está disponible para la implementación azul/verde. Para continuar con la transición, le recomendamos que elimine y vuelva a crear la implementación azul/verde y todas las bases de datos verdes. Para ello, seleccione Acciones, Eliminar con bases de datos verdes.

Acciones de conmutación

Al conmutar una implementación azul/verde, RDS realiza las siguientes acciones:

1. Realiza comprobaciones de barreras de protección para verificar si los entornos azul y verde están listos para la conmutación.
2. Detiene las nuevas operaciones de escritura en la instancia de base de datos principal en ambos entornos.
3. Elimina las conexiones a las instancias de base de datos en ambos entornos y no permite nuevas conexiones.
4. Espera a que la replicación alcance el entorno verde para que el entorno verde esté sincronizado con el entorno azul.
5. Cambia el nombre de las instancias de base de datos en ambos entornos.

RDS cambia el nombre de las instancias de base de datos del entorno verde para que coincidan con el de las instancias de base de datos del entorno azul. Por ejemplo, suponga que el nombre de una instancia de base de datos en el entorno azul es `mydb`. Suponga también que el nombre de la instancia de base de datos correspondiente en el entorno verde es `mydb-green-abc123`. Durante la conmutación, el nombre de la instancia de base de datos del entorno verde se cambia a `mydb`.

RDS cambia el nombre de las instancias de base de datos en el entorno azul añadiendo `-old`*n* al nombre actual, donde *n* es un número. Por ejemplo, suponga que el nombre de una instancia de base de datos en el entorno azul es `mydb`. Tras la conmutación, el nombre de la instancia de base de datos puede ser `mydb-old1`.

RDS también cambia el nombre de los puntos de conexión del entorno verde para que coincidan con los puntos de conexión correspondientes del entorno azul, de modo que no sea necesario realizar cambios en la aplicación.

6. Permite conexiones a bases de datos en ambos entornos.
7. Permite operaciones de escritura en la instancia de base de datos principal del nuevo entorno de producción.

   Tras la transición, la instancia de base de datos principal de producción anterior solo permite operaciones de lectura hasta que ajuste el parámetro `read_only` (para RDS para MySQL) o el parámetro `default_transaction_read_only` (para RDS para PostgreSQL) en `0` y reinicie la instancia de base de datos.

Puede supervisar el estado de una conmutación mediante Amazon EventBridge. Para obtener más información, consulte the section called “Eventos de implementación azul/verde”.

Si tiene etiquetas configuradas en el entorno azul, estas etiquetas se copian en el nuevo entorno de producción durante la transición. Para obtener más información acerca de las etiquetas, consulte Etiquetado de los recursos de y Amazon RDS.

Si se inicia la conmutación y, a continuación, se detiene antes de finalizar por cualquier motivo, los cambios se revierten y no se realiza ningún cambio en ninguno de los entornos.

Prácticas recomendadas para realizar la conmutación

Antes de la transición, le recomendamos encarecidamente que siga los procedimientos recomendadas y complete las siguientes tareas:

- Pruebe minuciosamente los recursos en el entorno verde. Asegúrese de que funcionan de manera adecuada y eficiente.
- Supervise las métricas relevantes de Amazon CloudWatch. Para obtener más información, consulte the section called “Verificación de las métricas de CloudWatch antes de la conmutación”.
- Identifique el mejor momento para realizar la conmutación.

  Durante la conmutación, las escrituras se interrumpen en las bases de datos de ambos entornos. Identifique un momento en el que el tráfico sea menor en su entorno de producción. Las transacciones de larga duración, como las DDL activas, pueden aumentar el tiempo de la conmutación, lo que se traduce en un tiempo de inactividad más prolongado para las cargas de trabajo de producción.

  Si hay una gran cantidad de conexiones en las instancias de base de datos, considere la posibilidad de reducirlas manualmente hasta la cantidad mínima necesaria para su aplicación antes de cambiar a la implementación azul/verde. Una forma de lograrlo consiste en crear un script que supervise el estado de la implementación azul/verde y comience a limpiar las conexiones cuando detecte que el estado ha cambiado a `SWITCHOVER_IN_PROGRESS`.
- Asegúrese de que las instancias de base de datos de ambos entornos se encuentren en el estado `Available`.
- Asegúrese de que la instancia de base de datos principal del entorno verde se encuentre en buen estado y se esté replicando.
- Asegúrese de que las configuraciones de red y cliente no aumenten el tiempo de vida (TTL) de la caché de DNS más de cinco segundos, que es el valor predeterminado para las zonas DNS de RDS.
  De lo contrario, las aplicaciones seguirán enviando tráfico de escritura al entorno azul después del cambio.
- Asegúrese de que la carga de datos esté completa antes de realizar el cambio. Para obtener más información, consulte the section called “Carga diferida e inicialización de almacenamiento”.
- Para las implementaciones azul/verde de RDS para PostgreSQL que utilizan replicación lógica, haga lo siguiente:
  - Revise las limitaciones de la replicación lógica y tome las medidas necesarias antes de la transición. Para obtener más información, consulte the section called “Limitaciones específicas de la replicación lógica para las implementaciones azul/verde”.
  - Ejecute la operación `ANALYZE` para actualizar la tabla `pg_statistics`. Esto reduce el riesgo de problemas de rendimiento tras la transición.

> **Note**
>
> Durante una conmutación, no puede modificar ninguna instancia de base de datos incluido en la conmutación.

Verificación de las métricas de CloudWatch antes de la conmutación

Antes de conmutar una implementación azul/verde, le recomendamos que compruebe los de las siguientes en Amazon CloudWatch.

- `DatabaseConnections`: utilice esta métrica para calcular el nivel de actividad de la implementación azul/verde y asegúrese de que el valor esté en un nivel aceptable para su implementación antes de realizar la conmutación. Si Información sobre rendimiento está activado, `DBLoad` es una métrica más precisa.

Para obtener más información, consulte the section called “Métricas de CloudWatch para RDS”.

Monitoreo del retardo de réplica antes de la transición

Antes de conmutar una implementación azul/verde, asegúrese de que el retraso de réplica esté próximo a cero para reducir el tiempo de inactividad.

RDS para MySQL y RDS para MariaDB

Para las implementaciones azul/verde de MySQL y MariaDB, compruebe la métrica `ReplicaLag` de CloudWatch en el entorno verde para identificar el retraso de réplica actual. Para obtener más información, consulte the section called “Diagnóstico y resolución de retardos entre réplicas de lectura”.

RDS para PostgreSQL

Para las implementaciones azul/verde de PostgreSQL que utilizan replicación física, consulte the section called “Supervisión y ajuste del proceso de replicación” para ver las instrucciones para identificar el retraso de réplica actual.

Para las implementaciones azul/verde de PostgreSQL que utilizan replicación lógica, compruebe la métrica `OldestReplicationSlotLag` de CloudWatch en el entorno verde para identificar el

retraso de réplica actual. Para obtener más información, consulte the section called “Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS”.

Además, puede ejecutar la siguiente consulta SQL en el entorno azul:

```
SELECT slot_name,
       confirmed_flush_lsn as flushed,
       pg_current_wal_lsn(),
       (pg_current_wal_lsn() - confirmed_flush_lsn) AS lsn_distance
FROM pg_catalog.pg_replication_slots
WHERE slot_type = 'logical';

slot_name        |    flushed    | pg_current_wal_lsn | lsn_distance
-----------------+---------------+--------------------+------------
logical_replica1 | 47D97/CF32980 | 47D97/CF3BAC8      | 37192
```

`confirmed_flush_lsn` representa el número de secuencia de registro (LSN) más reciente que se envió a la réplica. `pg_current_wal_lsn` representa la ubicación actual de la base de datos. Un valor 0 en `lsn_distance` significa que la réplica está funcionando al mismo ritmo.

Para saber en qué momento las implementaciones azul/verde utilizan la replicación física en lugar de la replicación lógica, consulte ???.

Conmutación de una implementación azul/verde

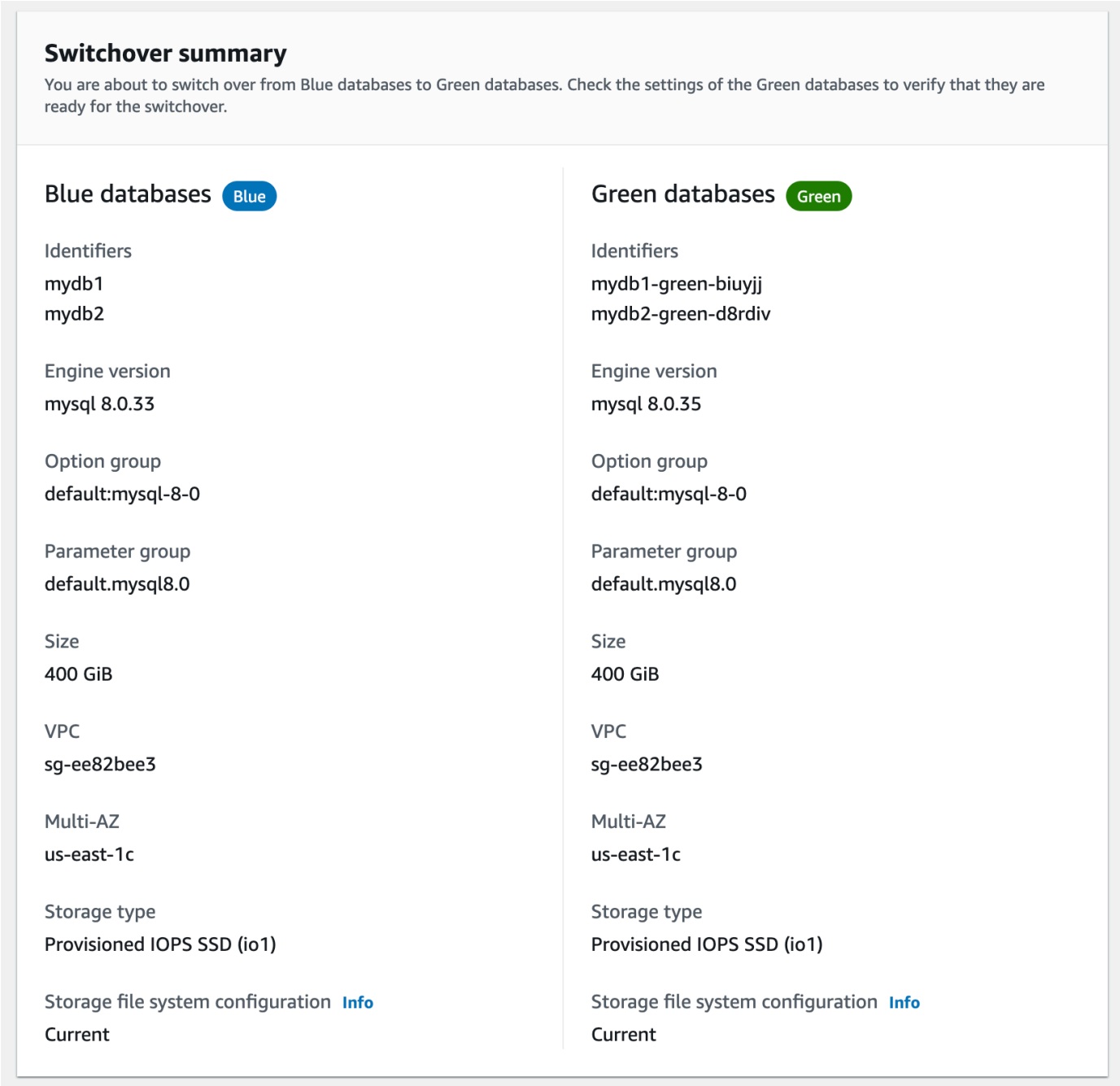
Puede conmutar una implementación azul/verde mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para conmutar una implementación azul/verde

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la implementación azul/verde que desee conmutar.
3. En Actions (Acciones), elija Switch over (Conmutar).

   Aparece la página Switch over (Conmutar).



4. En la página Switch over (Conmutar), consulte el resumen de la conmutación. Asegúrese de que los recursos de ambos entornos coincidan con lo que espera. Si no es así, seleccione Cancel (Cancelar).
5. En Ajustes de tiempo de espera, introduzca el límite de tiempo para la transición.
6. Si la instancia ejecuta RDS para PostgreSQL, revise y confirme las recomendaciones previas a la transición. Para obtener más información, consulte the section called “Limitaciones específicas de la replicación lógica para las implementaciones azul/verde”.

7. Elija Switch over (Conmutar).

AWS CLI

Para conmutar una implementación azul/verde mediante la AWS CLI, utilice el comando switchover-blue-green-deploy con las siguientes opciones:

- `--blue-green-deployment-identifier`: especifique el ID de recurso de la implementación azul/verde.
- `--switchover-timeout`: especifique el límite de tiempo para la conmutación, en segundos. El valor predeterminado es 300.

Example Conmutar una implementación azul/verde

Para Linux, macOS o Unix:

```
aws rds switchover-blue-green-deployment \
    --blue-green-deployment-identifier bgd-1234567890abcdef \
    --switchover-timeout 600
```

Para Windows:

```
aws rds switchover-blue-green-deployment ^
    --blue-green-deployment-identifier bgd-1234567890abcdef ^
    --switchover-timeout 600
```

API de RDS

Para conmutar una implementación azul/verde mediante la API de Amazon RDS, utilice la operación `SwitchoverBlueGreenDeployment` con los siguientes parámetros:

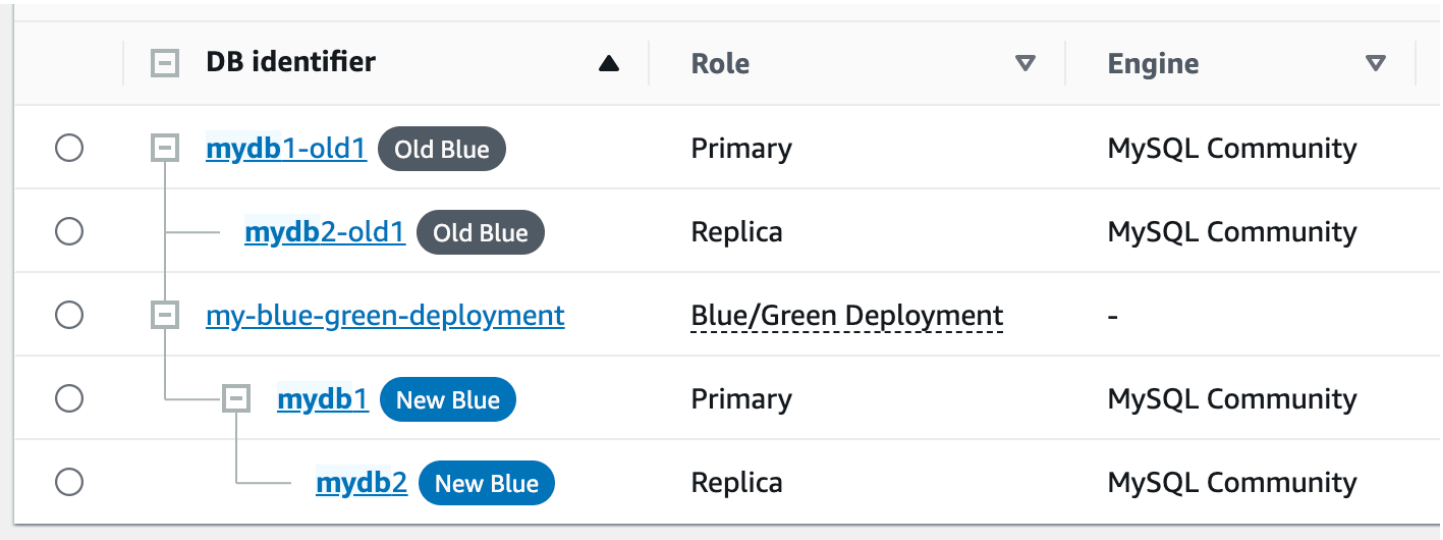
- `BlueGreenDeploymentIdentifier`: especifique el ID de recurso de la implementación azul/verde.
- `SwitchoverTimeout`: especifique el límite de tiempo para la conmutación, en segundos. El valor predeterminado es 300.

Después de la conmutación

Tras una conmutación, se conservan las instancias de base de datos del entorno azul anterior. A estos recursos se les aplican los costos estándar. La replicación entre los entornos azul y verde se detienen.

RDS cambia el nombre de las instancias de base de datos en el entorno azul añadiendo `-old`*n* al nombre del recurso actual, donde *n* es un número. Las instancias de base de datos del antiguo entorno azul son de solo lectura hasta que establezca el parámetro `read_only` (para RDS para MySQL) o el parámetro `default_transaction_read_only` (para RDS para PostgreSQL) en `0`. RDS cambia el nombre de las instancias de base de datos en el entorno verde `-new`*n*.

Si elimina el recurso de implementación azul/verde, RDS retiene los recursos `-old`*n* y `-new`*n*.



Actualización del nodo principal para los consumidores

RDS ofrece réplicas de lectura totalmente gestionadas. Sin embargo, también ofrece la opción de configurar réplicas autogestionadas, también conocidas como réplicas externas. Las réplicas externas permiten utilizar recursos de terceros como destinos de replicación.

Tras realizar la transición de una implementación azul/verde de RDS para MariaDB o RDS para MySQL, si la instancia de base de datos azul tenía réplicas externas o consumidores de registros binarios antes de la transición, debe actualizar su nodo principal tras la transición para mantener la continuidad de la replicación.

Para actualizar el nodo principal

1. Tras la transición, la instancia de base de datos de que anteriormente estaba en el entorno verde emite un evento que contiene el nombre del archivo de registro maestro y la posición del registro maestro. Para localizar el evento, vaya a la consola de RDS y seleccione Eventos en el panel de navegación izquierdo.
2. Filtre por eventos en los que la fuente sea el nombre de la antigua instancia de base de datos del verde, antes de realizar la transición.
3. Localice el evento que contiene las coordenadas del registro binario. El mensaje del evento es similar a: `Binary log coordinates in green environment after switchover: file mysql-bin-changelog.000003 and position 40134574`.
4. Asegúrese de que el consumidor o la réplica hayan aplicado todos los registros binarios del antiguo entorno azul. A continuación, utilice las coordenadas del registro binario proporcionadas para reanudar la replicación en los consumidores. Por ejemplo, si ejecuta una réplica de MySQL en EC2, puede usar los siguientes comandos:

   MySQL 8.0.22 y versiones anteriores principales y secundarias

   ```
   CHANGE MASTER TO MASTER_HOST='{new-writer-endpoint}', MASTER_LOG_FILE='mysql-bin-changelog.000003', MASTER_LOG_POS=40134574;
   ```

   MySQL 8.0.23 y versiones posteriores principales y secundarias

   ```
   CHANGE REPLICATION SOURCE TO SOURCE_HOST='{new-writer-endpoint}',
    SOURCE_LOG_FILE='mysql-bin-changelog.000003', SOURCE_LOG_POS=40134574;
   ```

Si el consumidor es otra instancia de base de datos de RDS para MySQL o RDS para MariaDB, ejecute los siguientes procedimientos almacenados en orden:

1. the section called “mysql.rds_stop_replication”
2. mysql.rds_reset_external_master (para la versión 8.0 y anteriores) o mysql_rds_reset_external_source (para la versión 8.4 y anteriores)
3. mysql.rds_set_external_master (para la versión 8.0 y anteriores) o mysql_rds_set_external_source (para la versión 8.4 y anteriores)
4. the section called “mysql.rds_start_replication”

Eliminación de una implementación azul/verde en Amazon RDS

Puede eliminar una implementación azul/verde antes o después de cambiarla.

Al eliminar una implementación azul/verde antes de cambiarla, Amazon RDS elimina opcionalmente las instancias de base de datos en el entorno verde:

- Si decide eliminar las instancias de base de datos en el entorno verde (`--delete-target`), deben tener desactivada la protección de eliminación.
- Si no elimina las instancias de base de datos en el entorno verde (`--no-delete-target`), eso significa que se retienen las instancias, pero ya no forman parte de una implementación azul/verde. En el caso de RDS para MySQL, la replicación continúa entre los entornos. En el caso de RDS para PostgreSQL, el entorno verde se convierte en un entorno independiente, por lo que se detiene la replicación.

La opción de eliminar las bases de datos verdes no está disponible en la consola después de la conmutación. Al eliminar las implementaciones azul/verde mediante la AWS CLI, no puede especificar la opción `--delete-target` si el estado de la implementación es `SWITCHOVER_COMPLETED`.

> **Important**
>
> Al eliminar una implementación azul/verde, eso no afecta al entorno azul.

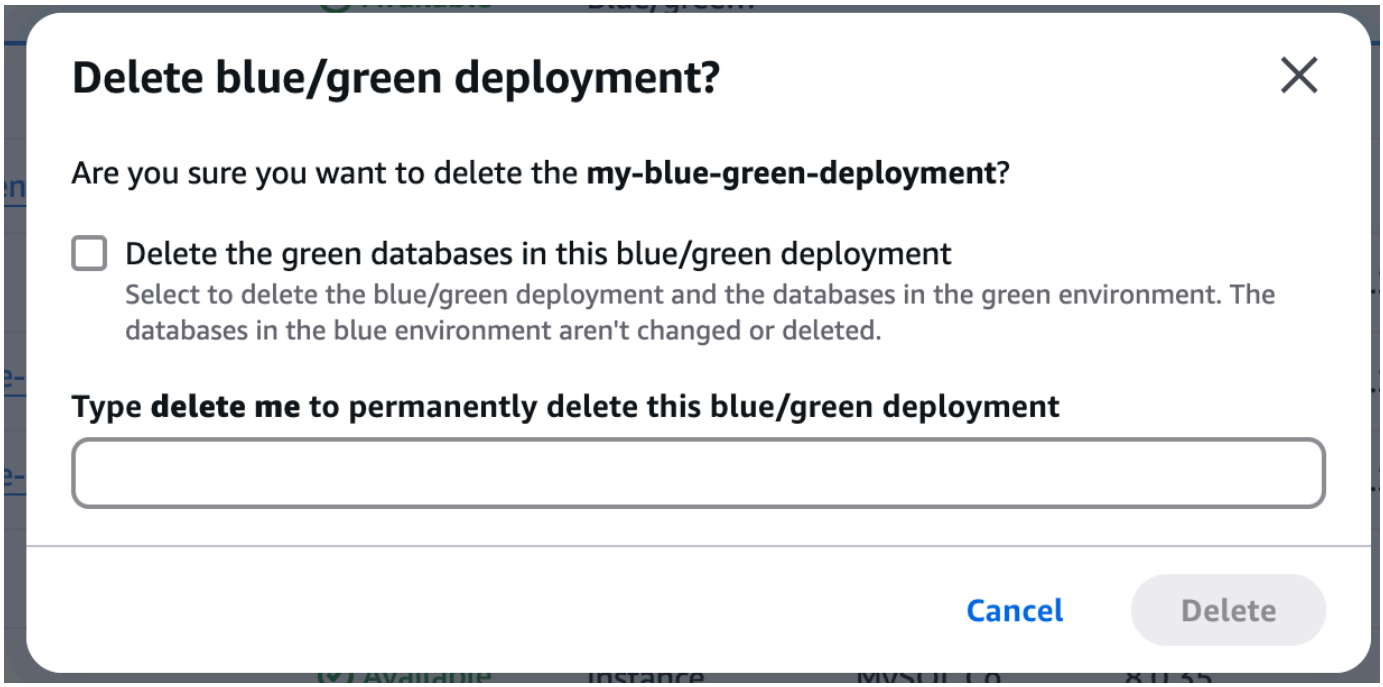
Puede eliminar una implementación azul/verde mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para eliminar una implementación azul/verde

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la implementación azul/verde que desee eliminar.
3. En Actions (Acciones), seleccione Delete (Eliminar).

Aparece la ventana ¿Eliminar la implementación azul/verde?



Para eliminar las bases de datos verdes, seleccione Eliminar las bases de datos verdes en esta implementación azul/verde.

4. En el cuadro, escriba **`delete me`**.
5. Elija Eliminar.

AWS CLI

Para eliminar una implementación azul/verde mediante la AWS CLI, utilice el comando delete-blue-green-deployment con las siguientes opciones:

- `--blue-green-deployment-identifier`: el identificador de recurso de la implementación azul/verde que se va a eliminar.
- `--delete-target`: especifica que se eliminan las instancias de base de datos del entorno verde. No puede especificar esta opción si la implementación azul/verde tiene un estado de `SWITCHOVER_COMPLETED`.
- `--no-delete-target`: especifica que se conservan las instancias de base de datos en el entorno verde.

Example Eliminar una implementación azul/verde y las instancias de base de datos del entorno verde

Para Linux, macOS o Unix:

```
aws rds delete-blue-green-deployment \
    --blue-green-deployment-identifier bgd-1234567890abcdef \
    --delete-target
```

Para Windows:

```
aws rds delete-blue-green-deployment ^
    --blue-green-deployment-identifier bgd-1234567890abcdef ^
    --delete-target
```

Example Elimine una implementación azul/verde pero conserve las instancias de base de datos en el entorno verde

Para Linux, macOS o Unix:

```
aws rds delete-blue-green-deployment \
    --blue-green-deployment-identifier bgd-1234567890abcdef \
    --no-delete-target
```

Para Windows:

```
aws rds delete-blue-green-deployment ^
    --blue-green-deployment-identifier bgd-1234567890abcdef ^
    --no-delete-target
```

API de RDS

Para eliminar una implementación azul/verde mediante la API de Amazon RDS, utilice la operación `DeleteBlueGreenDeployment` con los siguientes parámetros:

- `BlueGreenDeploymentIdentifier`: el identificador de recurso de la implementación azul/verde que se va a eliminar.
- `DeleteTarget`: especifique `TRUE` para eliminar las instancias de base de datos en el entorno verde o para conservarlas . No puede ser `TRUE` si la implementación azul/verde tiene un estado de `SWITCHOVER_COMPLETED`.

Copia de seguridad, restauración y exportación de datos

Esta sección muestra cómo crear copias de seguridad, restauraciones y exportaciones de una instancia de base de datos de Amazon RDS o un clúster de base de datos multi-AZ.

Para obtener información sobre cómo crear copias de seguridad de una instancia de base de datos de Amazon RDS o un clúster de base de datos multi-AZ, consulte los siguientes temas.

- Introducción a las copias de seguridad
- Administración de las copias de seguridad automatizadas
- Administración de copias de seguridad manuales

Para obtener información sobre cómo restaurar una instancia de base de datos de Amazon RDS o un clúster de base de datos multi-AZ, consulte Restauración a una instancia de base de datos.

Para obtener información sobre cómo copiar, compartir o exportar instantáneas de base de datos, consulte los siguientes temas.

- Copia de una instantánea de base de datos para Amazon RDS
- Uso compartido de una instantánea manual de base de datos de Amazon RDS
- Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS

Para obtener información sobre cómo ver copias de seguridad automatizadas administradas por AWS Backup, consulte Utilización de AWS Backup para administrar copias de seguridad automatizadas para Amazon RDS.

Introducción a las copias de seguridad

Amazon RDS crea y guarda copias de seguridad automatizadas de la instancia de base de datos o el clúster de base de datos Multi-AZ durante el período de copia de seguridad de su instancia de base de datos. RDS; crea una instantánea del volumen de almacenamiento de la instancia de base de datos, creando una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. RDS guarda las copias de seguridad automatizadas de la instancia de base de datos en función del periodo de retención de copia de seguridad especificado. Si es necesario, puede recuperar la instancia de base de datos a cualquier momento dado durante el período de retención de copia de seguridad.

Las copias de seguridad automatizadas siguen estas reglas:

- Su instancia de base de datos debe tener el estado `available` para que puedan realizarse backups automatizados. Las copias de seguridad automatizadas no se producen mientras la instancia de base de datos está en un estado distinto de `available`, por ejemplo, `storage_full`.
- Las copias de seguridad automáticas no se producen mientras una copia de una instantánea de base de datos se está ejecutando en la misma Región de AWS para la misma base de datos.

También puede realizar un backup de su instancia de base de datos manualmente, mediante la creación de una instantánea de base de datos. Para obtener más información acerca de la creación de una instantánea de base de datos de forma manual, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

La primera instantánea de una instancia de base de datos contiene los datos de la base de datos completa. Las instantáneas posteriores de la misma base de datos son incrementales, lo que significa que solo se guardan los datos que han cambiado después de la última instantánea.

Puede copiar tanto las instantáneas de base de datos automáticas como las manuales y compartir las instantáneas de base de datos manuales. Para obtener más información acerca de la copia de una instantánea de base de datos, consulte Copia de una instantánea de base de datos para Amazon RDS. Para obtener más información acerca del uso compartido de una instantánea de base de datos, consulte Uso compartido de una instantánea manual de base de datos de Amazon RDS.

Almacenamiento de copia de seguridad

El almacenamiento de copia de seguridad de Amazon RDS de cada Región de AWS se compone de las copias de seguridad automáticas y las instantáneas de base de datos manuales de esa región. El total del espacio de almacenamiento de copias de seguridad equivale a la suma del almacenamiento de todos las copias de seguridad de una región. Mover una instantánea de base de datos a otra región incrementa el almacenamiento de backup en la región de destino. Las copias de seguridad se almacenan en Amazon S3.

Para obtener más información acerca de los costos de almacenamiento de copias de seguridad, consulte Precios de Amazon RDS.

Si decide retener copias de seguridad automatizadas al eliminar una instancia de base de datos, las copias de seguridad automatizadas se guardan durante todo el período de retención. Si no elige Retain automated backups (Conservar copias de seguridad automatizadas) al eliminar una instancia de base de datos, todas las copias de seguridad automatizadas se eliminan con la instancia de base de datos. Tras eliminarlas, las copias de seguridad automatizadas no se pueden recuperar. Si opta por hacer que Amazon RDS cree una instantánea de base de datos final antes de que elimine su instancia de base de datos, podrá usarla para recuperar la instancia de base de datos. También puede utilizar una instantánea manual creada anteriormente. Las instantáneas manuales no se eliminan. Puede disponer de hasta 100 instantáneas manuales por región.

Administración de las copias de seguridad automatizadas

En esta sección, se muestra cómo administrar copias de seguridad automatizadas de instancias de base de datos y clústeres de base de datos multi-AZ.

Temas

- Intervalo de copia de seguridad
- Backup retention period (Periodo de retención de copia de seguridad)
- Habilitar las copias de seguridad automatizadas
- Retener copias de seguridad automatizadas
- Eliminación de las copias de seguridad automatizadas retenidas
- Copias de seguridad automatizadas con motores de almacenamiento de MySQL no compatibles
- Copias de seguridad automatizadas con motores de almacenamiento de MariaDB no compatibles
- Replicación de las copias de seguridad automatizadas en otra Región de AWS

Intervalo de copia de seguridad

Los backups automatizados se producen a diario durante la ventana de copia de seguridad preferida. Si la copia de seguridad requiere más tiempo del asignado al periodo de copia de seguridad, la copia de seguridad continúa cuando finaliza el periodo hasta que se completa. El periodo de copia de seguridad no se puede superponer al periodo de mantenimiento semanal de la instancia de base de datos o el clúster de base de datos Multi-AZ.

Durante la ventana de copia de seguridad automático, las E/S de almacenamiento pueden quedar suspendidas brevemente mientras se inicializa el proceso de copia de seguridad (normalmente durante unos pocos segundos). Pueden producirse latencias elevadas durante unos minutos mientras se realizan los backups para las implementaciones Multi-AZ. Para MariaDB, MySQL, Oracle y PostgreSQL, la actividad de E/S no se suspende en la instancia principal durante la copia de seguridad para las implementaciones multi-AZ, ya que esta copia de seguridad se realiza desde la instancia en espera. En SQL Server, la actividad de E/S se suspende brevemente durante la copia de seguridad para las implementaciones Multi-AZ y Single-AZ, ya que la copia de seguridad se realiza desde la principal. Para Db2, la actividad de E/S también se suspende brevemente durante la copia de seguridad, aunque esta se realice desde la instancia en espera.

Las copias de seguridad automáticas pueden omitirse ocasionalmente si la instancia o el clúster de base de datos tiene una carga de trabajo pesada en el momento en que se supone que

debe iniciarse una copia de seguridad. Si se omite una copia de seguridad, puede realizar una recuperación a un momento dado (PITR) y se intenta realizar una copia de seguridad durante el siguiente periodo de copia de seguridad. Para obtener más información acerca de PITR, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Si no especifica un periodo preferido para la copia de seguridad al crear la instancia de base de datos o el clúster de base de datos Multi-AZ, Amazon RDS asigna un periodo de copia de seguridad predeterminado de 30 minutos. Este periodo se selecciona al azar dentro de un bloque de 8 horas por cada Región de AWS. En la tabla siguiente se enumeran los bloques de tiempo para cada Región de AWS desde la que se asignan los periodos de copia de seguridad predeterminados.

Nombre de la región	Región	Bloque de tiempo
Este de EE. UU. (Norte de Virginia)	us-east-1	03:00–11:00 UTC
Este de EE. UU. (Ohio)	us-east-2	03:00 — 11:00 UTC
Oeste de EE. UU. (Norte de California)	us-west-1	06:00 — 14:00 UTC
Oeste de EE. UU. (Oregón)	us-west-2	06:00–14:00 UTC
África (Ciudad del Cabo)	af-south-1	03:00–11:00 UTC
Asia-Pacífico (Hong Kong)	ap-east-1	06:00–14:00 UTC
Asia-Pacífico (Hyderabad)	ap-south-2	06:30 – 14:30 UTC
Asia-Pacífico (Yakarta)	ap-southeast-3	08:00 a 16:00 h UTC
Asia-Pacífico (Malasia)	ap-southeast-5	09:00–17:00 UTC

Nombre de la región	Región	Bloque de tiempo
Asia-Pacífico (Melbourne)	ap-southeast-4	11:00–19:00 UTC
Asia Pacífico (Bombay)	ap-south-1	16:30 — 00:30 UTC
Asia-Pacífico (Osaka)	ap-northeast-3	00:00 — 08:00 UTC
Asia-Pacífico (Seúl)	ap-northeast-2	13:00 — 21:00 UTC
Asia-Pacífico (Singapur)	ap-southeast-1	14:00 — 22:00 UTC
Asia Pacífico (Sídney)	ap-southeast-2	12:00 — 20:00 UTC
Asia Pacífico (Tokio)	ap-northeast-1	13:00 — 21:00 UTC
Canadá (centro)	ca-central-1	03:00 — 11:00 UTC
Oeste de Canadá (Calgary)	ca-west-1	18:00 — 02:00 UTC
China (Pekín)	cn-north-1	06:00–14:00 UTC
China (Ningxia)	cn-northwest-1	06:00–14:00 UTC
Europe (Fráncfort)	eu-central-1	20:00 — 04:00 UTC
Europe (Irlanda)	eu-west-1	22:00 — 06:00 UTC
Europe (Londres)	eu-west-2	22:00 — 06:00 UTC
Europa (Milán)	eu-south-1	02:00 — 10:00 UTC
Europa (París)	eu-west-3	07:29 — 14:29 UTC
Europa (España)	eu-south-2	02:00 — 10:00 UTC

Nombre de la región	Región	Bloque de tiempo
Europa (Estocolmo)	eu-north-1	23:00 — 07:00 UTC
Europa (Zúrich)	eu-central-2	02:00 — 10:00 UTC
Israel (Tel Aviv)	il-central-1	03:00 — 11:00 UTC
Medio Oriente (Baréin)	me-south-1	06:00–14:00 UTC
Medio Oriente (EAU)	me-central-1	05:00 a 13:00 h UTC
América del Sur (São Paulo)	sa-east-1	23:00 — 07:00 UTC
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	17:00 — 01:00 UTC
AWS GovCloud (Oeste de EE. UU.)	us-gov-west-1	06:00–14:00 UTC

Backup retention period (Periodo de retención de copia de seguridad)

Puede configurar el periodo de retención de copia de seguridad al crear una instancia de base de datos o un clúster de base de datos Multi-AZ. Si crea una instancia de base de datos con la API de Amazon RDS o la AWS CLI y no configura el periodo de retención de copia de seguridad, el periodo predeterminado de retención de copia de seguridad es un día. Si crea una instancia de base de datos con la consola, el periodo de retención de copia de seguridad predeterminado es de siete días.

Después de crear una instancia o clúster de base de datos, puede modificar el periodo de retención de copia de seguridad. Puede asignar al período de retención de copia de seguridad de una instancia de base de datos un valor de entre 0 y 35 días. Establecer el período de retención de la copia de seguridad en 0 desactiva las copias de seguridad automatizadas. Para un clúster de base de datos Multi-AZ, puede configurar el periodo retención de copia de seguridad entre 1 y 35 días. Los límites de instantáneas manuales (100 por región) no se aplican a las copias de seguridad automáticas.

> **Important**
>
> Se produce una interrupción si se cambia el periodo de retención de copia de seguridad de una instancia de base de datos de 0 a un valor distinto de 0 o de un valor distinto de 0 a 0.

RDS no contempla el tiempo que se pasa en el estado `stopped` cuando se calcula el periodo de retención de copia de seguridad. Las copias de seguridad automáticas no se crean mientras una instancia o clúster de base de datos esté detenido. Las copias de seguridad se pueden retener durante más tiempo que el periodo de retención de copia de seguridad si se ha detenido una instancia de base de datos.

Habilitar las copias de seguridad automatizadas

Si la instancia de base de datos no tiene habilitados las copias de seguridad automatizadas, puede habilitarlos en cualquier momento. Para habilitar las copias de seguridad automatizadas, establezca el periodo de retención de copia de seguridad en un valor positivo distinto de cero. Cuando se activan las copias de seguridad automatizadas, su instancia de base de datos se desconecta y se crea una copia de seguridad de inmediato.

> **Note**
>
> Si administra las copias de seguridad en AWS Backup, no puede habilitar copias de seguridad automatizadas. Para obtener más información, consulte Utilización de AWS Backup para administrar copias de seguridad automatizadas para Amazon RDS.

Consola

Para habilitar las copias de seguridad automatizadas inmediatamente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija la instancia de base de datos o el clúster de base de datos Multi-AZ que desea modificar.
3. Elija Modificar.
4. En Periodo de retención de copia de seguridad, elija un valor positivo distinto de cero, por ejemplo, tres días.

5. Elija Continue.
6. Seleccione Apply immediately (Aplicar inmediatamente).
7. Elija Modificar la instancia de base de datos o Modificar clúster para guardar los cambios y habilitar las copias de seguridad automáticas.

AWS CLI

Para habilitar las copias de seguridad automáticas, utilice el comando modify-db-instance o modify-db-cluster de AWS CLI.

Incluya los siguientes parámetros:

- `--db-instance-identifier` (o `--db-cluster-identifier` para un clúster de base de datos Multi-AZ)
- `--backup-retention-period`
- `--apply-immediately` o `--no-apply-immediately`

En este ejemplo, habilitaremos las copias de seguridad automatizadas estableciendo el periodo de retención de copia de seguridad en 3 días. Los cambios se aplican inmediatamente.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my_db_instance  \
    --backup-retention-period 3 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my_db_instance  ^
    --backup-retention-period 3 ^
    --apply-immediately
```

API de RDS

Para habilitar las copias de seguridad automáticas, utilice la operación ModifyDBInstance o ModifyDBCluster de la API de RDS con los siguientes parámetros obligatorios:

- `DBInstanceIdentifier` o `DBClusterIdentifier`
- `BackupRetentionPeriod`

Visualizar copias de seguridad automatizadas

Para ver las copias de seguridad automatizadas, elija Automated backups (Copias de seguridad automatizadas) en el panel de navegación. Para ver instantáneas individuales asociadas a una copia de seguridad automatizada, elija Snapshots (Instantáneas) en el panel de navegación. También puede describir instantáneas individuales asociadas con una copia de seguridad automatizada. Desde ahí, puede restaurar una instancia de base de datos directamente a partir de una de esas instantáneas.

Las instantáneas automáticas siguen el patrón `rds:<database-name>-yyyy-mm-dd-hh-mm`, donde `yyyy-mm-dd-hh-mm` representa la fecha y la hora en la que se creó la instantánea.

Para describir las copias de seguridad automatizadas para sus instancias de bases de datos mediante la AWS CLI, utilice uno de los siguientes comandos:

```
aws rds describe-db-instance-automated-backups --db-instance-
identifier DBInstanceIdentifier
```

o

```
aws rds describe-db-instance-automated-backups --dbi-resource-id DbiResourceId
```

Para describir las copias de seguridad automatizadas retenidas para sus instancias de bases de datos existentes mediante la API de RDS, llame a la `DescribeDBInstanceAutomatedBackups` acción con uno de los siguientes parámetros:

- `DBInstanceIdentifier`
- `DbiResourceId`

Retener copias de seguridad automatizadas

> **Note**
>
> Solo puede retener copias de seguridad automáticas de instancias de base de datos, no de clústeres de base de datos Multi-AZ.

Cuando elimine una instancia de base de datos, puede optar por retener las copias de seguridad automatizadas. Las copias de seguridad automatizadas se retienen durante un número de días equivalente al periodo de retención configurado para la instancia de base de datos en el momento de eliminarla.

Las copias de seguridad automatizadas contienen instantáneas de sistema y registros de transacción de una instancia de base de datos. También incluyen propiedades de instancia de base de datos, como el almacenamiento asignado y la clase de instancia de base de datos, necesarias para restaurarlas a una instancia activa.

Las copias de seguridad automatizadas y las instantáneas manuales retenidas incurrirán en cargos de facturación hasta que se eliminen. Para obtener más información, consulte Costos de retención.

Puede conservar copias de seguridad automatizadas para instancias de RDS que ejecuten motores MySQL, MariaDB, PostgreSQL, Oracle y Microsoft SQL Server.

Puede restaurar o eliminar copias de seguridad automatizadas con la AWS Management Console, la API de RDS y la AWS CLI.

Temas

- Período de retención
- Visualización de copias de seguridad retenidas
- Restauración
- Costos de retención
- Limitaciones

Período de retención

Las instantáneas de sistema y los registros de transacción en una copia de seguridad automatizada expiran del mismo modo que para la instancia de base de datos de origen. Dado que no hay nuevas

instantáneas ni registros creados para esta instancia, las copias de seguridad automatizadas conservadas vencen completamente al final. Efectivamente, duran tanto como habría durado la última instantánea de sistema, sobre la base de la configuración del periodo de retención que tenía la instancia de origen cuando la eliminó. Las copias de seguridad automatizadas conservadas se eliminan del sistema después de que vence la última instantánea del sistema.

Puede eliminar una copia de seguridad automatizada conservada del mismo modo que puede eliminar una instancia de base de datos. Puede restaurar o eliminar copias de seguridad automatizadas con la consola o la operación de la API de RDS `DeleteDBInstanceAutomatedBackup`.

Las instantáneas finales son independientes de las copias de seguridad automatizadas conservadas. Recomendamos encarecidamente que tome una instantánea final aunque retenga las copias de seguridad automáticas, ya que las copias de seguridad retenidas vencen por completo. La instantánea final no vence.

Visualización de copias de seguridad retenidas

Para ver las copias de seguridad automatizadas retenidas, elija Automated backups (Copias de seguridad automatizadas) en el panel de navegación y, a continuación, elija Retained (Retenido). Para ver instantáneas individuales asociadas a una copia de seguridad automatizada retenida, elija Snapshots (Instantáneas) en el panel de navegación. También puede describir instantáneas individuales asociadas con una copia de seguridad automatizada conservada. Desde ahí, puede restaurar una instancia de base de datos directamente a partir de una de esas instantáneas.

Para describir las copias de seguridad automatizadas retenidas mediante AWS CLI, utilice el siguiente comando:

```
aws rds describe-db-instance-automated-backups --dbi-resource-id DbiResourceId
```

Para describir sus copias de seguridad automatizadas retenidas mediante la API de RDS, llame a la `DescribeDBInstanceAutomatedBackups` acción con el parámetro `DbiResourceId`.

Restauración

Para obtener información sobre cómo restaurar instancias de base de datos a partir de copias de seguridad automatizadas, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Costos de retención

El costo de una copia de seguridad automatizada conservada es el costo del almacenamiento total de las instantáneas del sistema asociadas con ella. No hay cobros adicionales para los registros de transacción o los metadatos de instancia. Todas las demás reglas de precios para copias de seguridad se aplican a las instancias restaurables.

Por ejemplo, supongamos que su almacenamiento total asignado para instancias en ejecución es de 100 GB. Supongamos también que tiene 50 GB de instantáneas manuales más 75 GB de instantáneas del sistema asociadas con una copia de seguridad automatizada conservada. En este caso, solo se le cobrará por los 25 GB adicionales de almacenamiento de copia de seguridad, así: (50 GB + 75 GB) – 100 GB = 25 GB.

Limitaciones

Las copias de seguridad automatizadas conservadas tienen las siguientes limitaciones:

- El número máximo de copias de seguridad automatizadas conservadas en una región de AWS es 40. No está incluido en la cuota de instancias de base de datos. Puede tener 40 instancias de base de datos en ejecución y 40 copias de seguridad automatizadas conservadas al mismo tiempo.
- Las copias de seguridad automatizadas conservadas no contienen información sobre parámetros o grupos de opciones.
- Puede restaurar una instancia eliminada a un momento dado que esté dentro del período de retención en el momento de la eliminación.
- Una copia de seguridad automatizada retenida no se puede modificar, ya que consiste en copias de seguridad del sistema, registros de transacciones y las propiedades de instancia de base de datos que existían en el momento cuando eliminó la instancia de origen.

Eliminación de las copias de seguridad automatizadas retenidas

Puede eliminar las copias de seguridad automatizadas retenidas cuando no sean necesarias.

Consola

Para eliminar una copia de seguridad automatizada retenida

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Automated backups (Copias de seguridad automatizadas).
3. En la pestaña Retained (Retenidas), elija la copia de seguridad automatizada retenida que desee eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. En la página de confirmación, introduzca **`delete me`** y elija Delete (Eliminar).

AWS CLI

Puede eliminar una copia de seguridad automatizada retenida mediante el comando de la AWS CLI delete-db-instance-automated-backup con la siguiente opción:

- `--dbi-resource-id`: identificador de recurso para la instancia de base de datos de origen.

  Puede encontrar el identificador de recursos para la instancia de base de datos de origen de una copia de seguridad automatizada retenida al ejecutar el comando de la AWS CLI describe-db-instance-automated-backups.

Example

El siguiente ejemplo elimina la copia de seguridad automatizada retenida con el identificador de recursos de la instancia de base de datos `db-123ABCEXAMPLE`.

Para Linux, macOS o:Unix

```
aws rds delete-db-instance-automated-backup \
    --dbi-resource-id db-123ABCEXAMPLE
```

En:Windows

```
aws rds delete-db-instance-automated-backup ^
    --dbi-resource-id db-123ABCEXAMPLE
```

API de RDS

Puede eliminar una copia de seguridad automatizada retenida mediante la operación de API de Amazon RDS DeleteDBInstanceAutomatedBackup con el siguiente parámetro:

- `DbiResourceId`: identificador de recurso para la instancia de base de datos de origen.

  Puede encontrar el identificador de recursos para la instancia de base de datos de origen de una copia de seguridad automatizada retenida utilizando la operación de la API de Amazon RDS DescribeDBInstanceAutomatedBackups.

Desactivar las copias de seguridad automatizadas

Puede que quiera deshabilitar temporalmente las copias de seguridad automatizadas en ciertas situaciones; por ejemplo, si carga grandes cantidades de datos.

> **Important**
>
> No es aconsejable deshabilitar las copias de seguridad automatizadas, ya que al hacerlo se deshabilita la recuperación a un momento dado. Al deshabilitar las copias de seguridad automáticas para una instancia de base de datos o un clúster de base de datos Multi-AZ, se eliminan todas las copias de seguridad automáticas para la base de datos. Si deshabilita y vuelve a habilitar las copias de seguridad automatizadas, solo podrá efectuar la recuperación a partir del momento en el que las copias de seguridad automatizadas se hayan habilitado de nuevo.

Consola

Para deshabilitar las copias de seguridad automatizadas inmediatamente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija la instancia de base de datos o el clúster de base de datos Multi-AZ que desea modificar.
3. Elija Modificar.
4. En Backup retention period (Periodo de retención de copia de seguridad), elija 0 days (0 días).
5. Elija Continue.
6. Seleccione Apply immediately (Aplicar inmediatamente).
7. Elija Modificar la instancia de base de datos o Modificar clúster para guardar los cambios y deshabilitar las copias de seguridad automáticas.

AWS CLI

Para deshabilitar inmediatamente las copias de seguridad automáticas, use el comando modify-db-instance o modify-db-cluster y asigne al periodo de retención de copia de seguridad el valor 0 con `--apply-immediately`.

Example

El siguiente ejemplo deshabilita inmediatamente las copias de seguridad automáticas en un clúster de base de datos Multi-AZ.

Para Linux, macOS o:Unix

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --backup-retention-period 0 \
    --apply-immediately
```

En:Windows

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --backup-retention-period 0 ^
    --apply-immediately
```

Para saber cuándo entra en vigor la modificación, llame a `describe-db-instances` para la instancia de base de datos (o a `describe-db-clusters` para el clúster de base de datos Multi-AZ) hasta que el valor del periodo de retención de copia de seguridad sea 0 y el estado `mydbcluster` sea disponible.

```
aws rds describe-db-clusters --db-cluster-identifier mydcluster
```

API de RDS

Para deshabilitar las copias de seguridad automáticas de forma inmediata, llame a la operación ModifyDBInstance o ModifyDBCluster con los siguientes parámetros:

- `DBInstanceIdentifier = mydbinstance` (o `DBClusterIdentifier = mydbcluster`)
- `BackupRetentionPeriod = 0`

Example

```
https://rds.amazonaws.com/
    ?Action=ModifyDBInstance
    &DBInstanceIdentifier=mydbinstance
    &BackupRetentionPeriod=0
    &SignatureVersion=2
    &SignatureMethod=HmacSHA256
    &Timestamp=2009-10-14T17%3A48%3A21.746Z
    &AWSAccessKeyId=<&AWS; Access Key ID>
    &Signature=<Signature>
```

Copias de seguridad automatizadas con motores de almacenamiento de MySQL no compatibles

Para el motor de base de datos de MySQL, las copias de seguridad automatizadas solo son compatibles para el motor de almacenamiento InnoDB. El uso de estas características con otros motores de almacenamiento de MySQL, incluido MyISAM, puede dar lugar a comportamientos poco fiables al restaurar desde copias de seguridad. Específicamente, dado que los motores de almacenamiento como MyISAM no admiten una recuperación de bloqueos fiable, las tablas pueden dañarse si se produce un bloqueo. Por este motivo, le animamos a usar el motor de almacenamiento de InnoDB.

- Para convertir las tablas de MyISAM existentes en tablas de InnoDB, puede usar el comando `ALTER TABLE`, por ejemplo: `ALTER TABLE table_name ENGINE=innodb, ALGORITHM=COPY;`
- Si opta por usar MyISAM, puede intentar reparar manualmente las tablas que se hayan dañado después de un bloqueo usando el comando `REPAIR`. Para obtener más información, consulte REPAIR TABLE Statement en la documentación de MySQL. Sin embargo, como se indica en la documentación de MySQL, es muy probable que no pueda recuperar todos los datos.
- Si desea crear una instantánea de sus tablas MyISAM antes de restaurar, siga estos pasos:
  1. Detenga toda la actividad de las tablas de MyISAM (es decir, cierre todas las sesiones).

     Puede cerrar todas las sesiones llamando al comando mysql.rds_kill para cada proceso devuelto por el comando `SHOW FULL PROCESSLIST`.
  2. Bloquee y vacíe cada una de las tablas de MyISAM. Por ejemplo, los siguientes comandos bloquean y vacían dos tablas llamadas `myisam_table1` y `myisam_table2`:

```
mysql> FLUSH TABLES myisam_table, myisam_table2 WITH READ LOCK;
```

3. Cree una instancia de base de datos o un clúster de base de datos Multi-AZ. Cuando la instantánea se haya completado, libere los bloqueos y reanude la actividad en las tablas de MyISAM. Puede liberar los bloqueos de las tablas usando el siguiente comando:

```
mysql> UNLOCK TABLES;
```

Estos pasos obligan a MyISAM a limpiar los datos almacenados en memoria en el disco, lo que garantiza un inicio limpio al restaurar desde una instantánea de base de datos. Para obtener más información acerca de la creación de una instantánea de base de datos, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Copias de seguridad automatizadas con motores de almacenamiento de MariaDB no compatibles

Para el motor de base de datos MariaDB, las copias de seguridad automatizadas solo son compatibles con el motor de almacenamiento InnoDB. El uso de estas características con otros motores de almacenamiento de MariaDB, incluido Aria, puede dar lugar a comportamientos poco fiables al restaurar desde copias de seguridad. Aunque Aria es una alternativa a MyISAM resistente a bloqueos, las tablas pueden dañarse si se produce un bloqueo. Por este motivo, le animamos a usar el motor de almacenamiento de InnoDB.

- Para convertir las tablas de Aria en tablas de InnoDB, puede usar el comando `ALTER TABLE`. Por ejemplo: `ALTER TABLE table_name ENGINE=innodb, ALGORITHM=COPY;`.
- Si opta por usar Aria, puede intentar reparar manualmente las tablas que se hayan dañado después de un bloqueo usando el comando `REPAIR TABLE`. Para obtener más información, consulte http://mariadb.com/kb/en/mariadb/repair-table/.
- Si desea crear una instantánea de sus tablas Aria antes de restaurar, siga estos pasos:
  1. Detenga toda la actividad de las tablas de Aria (es decir, cierre todas las sesiones).
  2. Bloquee y vacíe cada una de las tablas de Aria.
  3. Cree una instancia de base de datos o un clúster de base de datos Multi-AZ. Cuando la instantánea se haya completado, libere los bloqueos y reanude la actividad en las tablas de Aria. Estos pasos obligan a Aria a limpiar los datos almacenados en memoria en el disco, lo que garantiza un inicio limpio al restaurar desde una instantánea de base de datos.

Replicación de las copias de seguridad automatizadas en otra Región de AWS

Para obtener una capacidad adicional de recuperación de desastres, puede configurar su instancia de base de datos de Amazon RDS para replicar las instantáneas y los registros de transacciones a una Región de AWS de destino de su elección. Cuando se configura la replicación de la copia de seguridad para una instancia de base de datos, RDS inicia una copia entre regiones de todas las instantáneas y los registros de transacciones tan pronto como estén listos en la instancia de base de datos.

Se aplican cargos por copia instantánea de base de datos a la transferencia de datos. Una vez que se copia la instantánea de base de datos, se aplican cargos estándares al almacenamiento en la región de destino. Para obtener más información, consulte Precios de RDS.

Para obtener un ejemplo de la utilización de la replicación de copias de seguridad, consulte la charla tecnológica en línea de AWS Managed Disaster Recovery with Amazon RDS para Oracle Cross-Region Automated Backups.

> **Note**
>
> No se admite la réplica de copia de seguridad automatizada para clústeres de base de datos multi-AZ.

Temas

- Disponibilidad en regiones y versiones
- Compatibilidad de la Región de AWS en el origen y el destino
- Habilitación de copias de seguridad automatizadas entre regiones
- Búsqueda de información sobre las copias de seguridad replicadas
- Restauración a un tiempo especificado desde una copia de seguridad replicada
- Detención de la replicación de la copia de seguridad automatizada
- Eliminación de las copias de seguridad replicadas

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de las copias de seguridad automatizadas entre regiones, consulte Regiones y motores de bases de datos admitidos para copias de seguridad automatizadas entre regiones en Amazon RDS.

Compatibilidad de la Región de AWS en el origen y el destino

La reproducción de copia de seguridad se admite entre las siguientes:Regiones de AWS

Región de origen	Regiones de destino disponibles
Asia Pacific (Bombay)	Asia Pacífico (Singapur) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón)
Asia Pacific (Osaka)	Asia Pacífico (Tokio)
Asia Pacific (Seoul)	Asia Pacífico (Singapur), Asia Pacífico (Tokio) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón)
Asia Pacífico (Singapur)	Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Sídney), Asia Pacífico (Tokio) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón)
Asia Pacífico (Sídney)	Asia Pacífico (Singapur) EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Norte de Californi a), EE. UU. Oeste (Oregón)
Asia Pacífico (Tokio)	Asia Pacífico (Osaka), Asia Pacífico (Seúl), Asia Pacífico (Singapur) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón)

Región de origen	Regiones de destino disponibles
Canada (Central)	Europe (Irlanda) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Norte de California), EE. UU. Oeste (Oregón)
China (Pekín)	China (Ningxia)
China (Ningxia)	China (Pekín)
Europa (Fráncfort)	Europa (Irlanda), Europa (Londres), Europa (París), Europa (Estocolmo) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón)
Europe (Irlanda)	Canada (Central) Europa (Fráncfort), Europa (Londres), Europa (París), Europa (Estocolmo) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Norte de California), EE. UU. Oeste (Oregón)
Europe (Londres)	Europa (Fráncfort), Europa (Irlanda), Europa (París), Europa (Estocolmo) EE.UU. Este (Norte de Virginia)
Europe (Paris)	Europa (Fráncfort), Europa (Irlanda), Europa (Londres), Europa (Estocolmo) EE.UU. Este (Norte de Virginia)
Europa (Estocolmo)	Europa (Fráncfort), Europa (Irlanda), Europa (Londres), Europa (París) EE.UU. Este (Norte de Virginia)

Región de origen	Regiones de destino disponibles
América del Sur (São Paulo)	EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio)
AWS GovCloud (EE. UU. Este)	AWS GovCloud (EE. UU. Oeste)
AWS GovCloud (EE. UU. Oeste)	AWS GovCloud (Este de EE. UU.)
EE.UU. Este (Norte de Virginia)	Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio) Canada (Central) Europa (Fráncfort), Europa (Irlanda), Europa (Londres), Europa (París), Europa (Estocolmo) América del Sur (São Paulo) EE. UU. Este (Ohio), EE. UU. Oeste (Norte de California), EE. UU. Oeste (Oregón)
US East (Ohio)	Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Tokio) Canada (Central) Europa (Fráncfort), Europa (Irlanda) América del Sur (São Paulo) EE. UU. Este (Norte de Virginia), EE. UU. Oeste (Norte de California), EE. UU. Oeste (Oregón)

Región de origen	Regiones de destino disponibles
EE.UU. Oeste (Norte de California)	Asia Pacífico (Sídney) Canada (Central) Europe (Irlanda) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Oregón)
EE.UU. Oeste (Oregón)	Asia Pacífico (Bombay), Asia Pacífico (Seúl), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Asia Pacífico (Tokio) Canada (Central) Europa (Fráncfort), Europa (Irlanda) EE. UU. Este (Norte de Virginia), EE. UU. Este (Ohio), EE. UU. Oeste (Norte de California)

También puede utilizar el comando `describe-source-regions` de la AWS CLI para averiguar qué Regiones de AWS se pueden replicar entre sí. Para obtener más información, consulte Búsqueda de información sobre las copias de seguridad replicadas.

Habilitación de copias de seguridad automatizadas entre regiones

Puede habilitar la reproducción de la copia de seguridad en las instancias de base de datos nuevas o existentes mediante la consola de Amazon RDS. También puede utilizar el comando `start-db-instance-automated-backups-replication` de la interfaz de línea de comandos (AWS CLI) o la operación `StartDBInstanceAutomatedBackupsReplication` de la API de RDS. Puede replicar hasta 20 copias de seguridad en cada destino Región de AWS para cada Cuenta de AWS.

> **Note**
>
> Para poder replicar copias de seguridad automatizadas, asegúrese de habilitarlas. Para obtener más información, consulte Habilitar las copias de seguridad automatizadas.

Consola

Puede habilitar la replicación de la copia de seguridad para una instancia de base de datos nueva o existente:

- Para una nueva instancia de base de datos, habilítela cuando lance la instancia. Para obtener más información, consulte Configuración de instancias de base de datos.
- Para una instancia de base de datos existente, utilice el siguiente procedimiento.

Para habilitar la replicación de la copia de seguridad para una instancia de base de datos existente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Automated backups (Copias de seguridad automatizadas).
3. En la pestaña Current Region (Región actual), elija la instancia de base de datos para la que desea habilitar la replicación de la copia de seguridad.
4. En Actions (Acciones), seleccione Manage cross-Region replication (Administrar replicación entre regiones).
5. En Backup replication (Replicación de la copia de seguridad), elija Enable replication to another Región de AWS (Habilitar replicación en otra región).
6. Elija la Destination Region (Región de destino).
7. Seleccione el Replicated backup retention period (Periodo de retención de copias de seguridad replicadas).
8. Si ha habilitado el cifrado en la instancia de base de datos de origen, elija AWS KMS key para cifrar las copias de seguridad o introducir un ARN de clave.
9. Seleccione Save (Guardar).

En la región de origen, las copias de seguridad replicadas se muestran en la pestaña Current Region (Región actual) de la página Automated backups (Copias de seguridad automatizadas). En la región de destino, las copias de seguridad replicadas se muestran en la pestaña Replicated backups (Copias de seguridad replicadas) de la página Automated backups (Copias de seguridad automatizadas).

AWS CLI

Habilite la replicación de la copia de seguridad mediante el comando `start-db-instance-automated-backups-replication` de la AWS CLI.

El siguiente ejemplo de la CLI replica las copias de seguridad automatizadas desde una instancia de base de datos en Región EE.UU. Oeste (Oregón) a Región EE.UU. Este (Norte de Virginia). También cifra las copias de seguridad replicadas utilizando una AWS KMS key en la región de destino.

Para habilitar la replicación de la copia de seguridad

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

```
aws rds start-db-instance-automated-backups-replication \
--region us-east-1 \
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase" \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE" \
--backup-retention-period 7
```

  En:Windows

```
aws rds start-db-instance-automated-backups-replication ^
--region us-east-1 ^
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase" ^
--kms-key-id "arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE" ^
--backup-retention-period 7
```

  La opción `--source-region` es necesaria cuando se cifran copias de seguridad entre las AWS GovCloud (Este de EE. UU.) y AWS GovCloud (EE. UU. Oeste). Para `--source-region`, especifique la Región de AWS de la instancia de base de datos de origen.

  Si no se ha especificado `--source-region`, asegúrese de especificar un valor de `--pre-signed-url`. Una URL prefirmada es una URL que contiene una solicitud firmada de Signature Version 4 para el comando `start-db-instance-automated-backups-replication` que se llama en la Región de AWS de origen. Para obtener más información sobre la opción `pre-signed-url`, consulte start-db-instance-automated-backups-replication en la Referencia de los comandos de AWS CLI.

API de RDS

Habilite la replicación de la copia de seguridad mediante la operación `StartDBInstanceAutomatedBackupsReplication` de la API de RDS con los siguientes parámetros:

- `Region` (si no llama a la operación de la API desde la región de destino)
- `SourceDBInstanceArn`
- `BackupRetentionPeriod`
- `KmsKeyId` (opcional)
- `PreSignedUrl` (requerido si usa `KmsKeyId`)

> **Note**
>
> Si cifra las copias de seguridad, también debe incluir una URL prefirmada. Para obtener más información sobre las direcciones URL prefirmadas, consulte los datos sobre las solicitudes de autenticación: uso de los parámetros de consulta (AWS Signature Version 4) en la referencia de la API de Amazon Simple Storage Service y el proceso de firma de Signature Version 4 en la referencia general de AWS.

Búsqueda de información sobre las copias de seguridad replicadas

Puede utilizar los siguientes comandos de la CLI para buscar información sobre las copias de seguridad replicadas:

- `describe-source-regions`
- `describe-db-instances`
- `describe-db-instance-automated-backups`

En el siguiente ejemplo de `describe-source-regions`, se enumeran las Regiones de AWS de origen desde las que se pueden reproducir las copias de seguridad automatizadas en la región de Oeste de EE. UU. (Oregón) de destino.

Para mostrar información sobre las regiones de origen

- Ejecute el comando siguiente.

```
aws rds describe-source-regions --region us-west-2
```

La salida muestra que las copias de seguridad se pueden replicar desde US East (N. Virginia), pero no desde EE.UU. Este (Ohio) o EE.UU. Oeste (Norte de California) en EE.UU. Oeste (Oregón).

```
{
    "SourceRegions": [
        ...
        {
            "RegionName": "us-east-1",
            "Endpoint": "https://rds.us-east-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": true
        },
        {
            "RegionName": "us-east-2",
            "Endpoint": "https://rds.us-east-2.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        },
            "RegionName": "us-west-1",
            "Endpoint": "https://rds.us-west-1.amazonaws.com",
            "Status": "available",
            "SupportsDBInstanceAutomatedBackupsReplication": false
        }
    ]
}
```

En el siguiente `describe-db-instances` ejemplo se muestran las copias de seguridad automatizadas de una instancia de base de datos.

Para mostrar las copias de seguridad replicadas para una instancia de base de datos

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

  ```
  aws rds describe-db-instances \
  --db-instance-identifier mydatabase
  ```

En:Windows

```
aws rds describe-db-instances ^
--db-instance-identifier mydatabase
```

La salida incluye las copias de seguridad replicadas.

```
{
    "DBInstances": [
        {
            "StorageEncrypted": false,
            "Endpoint": {
                "HostedZoneId": "Z1PVIF0B656C1W",
                "Port": 1521,
            ...

            "BackupRetentionPeriod": 7,
            "DBInstanceAutomatedBackupsReplications":
 [{"DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-
L2IJCEXJP7XQ7HOJ4SIEXAMPLE"}]
        }
    ]
}
```

En el siguiente `describe-db-instance-automated-backups` ejemplo se muestran las copias de seguridad automatizadas de una instancia de base de datos.

Para mostrar las copias de seguridad automatizadas para una instancia de base de datos

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

  ```
  aws rds describe-db-instance-automated-backups \
  --db-instance-identifier mydatabase
  ```

  En:Windows

  ```
  aws rds describe-db-instance-automated-backups ^
  ```

```
--db-instance-identifier mydatabase
```

El resultado muestra la instancia de base de datos de origen y las copias de seguridad automatizadas en EE.UU. Oeste (Oregón), con las copias de seguridad replicadas en US East (N. Virginia).

```
{
    "DBInstanceAutomatedBackups": [
        {
            "DBInstanceArn": "arn:aws:rds:us-west-2:868710585169:db:mydatabase",
            "DbiResourceId": "db-L2IJCEXJP7XQ7HOJ4SIEXAMPLE",
            "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-west-2:123456789012:auto-
backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE",
            "BackupRetentionPeriod": 7,
            "DBInstanceAutomatedBackupsReplications":
 [{"DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-east-1:123456789012:auto-backup:ab-
L2IJCEXJP7XQ7HOJ4SIEXAMPLE"}]
            "Region": "us-west-2",
            "DBInstanceIdentifier": "mydatabase",
            "RestoreWindow": {
                "EarliestTime": "2020-10-26T01:09:07Z",
                "LatestTime": "2020-10-31T19:09:53Z",
            }
            ...
        }
    ]
}
```

En el siguiente `describe-db-instance-automated-backups` ejemplo se utiliza la opción `--db-instance-automated-backups-arn` para mostrar las copias de seguridad replicadas en la región de destino.

Para mostrar las copias de seguridad replicadas

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

  ```
  aws rds describe-db-instance-automated-backups \
  ```

```
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-
backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE"
```

En:Windows

```
aws rds describe-db-instance-automated-backups ^
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-
backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE"
```

La salida muestra la instancia de base de datos de origen en EE.UU. Oeste (Oregón), con las copias de seguridad replicadas en US East (N. Virginia).

```
{
    "DBInstanceAutomatedBackups": [
        {
            "DBInstanceArn": "arn:aws:rds:us-west-2:868710585169:db:mydatabase",
            "DbiResourceId": "db-L2IJCEXJP7XQ7HOJ4SIEXAMPLE",
            "DBInstanceAutomatedBackupsArn": "arn:aws:rds:us-east-1:123456789012:auto-
backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE",
            "Region": "us-west-2",
            "DBInstanceIdentifier": "mydatabase",
            "RestoreWindow": {
                "EarliestTime": "2020-10-26T01:09:07Z",
                "LatestTime": "2020-10-31T19:01:23Z"
            },
            "AllocatedStorage": 50,
            "BackupRetentionPeriod": 7,
            "Status": "replicating",
            "Port": 1521,
            ...
        }
    ]
}
```

Restauración a un tiempo especificado desde una copia de seguridad replicada

Puede restaurar una instancia de base de datos a un punto específico en el tiempo desde una copia de seguridad replicada mediante la consola de Amazon RDS. También puede utilizar el comando `restore-db-instance-to-point-in-time` de la interfaz de línea de comandos (AWS CLI) o la operación `RestoreDBInstanceToPointInTime` de la API de RDS.

Para obtener información general sobre la recuperación en un momento dado (PITR), consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

> **Note**
>
> En RDS para SQL Server, los grupos de opciones no se copian en las regiones de Regiones de AWS cuando se reproducen las copias de seguridad automatizadas. Si ha asociado un grupo de opciones personalizado con la RDS para SQL Server instancia de base de datos, puede volver a crear ese grupo de opciones en la región de destino. A continuación, restaure la instancia de base de datos en la región de destino y asocie el grupo de opciones personalizadas con ella. Para obtener más información, consulte Trabajo con grupos de opciones.

Consola

Para restaurar una instancia de base de datos a un tiempo especificado desde una copia de seguridad replicada

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione la región de destino (en la que se replican las copias de seguridad) en el selector de región.
3. En el panel de navegación, seleccione Automated backups (Copias de seguridad automatizadas).
4. En la pestaña Replicated backups (Copias de seguridad replicadas), elija la instancia de base de datos que desea restaurar.
5. Para Actions (Acciones), seleccione Restore to point in time (Restaurar a un momento dado).
6. Elija Latest restorable time (Última hora de restauración) para restaurar a la última hora posible o elija Custom (Personalizar) para elegir una hora.

   Si elige Custom (Personalizar), escriba la fecha y hora en la que quiere restaurar la instancia.

> **Note**
>
> Las horas se muestran en su zona horaria local, que se indica mediante una diferencia de la hora universal coordinada (UTC). Por ejemplo, UTC-5 es la hora estándar del Este/horario de verano central.

7. En Identificador de instancias de bases de datos, escriba el nombre la instancia de bases de datos restaurada de destino.
8. (Opcional) Elija otras opciones según sea necesario, como habilitar el escalado automático.
9. Elija Restore to point in time (Restaurar a un momento dado).

AWS CLI

Utilice el comando `restore-db-instance-to-point-in-time` de la AWS CLI para crear una nueva instancia de base de datos.

Para restaurar una instancia de base de datos a un tiempo especificado desde una copia de seguridad replicada

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-automated-backups-arn "arn:aws:rds:us-
east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE" \
    --target-db-instance-identifier mytargetdbinstance \
    --restore-time 2020-10-14T23:45:00.000Z
```

  En:Windows

```
aws rds restore-db-instance-to-point-in-time ^
    --source-db-instance-automated-backups-arn "arn:aws:rds:us-
east-1:123456789012:auto-backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE" ^
    --target-db-instance-identifier mytargetdbinstance ^
    --restore-time 2020-10-14T23:45:00.000Z
```

API de RDS

Para restaurar una instancia de base de datos a un momento especificado, llame a la operación `RestoreDBInstanceToPointInTime` de la API de Amazon RDS con los siguientes parámetros:

- `SourceDBInstanceAutomatedBackupsArn`
- `TargetDBInstanceIdentifier`
- `RestoreTime`

Detención de la replicación de la copia de seguridad automatizada

Puede detener la replicación de la copia de seguridad para las instancias de base de datos mediante la consola de Amazon RDS. También puede utilizar el comando `stop-db-instance-automated-backups-replication` de la interfaz de línea de comandos (AWS CLI) o la operación `StopDBInstanceAutomatedBackupsReplication` de la API de RDS.

Las copias de seguridad replicadas se conservan, sujetas al periodo de retención de copias de seguridad establecido cuando se crearon.

Consola

Detenga la replicación de la copia de seguridad desde la página Automated backups (Copias de seguridad automatizadas) en la región de origen.

Para detener la replicación de la copia de seguridad en una Región de AWS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione la región de origen en el Region selector (Selector de regiones).
3. En el panel de navegación, seleccione Automated backups (Copias de seguridad automatizadas).
4. En la pestaña Current Region (Región actual), elija la instancia de base de datos para la que desea detener la replicación de la copia de seguridad.
5. En Actions (Acciones), seleccione Manage cross-Region replication (Administrar replicación entre regiones).
6. En Backup replication (Replicación de la copia de seguridad), desactive la casilla Enable replication to another Región de AWS (Habilitar replicación en otra región) (.

7. Seleccione Save (Guardar).

Las copias de seguridad replicadas se muestran en la pestaña Retained (Conservados) de la página Automated backups (Copias de seguridad automatizadas) en la región de destino.

AWS CLI

Detenga la replicación de la copia de seguridad mediante el comando `stop-db-instance-automated-backups-replication` de la AWS CLI.

En el siguiente ejemplo de la CLI se detiene la replicación de las copias de seguridad automatizadas de una instancia de base de datos en la región EE.UU. Oeste (Oregón).

Para detener la replicación de la copia de seguridad

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

```
aws rds stop-db-instance-automated-backups-replication \
--region us-east-1 \
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase"
```

  En:Windows

```
aws rds stop-db-instance-automated-backups-replication ^
--region us-east-1 ^
--source-db-instance-arn "arn:aws:rds:us-west-2:123456789012:db:mydatabase"
```

API de RDS

Detenga la replicación de la copia de seguridad mediante la operación `StopDBInstanceAutomatedBackupsReplication` de la API de RDS con los siguientes parámetros:

- `Region`
- `SourceDBInstanceArn`

Eliminación de las copias de seguridad replicadas

Puede eliminar las copias de seguridad replicadas para las instancias de base de datos mediante la consola de Amazon RDS. También puede utilizar el comando `delete-db-instance-automated-backups` de la interfaz de línea de comandos (AWS CLI) o la operación `DeleteDBInstanceAutomatedBackup` de la API de RDS.

Consola

Elimine las copias de seguridad replicadas en la región de destino de la página Automated backups (Copias de seguridad automatizadas).

Para eliminar las copias de seguridad replicadas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione la región de destino en el Region selector (Selector de regiones).
3. En el panel de navegación, seleccione Automated backups (Copias de seguridad automatizadas).
4. En la pestaña Replicated backups (Copias de seguridad replicadas), elija la instancia de base de datos para la que desea eliminar las copias de seguridad replicadas.
5. En Actions (Acciones), elija Delete (Eliminar).
6. En la página de confirmación, introduzca **`delete me`** y elija Delete (Eliminar).

AWS CLI

Elimine las copias de seguridad replicadas mediante el comando `delete-db-instance-automated-backup` de la AWS CLI.

Puede utilizar el comando `describe-db-instances` de la CLI para buscar los nombres de recursos de Amazon (ARN) de las copias de seguridad replicadas. Para obtener más información, consulte Búsqueda de información sobre las copias de seguridad replicadas.

Para eliminar las copias de seguridad replicadas

- Ejecute uno de los siguientes comandos.

  Para Linux, macOS o:Unix

```
aws rds delete-db-instance-automated-backup \
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-
backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE"
```

En:Windows

```
aws rds delete-db-instance-automated-backup ^
--db-instance-automated-backups-arn "arn:aws:rds:us-east-1:123456789012:auto-
backup:ab-L2IJCEXJP7XQ7HOJ4SIEXAMPLE"
```

API de RDS

Elimine las copias de seguridad replicadas mediante la operación `DeleteDBInstanceAutomatedBackup` de la API de RDS con el parámetro `DBInstanceAutomatedBackupsArn`.

Administración de copias de seguridad manuales

En esta sección, se muestra cómo administrar copias de seguridad manuales de instancias de base de datos y clústeres de base de datos.

Para obtener información sobre cómo crear una instantánea de base de datos para una instancia de base de datos de Single-AZ, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Para obtener información sobre cómo crear una instantánea de base de datos para un clúster de base de datos multi-AZ, consulte Creación de una instantánea de clúster de base de datos multi-AZ.

Para obtener información sobre la eliminación de una instantánea de base de datos, consulte Eliminación de una instantánea de base de datos para Amazon RDS.

Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS

Amazon RDS crea una instantánea del volumen de almacenamiento de la instancia de base de datos; para ello, hace una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. La creación de esta instantánea de base de datos en una instancia de base de datos Single-AZ provoca una breve suspensión de E/S que puede durar desde unos segundos hasta unos minutos, dependiendo del tamaño y la clase de la instancia de base de datos. Para MariaDB, MySQL, Oracle y PostgreSQL, la actividad de E/S no se suspende en la instancia principal durante el backup para los despliegues Multi-AZ, ya que el backup se realiza desde la instancia en espera. En SQL Server, la actividad de E/S se suspende brevemente durante la copia de seguridad para las implementaciones Multi-AZ.

Cuando se crea una instantánea de base de datos, se debe identificar la instancia de base de datos cuya copia de seguridad se va a realizar y, a continuación, se debe asignar un nombre a la instantánea de base de datos para poder restaurarla posteriormente. El tiempo que tarda en crearse una instantánea varía en función del tamaño de sus bases de datos. Dado que la instantánea incluye todo el volumen de almacenamiento, el tamaño de los archivos (por ejemplo, archivos temporales) también afecta a la cantidad de tiempo que tarda en crearse la instantánea.

> **Note**
>
> Su instancia de base de datos debe tener el estado `available` para poder realizar una instantánea de la base de datos.
>
> Para las instancias de base de datos de PostgreSQL, es posible que los datos de las tablas sin registrar no se restauren a partir de instantáneas. Para obtener más información, consulte Prácticas recomendadas para trabajar con PostgreSQL.

A diferencia de las copias de seguridad automatizadas, las instantáneas manuales no están sujetas al periodo de retención de copia de seguridad. Las instantáneas no caducan.

Para copias de seguridad a largo plazo de datos de MariaDB, MySQL y PostgreSQL, se recomienda que exporte datos de instantáneas a Amazon S3. Si la versión principal de su motor de base de datos ya no es compatible, no puede restaurar a esa versión desde una instantánea. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS.

Puede crear una instantánea de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para crear una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).

   Aparece la lista Instantáneas manuales.
3. Elija Take Snapshot (Realizar una instantánea).

   Aparece la ventana Take DB Snapshot (Realizar una instantánea de base de datos).
4. Seleccione la instancia de base de datos para la que desea tomar una instantánea.
5. Introduzca el nombre de la instantánea.
6. Elija Take Snapshot (Realizar una instantánea).

Aparecerá la página Instantáneas manuales, con el estado de la nueva instantánea de base de datos mostrada como `Creating`. Después de que su estado es `Available`, puede ver su tiempo de creación.

AWS CLI

Cuando se crea una instantánea de base de datos con la AWS CLI, se debe identificar la instancia de base de datos cuya copia de seguridad se va a realizar y, a continuación, se debe asignar un nombre a la instantánea de base de datos para poder restaurarla posteriormente. Puede hacerlo utilizando el comando AWS CLI de la `create-db-snapshot` con los siguientes parámetros:

- `--db-instance-identifier`
- `--db-snapshot-identifier`

En este ejemplo, se crea una instantánea de base de datos denominada *`mydbsnapshot`* para una instancia de base de datos denominada *`mydbinstance`*.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-snapshot \
    --db-instance-identifier mydbinstance \
    --db-snapshot-identifier mydbsnapshot
```

En:Windows

```
aws rds create-db-snapshot ^
    --db-instance-identifier mydbinstance ^
    --db-snapshot-identifier mydbsnapshot
```

API de RDS

Cuando se crea una instantánea de base de datos con la API de Amazon RDS, se debe identificar la instancia de base de datos cuya copia de seguridad se va a realizar y, después, se debe asignar un nombre a la instantánea de base de datos para poder restaurarla en el futuro. Para ello, use el comando `CreateDBSnapshot` de la API de Amazon RDS con los siguientes parámetros:

- `DBInstanceIdentifier`
- `DBSnapshotIdentifier`

Creación de una instantánea de clúster de base de datos multi-AZ

Cuando se crea una instantánea de un clúster de base de datos Multi-AZ, se tiene que asegurar de identificar el clúster de base de datos cuya copia de seguridad se va a realizar y, a continuación, se debe asignar un nombre a la instantánea del clúster de base de datos para poder restaurarla posteriormente. También puede compartir una instantánea de clúster de base de datos Multi-AZ. Para obtener instrucciones, consulte the section called “Compartir una instantánea de base de datos”.

Puede crear una instantánea de clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS.

Para copias de seguridad a largo plazo, se recomienda exportar datos de instantáneas a Amazon S3. Si la versión principal de su motor de base de datos ya no es compatible, no puede restaurar a esa versión desde una instantánea. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS.

Consola

Para crear una instantánea de clúster de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. En la lista, elija el clúster de base de datos Multi-AZ al que quiere tomar una instantánea.
4. En Actions (Acciones), elija Take snapshot (Realizar instantánea).

   Aparece la ventana Take DB Snapshot (Realizar una instantánea de base de datos).
5. En Snapshot name (Nombre de la instantánea), ingrese el nombre de la instantánea.
6. Elija Take Snapshot (Realizar una instantánea).

Aparece la página Snapshots (Instantáneas) y `Creating` se muestra como el estado de la nueva instantánea del clúster de base de datos Multi-AZ. Después de que su estado es `Available`, puede ver su tiempo de creación.

AWS CLI

Puede crear una instantánea de clúster de base de datos Multi-AZ mediante el comando de la AWS CLI create-db-cluster-snapshot con las siguientes opciones:

- `--db-cluster-identifier`
- `--db-cluster-snapshot-identifier`

En este ejemplo, se crea una instantánea de clúster de base de datos Multi-AZ denominada *`mymultiazdbclustersnapshot`* para un clúster de base de datos denominado *`mymultiazdbcluster`*.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-cluster-snapshot \
    --db-cluster-identifier mymultiazdbcluster \
    --db-cluster-snapshot-identifier mymultiazdbclustersnapshot
```

En:Windows

```
aws rds create-db-cluster-snapshot ^
    --db-cluster-identifier mymultiazdbcluster ^
    --db-cluster snapshot-identifier mymultiazdbclustersnapshot
```

API de RDS

Puede crear una instantánea de clúster de base de datos Multi-AZ mediante la operación de la API de Amazon RDS create-db-cluster-snapshot con las siguientes opciones:

- `DBClusterIdentifier`
- `DBClusterSnapshotIdentifier`

Eliminación de una instantánea de clúster de base de datos Multi-AZ

Puede eliminar las instantáneas de base de datos Multi-AZ administradas por Amazon RDS cuando ya no las necesite. Para obtener instrucciones, consulte the section called “Eliminación de una instantánea de base de datos”.

Eliminación de una instantánea de base de datos para Amazon RDS

Puede eliminar las instantáneas de base de datos administradas por Amazon RDS cuando ya no las necesite.

> **Note**
>
> Para eliminar copias de seguridad administradas por AWS Backup, utilice la consola de AWS Backup. Para obtener más información sobre AWS Backup, consulte la Guía para desarrolladores de AWS Backup.

Eliminación de una instantánea de base de datos

Puede eliminar una instantánea de base de datos manual, compartida o pública con la AWS Management Console, la AWS CLI o la API de RDS.

Para eliminar una instantánea compartida o pública, debe iniciar sesión en la cuenta de AWS propietaria de la instantánea.

Si dispone de instantáneas de base de datos automatizadas que desea eliminar sin quitar la instancia de base de datos, cambie el periodo de retención de copia de seguridad para la instancia de copia de seguridad a 0. Las instantáneas automatizadas se eliminan cuando se aplica el cambio. Puede aplicar el cambio de inmediato si no desea esperar hasta el siguiente periodo de mantenimiento. Una vez que se complete el cambio, puede volver a habilitar las copias de seguridad automáticas estableciendo el periodo de retención de copia de seguridad a un número superior a 0. Para obtener más información acerca de la modificación de una instancia de base de datos , consulte Modificación de una instancia de base de datos de Amazon RDS.

Las copias de seguridad automatizadas y las instantáneas manuales retenidas incurrirán en cargos de facturación hasta que se eliminen. Para obtener más información, consulte Costos de retención.

Si ha eliminado una instancia de base de datos, puede eliminar sus instantáneas de base de datos automatizadas quitando las copias de seguridad automatizadas para la instancia de base de datos. Para obtener información acerca de los backups automatizados, consulte Introducción a las copias de seguridad.

Consola

Para eliminar una instantánea de base de datos, realice el siguiente procedimiento:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).

   Aparece la lista Instantáneas manuales.
3. Elija la instantánea de base de datos que desee eliminar.
4. En Actions (Acciones), elija Delete Snapshot (Eliminar instantánea).
5. En la página de confirmación, elija Delete (Eliminar).

AWS CLI

Puede eliminar una instantánea de base de datos usando el comando delete-db-snapshot de la AWS CLI.

Las siguientes opciones se usan para eliminar una instantánea de base de datos.

- `--db-snapshot-identifier`: identificador de la instantánea de base de datos.

Example

El código siguiente elimina la instantánea de base de datos `mydbsnapshot`.

Para Linux, macOS o:Unix

```
aws rds delete-db-snapshot \
    --db-snapshot-identifier mydbsnapshot
```

En:Windows

```
aws rds delete-db-snapshot ^
    --db-snapshot-identifier mydbsnapshot
```

API de RDS

Puede eliminar una instantánea de base de datos mediante la operación de la API de Amazon RDS DeleteDBSnapshot.

Los siguientes parámetros se usan para eliminar una instantánea de base de datos.

- `DBSnapshotIdentifier`: identificador de la instantánea de base de datos.

Restauración a una instancia de base de datos

En esta sección se muestra cómo restaurar a una instancia de base de datos. En esta página se muestra cómo restaurar a una instancia de base de datos de Amazon RDS a partir de una instantánea de base de datos.

Amazon RDS crea una instantánea del volumen de almacenamiento de la instancia de base de datos; para ello, hace una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. Para crear una nueva instancia de base de datos, puede restaurar a partir de una instantánea de base de datos. Se proporciona el nombre de la instantánea de la base de datos que se va a restaurar y, a continuación, se proporciona un nombre para la nueva instancia de la base de datos que se crea a partir de la restauración. No puede restaurar desde una instantánea de base de datos en una instancia de base de datos ya existente; al restaurar se crea una nueva instancia de base de datos.

Puede usar la instancia de base de datos restaurados tan pronto como su estado sea `available`. La instancia de base de datos continúa cargando datos en segundo plano. Esto se conoce como carga diferida.

Si accede a datos que aún no se han cargado, la instancia de base de datos descarga inmediatamente los datos solicitados de Amazon S3 y, luego, continúa cargando el resto de los datos en segundo plano. Para obtener más información, consulte Instantáneas de Amazon EBS.

Para ayudar a mitigar los efectos de la carga diferida en tablas a las que requiere acceso rápido, puede realizar operaciones que implican análisis de tablas completas, como `SELECT *`. Esto permite a Amazon RDS descargar todos los datos de la tabla respaldados desde S3.

Puede restaurar una instancia de base de datos empleando un tipo de almacenamiento distinto del de la instantánea de origen. En este caso, el proceso de restauración será más lento a causa del trabajo adicional requerido para migrar los datos al nuevo tipo de almacenamiento. En caso de restaurar desde o hasta un almacenamiento magnético, el proceso de migración será el más lento. Esto se debe a que el almacenamiento magnético no tiene la capacidad IOPS de los almacenamientos con IOPS aprovisionadas o de uso general (SSD).

Puede usar AWS CloudFormation para restaurar una instancia de base de datos desde una instantánea de instancia de base de datos. Para obtener más información, consulte AWS::RDS::DBInstance en la AWS CloudFormationGuía del usuario.

> **Note**
>
> No puede restaurar una instancia de base de datos desde una instantánea de base de datos que esté compartida y cifrada. En lugar de ello, puede hacer una copia de la instantánea de base de datos y restaurar la instancia de base de datos desde la copia. Para obtener más información, consulte Copia de una instantánea de base de datos para Amazon RDS.

Para obtener información sobre la restauración de una instancia de base de datos con una versión del Soporte extendido de RDS, consulte Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS.

Restauración a partir de una instantánea

Puede restaurar una instancia de base de datos desde una instantánea de clúster de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> No puede reducir la cantidad de almacenamiento al restaurar una instancia de base de datos. Cuando aumente el almacenamiento asignado, este aumento debe ser de al menos el 10 por ciento. Si intenta aumentar el valor en menos del 10 por ciento, obtendrá un error. No puede aumentar el almacenamiento asignado al restaurar instancias de base de datos de RDS para SQL Server.

Consola

Para restaurar una instancia de base de datos a partir de una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de base de datos desde la que desea restaurar.
4. En Actions (Acciones), elija Restore snapshot (Restaurar instantánea).
5. En la página Restore snapshot (Restaurar instantánea), en DB Instance Identifier (Identificador de instancias de bases de datos), escriba el nombre de la instancia de base de datos restaurada.

6. Especifique otras opciones, como el tamaño de almacenamiento asignado.

   Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

7. Elija Restore DB Instance (Restaurar instancia de base de datos).

AWS CLI

Para restaurar una instancia de base de datos desde una instantánea, use el comando restore-db-instance-from-db-snapshot de la AWS CLI.

En este ejemplo, se restaura a partir de una instantánea de base de datos creada previamente con el nombre `mydbsnapshot`. Restaura a una instancia de base de datos nueva con el nombre `mynewdbinstance`. En este ejemplo también se establece el tamaño de almacenamiento asignado.

Puede especificar otras opciones. Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

Example

Para Linux, macOS o Unix:

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier mynewdbinstance \
    --db-snapshot-identifier mydbsnapshot \
    --allocated-storage 100
```

Para Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier mynewdbinstance ^
    --db-snapshot-identifier mydbsnapshot ^
    --allocated-storage 100
```

Este comando devuelve un resultado similar al siguiente:

```
DBINSTANCE  mynewdbinstance  db.t3.small  MySQL     50       sa              creating
 3  n  8.0.28  general-public-license
```

API de RDS

Para restaurar una instancia de base de datos desde una instantánea de base de datos, use la función RestoreDBInstanceFromDBSnapshot de la API de Amazon RDS con los parámetros siguientes:

- `DBInstanceIdentifier`
- `DBSnapshotIdentifier`

Consideraciones

Para ver los aspectos a tener en cuenta al restaurar a una instancia de base de datos a partir de una instantánea de base de datos, consulte los temas siguientes.

Temas

- Consideraciones relativas al grupo de parámetros
- Consideraciones relativas al grupo de seguridad
- Consideraciones relativas al grupo de opciones
- Consideraciones de etiquetado de recursos
- Consideraciones sobre Db2
- Consideraciones sobre Microsoft SQL Server
- Aspectos a tener en cuenta de MySQL
- Consideraciones sobre Oracle Database

Consideraciones relativas al grupo de parámetros

Recomendamos retener el grupo de parámetros de base de datos de todas las instantáneas de base de datos que cree para así poder asociar el grupo de parámetros correcto a la instancia de base de datos restaurada.

El grupo de parámetros de base de datos predeterminado se asocia a la instancia restaurada, a menos que elija uno distinto. No hay ninguna configuración de parámetros personalizada disponible en el grupo de parámetros predeterminado.

Puede especificar el grupo de parámetros al restaurar la instancia de base de datos.

Para obtener más información acerca de los grupos de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.

Consideraciones relativas al grupo de seguridad

Al restaurar una instancia de base de datos, la nube privada virtual (VPC) predeterminada, el grupo de subredes de base de datos y el grupo de seguridad de la VPC se asocian a la instancia restaurada, a menos que elija otras distintas.

- Si utiliza la consola de Amazon RDS, puede especificar un grupo de seguridad de VPC personalizado para asociarlo con la instancia o crear un nuevo grupo de seguridad de la VPC.
- Si utiliza la AWS CLI, puede especificar un grupo de seguridad de VPC personalizado para asociarlo con la instancia. Para ello, incluya la opción `--vpc-security-group-ids` en el comando `restore-db-instance-from-db-snapshot`.
- Si está utilizando la API de Amazon RDS, puede incluir el parámetro `VpcSecurityGroupIds.VpcSecurityGroupId.N` en la acción `RestoreDBInstanceFromDBSnapshot`.

En cuanto finalice la restauración y su nueva instancia de base de datos esté disponible, también puede cambiar la configuración de la VPC mediante la modificación de la instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Consideraciones relativas al grupo de opciones

Al restaurar una instancia de base de datos, el grupo de opciones de base de datos predeterminado se asocia a la instancia de base de datos restaurada en la mayoría de los casos.

Hay una excepción cuando la instancia de base de datos de origen está asociada a un grupo de opciones que contiene una opción persistente o permanente. Por ejemplo, si la instancia de base de datos de origen utiliza el cifrado de datos transparente (TDE) de Oracle, la instancia de base de datos restaurada debe utilizar un grupo de opciones que tenga la opción TDE.

Si restaura una instancia de base de datos en una VPC diferente, debe llevar a cabo uno de los siguientes procedimientos para asignar un grupo de opciones de base de datos:

- Asigne el grupo de opciones predeterminado de ese grupo de VPC a la instancia.
- Asigne otro grupo de opciones que esté vinculado a esa VPC.

- Crear un nuevo grupo de opciones y asignarlo a la instancia de base de datos. Con las opciones persistentes o permanentes, como TDE de Oracle, debe crear un grupo de opciones nuevo que incluya la opción persistente o permanente.

Para obtener más información acerca de los grupos de opciones de base de datos, consulte Trabajo con grupos de opciones.

Consideraciones de etiquetado de recursos

Al restaurar una instancia de base de datos desde una instantánea de base de datos, RDS comprueba si se especifican nuevas etiquetas. En caso afirmativo, las nuevas etiquetas se agregan a la instancia de base de datos restaurada. Si no hay etiquetas nuevas, RDS agrega las etiquetas de la instancia de base de datos de origen al crear la instantánea de la instancia de base de datos restaurada.

Para obtener más información, consulte Copia de etiquetas a instantáneas de base de datos.

Consideraciones sobre Db2

Con el modelo BYOL, las instancias de base de datos de Amazon RDS para Db2 deben estar asociadas a un grupo de parámetros personalizado que contenga su IBM Site ID y su IBM Customer ID. De lo contrario, los intentos de restaurar una instancia de base de datos a partir de una instantánea fallarán. Las instancias de base de datos de Amazon RDS para Db2 también deben estar asociadas a una licencia autoadministrada de AWS License Manager. Para obtener más información, consulte Traiga su propia licencia para Db2.

Con la licencia Db2 a través del modelo AWS Marketplace, necesita una suscripción de AWS Marketplace activa para la edición de IBM Db2 concreta que quiera usar. Si aún no tiene una, suscríbase a Db2 en AWS Marketplace para esa edición de IBM Db2. Para obtener más información, consulte Licencia de Db2 a través de AWS Marketplace.

Consideraciones sobre Microsoft SQL Server

Cuando se restaura una RDS para una instantánea de base de datos de Microsoft SQL Server a una nueva instancia, siempre es posible restaurar con la misma edición de la instantánea. En algunos casos también es posible cambiar la edición de la instancia de base de datos. Estas son las limitaciones que aplican para cambiar de edición:

- La instantánea de base de datos debe tener asignado suficiente almacenamiento para la nueva edición.
- Solo se admiten los cambios de edición siguientes:
  - De Standard Edition a Enterprise Edition
  - De Web Edition a Standard Edition o Enterprise Edition
  - De Express Edition a Web Edition, Standard Edition o Enterprise Edition

Si desea cambiar de una edición a otra nueva y no es posible hacerlo restaurando una instantánea, puede intentar usar la característica de copia de seguridad y restauración nativa. SQL Server comprueba si la base de datos es compatible con la nueva edición partiendo de las características de SQL Server que hay habilitadas en ella. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Aspectos a tener en cuenta de MySQL

Para restaurar a partir de una instantánea de base de datos de RDS para MySQL con una versión de motor no compatible, es posible que tenga que actualizar la instantánea de base de datos más de una vez. Para obtener más información sobre las opciones de actualización, consulte Opciones de actualización para instantáneas de bases de datos con versiones de motor no compatibles con RDS para MySQL.

Para obtener más información sobre la actualización de la versión del motor de una instantánea de base de datos de RDS para MySQL, Actualización de una versión del motor de instantáneas de base de datos de MySQL.

Consideraciones sobre Oracle Database

Al restaurar una base de datos Oracle a partir de una instantánea de base de datos, tenga en cuenta lo siguiente:

- Antes de restaurar una instantánea de base de datos, puede actualizarla a una versión de base de datos de Oracle posterior. Para obtener más información, consulte Actualización de una instantánea de base de datos de Oracle.
- Si restaura una instantánea de una instancia de CDB que utiliza la configuración de un solo inquilino, puede cambiar el nombre de la PDB. No puede cambiar los nombres de la PDB cuando la instancia de CDB utiliza la configuración de varios inquilinos. Para obtener más información, consulte Copia de seguridad y restauración de una CDB.

- No puede cambiar el nombre del CDB, que siempre es `RDSCDB`. Este nombre de CDB es igual para todas las instancias de CDB.
- No puede interactuar directamente con las bases de datos de inquilinos en una instantánea de base de datos. Si restaura una instantánea de una instancia de CDB que utiliza la configuración de varios inquilinos, restaurará todas sus bases de datos de inquilinos. Puede usar describe-db-snapshot-tenant-databases para inspeccionar las bases de datos de inquilinos en una instantánea de base de datos antes de restaurarla.
- Si utiliza Oracle GoldenGate, conserve siempre el grupo de parámetros con el parámetro `compatible`. Cuando restaure una instancia de base de datos desde una instantánea de base de datos, especifique el grupo de parámetros con un valor `compatible` igual o superior.
- Puede optar por cambiar el nombre de la base de datos al restaurar una instantánea de base de datos. Si el tamaño total del registro REDO en línea es superior a 20 GB, RDS podría restablecer el tamaño del registros REDO en línea a su configuración predeterminada de 512 MB (4 x 128 MB). El tamaño más pequeño permite que la operación de restauración se complete en un tiempo razonable. Puede volver a crear los registros REDO en línea más adelante y cambiar el tamaño.
- Puede administrar la contraseña de usuario principal en AWS Secrets Manager. Para obtener más información, consulte Descripción general de la administración de contraseñas de usuarios maestros con AWS Secrets Manager.

Restauración de una instancia de base de datos a un momento especificado para Amazon RDS

Puede restaurar una instancia de base de datos a un momento específico creando una nueva instancia de base de datos sin modificar la instancia de base de datos de origen.

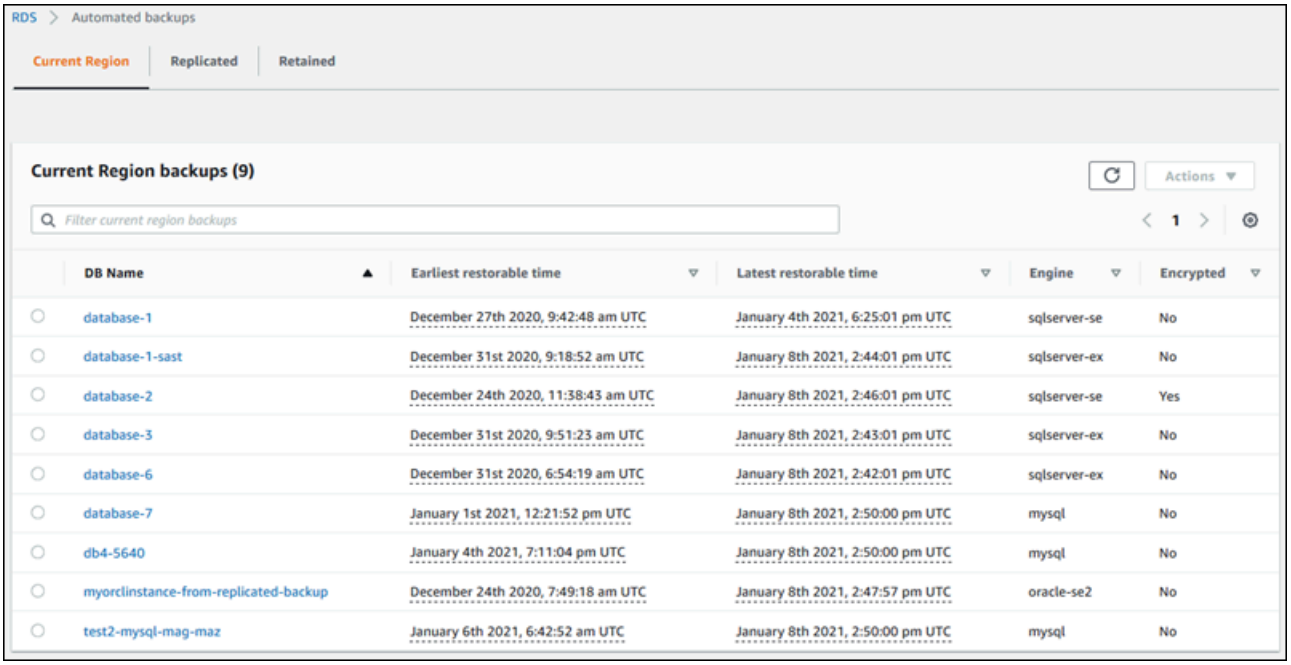
Cuando se restaura una instancia de base de datos a un momento específico en el tiempo, puede elegir el grupo de seguridad de nube virtual privada (VPC) predeterminado. O bien, puede aplicar un grupo de seguridad de VPC personalizado a la instancia de base de datos.

Las instancias de base de datos restauradas se asocian automáticamente con los grupos de opciones y parámetros de base de datos predeterminados. Sin embargo, puede aplicar un grupo de parámetros y opciones personalizados especificándolos durante una restauración.

Si la instancia de base de datos de origen tiene etiquetas de recursos, RDS agrega las etiquetas más recientes a la instancia de base de datos restaurada.

RDS carga los registros de transacciones para las instancias de base de datos en Simple Storage Service (Amazon S3) cada cinco minutos. Para ver el último momento que se puede restaurar para una instancia de base de datos, use el comando describe-db-instances de la AWS CLI y compruebe el valor que se devuelve en el campo `LatestRestorableTime` para la instancia de base de datos. Para consultar la hora restaurable más reciente para cada instancia de base de datos en la consola de Amazon RDS, elija Copias de seguridad automatizadas.

Puede restaurar a cualquier punto en el tiempo dentro del periodo de retención de copia de seguridad. Para consultar la hora restaurable más reciente para cada instancia de base de datos, elija Copias de seguridad automatizadas en la consola de Amazon RDS.



> **Note**
>
> Se recomienda restaurar el mismo tamaño de instancia de base de datos o similar, y IOPS si utiliza almacenamiento de IOPS provisionadas, como instancia de base de datos de origen. Podría aparecer un error si, por ejemplo, elige un tamaño de instancia de base de datos con un valor de IOPS incompatible.

Para obtener información sobre la restauración de una instancia de base de datos con una versión del Soporte extendido de RDS, consulte Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS.

Respecto de algunos de los motores de base de datos de Amazon RDS, hay que tener en cuenta algunas cuestiones especiales si la restauración se ejecuta desde un momento determinado:

- Si utiliza la autenticación por contraseña con una instancia de base de datos de Amazon RDS para Db2, las acciones de administración de usuarios, incluida `rdsadmin.add_user`, no se capturarán en los registros. Estas acciones requieren una copia de seguridad completa de la instantánea.

  Con el modelo BYOL, las instancias de base de datos de RDS para Db2 deben estar asociadas a un grupo de parámetros personalizado que contenga su IBM Site ID y su IBM Customer ID. De lo contrario, los intentos de restaurar una instancia de base de datos a un momento dado fallarán. Las instancias de base de datos de Amazon RDS para Db2 también deben estar asociadas a

una licencia autoadministrada de AWS License Manager. Para obtener más información, consulte Traiga su propia licencia para Db2.

Con la licencia Db2 a través del modelo AWS Marketplace, necesita una suscripción de AWS Marketplace activa para la edición de IBM Db2 concreta que quiera usar. Si aún no tiene una, suscríbase a Db2 en AWS Marketplace para esa edición de IBM Db2. Para obtener más información, consulte Licencia de Db2 a través de AWS Marketplace.

- Cuando se restaura una instancia de base de datos de RDS para Oracle en un momento dado, se puede especificar un motor de base de datos, un modelo de licencia y un DBName (SID) diferentes para la instancia de base de datos restaurada. También puede especificar que RDS debe almacenar y administrar las contraseñas de usuario principal en AWS Secrets Manager. Para obtener más información, consulte Descripción general de la administración de contraseñas de usuarios maestros con AWS Secrets Manager.
- Cuando se restaura una instancia de base de datos de Microsoft SQL Server a un momento dado, cada base de datos de esa instancia se restaura a un momento dado situado a un máximo de un segundo de cada una de las bases de datos que componen la instancia. Las transacciones que afectan a varias bases de datos de la instancia podrían restaurarse de un modo incoherente.
- Los modos `OFFLINE`, `EMERGENCY` y `SINGLE_USER` no son compatibles con una instancia de base de datos de SQL Server. Si una base de datos se configura en uno de estos modos, el último momento restaurable dejará de avanzar para toda la instancia.
- Algunas acciones, como cambiar el modelo de recuperación de una base de datos de SQL Server, pueden interrumpir la secuencia de registros que se usan para la recuperación a un momento dado. En algunos casos, Amazon RDS puede detectar este problema, y se impide que el último tiempo restaurable avance; en otros casos (por ejemplo, si una base de datos de SQL Server usa el modelo de recuperación `BULK_LOGGED`), no se detecta la interrupción en la secuencia de registros. Puede que no sea posible restaurar una instancia de base de datos de SQL Server a un momento dado si hay una interrupción en la secuencia de registros. Por estos motivos, Amazon RDS no permite cambiar el modelo de recuperación de las bases de datos de SQL Server.

También puede utilizar AWS Backup para administrar copias de seguridad de las instancias de base de datos de Amazon RDS. Si su instancia de base de datos está asociada a un plan de copia de seguridad en AWS Backup, ese plan se utiliza para la recuperación puntual. Las copias de seguridad que se crearon con AWS Backup tienen nombres que terminan en `awsbackup:`*`AWS-Backup-job-number`*. Para obtener más información sobre AWS Backup, consulte la Guía para desarrolladores de AWS Backup.

> **Note**
>
> La información de este tema se aplica a Amazon RDS. Para obtener más información sobre cómo restaurar un clúster de base de datos de Amazon Aurora, consulte Restoring a DB cluster to a specified time (Restauración de un clúster de base de datos a un momento específico).

Puede restaurar una instancia de base de datos a un momento dado con la AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> No puede reducir la cantidad de almacenamiento al restaurar una instancia de base de datos. Cuando aumente el almacenamiento asignado, este aumento debe ser de al menos el 10 por ciento. Si intenta aumentar el valor en menos del 10 por ciento, obtendrá un error. No puede aumentar el almacenamiento asignado al restaurar instancias de base de datos de RDS para SQL Server.

Consola

Para restaurar una instancia de base de datos a un momento específico

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Automated backups (Copias de seguridad automatizadas).

   Las copias de seguridad automatizadas se muestran en la pestaña Current Region (Región actual).
3. Elija la instancia de base de datos que quiere restaurar.
4. Para Actions (Acciones), elija Restore to point in time (Restaurar a un momento dado).

   Aparecerá la ventana Restore to point in time (Restaurar a un momento dado).
5. Elija Latest restorable time (Última hora de restauración) para restaurar a la última hora posible o elija Custom (Personalizar) para elegir una hora.

   Si elige Personalizar, ingrese la fecha y la hora a la que desea restaurar la instancia.

> **Note**
>
> Las horas se muestran en su zona horaria local, que se indica mediante una diferencia de la hora universal coordinada (UTC). Por ejemplo, UTC-5 es la hora estándar del Este/horario de verano central.

6. En Identificador de instancias de bases de datos, escriba el nombre la instancia de bases de datos restaurada de destino. El nombre debe ser único.
7. Elija otras opciones según sea necesario, como la clase de instancia de base de datos, el almacenamiento y si quiere utilizar el escalado automático de almacenamiento.

   Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.
8. Elija Restore to point in time (Restaurar a un momento dado).

AWS CLI

Para restaurar una instancia de base de datos a un momento específico, utilice el comando de la AWS CLIrestore-db-instance-to-point-in-time para crear una nueva instancia de base de datos. En este ejemplo, también se establece el tamaño de almacenamiento asignado y se habilita el autoescalado de almacenamiento.

Para esta operación se admite el etiquetado de recursos. Al utilizar la opción `--tags`, se ignoran las etiquetas de la instancia de base de datos de origen y se utilizan las proporcionadas. De lo contrario, se utilizan las etiquetas más recientes de la instancia de origen.

Puede especificar otras opciones. Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

Example

Para Linux, macOS o Unix:

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-identifier mysourcedbinstance \
    --target-db-instance-identifier mytargetdbinstance \
    --restore-time 2017-10-14T23:45:00.000Z \
    --allocated-storage 100 \
```

```
    --max-allocated-storage 1000
```

Para Windows:

```
aws rds restore-db-instance-to-point-in-time ^
    --source-db-instance-identifier mysourcedbinstance ^
    --target-db-instance-identifier mytargetdbinstance ^
    --restore-time 2017-10-14T23:45:00.000Z ^
    --allocated-storage 100 ^
    --max-allocated-storage 1000
```

API de RDS

Para restaurar una instancia de base de datos a un momento especificado, llame a la operación `RestoreDBInstanceToPointInTime` de la API de Amazon RDS con los siguientes parámetros:

- `SourceDBInstanceIdentifier`
- `TargetDBInstanceIdentifier`
- `RestoreTime`

Restauración de un clúster de base de datos Multi-AZ a un momento indicado

Para restaurar un clúster de base de datos Multi-AZ a un momento específico, cree un nuevo clúster de base de datos Multi-AZ.

RDS carga de forma continua los registros de transacciones para los clústeres de base de datos Multi-AZ en Amazon S3. Puede restaurar a cualquier punto en el tiempo dentro del periodo de retención de copia de seguridad. Para consultar el momento restaurable más tardío de un clúster de base de datos Multi-AZ, utilice el comando de la AWS CLI describe-db-clusters. Observe el valor devuelto en el campo `EarliestRestorableTime` del clúster de base de datos. Para ver la última hora restaurable para un clúster de base de datos Multi-AZ, observe el valor devuelto en el campo `LatestRestorableTime` para el clúster de base de datos.

Cuando restaura un clúster de base de datos multi-AZ a un momento determinado, puede elegir el grupo de seguridad de VPC predeterminado para su clúster de base de datos multi-AZ, o puede aplicar un grupo de seguridad de VPC personalizado a su clúster de base de datos multi-AZ.

Los clústeres Multi-AZ de base de datos restaurados se asocian automáticamente con el grupo de parámetros del clúster de base de datos predeterminado. Sin embargo, puede aplicar un grupo de parámetros del clúster de base de datos personalizado al especificarlos durante una restauración.

Si el clúster de base de datos de origen tiene etiquetas de recursos, RDS agrega las etiquetas más recientes al clúster de base de datos restaurado.

> **Note**
>
> Se recomienda restaurar al mismo tamaño de clúster de base de datos Multi-AZ o similar, como clúster de base de datos de origen. También recomendamos que realice la restauración con el mismo valor de IOPS o similar si utiliza el almacenamiento de IOPS aprovisionadas. Podría aparecer un error si, por ejemplo, elige un tamaño de clúster de base de datos con un valor de IOPS incompatible.
>
> Si el clúster de base de datos multi-AZ de origen utiliza almacenamiento SSD de uso general (gp3) y tiene menos de 400 GiB de almacenamiento asignado, no puede modificar las IOPS aprovisionadas para el clúster de base de datos restaurado.

Para obtener información sobre la restauración de un clúster de base de datos multi-AZ con una versión del Soporte extendido de RDS, consulte Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS.

Puede restaurar un clúster de base de datos Multi-AZ a un momento dado mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

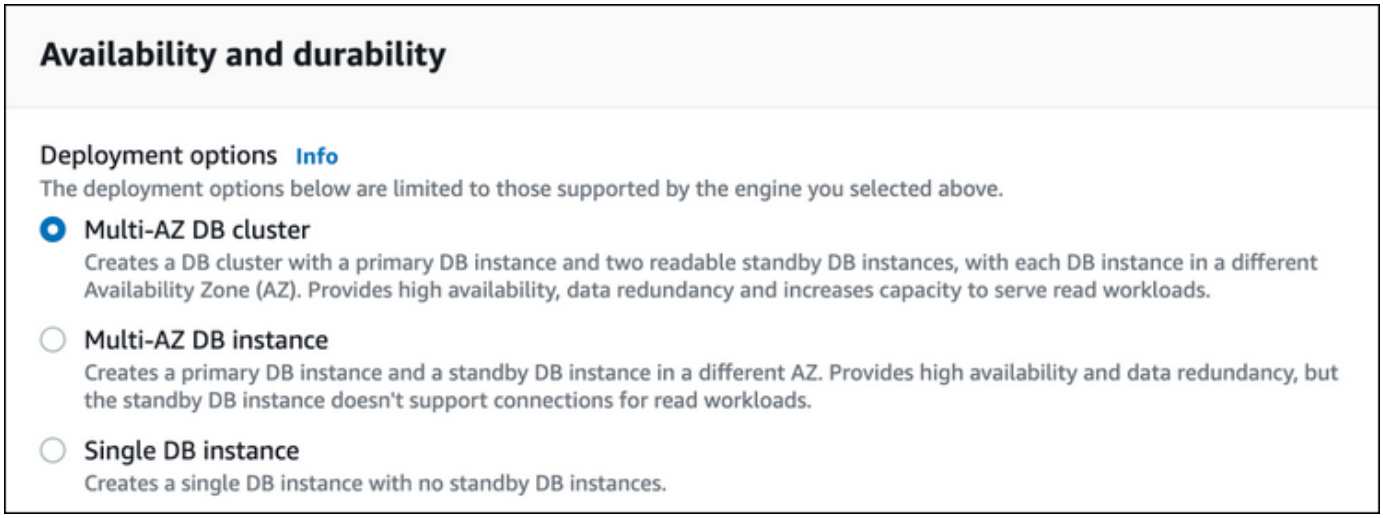
Para restaurar un clúster de base de datos Multi-AZ a un momento indicado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el clúster de base de datos Multi-AZ que quiere restaurar.
4. Para Actions (Acciones), elija Restore to point in time (Restaurar a un momento dado).

   Aparecerá la ventana Restore to point in time (Restaurar a un momento dado).
5. Elija Latest restorable time (Última hora de restauración) para restaurar a la última hora posible o elija Custom (Personalizar) para elegir una hora.

   Si elige Custom (Personalizar), ingrese la fecha y hora a la que quiere restaurar el clúster de base de datos Multi-AZ.

   > **Note**
   >
   > Las horas se muestran en su zona horaria local, que se indica mediante una diferencia de la hora universal coordinada (UTC). Por ejemplo, UTC-5 es la hora estándar del Este/horario de verano central.
6. En DB cluster identifier (Identificador del clúster de base de datos), ingrese el nombre del clúster de base de datos Multi-AZ restaurado.
7. En Availability and durability (Disponibilidad y durabilidad), elija Multi-AZ DB cluster (Clúster de base de datos Multi-AZ).



8. En DB instance class (Clase de instancia de base de datos), elija la clase de instancia de base de datos.

   Actualmente, los clústeres de base de datos Multi-AZ solo admiten clases de instancias de base de datos db.m6gd y db.r6gd. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .
9. En el resto de secciones, especifique los ajustes de configuración del clúster de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.
10. Elija Restore to point in time (Restaurar a un momento dado).

AWS CLI

Para restaurar un clúster de base de datos Multi-AZ a un momento indicado, use el comando de la AWS CLI restore-db-cluster-to-point-in-time para crear un nuevo clúster de base de datos Multi-AZ.

Actualmente, los clústeres de base de datos Multi-AZ solo admiten clases de instancias de base de datos db.m6gd y db.r6gd. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-cluster-to-point-in-time \
    --source-db-cluster-identifier mysourcemultiazdbcluster \
    --db-cluster-identifier mytargetmultiazdbcluster \
```

```
    --restore-to-time 2021-08-14T23:45:00.000Z \
    --db-cluster-instance-class db.r6gd.xlarge
```

En:Windows

```
aws rds restore-db-cluster-to-point-in-time ^
    --source-db-cluster-identifier mysourcemultiazdbcluster ^
    --db-cluster-identifier mytargetmultiazdbcluster ^
    --restore-to-time 2021-08-14T23:45:00.000Z ^
    --db-cluster-instance-class db.r6gd.xlarge
```

API de RDS

Para restaurar un clúster de base de datos a un momento especificado, llame a la operación de la API de Amazon RDS RestoreDBClusterToPointInTime con los siguientes parámetros:

- `SourceDBClusterIdentifier`
- `DBClusterIdentifier`
- `RestoreToTime`

Restauración de una instantánea de clúster de base de datos Multi-AZ

Puede restaurar una instantánea en clúster de base de datos Multi-AZ mediante la AWS Management Console, la AWS CLI o la API de RDS. Puede restaurar cada uno de estos tipos de instantáneas en un clúster de base de datos Multi-AZ:

- Instantánea de una implementación Single-AZ
- Una instantánea de una implementación de clúster de base de datos multi-AZ con una sola instancia de base de datos
- Instantánea de un clúster de base de datos Multi-AZ

Para obtener información sobre las implementaciones Multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

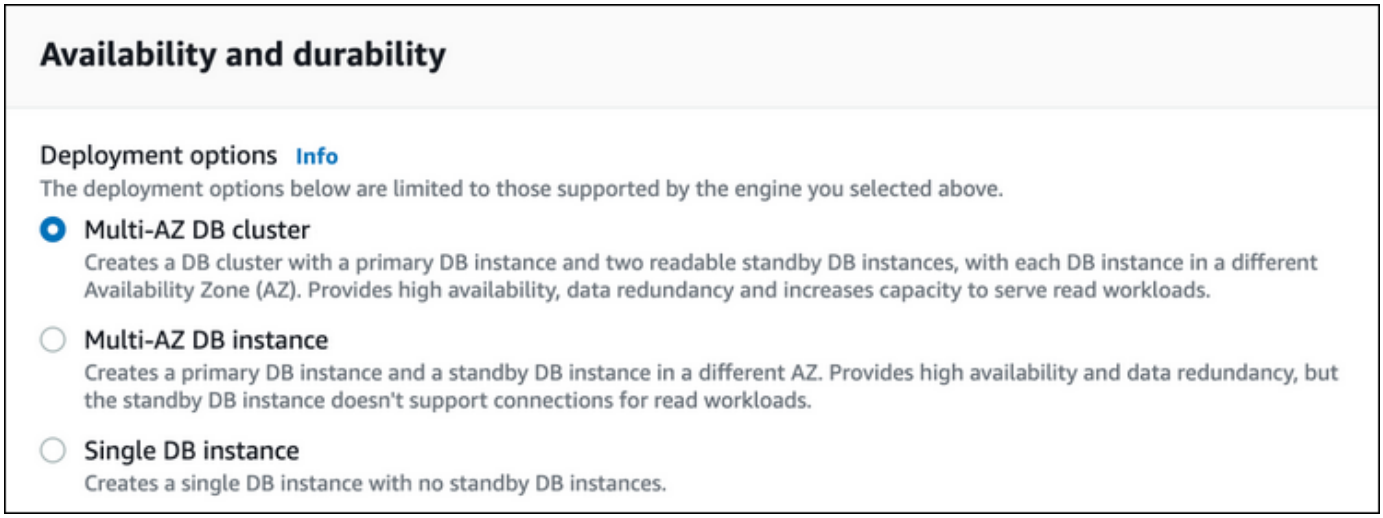
> **Tip**
>
> Puede migrar una implementación single-AZ o una implementación de clúster de base de datos multi-AZ a una implementación de clúster de base de datos multi-AZ restaurando una instantánea.

Para obtener información sobre la restauración de un clúster de base de datos multi-AZ con una versión del Soporte extendido de RDS, consulte Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS.

Consola

Para restaurar una instantánea en un clúster de base de datos Multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea desde la que desea restaurar.
4. En Actions (Acciones), elija Restore snapshot (Restaurar instantánea).
5. En la página Restore snapshot (Restaurar instantánea), en Availability and durability (Disponibilidad y durabilidad), elija Multi-AZ DB cluster(Clúster de base de datos Multi-AZ).



6. En DB cluster identifier (Identificador del clúster de base de datos), ingrese el nombre del clúster de base de datos Multi-AZ restaurado.
7. En el resto de secciones, especifique los ajustes de configuración del clúster de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración para la creación de clústeres de base de datos Multi-AZ.
8. Elija Restore DB Instance (Restaurar instancia de base de datos).

AWS CLI

Para restaurar una instantánea en un clúster de base de datos Multi-AZ, use el comando de la AWS CLI restore-db-cluster-from-snapshot.

En este ejemplo, se restaura a partir de una instantánea creada previamente denominada `mysnapshot`. Restaura a un nuevo clúster de base de datos Multi-AZ con el nombre `mynewmultiazdbcluster`. También especifica la clase de instancia de base de datos utilizada por las instancias de base de datos del clúster de base de datos Multi-AZ. Especifique `mysql` o `postgres` para el motor DB.

Para la opción `--snapshot-identifier`, puede usar el nombre o el Nombre de recurso de Amazon (ARN) para especificar una instantánea de clúster de base de datos. Sin embargo, puede utilizar únicamente el ARN para especificar una instantánea de base de datos.

Para la opción `--db-cluster-instance-class`, especifique la clase de instancia de base de datos para el nuevo cluster de base de datos Multi-AZ. Los clústeres de base de datos Multi-AZ solo admiten clases de instancias de base de datos db.m6gd y db.r6gd. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

También puede especificar otras opciones.

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-cluster-from-snapshot \
    --db-cluster-identifier mynewmultiazdbcluster \
    --snapshot-identifier mysnapshot \
    --engine mysql|postgres \
    --db-cluster-instance-class db.r6gd.xlarge
```

En:Windows

```
aws rds restore-db-cluster-from-snapshot ^
    --db-cluster-identifier mynewmultiazdbcluster ^
    --snapshot-identifier mysnapshot ^
    --engine mysql|postgres ^
    --db-cluster-instance-class db.r6gd.xlarge
```

Después de restaurar el clúster de base de datos, puede añadir el clúster de base de datos Multi-AZ al grupo de seguridad asociado a él o a la instancia de base de datos que utilizó para crear la instantánea, si procede. Con esta acción, se obtienen las mismas funciones del clúster de base de datos o instancia de base de datos anterior.

API de RDS

Para restaurar una instantánea de base de datos en un clúster de base de datos Multi-AZ, llame a la operación de la API RDS RestoreDBClusterFromSnapshot con los parámetros siguientes:

- `DBClusterIdentifier`
- `SnapshotIdentifier`
- `Engine`

También puede especificar otros parámetros opcionales.

Después de restaurar el clúster de base de datos, puede añadir el clúster de base de datos Multi-AZ al grupo de seguridad asociado a él o a la instancia de base de datos que utilizó para crear la instantánea, si procede. Con esta acción, se obtienen las mismas funciones del clúster de base de datos o instancia de base de datos anterior.

Restauración desde una instantánea de clúster de base de datos Multi-AZ a una instancia de base de datos

Una instantánea de clúster de base de datos Multi-AZ es una instantánea del volumen de almacenamiento del clúster de base de datos, que crea una copia de seguridad de todo el clúster, no solo de las bases de datos individuales. Puede restaurar una instantánea de clúster de base de datos Multi-AZ a una implementación Single-AZ o a una implementación de instancia de base de datos Multi-AZ. Para obtener información sobre las implementaciones Multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

> **Note**
>
> También puede restaurar una instantánea de clúster de base de datos Multi-AZ a un nuevo clúster de base de datos Multi-AZ. Para obtener instrucciones, consulte Restauración de una instantánea de clúster de base de datos Multi-AZ.

Para obtener información sobre la restauración de un clúster de base de datos multi-AZ con una versión del Soporte extendido de RDS, consulte Restauración de una instancia de base de datos o un clúster de base de datos multi-AZ con Soporte extendido de Amazon RDS.

Utiliza la AWS Management Console, la AWS CLI o la API de RDS para restaurar una instantánea de clúster de base de datos Multi-AZ a una implementación Single-AZ o a una implementación de instancia de base de datos Multi-AZ.

Consola

Para restaurar una instantánea de clúster de base de datos Multi-AZ a una implementación Single-AZ o a una implementación de instancia de base de datos Multi-AZ.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de clúster de base de datos Multi-AZ desde la que desea restaurar.
4. En Actions (Acciones), elija Restore snapshot (Restaurar instantánea).
5. En la página Restore snapshot (Restaurar instantánea), en Availability and durability (Disponibilidad y durabilidad), elija una de las siguientes opciones:

- Instancia de base de datos única: restaura la instantánea en una sola instancia de base de datos sin ninguna instancia de base de datos en espera.
- Instancia de base de datos Multi-AZ: restaura la instantánea en una implementación de instancia de base de datos Multi-AZ con una sola instancia de base de datos principal y una sola instancia de base de datos en espera.

6. En DB Instance Identifier (Identificador de instancias de bases de datos), escriba el nombre de la instancia de base de datos restaurada.
7. En el resto de secciones, especifique los ajustes de configuración de la instancia de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.
8. Elija Restore DB Instance (Restaurar instancia de base de datos).

AWS CLI

Para restaurar una instantánea de clúster de base de datos Multi-AZ en una implementación de instancia de base de datos, utilice el comando de la AWS CLI restore-db-instance-from-db-snapshot.

En este ejemplo, se restaura desde una instantánea del clúster de base de datos Multi-AZ creada previamente denominada `myclustersnapshot`. Se restaura en una nueva implementación de la instancia de base de datos Multi-AZ con una instancia de base de datos principal denominada `mynewdbinstance`. Para la opción `--db-cluster-snapshot-identifier`, especifique el nombre de la instantánea del clúster de base de datos Multi-AZ.

Para la opción `--db-instance-class`, especifique la clase de instancia de base de datos para la nueva implementación de instancia de base de datos. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

También puede especificar otras opciones.

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier mynewdbinstance \
    --db-cluster-snapshot-identifier myclustersnapshot \
    --engine mysql \
    --multi-az \
```

```
    --db-instance-class db.r6g.xlarge
```

En:Windows

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier mynewdbinstance ^
    --db-cluster-snapshot-identifier myclustersnapshot ^
    --engine mysql ^
    --multi-az ^
    --db-instance-class db.r6g.xlarge
```

Después de restaurar la instancia de base de datos, puede añadirla al grupo de seguridad asociado al clúster de base de datos Multi-AZ que utilizó para crear la instantánea, si procede. Con esta acción, se obtienen las mismas funciones del clúster de base de datos Multi-AZ anterior.

API de RDS

Para restaurar un clúster de base de datos Multi-AZ en una implementación de instancias de base de datos, llame a la operación de la API de RDS RestoreDBInstanceFromDBSnapshot con los parámetros siguientes:

- `DBInstanceIdentifier`
- `DBClusterSnapshotIdentifier`
- `Engine`

También puede especificar otros parámetros opcionales.

Después de restaurar la instancia de base de datos, puede añadirla al grupo de seguridad asociado al clúster de base de datos Multi-AZ que utilizó para crear la instantánea, si procede. Con esta acción, se obtienen las mismas funciones del clúster de base de datos Multi-AZ anterior.

Tutorial: restauración de una instancia de base de datos de Amazon RDS a partir de una instantánea de base de datos

A menudo al trabajar con Amazon RDS puede tener una instancia de base de datos con la que se trabaja de cuando en cuando pero que no se necesita todo el tiempo. Por ejemplo, supongamos que tiene una encuesta trimestral para los clientes que usa una instancia Amazon EC2 para alojar un sitio web de la encuesta. También tiene una instancia de base de datos que se utiliza para almacenar los resultados de la encuesta. Una forma de ahorrar dinero en un escenario de este tipo es tomar una instantánea de la instancia de la base de datos después de completar la encuesta. A continuación, elimina la instancia de base de datos y la restaura cuando necesite volver a realizar la encuesta.

Al restaurar la instancia de base de datos, debe indicar el nombre de la instantánea de la base de datos desde la que se restaura. A continuación, proporcione un nombre para la nueva instancia de base de datos que se cree a partir de la restauración.

Para obtener información detallada sobre cómo restaurar instancias de base de datos desde instantáneas, consulte Restauración a una instancia de base de datos.

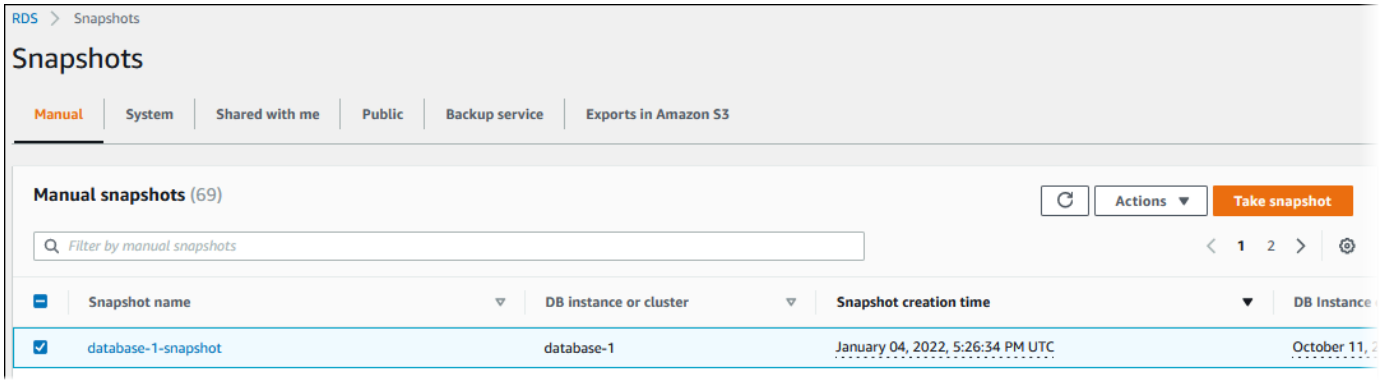
Para obtener más información sobre la administración de claves de AWS KMS para Amazon RDS, consulte Administración de AWS KMS key.

Restauración de una instancia de base de datos desde una instantánea de base de datos

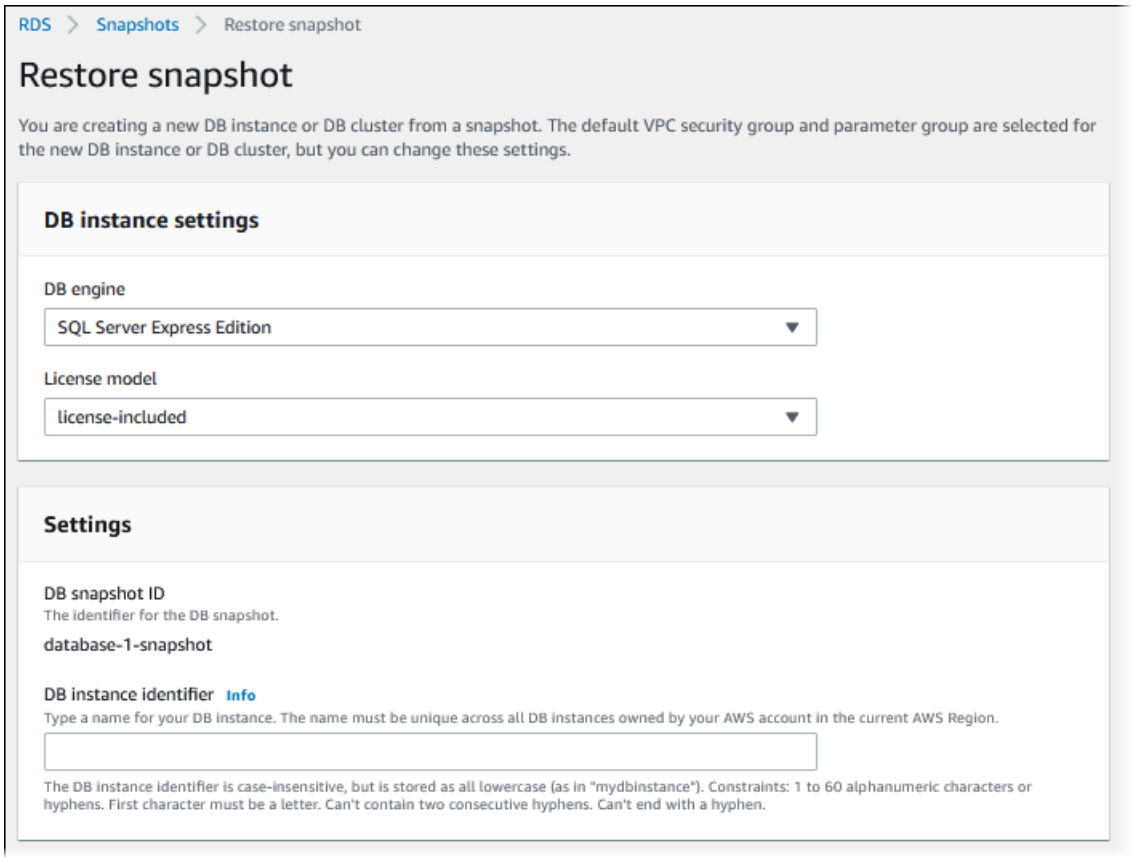
Use el procedimiento siguiente para restaurar a partir de una instantánea en la AWS Management Console.

Para restaurar una instancia de base de datos a partir de una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de base de datos desde la que desea restaurar.
4. En Actions (Acciones), elija Restore snapshot (Restaurar instantánea).



Aparecerá la página Restore snapshot (Restaurar instantánea).



5. En DB instance settings (Configuración de la instancia de base de datos), use la configuración predeterminada para DB engine (Motor de base de datos) y License model (Modelo de licencia) (para Oracle o Microsoft SQL Server).
6. En Settings (Configuración), en DB instance identifier (Identificador de instancias de bases de datos), ingrese el nombre único que quiere usar para la instancia de base de datos restaurada; por ejemplo, **`mynewdbinstance`**.

Si desea restaurar a partir de una instancia de base de datos que eliminó después de crear la instantánea de base de datos, puede usar el nombre de esa instantánea de base de datos.

7. En Disponibilidad y durabilidad, elija si quiere crear una instancia en espera en otra zona de disponibilidad.

   Para este tutorial, no cree una instancia en espera.

8. En Connectivity (Conectividad), utilice la configuración predeterminada en los siguientes casos:

   - Virtual Private Cloud (VPC) (Nube virtual privada [VPC])
   - DB subnet group (Grupo de subredes de base de datos)
   - Public access (Acceso público)
   - VPC security group (firewall) [Grupo de seguridad de VPC (firewall)]

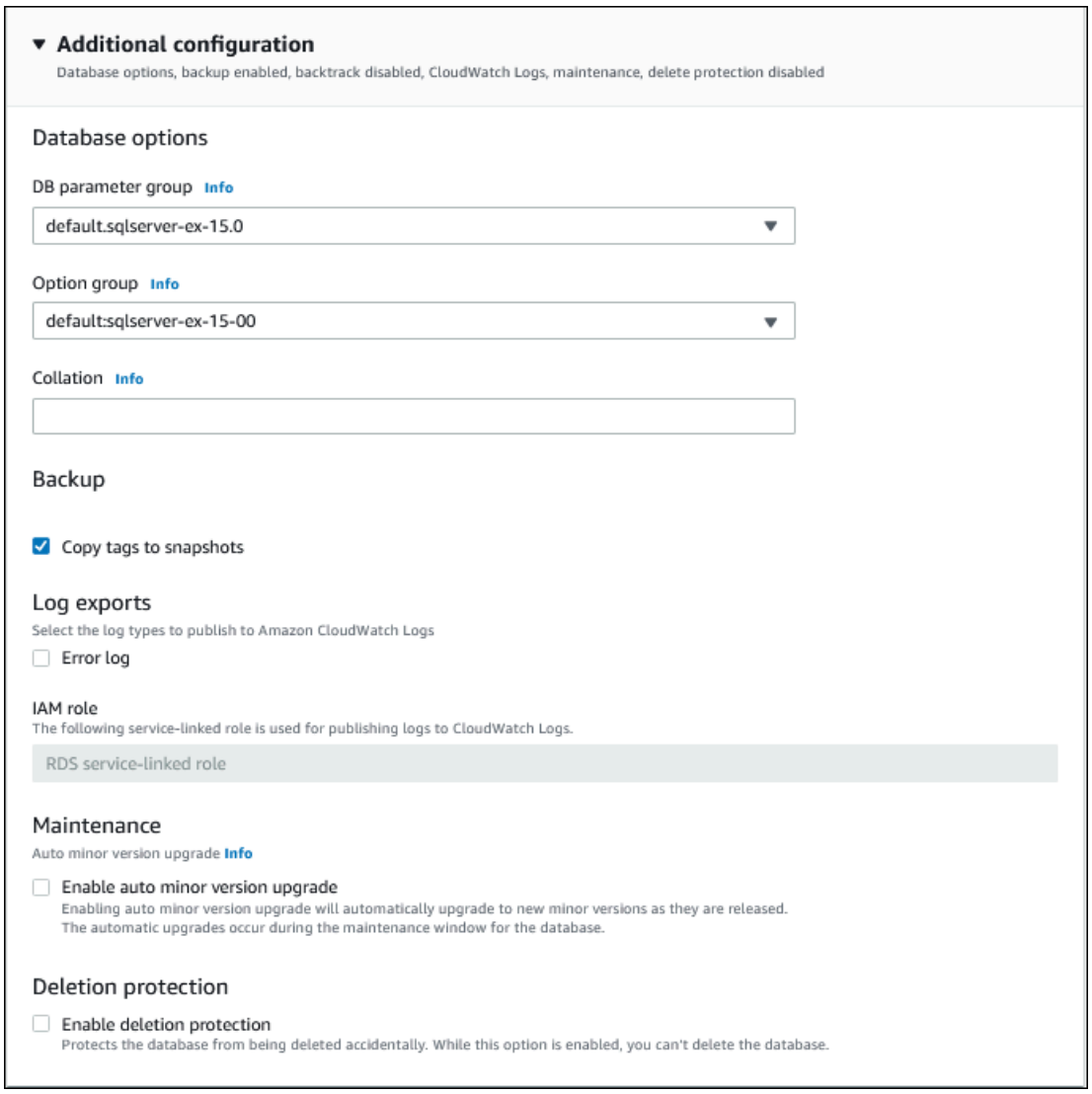
9. Elija la clase de instancia de base de datos.

   En este tutorial, elija Burstable classes (includes t classes) (Clases por ráfagas [incluye clases t]) y, a continuación, elija db.t3.small.

10. En Encryption (Cifrado), use la configuración predeterminada.

    Si la instancia de base de datos de origen de la instantánea se cifró, la instancia de base de datos restaurada también se cifra. No puede hacerlo sin cifrar.

11. Amplíe Additional configuration (Configuración adicional) en la parte inferior de la página.



12. Haga lo siguiente en Database options (Opciones de la base de datos):

    a. Elija el grupo de parámetros de base de datos.

       En este tutorial, utilice el grupo de parámetros predeterminado.

    b. Elija el grupo de opciones.

       En este tutorial, utilice el grupo de opciones predeterminado.

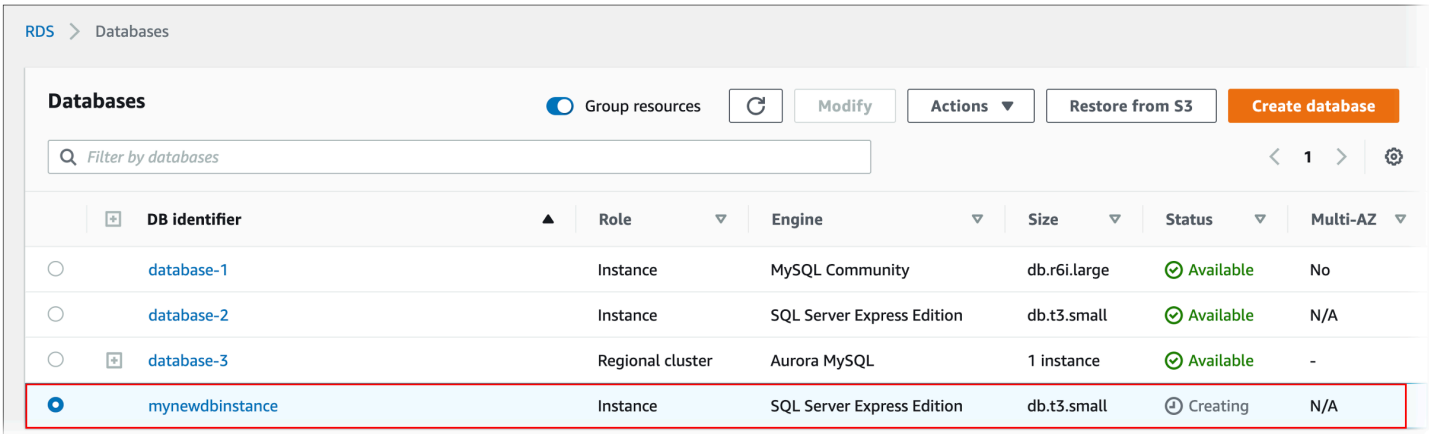
       > **Important**
       >
       > En algunos casos, es posible que desee realizar la restauración desde una instantánea de base de datos de una instancia de base de datos que utiliza una

opción persistente o permanente. Si es así, asegúrese de elegir un grupo de opciones que utilice la misma opción.

c. En Deletion protection (Protección contra eliminación), marque la casilla de verificación Enable deletion protection (Habilitar la protección contra eliminación).

13. Elija Restore DB Instance (Restaurar instancia de base de datos).

La página Databases (Bases de datos) muestra la instancia de base de datos restaurada, con el estado `Creating`.



Copia de una instantánea de base de datos para Amazon RDS

Con Amazon RDS, puede copiar copias de seguridad automatizadas o instantáneas de bases de datos manuales. Después de copiar una instantánea, la copia es una instantánea manual. Puede hacer varias copias de una copia de seguridad automatizada o instantánea manual, pero cada copia debe tener un identificador único.

Puede copiar una instantánea en la misma Región de AWS, entre Regiones de AWS y puede copiar instantáneas compartidas.

Copia de una instantánea de base de datos

Para cada Cuenta de AWS, puede copiar hasta 20 instantáneas de base de datos a la vez de una Región de AWS a otra. Si copia una instantánea de base de datos en otra Región de AWS, crea una instantánea de base de datos manual que se conserva en esa Región de AWS. Al copiar una instantánea de base de datos fuera de la Región de AWS origen, se producen cargos por transferencia de datos de Amazon RDS.

Para obtener más información acerca de los precios de las transferencias de datos, consulte Precios de Amazon RDS.

Una vez que la copia de la instantánea de base de datos se ha creado en la nueva Región de AWS, la copia de la instantánea de base de datos se comporta como las demás instantáneas de base de datos de esa Región de AWS.

Puede copiar una instantánea de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS.

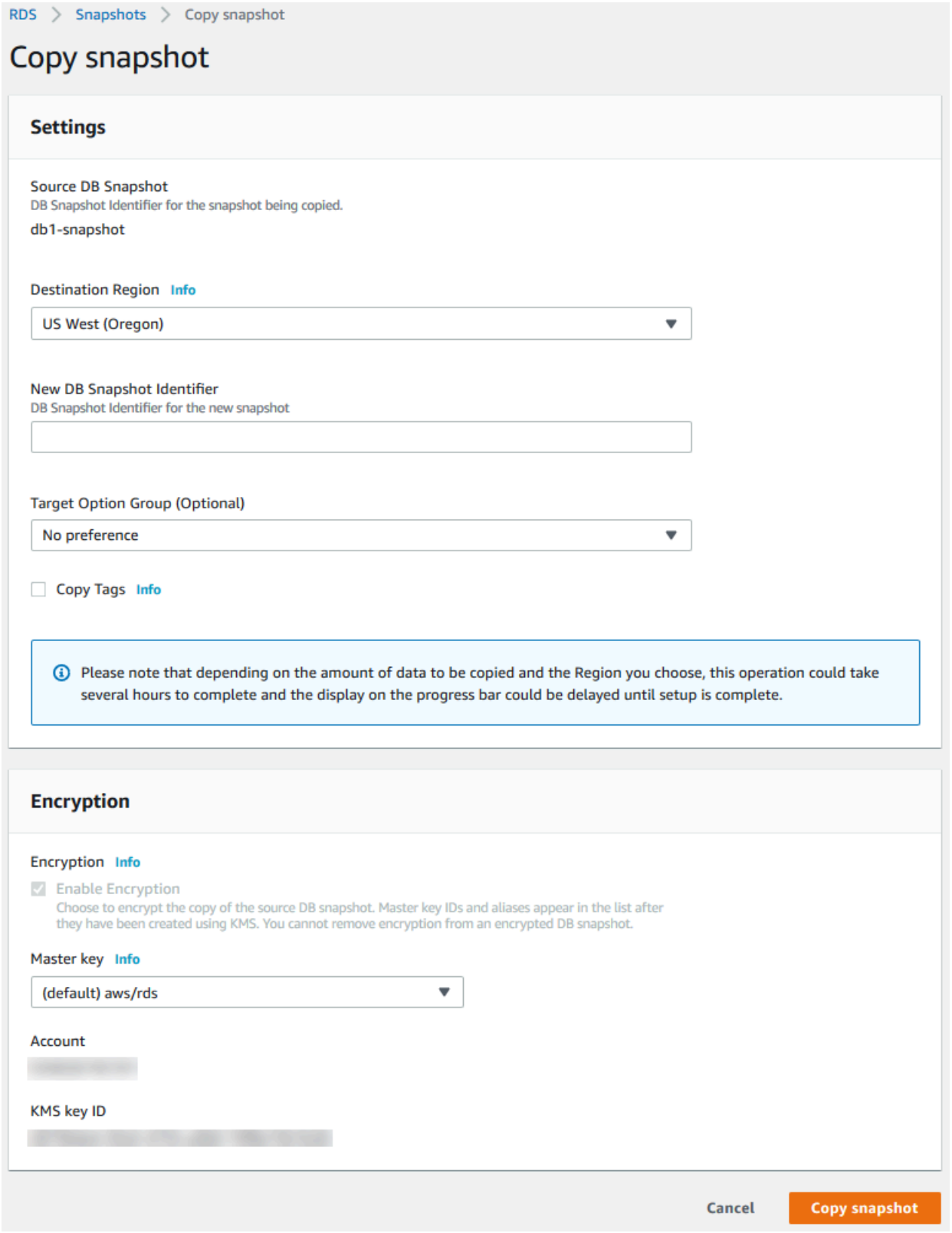
Consola

Este procedimiento copia una instantánea de base de datos cifrada o sin cifrar, en la misma Región de AWS o entre regiones, por medio de la AWS Management Console.

Para copiar una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Seleccione la instantánea de base de datos que desea copiar.
4. En Actions (Acciones), elija Copy snapshot (Copiar instantánea).

Aparece la página Copy snapshot (Copiar instantánea).



5. En Target option group (optional) (Grupo de opciones de destino [opciona]), elija un nuevo grupo de opciones, si lo desea.

   Especifique esta opción si va a copiar una instantánea de una Región de AWS a otra y su instancia de base de datos usa un grupo de opciones distinto del predeterminado.

   Si su instancia de base de datos de origen usa el Cifrado de datos transparente para Oracle o Microsoft SQL Server, debe especificar esta opción cuando copie entre regiones. Para obtener más información, consulte Aspectos a tener en cuenta sobre los grupos de opciones.

6. (Opcional) Para copiar la instantánea de base de datos en una Región de AWS diferente, en Destination Region (Región de destino) elija la nueva Región de AWS.

   > **Note**
   >
   > La Región de AWS de destino debe tener la misma versión del motor de base de datos disponible que la Región de AWS de origen.

7. En New DB Snapshot Identifier (Nuevo identificador de instantánea de base de datos), escriba el nombre de la copia de la instantánea de base de datos.

   Puede hacer varias copias de una copia de seguridad automatizada o instantánea manual, pero cada copia debe tener un identificador único.

8. (Opcional) Seleccione Copy Tags (Copiar etiquetqas) para copiar las etiquetas y los valores de la instantánea en la copia de la instantánea.

9. (Opcional) EnEncryption (Cifrado), haga lo siguiente:

   a. Elija Enable Encryption (Habilitar cifrado) si la instantánea de base de datos no está cifrada, pero desea cifrar la copia.

      > **Note**
      >
      > Si la instantánea de base de datos está cifrada, debe cifrar la copia, por lo que la casilla de verificación ya está seleccionada.

   b. En AWS KMS key, especifique el identificador de la clave de KMS que se debe utilizar para cifrar la copia de la instantánea de base de datos.

10. Elija Copy Snapshot (Copiar instantánea).

AWS CLI

Puede copiar una instantánea de base de datos usando el comando copy-db-snapshot de la AWS CLI. Si desea copiar la instantánea en una nueva Región de AWS, ejecute el comando en la nueva Región de AWS.

Las siguientes opciones se usan para copiar una instantánea de base de datos. No todas las opciones son necesarias para todos los escenarios. Use las descripciones y los ejemplos siguientes para determinar qué opciones se deben usar.

- `--source-db-snapshot-identifier`: identificador de la instantánea de base de datos de origen.
  - Si la instantánea de origen está en la misma Región de AWS que la copia, especifique un identificador de instantánea de base de datos válido. Por ejemplo, `rds:mysql-instance1-snapshot-20130805`.
  - Si la instantánea de origen está en la misma Región de AWS que la copia y la ha compartido con suCuenta de AWS, especifique un ARN de instantánea de base de datos válido. Por ejemplo, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
  - Si la instantánea de origen está en una Región de AWS distinta de la de la copia, especifique un ARN de instantánea de base de datos válido. Por ejemplo, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
  - Si va a copiar desde una instantánea de base de datos manual compartida, este parámetro debe ser el nombre de recurso de Amazon (ARN) de la instantánea de base de datos compartida.
  - Si va a copiar una instantánea cifrada, este parámetro debe estar en el formato de ARN de la Región de AWS de origen y debe coincidir con `SourceDBSnapshotIdentifier` en el parámetro `PreSignedUrl`.
- `--target-db-snapshot-identifier`: identificador de la nueva copia de la instantánea de base de datos cifrada.
- `--copy-option-group`: copie el grupo de opciones de una instantánea que se haya compartido con su Cuenta de AWS.
- `--copy-tags`: incluya la opción de copiar etiquetas para copiar las etiquetas y los valores de la instantánea en la copia de la instantánea.
- `--option-group-name`: grupo de opciones que se debe asociar con la copia de la instantánea.

Especifique esta opción si va a copiar una instantánea de una Región de AWS a otra y su instancia de base de datos usa un grupo de opciones distinto del predeterminado.

Si su instancia de base de datos de origen usa el Cifrado de datos transparente para Oracle o Microsoft SQL Server, debe especificar esta opción cuando copie entre regiones. Para obtener más información, consulte Aspectos a tener en cuenta sobre los grupos de opciones.

- `--kms-key-id`: identificador de la clave de KMS de una instantánea de base de datos cifrada. El identificador de la clave de KMS es el nombre de recurso de Amazon (ARN), el identificador de la clave o el alias de clave de la clave de KMS.
  - Si copia una instantánea de base de datos cifrada desde su Cuenta de AWS, puede especificar un valor para este parámetro y cifrar la copia con una nueva clave de KMS. Si no especifica ningún valor para este parámetro, la copia de la instantánea de base de datos se cifra con la misma clave de KMS que la instantánea de base de datos de origen.
  - Si copia una instantánea de base de datos cifrada que se ha compartido desde otra Cuenta de AWS, debe especificar un valor para este parámetro.
  - Si especifica este parámetro al copiar una instantánea sin cifrar, la copia se cifra.
  - Si copia una instantánea cifrada en otra Región de AWS, debe especificar una clave de KMS para la región de Región de AWS de destino. Las claves de KMS son específicas de la Región de AWS en la que se han creado y no se pueden utilizar las claves de cifrado de una Región de AWS en otra Región de AWS.

Example Origen sin cifrar, a la misma región

El siguiente código crea una copia de una instantánea, con el nuevo nombre `mydbsnapshotcopy`, en la misma Región de AWS que la instantánea de origen. Cuando se crea la copia, las etiquetas y el grupo de opciones de la base de datos de la instantánea original se copian en la copia de la instantánea.

Para Linux, macOS o Unix:

```
aws rds copy-db-snapshot \
    --source-db-snapshot-identifier arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805 \
    --target-db-snapshot-identifier mydbsnapshotcopy \
    --copy-option-group \
    --copy-tags
```

Para Windows:

```
aws rds copy-db-snapshot ^
    --source-db-snapshot-identifier arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805 ^
    --target-db-snapshot-identifier mydbsnapshotcopy ^
    --copy-option-group ^
    --copy-tags
```

Example Origen sin cifrar, entre regiones

El siguiente código crea una copia de una instantánea, con el nuevo nombre `mydbsnapshotcopy`, en la Región de AWS en la que se ejecuta el comando.

Para Linux, macOS o Unix:

```
aws rds copy-db-snapshot \
    --source-db-snapshot-identifier arn:aws:rds:us-east-1:123456789012:snapshot:mysql-instance1-snapshot-20130805 \
    --target-db-snapshot-identifier mydbsnapshotcopy
```

Para Windows:

```
aws rds copy-db-snapshot ^
    --source-db-snapshot-identifier arn:aws:rds:us-east-1:123456789012:snapshot:mysql-instance1-snapshot-20130805 ^
    --target-db-snapshot-identifier mydbsnapshotcopy
```

Example Origen cifrado, entre regiones

El siguiente ejemplo de código copia una instantánea de base de datos cifrada de la región EE.UU. Oeste (Oregón) a la región US East (N. Virginia). Ejecute el comando en la región de destino (us-east-1).

Para Linux, macOS o Unix:

```
aws rds copy-db-snapshot \
    --source-db-snapshot-identifier arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20161115 \
    --target-db-snapshot-identifier mydbsnapshotcopy \
    --kms-key-id my-us-east-1-key \
```

```
    --option-group-name custom-option-group-name
```

Para Windows:

```
aws rds copy-db-snapshot ^
    --source-db-snapshot-identifier arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20161115 ^
    --target-db-snapshot-identifier mydbsnapshotcopy ^
    --kms-key-id my-us-east-1-key ^
    --option-group-name custom-option-group-name
```

El parámetro `--source-region` es necesario cuando se copia una instantánea cifrada entre las regiones AWS GovCloud (Este de EE. UU.) y AWS GovCloud (EE. UU. Oeste). Para `--source-region`, especifique la Región de AWS de la instancia de base de datos de origen.

Si no se ha especificado `--source-region`, especifique un valor de `--pre-signed-url`. Una URL prefirmada es una URL que contiene una solicitud firmada de Signature Version 4 para el comando `copy-db-snapshot` que se llama en la Región de AWS de origen. Para obtener más información acerca de la opción `pre-signed-url`, consulte copy-db-snapshot en la Referencia de los comandos de AWS CLI.

API de RDS

Puede copiar una instantánea de base de datos usando la operación CopyDBSnapshot de la API de Amazon RDS. Si desea copiar la instantánea en una nueva Región de AWS, realice la acción en la nueva Región de AWS.

Los siguientes parámetros se usan para copiar una instantánea de base de datos. No todos los parámetros son necesarios para todos los escenarios. Use las descripciones y los ejemplos siguientes para determinar qué parámetros se deben usar.

- `SourceDBSnapshotIdentifier`: identificador de la instantánea de base de datos de origen.
  - Si la instantánea de origen está en la misma Región de AWS que la copia, especifique un identificador de instantánea de base de datos válido. Por ejemplo, `rds:mysql-instance1-snapshot-20130805`.
  - Si la instantánea de origen está en la misma Región de AWS que la copia y la ha compartido con suCuenta de AWS, especifique un ARN de instantánea de base de datos válido. Por ejemplo, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.

  - Si la instantánea de origen está en una Región de AWS distinta de la de la copia, especifique un ARN de instantánea de base de datos válido. Por ejemplo, `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20130805`.
  - Si va a copiar desde una instantánea de base de datos manual compartida, este parámetro debe ser el nombre de recurso de Amazon (ARN) de la instantánea de base de datos compartida.
  - Si va a copiar una instantánea cifrada, este parámetro debe estar en el formato de ARN de la Región de AWS de origen y debe coincidir con `SourceDBSnapshotIdentifier` en el parámetro `PreSignedUrl`.
- `TargetDBSnapshotIdentifier`: identificador de la nueva copia de la instantánea de base de datos cifrada.
- `CopyOptionGroup`: defina este parámetro como `true` para copiar el grupo de opciones desde una instantánea compartida en la copia de la instantánea. El valor predeterminado es `false`.
- `CopyTags`: defina este parámetro como `true` para copiar las etiquetas y los valores de la instantánea en la copia de la instantánea. El valor predeterminado es `false`.
- `OptionGroupName`: grupo de opciones que se debe asociar con la copia de la instantánea.

  Especifique este parámetro si va a copiar una instantánea de una Región de AWS en otra y su instancia de base de datos usa un grupo de opciones distinto del predeterminado.

  Si su instancia de base de datos de origen usa el cifrado de datos transparente para Oracle o Microsoft SQL Server, debe especificar este parámetro cuando copie entre regiones. Para obtener más información, consulte Aspectos a tener en cuenta sobre los grupos de opciones.
- `KmsKeyId`: identificador de la clave de KMS de una instantánea de base de datos cifrada. El identificador de la clave de KMS es el nombre de recurso de Amazon (ARN), el identificador de la clave o el alias de clave de la clave de KMS.
  - Si copia una instantánea de base de datos cifrada desde su Cuenta de AWS, puede especificar un valor para este parámetro y cifrar la copia con una nueva clave de KMS. Si no especifica ningún valor para este parámetro, la copia de la instantánea de base de datos se cifra con la misma clave de KMS que la instantánea de base de datos de origen.
  - Si copia una instantánea de base de datos cifrada que se ha compartido desde otra Cuenta de AWS, debe especificar un valor para este parámetro.
  - Si especifica este parámetro al copiar una instantánea sin cifrar, la copia se cifra.
  - Si copia una instantánea cifrada en otra Región de AWS, debe especificar una clave de KMS para la región de Región de AWS de destino. Las claves de KMS son específicas de la Región

de AWS en la que se han creado y no se pueden utilizar las claves de cifrado de una Región de AWS en otra Región de AWS.

- `PreSignedUrl`: la URL que contiene una solicitud firmada de Signature Version 4 para la operación `CopyDBSnapshot` de la API en la Región de AWS de origen que contiene la instantánea de la base de datos fuente que se desea copiar.

  Debe especificar este parámetro cuando copie una instantánea de base de datos cifrada desde otra Región de AWS con la API de Amazon RDS. Puede especificar la opción de la región de origen en lugar de este parámetro cuando copie una instantánea de base de datos cifrada desde otra Región de AWS con la AWS CLI.

  La URL prefirmada debe ser una solicitud válida para la operación de la API `CopyDBSnapshot` que se puede ejecutar en la Región de AWS de origen que contiene la instantánea de base de datos cifrada que se va a copiar. La solicitud de la URL prefirmada debe contener los siguientes valores de parámetros:

  - `DestinationRegion`: la Región de AWS en la que se copiará la instantánea de base de datos cifrada. Esta Región de AWS es la misma en la que se llama a la operación `CopyDBSnapshot` que contiene esta URL prefirmada.

    Por ejemplo, supongamos que copia una instantánea de base de datos cifrada desde la región us-west-2 a la región us-east-1. A continuación, llame la operación `CopyDBSnapshot` en la región us-east-1 y proporcione una URL prefirmada que contenga una llamada a la operación `CopyDBSnapshot` en la región us-west-2. En este ejemplo, el valor de `DestinationRegion` en la URL prefirmada se debe establecer en la región us-east-1.

  - `KmsKeyId`: el identificador de la clave de KMS que se va a utilizar para cifrar la copia de la instantánea de base de datos en la Región de AWS de destino. Es el mismo identificador tanto para la operación `CopyDBSnapshot` a la que se llama en la Región de AWS de destino como para la operación contenida en la URL prefirmada.

  - `SourceDBSnapshotIdentifier`: identificador de la instantánea de base de datos para la instantánea cifrada que se va a copiar. Este identificador debe estar en el formato de Nombre de recurso de Amazon (ARN) para la Región de AWS de origen. Por ejemplo, si copia una instantánea de base de datos cifrada de la región us-west-2, el `SourceDBSnapshotIdentifier` tendrá un aspecto similar al del siguiente ejemplo: `arn:aws:rds:us-west-2:123456789012:snapshot:mysql-instance1-snapshot-20161115`.

Para obtener más información acerca de las solicitudes firmadas en Signature Version 4, consulte lo siguiente:

- Autenticación de solicitudes: mediante parámetros de consulta (AWS Signature Version 4) en la referencia de la API de Amazon Simple Storage Service
- Proceso de firma Signature Version 4 en la Referencia general de AWS

Example Origen sin cifrar, a la misma región

El siguiente código crea una copia de una instantánea, con el nuevo nombre `mydbsnapshotcopy`, en la misma Región de AWS que la instantánea de origen. Cuando se crea la copia, todas las etiquetas de la instantánea original se copian en la copia de la instantánea.

```
https://rds.us-west-1.amazonaws.com/
 ?Action=CopyDBSnapshot
 &CopyTags=true
 &SignatureMethod=HmacSHA256
 &SignatureVersion=4
 &SourceDBSnapshotIdentifier=mysql-instance1-snapshot-20130805
 &TargetDBSnapshotIdentifier=mydbsnapshotcopy
 &Version=2013-09-09
 &X-Amz-Algorithm=AWS4-HMAC-SHA256
 &X-Amz-Credential=AKIADQKE4SARGYLE/20140429/us-west-1/rds/aws4_request
 &X-Amz-Date=20140429T175351Z
 &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
 &X-Amz-Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Example Origen sin cifrar, entre regiones

El siguiente código crea una copia de una instantánea, con el nuevo nombre `mydbsnapshotcopy`, en la región EE.UU. Oeste (Norte de California).

```
https://rds.us-west-1.amazonaws.com/
 ?Action=CopyDBSnapshot
 &SignatureMethod=HmacSHA256
 &SignatureVersion=4
 &SourceDBSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-east-1%3A123456789012%3Asnapshot
%3Amysql-instance1-snapshot-20130805
 &TargetDBSnapshotIdentifier=mydbsnapshotcopy
 &Version=2013-09-09
```

```
 &X-Amz-Algorithm=AWS4-HMAC-SHA256
 &X-Amz-Credential=AKIADQKE4SARGYLE/20140429/us-west-1/rds/aws4_request
 &X-Amz-Date=20140429T175351Z
 &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
 &X-Amz-Signature=9164337efa99caf850e874a1cb7ef62f3cea29d0b448b9e0e7c53b288ddffed2
```

Example Origen cifrado, entre regiones

El siguiente código crea una copia de una instantánea, con el nuevo nombre `mydbsnapshotcopy`, en la región US East (N. Virginia).

```
https://rds.us-east-1.amazonaws.com/
    ?Action=CopyDBSnapshot
    &KmsKeyId=my-us-east-1-key
    &OptionGroupName=custom-option-group-name
    &PreSignedUrl=https%253A%252F%252Frds.us-west-2.amazonaws.com%252F
         %253FAction%253DCopyDBSnapshot
         %2526DestinationRegion%253Dus-east-1
         %2526KmsKeyId%253Dmy-us-east-1-key
         %2526SourceDBSnapshotIdentifier%253Darn%25253Aaws%25253Ards%25253Aus-
west-2%25253A123456789012%25253Asnapshot%25253Amysql-instance1-snapshot-20161115
         %2526SignatureMethod%253DHmacSHA256
         %2526SignatureVersion%253D4
         %2526Version%253D2014-10-31
         %2526X-Amz-Algorithm%253DAWS4-HMAC-SHA256
         %2526X-Amz-Credential%253DAKIADQKE4SARGYLE%252F20161117%252Fus-west-2%252Frds
%252Faws4_request
         %2526X-Amz-Date%253D20161117T215409Z
         %2526X-Amz-Expires%253D3600
         %2526X-Amz-SignedHeaders%253Dcontent-type%253Bhost%253Buser-agent%253Bx-amz-
content-sha256%253Bx-amz-date
         %2526X-Amz-Signature
%253D255a0f17b4e717d3b67fad163c3ec26573b882c03a65523522cf890a67fca613
    &SignatureMethod=HmacSHA256
    &SignatureVersion=4
    &SourceDBSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-west-2%3A123456789012%3Asnapshot
%3Amysql-instance1-snapshot-20161115
    &TargetDBSnapshotIdentifier=mydbsnapshotcopy
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
    &X-Amz-Date=20161117T221704Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
```

```
&X-Amz-Signature=da4f2da66739d2e722c85fcfd225dc27bba7e2b8dbea8d8612434378e52adccf
```

Limitaciones

A continuación se indican algunas limitaciones al copiar instantáneas:

- No puede copiar una instantánea en o desde la región de China (Pekín) o la región de China (Ningxia).
- Puede copiar una instantánea entre AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste). Sin embargo, no puede copiar una instantánea entre estas regiones de GovCloud (EE. UU.) y las regiones que no sean de GovCloud (EE. UU.).
- Si elimina una instantánea de origen antes de que la instantánea de destino esté disponible, la copia de la instantánea podría generar un error. Compruebe que la instantánea de destino tiene el estado `AVAILABLE` antes de eliminar una instantánea de origen.
- Puede tener hasta 20 solicitudes de copia de instantánea en curso en una única región de destino por cuenta.
- Si solicita varias copias de instantáneas de la misma instancia de base de datos de origen, se ponen a la cola internamente. Las copias solicitadas posteriormente no se iniciarán hasta que se completen las copias de instantáneas anteriores. Para obtener más información, consulte el tema sobre por qué la creación de instantáneas de EBS o la AMI de EC2 es lenta en el Centro de conocimientos de AWS.
- Dependiendo de las Regiones de AWS implicadas y de la cantidad de datos que se vayan a copiar, una copia de instantánea entre regiones puede tardar horas en completarse. En algunos casos, puede haber un gran número de solicitudes de copia de instantáneas entre regiones desde una región. En estos casos, Amazon RDS puede poner nuevas solicitudes de copia entre regiones desde esa región de origen en una cola hasta que alguna de las copias en curso se complete. No se muestra ninguna información de progreso sobre las solicitudes de copia mientras están en la cola. La información de progreso se muestra cuando comienza la copia.
- Si una copia sigue pendiente al iniciar otra copia, la segunda copia no se iniciará hasta que finalice la primera copia.
- No puede copiar una instantánea de un clúster de base de datos multi-AZ.
- Solo puede copiar instantáneas de instancias de base de datos que usen volúmenes io2 para Regiones de AWS donde estén disponibles los volúmenes io2 Block Express. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Consideraciones

Para ver las aspectos a tener en cuenta al copiar una instantánea de base de datos, consulte los temas siguientes.

Temas

- Retención de instantáneas
- Factores importantes sobre la copia de instantáneas compartidas
- Aspectos a tener en cuenta sobre la copia de instantáneas de cifrado
- Aspectos a tener en cuenta sobre la copia de instantáneas incrementales
- Aspectos a tener en cuenta sobre la copia de instantáneas entre regiones
- Aspectos a tener en cuenta sobre los grupos de opciones
- Aspectos a tener en cuenta sobre los grupos de parámetros

Retención de instantáneas

Amazon RDS elimina copias de seguridad automatizadas en varias situaciones:

- Al final de su periodo de retención.
- Cuando desactiva las copias de seguridad automatizadas para una instancia de base de datos.
- Cuando se elimina una instancia de base de datos.

Si desea conservar una copia de seguridad automatizada durante un periodo más largo, cópiela para crear una instantánea manual que se conservará hasta que la elimine. Es posible que los costos de almacenamiento de Amazon RDS se apliquen a las instantáneas manuales si exceden el espacio de almacenamiento predeterminado.

Para obtener más información acerca de los costos de almacenamiento de copias de seguridad, consulte Precios de Amazon RDS.

Factores importantes sobre la copia de instantáneas compartidas

Puede copiar instantáneas compartidas con usted por otras Cuentas de AWS. En algunos casos, puede copiar una instantánea cifrada que se ha compartido desde otra Cuenta de AWS. En estos casos, debe tener acceso a la AWS KMS key que se utilizó para cifrar la instantánea.

> **Note**
>
> Los costos de almacenamiento de Amazon RDS se aplican a las instantáneas compartidas que copie. Amazon RDS podría asociar el ARN de la instancia de base de datos de origen a la instantánea que ha copiado.

Puede copiar una instantánea de base de datos compartida entre Regiones de AWS, siempre que esté sin cifrar. No obstante, si la instantánea de base de datos está cifrada, solo puede copiarla en la misma región.

> **Note**
>
> La copia de instantáneas incrementales compartidas en la misma Región de AWS se admite cuando no están cifradas o cuando están cifradas con la misma clave de KMS que la instantánea completa inicial. Si utiliza una clave KMS diferente para cifrar instantáneas posteriores al copiarlas, esas instantáneas compartidas son instantáneas completas. Para obtener más información, consulte Aspectos a tener en cuenta sobre la copia de instantáneas incrementales.

Aspectos a tener en cuenta sobre la copia de instantáneas de cifrado

Puede copiar una instantánea que se haya cifrado con una clave de KMS. Si copia una instantánea cifrada, la copia de la instantánea se debe cifrar también. Si copia una instantánea cifrada dentro de la misma Región de AWS, puede cifrar la copia con la misma clave de KMS que la instantánea original. O bien puede especificar una clave de KMS diferente.

Si copia una instantánea cifrada entre regiones, debe especificar una clave de KMS valida en la Región de AWS de destino. Puede ser una clave de KMS específica de la región o una clave de varias regiones. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en AWS KMS.

La instantánea de origen permanece cifrada durante todo el proceso de copia. Para obtener más información, consulte Limitaciones de las instancias de base de datos cifrados de Amazon RDS.

También puede cifrar una copia de una instantánea sin cifrar. De esta forma, puede añadir rápidamente el cifrado a una instancia de base de datos que antes estaba sin cifrar. Para ello, cree

una instantánea de su instancia de base de datos cuando todo esté listo para cifrarla. A continuación, puede crear una copia de dicha instantánea y especificar una clave de KMS para cifrar esa copia de la instantánea. A continuación, puede restaurar una instancia de base de datos cifrado desde la instantánea cifrada.

> **Important**
>
> Cuando utiliza instrucciones de denegación explícitas para todos los recursos (*) en políticas de claves de AWS KMS con servicios administrados como Amazon RDS, debe especificar una condición para permitir que la cuenta propietaria del recurso acceda. Es posible que la operación de copia produzca un error sin esta condición, incluso si la regla de denegación incluye excepciones para el usuario de IAM.

Para obtener más información sobre la administración de claves de AWS KMS para Amazon RDS, consulte Administración de AWS KMS key.

Aspectos a tener en cuenta sobre la copia de instantáneas incrementales

Una instantánea incremental contiene solo los datos que han cambiado tras la instantánea más reciente de la misma instancia de base de datos. La copia de instantáneas incrementales es más rápida y genera un costo de almacenamiento más bajo que la copia de instantáneas completa.

Si una copia de instantánea es incremental depende de la copia de la instantánea completada más recientemente y de la instantánea de origen. Si se ha borrado la copia más reciente de la instantánea, la siguiente copia será una copia completa, no una copia incremental. Una copia de la instantánea será del mismo tipo que la instantánea de origen. Si la instantánea de origen es una instantánea incremental, la copia de la instantánea será una instantánea incremental.

Al copiar una instantánea entre Cuentas de AWS, la copia es incremental solo si se cumplen todas las siguientes condiciones:

- La copia más reciente de la instantánea es de la misma instancia de base de datos de origen y sigue existiendo en la cuenta de destino.
- Todas las copias de la instantánea en la cuenta de destino, bien no están cifradas, o bien se cifraron con la misma clave de KMS.
- Si la instancia de base de datos de origen es una instancia Multi-AZ, no se ha conmutado por error a otra AZ desde que se tomó la última instantánea de ella.

En los siguientes ejemplos, se muestra la diferencia entre las instantáneas completas y progresivas. Se aplican a instantáneas compartidas y no compartidas.

Instantánea	Clave de cifrado	Completa o progresiva
S1	K1	Completa
S2	K1	Progresiva de S1
S3	K1	Progresiva de S2
S4	K1	Progresiva de S3
Copia de S1 (S1C)	K2	Completa
Copia de S2 (S2C)	K3	Completa
Copia de S3 (S3C)	K3	Progresiva de S2C
Copia de S4 (S4C)	K3	Progresiva de S3C
Copia 2 de S4 (S4C2)	K4	Completa

> **Note**
>
> En estos ejemplos, las instantáneas S2, S3 y S4 son progresivas solo si la instantánea anterior sigue existiendo.
> Lo mismo sucede con las copias. Las copias de las instantáneas S3C y S4C son progresivas solo si la copia anterior sigue existiendo.

Para obtener información sobre cómo copiar instantáneas incrementales en Regiones de AWS, consulte Copias completas e incrementales.

Aspectos a tener en cuenta sobre la copia de instantáneas entre regiones

Puede copiar instantáneas de base de datos en Regiones de AWS. Sin embargo, existen ciertas restricciones y consideraciones para la copia de instantáneas entre regiones.

Solicitudes de copia de instantáneas de base de datos entre regiones

Para comunicarse con la región de origen para solicitar la copia de una instantánea de base de datos entre regiones, el solicitante (rol de IAM o usuario de IAM) debe tener acceso a la instantánea de base de datos de origen y a la región de origen.

Ciertas condiciones en la política de IAM del solicitante pueden generar un error en la solicitud. En los siguientes ejemplos se supone que está copiando la instantánea de base de datos de EE.UU. Este (Ohio) a US East (N. Virginia). Estos ejemplos muestran condiciones en la política de IAM del solicitante que generan un error en la solicitud:

- La política del solicitante tiene una condición para la `aws:RequestedRegion`.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": "us-east-1"
    }
}
```

  La solicitud falla porque la política no permite el acceso a la región de origen. Para que una solicitud sea correcta, se deben especificar las regiones de origen y destino.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "StringEquals": {
        "aws:RequestedRegion": [
            "us-east-1",
            "us-east-2"
        ]
    }
}
```

- La política del solicitante no permite el acceso a la instantánea de base de datos de origen.

```
...
```

```
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "arn:aws:rds:us-east-1:123456789012:snapshot:target-snapshot"
...
```

Para una solicitud correcta, especifique las instantáneas de origen y de destino.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": [
    "arn:aws:rds:us-east-1:123456789012:snapshot:target-snapshot",
    "arn:aws:rds:us-east-2:123456789012:snapshot:source-snapshot"
]
...
```

- La política del solicitante niega `aws:ViaAWSService`.

```
...
"Effect": "Allow",
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "Bool": {"aws:ViaAWSService": "false"}
}
```

La comunicación con la región de origen la efectúa RDS en nombre del solicitante. Para que una solicitud sea correcta, no deniegue las llamadas realizadas por los servicios de AWS.

- La política del solicitante tiene una condición para `aws:SourceVpc` o `aws:SourceVpce`.

Estas solicitudes pueden fallar porque cuando RDS realiza la llamada a la región remota, esta no procede del punto de conexión de la VPC o la VPC especificada.

Si es necesario utilizar una de las condiciones anteriores que generarían un error en una solicitud, se puede incluir una segunda instrucción con `aws:CalledVia` en la política para que la solicitud se realice correctamente. Por ejemplo, se puede usar `aws:CalledVia` con `aws:SourceVpce`, como se muestra aquí:

```
...
"Effect": "Allow",
```

```
"Action": "rds:CopyDBSnapshot",
"Resource": "*",
"Condition": {
    "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
     }
},
{
    "Effect": "Allow",
    "Action": [
        "rds:CopyDBSnapshot"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "rds.amazonaws.com"
            ]
        }
    }
}
```

Para obtener más información, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

Autorización de copia de la instantánea

Después de que una solicitud de copia de instantánea de base de datos entre regiones devuelve `success`, RDS inicia la copia en segundo plano. Se crea una autorización para que RDS acceda a la instantánea de origen. Esta autorización vincula la instantánea de base de datos de origen a la instantánea de base de datos de destino y permite que RDS copie solo en la instantánea de destino especificada.

La autorización es verificada por RDS mediante el permiso `rds:CrossRegionCommunication` en el rol de IAM vinculado al servicio. Si la copia está autorizada, RDS se comunica con la región de origen y completa la copia.

RDS no tiene acceso a instantáneas de base de datos que no estaban autorizadas previamente por una solicitud de `CopyDBSnapshot`. La autorización se revoca cuando se completa la copia.

RDS utiliza el rol vinculado a servicios para verificar la autorización en la región de origen. Si elimina la función vinculada a servicios durante el proceso de copia, se produce un error en la copia.

Para obtener más información, consulte Usar roles vinculados a servicios en la Guía del usuario de IAM.

Uso de credenciales de AWS Security Token Service

Los tokens de sesión del punto de conexión global de AWS Security Token Service (AWS STS) son válidos únicamente en Regiones de AWS que están habilitadas de forma predeterminada (regiones comerciales). Si utiliza credenciales de la operación de la API `assumeRole` en AWS STS, utilice el punto de conexión regional si la región de origen es una región registrada. De lo contrario, la solicitud devuelve un error. Esto ocurre porque las credenciales deben ser válidas en ambas regiones, lo cual se cumple para las regiones registradas solo cuando se utiliza el punto de conexión regional de AWS STS.

Para utilizar el punto de conexión global, asegúrese de que está habilitado para operaciones en ambas regiones. Establezca el punto de conexión global en `Valid in all Regiones de AWS` en la configuración de la cuenta de AWS STS.

La misma regla se aplica a las credenciales del parámetro URL prefirmado.

Para obtener más información, consulte Administración de AWS STS en una Región de AWS en la guía del usuario de IAM.

Latencia y múltiples solicitudes de copia

Dependiendo de las Regiones de AWS implicadas y de la cantidad de datos que se vayan a copiar, una copia de instantánea entre regiones puede tardar horas en completarse.

En algunos casos, puede haber un gran número de solicitudes de copia de instantáneas entre regiones desde una Región de AWS. En estos casos, Amazon RDS puede poner nuevas solicitudes de copia entre regiones desde esa Región de AWS de origen en una cola hasta que alguna de las copias en curso se complete. No se muestra ninguna información de progreso sobre las solicitudes de copia mientras están en la cola. La información de progreso se muestra cuando comienza la copia.

Copias completas e incrementales

Al copiar una instantánea en una región Región de AWS que es distinta de la región de la instantánea de origen, la primera copia es una copia de la instantánea completa, incluso si copia una instantánea incremental. Una copia de la instantánea completa contiene todos los datos y metadatos necesarios para restaurar la instancia de base de datos. Tras la primera copia de la instantánea,

puede copiar instantáneas incrementales de la misma instancia de base de datos en la misma región de destino dentro de la misma Cuenta de AWS. Para obtener más información sobre las instantáneas incrementales, consulte Aspectos a tener en cuenta sobre la copia de instantáneas incrementales.

La copia de instantáneas incrementales en Regiones de AWS se admite tanto para las instantáneas sin cifrar como para las cifradas.

Al copiar una instantánea en Regiones de AWS, la copia es incremental si se cumplen los siguientes criterios:

- La instantánea se ha copiado previamente a la región de destino.
- La copia más reciente de la instantánea sigue presente en la región de destino.
- Todas las copias de la instantánea en la región de destino, bien no están cifradas, o bien se cifraron con la misma clave de KMS.

Aspectos a tener en cuenta sobre los grupos de opciones

Los grupos de opciones de bases de datos son específicos de la Región de AWS en la que se crean y no es posible usar un grupo de opciones de una Región de AWS en otra Región de AWS.

Para las bases de datos de Oracle, puede utilizar la AWS CLI o la API de RDS para copiar el grupo de opciones de base de datos personalizado de una instantánea que se haya compartido con su Cuenta de AWS. Solo puede copiar grupos de opciones dentro de la misma Región de AWS. El grupo de opciones no se copia si ya se ha copiado en la cuenta de destino y no se ha realizado ningún cambio desde que se copió. Si el grupo de opciones de origen se ha copiado anteriormente, pero ha cambiado desde que se copió, RDS copia la nueva versión en la cuenta de destino. Los grupos de opciones predeterminados no se copian.

Al copiar una instantánea entre regiones, puede especificar un nuevo grupo de opciones para la instantánea. Es recomendable preparar un nuevo grupo de opciones antes de copiar la instantánea. En la Región de AWS de destino, cree un grupo de opciones con la misma configuración que la instancia de base de datos original. Si ya existe uno en la Región de AWS nueva, puede usarlo.

En algunos casos, puede copiar una instantánea y no especificar un nuevo grupo de opciones para la instantánea. En estos casos, al restaurar la instantánea, la instancia de la base de datos obtiene el grupo de opciones predeterminado. Para aplicar a la nueva de instancia de la base de datos las mismas opciones que al original, se debe hacer lo siguiente:

1. En la Región de AWS de destino, cree un grupo de opciones con la misma configuración que la instancia de base de datos original. Si ya existe uno en la Región de AWS nueva, puede usarlo.
2. Después de restaurar la instantánea en la Región de AWS de destino, modifique la instancia de base de datos y agregue el grupo de opciones nuevo o ya existente del paso anterior.

Aspectos a tener en cuenta sobre los grupos de parámetros

Cuando se copia una instantánea entre regiones, la copia no incluye el grupo de parámetros empleado por la instancia de base de datos original. Cuando se restaura una instantánea para crear una nueva instancia de base de datos, la instancia de base de datos usa el grupo de parámetros predeterminado para la Región de AWS en la que se creó. Para aplicar a la instancia de la base de datos los mismos parámetros que al original, se debe hacer lo siguiente:

1. En la Región de AWS de destino, cree un grupo de parámetros del clúster de base de datos con la misma configuración que la instancia de base de datos. Si ya existe uno en la Región de AWS nueva, puede usarlo.
2. Después de restaurar la instantánea en la Región de AWS de destino, modifique la instancia de base de datos y agregue el grupo de parámetros nuevo o existente del paso anterior.

Uso compartido de una instantánea manual de base de datos de Amazon RDS

Al utilizar Amazon RDS, puede compartir una instantánea manual de base de datos de las siguientes maneras:

- Al compartir una instantánea manual de base de datos, ya sea cifrada o no cifrada, permite que las Cuentas de AWS autorizadas copien la instantánea.
- Si se comparte una instantánea manual de base de datos sin cifrar, las Cuentas de AWS autorizadas podrán restaurar directamente una instancia de base de datos a partir de la instantánea en lugar de hacer una copia de ella y restaurarla. Sin embargo, no puede restaurar una instancia de base de datos desde una instantánea de base de datos que esté compartida y cifrada. En lugar de ello, puede hacer una copia de la instantánea de base de datos y restaurar la instancia de base de datos desde la copia.

> **Note**
>
> Para compartir una instantánea automatizada, cree una instantánea manual copiando la instantánea automatizada y, a continuación, comparta esa copia. Este proceso también se aplica a los recursos generados por Backup de AWS.

Para obtener más información acerca de la copia de instantáneas, consulte Copia de una instantánea de base de datos para Amazon RDS. Para obtener más información sobre cómo restaurar una instancia de base de datos desde una instantánea de base de datos, consulte Restauración a una instancia de base de datos.

Puede compartir una instantánea manual con otras 20 Cuentas de AWS como máximo.

Cuando se comparten instantáneas manuales con otras Cuentas de AWS, se aplican las restricciones siguientes:

- Cuando se restaura una instancia de base de datos a partir de una instantánea compartida mediante la AWS Command Line Interface (AWS CLI) o la API de Amazon RDS, se debe especificar el nombre de recurso de Amazon (ARN) de la instantánea compartida como identificador de instantánea.

- No puede compartir una instantánea de base de datos que utilice un grupo de opciones con opciones permanentes o persistentes, excepto para las instancias de base de datos de Oracle que tengan la opción `Timezone` o `OLS` (o ambas).

  Una opción permanente no se puede eliminar de un grupo de opciones. Los grupos de opciones con opciones persistentes no se pueden eliminar de una instancia de base de datos una vez que el grupo de opciones se ha asignado a la instancia de base de datos.

  En la siguiente tabla se muestran las opciones permanentes y persistentes, y sus motores de base de datos correspondientes.

Nombre de la opción	Persistente	Permanente	Motor de base de datos
TDE	Sí	No	Microsoft SQL Server Enterprise Edition
TDE	Sí	Sí	Oracle Enterprise Edition
Zona horaria	Sí	Sí	Oracle Enterprise Edition Oracle Standard Edition Oracle Standard Edition One Oracle Standard Edition 2

  Para obtener las instancias de base de datos de Oracle, puede copiar las instantáneas de base de datos que tengan la opción `Timezone` u `OLS` (o ambas). Para hacerlo, especifique un grupo de opciones de destinos que incluya estas opciones cuando copie la instantánea de base de datos. La opción OLS es permanente y persistente solo para las instancias de base de datos de Oracle que ejecuten la versión 12.2 o superior de Oracle. Para obtener más información sobre estas opciones, consulte Zona horaria Oracle y Oracle Label Security.

- No puede compartir una instantánea de un clúster de base de datos multi-AZ.

Consulte los siguientes temas para obtener información sobre cómo compartir instantáneas públicas, compartir instantáneas cifradas y dejar de compartir instantáneas.

Temas

- Uso compartido de instantáneas públicas para Amazon RDS
- Uso compartido de instantáneas cifradas para Amazon RDS
- Detención del uso compartido de instantáneas para Amazon RDS

Uso compartido de una instantánea

Puede compartir una instantánea de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Con la consola de Amazon RDS, puede compartir una instantánea manual de base de datos con un máximo de 20 Cuentas de AWS. También puede utilizar la consola para dejar de compartir una instantánea manual con una o varias cuentas.

Para compartir una instantánea manual de un de base de datos mediante la consola de Amazon RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Seleccione la instantánea manual que desea compartir.
4. En Actions) (Acciones), elija Share Snapshot (Compartir instantánea).
5. Elija una de las siguientes opciones para DB Snapshot Visibility (Visibilidad de instantánea de base de datos).

    - Si el origen está sin cifrar, elija Público para permitir que todas las cuentas de AWS restauren una instancia de base de datos a partir de la instantánea de clúster de base de datos manual, o elija Privado para permitir que únicamente las Cuentas de AWS que especifique restauren una instancia de base de datos a partir de una instantánea de base de datos manual.

    > **Warning**
    >
    > Si establece Visibilidad de instantánea de base de datos en Pública, todas las Cuentas de AWS pueden restaurar una instancia de base de datos a partir de la instantánea de

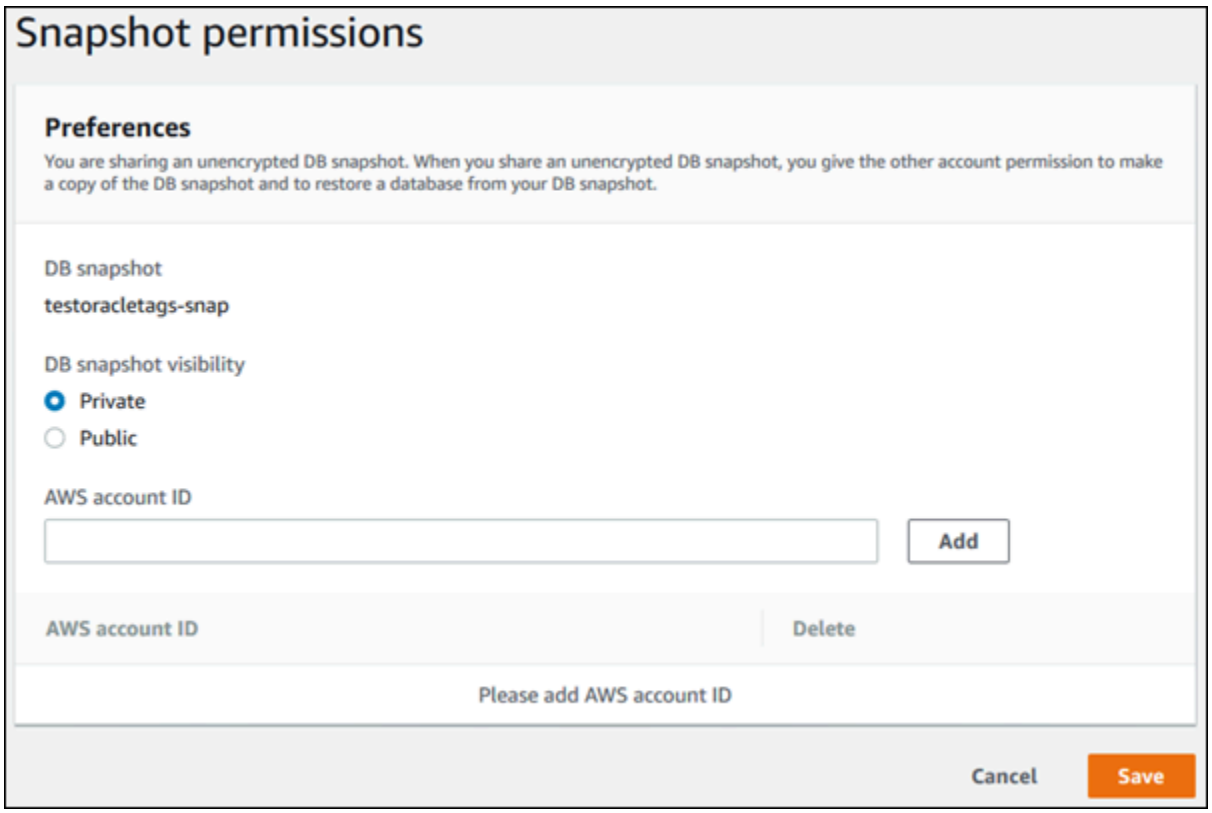
base de datos manual y tener acceso a sus datos. No comparta como Public (Pública) ninguna instantánea de base de datos manual que contenga información confidencial. Para obtener más información, consulte Uso compartido de instantáneas públicas para Amazon RDS.

- Si el original está cifrado, DB Snapshot Visibility (Visibilidad de instantánea de base de datos) se establece en Private (Privada), ya que las instantáneas cifradas no se pueden compartir como públicas.

> **Note**
>
> Las instantáneas que se hayan cifrado con la AWS KMS key predeterminada no se pueden compartir. Para obtener información acerca de cómo solucionar este problema, consulte Uso compartido de instantáneas cifradas para Amazon RDS.

6. En ID de cuenta de AWS, escriba el identificador de cuenta de Cuenta de AWS para una cuenta a la que desea permitir restaurar una instancia de base de datos desde su instantánea manual y, luego, elija Añadir. Repita esta acción para incluir identificadores de Cuenta de AWS adicionales, hasta un máximo de 20 Cuentas de AWS.

   Si comete un error al añadir un identificador de Cuenta de AWS a la lista de cuentas permitidas, puede eliminarlo de la lista seleccionando Eliminar a la derecha del identificador incorrecto de la Cuenta de AWS.



7. Después de añadir los identificadores de todas las Cuentas de AWS a las que desea permitir la restauración de la instantánea manual, elija Guardar para guardar los cambios.

AWS CLI

Para compartir una instantánea de base de datos, use el comando `aws rds modify-db-snapshot-attribute`. Use el parámetro `--values-to-add` para añadir la lista de los ID de Cuentas de AWS que tienen autorización para restaurar la instantánea manual.

Example de compartir una instantánea con una sola cuenta

En el siguiente ejemplo, se habilita el identificador `123456789012` de la Cuenta de AWS para restaurar la instantánea de base de datos denominada `db7-snapshot`.

Para Linux, macOS o:Unix

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier db7-snapshot \
--attribute-name restore \
--values-to-add 123456789012
```

En:Windows

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier db7-snapshot ^
--attribute-name restore ^
--values-to-add 123456789012
```

Example de compartir una instantánea con varias cuentas

E el siguiente ejemplo, se habilitan dos identificadores de Cuenta de AWS, `111122223333` y `444455556666`, para restaurar la instantánea de base de datos denominada `manual-snapshot1`.

Para Linux, macOS o:Unix

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier manual-snapshot1 \
--attribute-name restore \
--values-to-add {"111122223333","444455556666"}
```

En:Windows

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier manual-snapshot1 ^
--attribute-name restore ^
--values-to-add "[\"111122223333\",\"444455556666\"]"
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Para enumerar las Cuentas de AWS habilitadas para restaurar una instantánea, utilice el comando `describe-db-snapshot-attributes` de la AWS CLI.

API de RDS

También puede compartir una instantánea manual de base de datos con otras Cuentas de AWS mediante la API de Amazon RDS. Para ello, llame a la operación `ModifyDBSnapshotAttribute`. Especifique `restore` en `AttributeName` y utilice el parámetro `ValuesToAdd` para añadir la lista de los ID de las Cuentas de AWS que tienen autorización para restaurar la instantánea manual.

Para hacer que una instantánea manual sea pública y puedan restaurarla todas las Cuentas de AWS, utilice el valor `all`. Sin embargo, tenga cuidado de no añadir el valor `all` para las instantáneas manuales que contienen información confidencial que no desea que esté disponible para todas las Cuentas de AWS. Además, tampoco especifique `all` para las instantáneas cifradas, ya que dichas instantáneas no pueden hacerse públicas.

Para ver una lista de todas las Cuentas de AWS que tienen permiso para restaurar una instantánea, utilice la operación `DescribeDBSnapshotAttributes` de la API.

Uso compartido de instantáneas públicas para Amazon RDS

Puede compartir una instantánea manual sin cifrar como pública, lo que hace que esté disponible para todas las Cuentas de AWS. Al compartir una instantánea como pública, asegúrese de que no contiene información privada.

Cuando una instantánea se comparte públicamente, da todos los permisos de Cuentas de AWS tanto para copiar la instantánea como para crear las instancias de base de datos desde ella.

No se le facturará el almacenamiento de copia de seguridad de instantáneas públicas propiedad de otras cuentas. Solo se le facturan las instantáneas de su propiedad.

Si copia una instantánea pública, es el propietario de la copia. Se le facturará el almacenamiento de copia de seguridad de su copia instantánea. Si crea una Instancia de base de datos desde una instantánea pública, se le facturará de esa Instancia de base de datos. Para obtener información acerca de los precios de Amazon RDS, consulte la página del producto de Amazon RDS.

Solo puede eliminar las instantáneas públicas de su propiedad. Para eliminar una instantánea compartida o pública, debe iniciar sesión en la Cuenta de AWS propietaria de la instantánea.

Visualización de instantáneas públicas propiedad de otras Cuentas de AWS

Puede ver instantáneas públicas propiedad de otras cuentas en una Región de AWS particular en la pestaña Public (Público) de la página Snapshots (Instantáneas) de la consola de Amazon RDS. Sus instantáneas (las que pertenecen a su cuenta) no aparecen en esta pestaña.

Para ver instantáneas públicas

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Instantáneas.
3. Seleccione la pestaña Public (Público).

Aparecen las instantáneas públicas. Puede ver qué cuenta posee una instantánea pública en la columna Owner (Propietario).

> **Note**
>
> Es posible que tenga que modificar las preferencias de la página, seleccionando el icono de engranaje en la parte superior derecha de la lista Public snapshots (Instantáneas públicas), para ver esta columna.

Consulta de sus propias instantáneas públicas

Puede utilizar el siguiente comando de la AWS CLI (solo para Unix) para ver las instantáneas públicas de su Cuenta de AWS en una región de AWS concreta.

```
aws rds describe-db-snapshots --snapshot-type public --include-public |
 grep account_number
```

El resultado devuelto es similar al siguiente ejemplo si tiene instantáneas públicas.

```
"DBSnapshotArn": "arn:aws:rds:us-east-1:123456789012:snapshot:mysnapshot1",
"DBSnapshotArn": "arn:aws:rds:us-east-1:123456789012:snapshot:mysnapshot2",
```

> **Note**
>
> Es posible que vea entradas duplicadas para `DBSnapshotIdentifier` o `SourceDBSnapshotIdentifier`.

Uso compartido de instantáneas públicas de versiones obsoletas del motor de base de datos

No se admite la restauración ni la copia de instantáneas públicas a partir de versiones obsoletas del motor de base de datos.

Los motores de base de datos de RDS para Oracle y de RDS para PostgreSQL permiten actualizar directamente las versiones del motor de instantáneas de base de datos. Puede actualizar sus

instantáneas y, a continuación, volver a compartirlas públicamente. Para más información, consulte los siguientes temas:

- Actualización de una instantánea de base de datos de Oracle
- Actualización de una versión del motor de instantáneas de base de datos de PostgreSQL

Para otros motores de base de datos, realice los siguientes pasos para que su instantánea pública no compatible existente se pueda restaurar o copiar:

1. Marque la instantánea como privada.
2. Restaurare la instantánea.
3. Actualice la instancia de base de datos restaurada a una versión del motor compatible.
4. Cree una instantánea.
5. Vuelva a compartir la instantánea públicamente.

Uso compartido de instantáneas cifradas para Amazon RDS

Puede compartir instantáneas de base de datos que se han cifrado "en reposo" utilizando el algoritmo de cifrado AES-256, como se describe en Cifrado de recursos de Amazon RDS.

Cuando se comparten instantáneas cifradas, se aplican las siguientes restricciones:

- No se pueden compartir instantáneas cifradas como públicas.
- No se pueden compartir instantáneas de Oracle o Microsoft SQL Server cifradas mediante el cifrado de datos transparente (TDE).
- No se puede compartir una instantánea que se ha cifrado utilizando la clave de KMS predeterminada de la Cuenta de AWS que compartió la instantánea.

  Para obtener más información sobre la administración de claves de AWS KMS para Amazon RDS, consulte Administración de AWS KMS key.

Para solucionar el problema de la clave de KMS predeterminada, realice las siguientes tareas:

1. Creación de una clave administrada por el cliente y concesión de acceso a ella.
2. Copia y compartición de la instantánea desde la cuenta de origen.
3. Copia de la instantánea compartida en la cuenta de destino.

Creación de una clave administrada por el cliente y concesión de acceso a ella

En primer lugar, debe crear una clave KMS personalizada en la misma Región de AWS que la instantánea de base de datos cifrada. Al crear la clave administrada por el cliente, le da acceso a ella a otra Cuenta de AWS.

> **Note**
>
> También puede usar una clave de KMS de otra cuenta de AWS cuando la política de claves conceda acceso a las cuentas de origen y destino.

Para crear una clave administrada por el cliente y dar acceso a ella

1. Inicie sesión en la AWS Management Console desde la Cuenta de AWS de origen.
2. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
3. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
4. En el panel de navegación, elija Claves administradas por el cliente.
5. Elija Crear clave.
6. En la página Configurar clave:
    a. En Tipo de clave, seleccione Simétrica.
    b. En Uso de claves, seleccione Cifrar y descifrar.
    c. Expanda Advanced options (Opciones avanzadas).
    d. En Origen del material de claves, seleccione Externo.
    e. En Regionalidad, seleccione Clave de una sola región.
    f. Elija Siguiente.
7. En la página Agregar etiquetas:
    a. Para Alias, introduzca un nombre que mostrar para su clave KMS, por ejemplo **`share-snapshot`**.
    b. (Opcional) Introduzca una descripción de su clave KMS.
    c. (Opcional) Agregue etiquetas a su clave KMS.
    d. Elija Siguiente.

8. En la página Definir permisos de administración de claves, elija Siguiente.
9. En la página Definir permisos de uso de claves:
    a. En Otras Cuentas de AWS, seleccione Agregar otra Cuenta de AWS.
    b. Introduzca el ID de la Cuenta de AWS a la que desee conceder acceso.

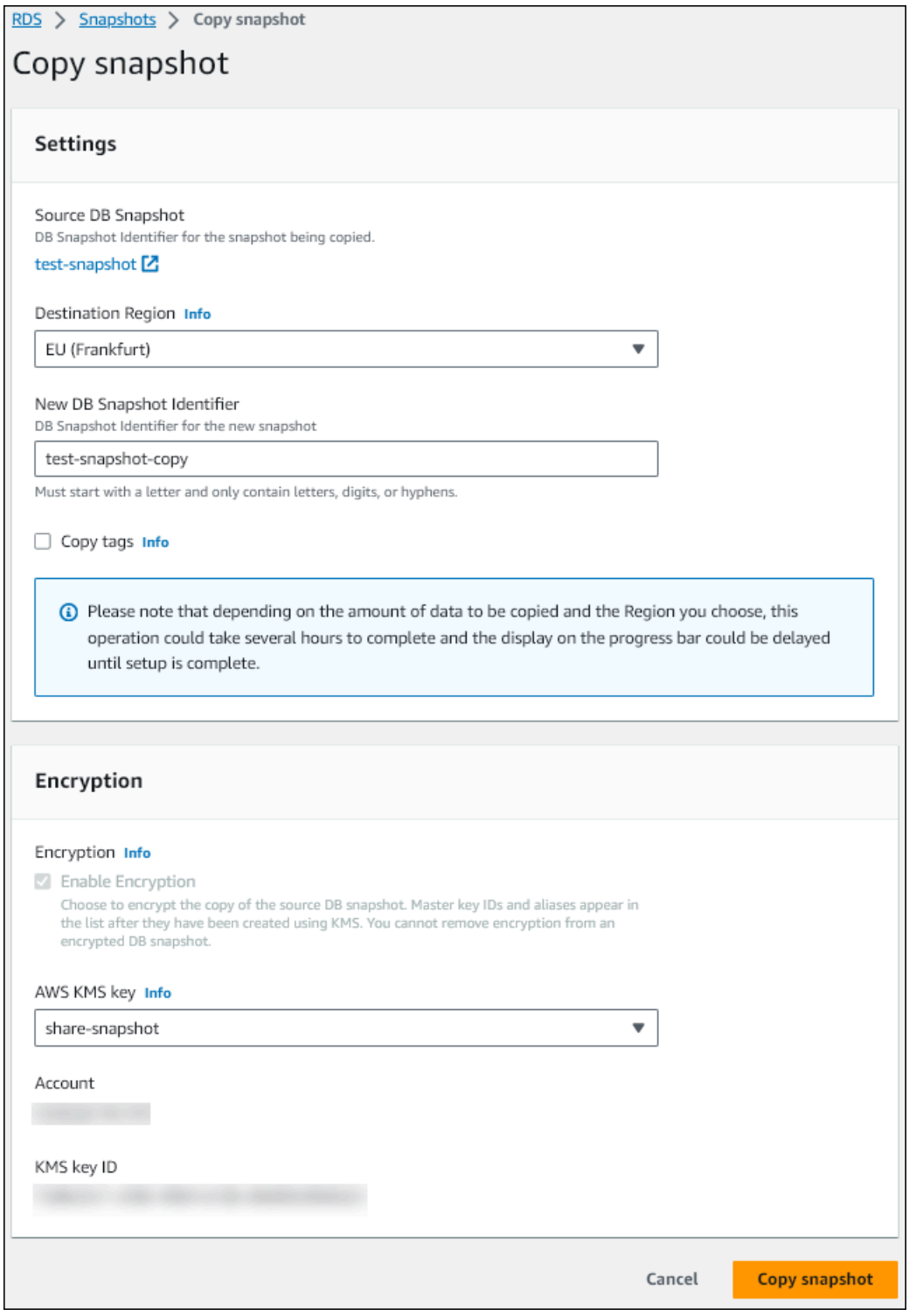
       Puede conceder acceso a varias Cuentas de AWS.
    c. Elija Siguiente.
10. Revise su clave KMS y, a continuación, seleccione Finalizar.

Copia y compartición de la instantánea desde la cuenta de origen

A continuación, debe copiar la instantánea de base de datos de origen en una nueva instantánea mediante la clave administrada por el cliente. A continuación, la debe compartir con la Cuenta de AWS de destino.

Para copiar y compartir la instantánea

1. Inicie sesión en la AWS Management Console desde la Cuenta de AWS de origen.
2. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
3. En el panel de navegación, elija Instantáneas.
4. Seleccione la instantánea de base de datos que desea copiar.
5. En Actions (Acciones), elija Copy snapshot (Copiar instantánea).
6. En la página Copiar instantánea:
    a. Para Región de destino, elija la Región de AWS en la que creó la clave administrada por el cliente en el procedimiento anterior.
    b. Introduzca el nombre de la copia de la instantánea de base de datos en Nuevo identificador de instantánea de base de datos.
    c. Para AWS KMS key, elija la clave administrada por el cliente que ha creado.



d. Elija Copy Snapshot (Copiar instantánea).

7. Cuando la copia de la instantánea esté disponible, selecciónela.
8. En Actions) (Acciones), elija Share Snapshot (Compartir instantánea).
9. En la página Permisos de la instantánea:

a. Introduzca el ID de la Cuenta de AWS con la que vaya a compartir la copia de la instantánea y, a continuación, seleccione Agregar.

b. Seleccione Save.

La instantánea ya se ha compartido.

Copia de la instantánea compartida en la cuenta de destino

Ahora puede copiar la instantánea compartida en la Cuenta de AWS de destino.

Para copiar la instantánea compartida

1. Inicie sesión en la AWS Management Console desde la Cuenta de AWS de destino.
2. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
3. En el panel de navegación, elija Instantáneas.
4. Seleccione la pestaña Compartido conmigo.
5. Seleccione la instantánea compartida.
6. En Actions (Acciones), elija Copy snapshot (Copiar instantánea).
7. Elija la configuración para copiar la instantánea como en el procedimiento anterior, pero utilice una AWS KMS key que pertenezca a la cuenta de destino.

   Elija Copy Snapshot (Copiar instantánea).

Detención del uso compartido de instantáneas para Amazon RDS

Para dejar de compartir una instantánea de base de datos, debe eliminar el permiso de la Cuenta de AWS de destino.

Consola

Para dejar de compartir una instantánea de base de datos manual con una Cuenta de AWS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).

3. Seleccione la instantánea manual que desea dejar de compartir.
4. Elija Actions (Acciones) y, a continuación, Share Snapshot (Compartir instantánea).
5. Para eliminar el permiso de una Cuenta de AWS, elija Eliminar para el identificador de cuenta de AWS correspondiente a esa cuenta en la lista de cuentas autorizadas.
6. Elija Guardar para guardar los cambios.

CLI

Para quitar un identificador de Cuenta de AWS de la lista, use el parámetro `--values-to-remove`.

Example de detener el uso compartido de instantáneas

En el siguiente ejemplo se impide que el ID 444455556666 de Cuenta de AWS se restaure desde la instantánea.

Para Linux, macOS o:Unix

```
aws rds modify-db-snapshot-attribute \
--db-snapshot-identifier manual-snapshot1 \
--attribute-name restore \
--values-to-remove 444455556666
```

En:Windows

```
aws rds modify-db-snapshot-attribute ^
--db-snapshot-identifier manual-snapshot1 ^
--attribute-name restore ^
--values-to-remove 444455556666
```

API de RDS

Para eliminar el permiso de uso compartido de una Cuenta de AWS, utilice la operación `ModifyDBSnapshotAttribute` con `AttributeName` establecido en `restore` y el parámetro `ValuesToRemove`. Para marcar una instantánea manual como privada, elimine el valor `all` de la lista de valores del atributo `restore`.

Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS

Puede exportar datos de instantáneas de bases de datos a un bucket de Amazon S3. El proceso de exportación se ejecuta en segundo plano y no afecta al rendimiento de la base de datos activa.

Al exportar una instantánea de base de datos, Amazon RDS extrae los datos de la instantánea y los almacena en un bucket de Amazon S3. Los datos se almacenan en formato Apache Parquet comprimido y consistente.

Puede exportar todos los tipos de instantáneas de base de datos, como instantáneas manuales, instantáneas del sistema automatizadas o instantáneas creadas por el servicio de AWS Backup. De forma predeterminada, se exportan todos los datos de la instantánea. Sin embargo, también puede optar por exportar conjuntos específicos de bases de datos, esquemas o tablas.

Después de exportar los datos, puede analizar los datos exportados directamente con herramientas como Amazon Athena o Amazon Redshift Spectrum. Para obtener más información sobre cómo utilizar Athena para leer los datos de Parquet, consulte Parquet SerDe en Guía del usuario de Amazon Athena. Para obtener más información sobre cómo utilizar Redshift Spectrum para leer datos de Parquet, vea Uso de COPY con formatos de datos de columnas en la Guía para desarrolladores de bases de datos Amazon Redshift.

> **Warning**
>
> No puede restaurar los datos de instantáneas exportados de S3 a una nueva instancia de base de datos ni importar datos de instantáneas de S3 a una instancia de base de datos existente. No obstante, puede procesar los datos mediante Amazon Athena o Redshift Spectrum para el análisis. Además, puede utilizar AWS Glue para transformar los datos y, a continuación, importarlos a Amazon RDS mediante herramientas como AWS DMS o scripts personalizados.

Para obtener más información sobre cómo exportar instantáneas de bases de datos a Amazon S3, consulte los siguientes temas.

Temas

- Supervisión de las exportaciones de instantáneas para Amazon RDS

- Cancelación de una tarea de exportación de instantáneas para Amazon RDS
- Mensajes de error para tareas de exportación de Amazon S3 para Amazon RDS
- Solución de problemas de errores de permisos de RDS para PostgreSQL
- Convenciones de nomenclatura de archivos para exportaciones a Amazon S3 para Amazon RDS
- Conversión de datos al exportar a un bucket de Amazon S3 para Amazon RDS

Información general acerca de la exportación de datos de instantáneas

Utilice el siguiente proceso para exportar datos de instantáneas de base de datos a un bucket de Amazon S3. Para obtener más detalles, consulte las siguientes secciones.

1. Identifique la instantánea que desee exportar.

   Utilice una instantánea automática o manual ya existente, o bien cree una instantánea manual de una instancia de base de datos o un clúster de base de datos multi-AZ.

2. Configure el acceso al bucket de Amazon S3.

   Un bucket es un contenedor de objetos o archivos de Amazon S3. Para proporcionar la información necesario para obtener acceso a un bucket, siga los siguientes pasos:

   a. Identifique el bucket de S3 al que se va a exportar la instantánea. El bucket de S3 debe estar en la misma región de AWS que la instantánea. Para obtener más información, consulte Identificación del bucket de Amazon S3 para exportación.

   b. Cree un rol de AWS Identity and Access Management (IAM) que conceda a la tarea de exportación de instantáneas acceso al bucket de S3. Para obtener más información, consulte Proporcionar acceso a un bucket de Amazon S3 mediante un rol de IAM.

3. Cree una AWS KMS key de cifrado simétrica para el cifrado del lado del servidor. La tarea de exportación de instantáneas utiliza la clave de KMS para configurar el cifrado del lado del servidor de AWS KMS al escribir los datos de exportación en S3.

   La política de clave KMS debe incluir los permisos `kms:CreateGrant` y `kms:DescribeKey`. Para obtener más información acerca del uso de claves KMS en Amazon RDS, consulte Administración de AWS KMS key.

   Además, si tiene una instrucción deny en la política de claves KMS, asegúrese de excluir explícitamente la entidad principal del servicio de AWS `export.rds.amazonaws.com`.

Puede utilizar una clave de KMS en su cuenta de AWS o puede utilizar una clave KMS en diversas cuentas. Para obtener más información, consulte Uso de una AWS KMS key en diversas cuentas para cifrar las exportaciones de Amazon S3.

4. Exporte la instantánea a Amazon S3 mediante la consola o el comando `start-export-task` de la CLI. Para obtener más información, consulte Exportación de una instantánea de base de datos a un bucket de Amazon S3.
5. Para obtener acceso a los datos exportados al bucket de Amazon S3, consulte Carga, descarga y administración de objetos en la Guía del usuario de Amazon Simple Storage Service.

Configuración del acceso a un bucket de Amazon S3

Para exportar los datos de una instantánea de base de datos a un archivo de Amazon S3, primero debe conceder permiso a la instantánea para obtener acceso al bucket de Amazon S3. Luego cree un rol de IAM para permitir que el servicio de Amazon RDS escriba en el bucket de Amazon S3.

Temas

- Identificación del bucket de Amazon S3 para exportación
- Proporcionar acceso a un bucket de Amazon S3 mediante un rol de IAM
- Uso de un bucket de Amazon S3 en diversas cuentas
- Uso de una AWS KMS key en diversas cuentas para cifrar las exportaciones de Amazon S3

Identificación del bucket de Amazon S3 para exportación

Identifique el bucket de Amazon S3 al que se exportará la instantánea de base de datos. Utilice un bucket de S3 ya existente, o bien cree un bucket S3 nuevo.

> **Note**
>
> El bucket de S3 al que se realizará la exportación debe estar en la misma región de AWS que la instantánea.

Para obtener más información acerca de cómo trabajar con buckets de Amazon S3, consulte lo siguiente en Guía del usuario de Amazon Simple Storage Service:

- ¿Cómo se consultan las propiedades de un bucket de S3?
- ¿Cómo puedo habilitar el cifrado predeterminado para un bucket de Amazon S3?
- ¿Cómo se puede crear un bucket de S3?

Proporcionar acceso a un bucket de Amazon S3 mediante un rol de IAM

Antes de exportar datos de instantáneas de bases de datos a Amazon S3, conceda a las tareas de exportación de instantáneas permiso de acceso de escritura al bucket de Amazon S3.

Para conceder este permiso, cree una política de IAM que proporcione acceso al bucket y cree un rol de IAM y adjunte la política al rol. Más adelante, asignará el rol de IAM a la tarea de exportación de instantáneas.

Para obtener más información sobre el uso de IAM con Amazon S3, consulte Identity and Access Management en Amazon S3 en la Guía del usuario de Amazon S3.

> **Important**
>
> Si prevé utilizar la AWS Management Console para exportar la instantánea, puede elegir crear la política de IAM y el rol automáticamente al exportar la instantánea. Para obtener instrucciones, consulte Exportación de una instantánea de base de datos a un bucket de Amazon S3.

Para dar a las tareas de instantáneas de base de datos acceso a Amazon S3

1. Cree una política de IAM. Esta política proporciona los permisos de bucket y objeto que permiten a la tarea de exportación de instantáneas obtener acceso a Amazon S3.

   En la política, incluya las siguientes acciones obligatorias para permitir transferir archivos desde Amazon RDS a un bucket de S3:

   - `s3:PutObject*`
   - `s3:GetObject*`
   - `s3:ListBucket`
   - `s3:DeleteObject*`
   - `s3:GetBucketLocation`

En la política, incluya los siguientes recursos para identificar el bucket de S3 y los objetos incluidos en él. En la siguiente lista de recursos se muestra el formato de nombre de recurso de Amazon (ARN) para obtener acceso a Amazon S3.

- `arn:aws:s3:::amzn-s3-demo-bucket`
- `arn:aws:s3:::amzn-s3-demo-bucket/*`

Para obtener más información sobre cómo crear una política de IAM para Amazon RDS, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM. Consulte también el Tutorial: Crear y asociar su primera política administrada por el cliente en la Guía del usuario de IAM.

El siguiente comando de la AWS CLI crea una política de IAM denominada `ExportPolicy` con estas opciones. Otorga acceso a un bucket denominado *amzn-s3-demo-bucket*.

> **Note**
>
> Después de crear la política, apunte el ARN de esta. Cuando asocia la política a un rol de IAM, necesita el ARN para realizar un paso posterior.

```
aws iam create-policy  --policy-name ExportPolicy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExportPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject*",
                "s3:ListBucket",
                "s3:GetObject*",
                "s3:DeleteObject*",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
```

```
        }
    ]
}'
```

2. Cree un rol de IAM que Amazon RDS pueda asumir en su nombre para acceder a sus buckets de Amazon S3. Para obtener más información, vea Crear un rol para delegar permisos a un IAM usuario en Guía del usuario de IAM.

   En el siguiente ejemplo se muestra cómo se usa el comando de la AWS CLI para crear un rol denominado `rds-s3-export-role`.

```
aws iam create-role  --role-name rds-s3-export-role  --assume-role-policy-document
 '{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
           "Service": "export.rds.amazonaws.com"
         },
        "Action": "sts:AssumeRole"
      }
    ]
  }'
```

3. Asocie la política de IAM que creó al rol de IAM creado.

   El siguiente comando de la AWS CLI asocia la política creada anteriormente al rol denominado `rds-s3-export-role`. Sustituya *`your-policy-arn`* por el ARN de la política que ha apuntado en el paso anterior.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-
export-role
```

Uso de un bucket de Amazon S3 en diversas cuentas

Puede utilizar buckets de Amazon S3 en cuentas de AWS. Para utilizar un bucket en diversas cuentas, agregue una política de bucket para permitir el acceso al rol de IAM que está utilizando para las exportaciones de S3. Para obtener más información, consulte el Ejemplo 2: Propietario del bucket que concede permisos de bucket en diversas cuentas.

Adjunte una política de bucket a su bucket, como se muestra en el siguiente ejemplo.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/Admin"
            },
            "Action": [
                "s3:PutObject*",
                "s3:ListBucket",
                "s3:GetObject*",
                "s3:DeleteObject*",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        }
    ]
}
```

Uso de una AWS KMS key en diversas cuentas para cifrar las exportaciones de Amazon S3

Puede utilizar una AWS KMS key en diversas cuentas para cifrar las exportaciones de Amazon S3. En primer lugar, agregue una política de claves a la cuenta local y, a continuación, agregue las políticas de IAM en la cuenta externa. Para obtener más información, consulte Allowing users in other accounts to use a KMS key (Permitir que los usuarios de otras cuentas utilicen una clave KMS).

Para utilizar una clave KMS en diversas cuentas

1. Agregue una política de claves a la cuenta local.

El siguiente ejemplo proporciona `ExampleRole` y `ExampleUser` en la cuenta externa 444455556666 permisos en la cuenta local 123456789012.

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::444455556666:role/ExampleRole",
            "arn:aws:iam::444455556666:user/ExampleUser"
        ]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
```

2. Agregar políticas de IAM a la cuenta externa.

   La siguiente política de IAM de ejemplo permite a la entidad principal utilizar la clave KMS en la cuenta 123456789012 para operaciones criptográficas. Para conceder este permiso a `ExampleRole` y `ExampleUser` de la cuenta 444455556666, adjunte la política en esa cuenta.

```
{
    "Sid": "Allow use of KMS key in account 123456789012",
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant"
    ],
```

```
    "Resource": "arn:aws:kms:us-
west-2:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Exportación de una instantánea de base de datos a un bucket de Amazon S3

Puede tener hasta cinco tareas de exportación de instantáneas de base de datos en curso por Cuenta de AWS.

> **Note**
>
> La exportación de instantáneas de RDS puede tardar un tiempo en función del tipo y tamaño de la base de datos. La tarea de exportación primero restaura y escala toda la base de datos antes de extraer los datos a Amazon S3. El progreso de la tarea durante esta fase se muestra como Starting (Iniciándose). Cuando la tarea cambia a exportar datos a S3, el progreso se muestra como In progress (En curso).
> El tiempo que tarda la exportación en completarse depende de los datos almacenados en la base de datos. Por ejemplo, las tablas con columnas de índice o claves primarias numéricas bien distribuidas se exportarán más rápido. Las tablas que no contienen una columna adecuada para la partición y las tablas con un solo índice en una columna basada en cadenas tardarán más tiempo. Este tiempo de exportación más prolongado se produce porque la exportación utiliza un proceso de subproceso único más lento.

Puede exportar una instantánea de base de datos a Amazon S3 mediante la AWS Management Console, la AWS CLI o la API de RDS. Para exportar una instantánea de base de datos a un bucket de Amazon S3 en diversas cuentas, utilice la AWS CLI o la API de RDS.

Si utiliza una función Lambda para exportar una instantánea, agregue la acción `kms:DescribeKey` a la política de la función Lambda. Para obtener más información, consulte Permisos de AWS Lambda.

Consola

La opción de la consola Export to Amazon S3 (Exportar a Amazon S3) solo aparece para las instantáneas que se pueden exportar a Amazon S3. Es posible que una instantánea no esté disponible para la exportación debido a las siguientes razones:

- El motor de base de datos no es compatible con la exportación de S3.
- La versión del motor de base de datos no es compatible con la exportación de S3.
- La exportación de S3 no se admite en la región de AWS donde se creó la instantánea.

Para exportar una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. En las pestañas, elija el tipo de instantánea que desee exportar.
4. En la lista de instantáneas, elija la instantánea que desee exportar.
5. En Actions (Acciones), seleccione Export to Amazon S3 (Exportar a Amazon S3).

   Se visualizará la ventana Export to Amazon S3 (Exportar a Amazon S3).
6. En Export Identifier (Identificador de exportación), escriba un nombre para identificar la tarea de exportación. Este valor también se utiliza para el nombre del archivo creado en el bucket de S3.
7. Elija los datos que desea exportar:

   - Seleccione All (Todo) para exportar todos los datos de la instantánea.
   - Seleccione Partial (Parcial) para exportar partes específicas de la instantánea. Para identificar qué partes de la instantánea exportar, introduzca una o más bases de datos, esquemas o tablas para Identifiers (Identificadores), separadas por espacios.

     Use el siguiente formato:

     ```
     database[.schema][.table] database2[.schema2][.table2] ... databasen[.scheman]
     [.tablen]
     ```

     Por ejemplo:

     ```
     mydatabase mydatabase2.myschema1 mydatabase2.myschema2.mytable1
      mydatabase2.myschema2.mytable2
     ```
8. Para el S3 bucket (Bucket de S3), elija el bucket al que desee realizar la exportación.

   Para asignar los datos exportados a la ruta de una carpeta en el bucket de S3, escriba la ruta opcional para el S3 prefix (Prefijo de S3).

9. Para el rol de IAM, elija un rol que le conceda acceso de escritura al bucket de S3 elegido o cree un nuevo rol.

   - Si ha creado un rol siguiendo los pasos indicados en Proporcionar acceso a un bucket de Amazon S3 mediante un rol de IAM, elija dicho rol.
   - Si no ha creado un rol que le conceda acceso de escritura al bucket de S3 elegido, elija Create a new role (Crear un nuevo rol) para crear el rol automáticamente. A continuación, escriba un nombre para el rol en el IAM role name (Nombre del rol de IAM).

10. En AWS KMS key, ingrese el ARN de la clave que debe utilizarse para cifrar los datos exportados.
11. Elija Export to Amazon S3 (Exportar a Amazon S3).

AWS CLI

Para exportar una instantánea de base de datos a Amazon S3 mediante la AWS CLI, ejecute el comando start-export-task con las siguientes opciones obligatorias:

- `--export-task-identifier`
- `--source-arn`
- `--s3-bucket-name`
- `--iam-role-arn`
- `--kms-key-id`

En los siguientes ejemplos, la tarea de exportación de instantáneas se denomina *my-snapshot-export*, y exporta una instantánea a un bucket de S3 denominado *amzn-s3-demo-bucket*.

Example

Para Linux, macOS o Unix:

```
aws rds start-export-task \
    --export-task-identifier my-snapshot-export \
    --source-arn arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name \
    --s3-bucket-name amzn-s3-demo-bucket \
    --iam-role-arn iam-role \
    --kms-key-id my-key
```

Para Windows:

```
aws rds start-export-task ^
    --export-task-identifier my-snapshot-export ^
    --source-arn arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name ^
    --s3-bucket-name amzn-s3-demo-bucket ^
    --iam-role-arn iam-role ^
    --kms-key-id my-key
```

A continuación, se muestra un resultado de ejemplo.

```
{
    "Status": "STARTING",
    "IamRoleArn": "iam-role",
    "ExportTime": "2019-08-12T01:23:53.109Z",
    "S3Bucket": "my-export-bucket",
    "PercentProgress": 0,
    "KmsKeyId": "my-key",
    "ExportTaskIdentifier": "my-snapshot-export",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-11-13T19:46:00.173Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:snapshot-name"
}
```

Para proporcionar la ruta de una carpeta del bucket S3 para la exportación de instantáneas, incluya la opción `--s3-prefix` en el comando start-export-task.

API de RDS

Para exportar una instantánea de base de datos a Amazon S3 con la API de Amazon RDS, ejecute la operación StartExportTask con los siguientes parámetros obligatorios:

- `ExportTaskIdentifier`
- `SourceArn`
- `S3BucketName`
- `IamRoleArn`
- `KmsKeyId`

Disponibilidad en regiones y versiones

La disponibilidad y compatibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de la exportación de instantáneas a S3, consulte Regiones y motores de base de datos admitidos para exportar instantáneas a S3 en Amazon RDS.

Limitaciones

Exportar datos de instantáneas de base de datos a Amazon S3 tiene las siguientes limitaciones:

- No puede ejecutar varias tareas de exportación para la misma instantánea de base de datos simultáneamente. Esto es cierto para las exportaciones completas y parciales.
- No se admite la exportación de instantáneas de base de datos que utilizan almacenamiento magnético.
- Las exportaciones a S3 no admiten prefijos S3 que contengan dos puntos (:).
- Los siguientes caracteres en la ruta del archivo S3 se convierten en guiones bajos (_) durante la exportación:

```
\ ` " (space)
```

- Si una base de datos, esquema o tabla tiene caracteres en su nombre distintos del siguiente, no se admite la exportación parcial. Sin embargo, puede exportar toda la instantánea de base de datos.
  - Letras latinas (A–Z)
  - Dígitos (0–9)
  - Símbolo de dólar ($)
  - Guion bajo (_)
- No se admiten espacios ( ) ni determinados caracteres en los nombres de columna de las tablas de bases de datos. Las tablas con los siguientes caracteres en los nombres de columna se omiten durante la exportación:

```
, ; { } ( ) \n \t = (space)
```

- Las tablas con barras diagonales (/) en el nombre se omiten durante la exportación.
- Las tablas temporales y no registradas de RDS para PostgreSQL se omiten durante la exportación.
- Si los datos contienen un objeto grande, como un BLOB o CLOB, cercano o superior a 500 MB, se producirá un error en la exportación.

- Si una tabla contiene una fila grande cercana o superior a 2 GB, la tabla se omite durante la exportación.
- Para exportaciones parciales, la lista `ExportOnly` tiene un tamaño máximo de 200 KB.
- Es muy recomendable que utilice un nombre exclusivo para cada tarea de exportación. Si no utiliza un nombre de tarea exclusivo, es posible que aparezca el siguiente mensaje de error como el que sigue:

  exportTaskAlreadyExistsFault: Se ha producido un error (exportTaskAlReadyExists) al llamar a la operación StartExportTask: la tarea de exportación con ID *xxxxx* ya existe.
- Puede eliminar una instantánea mientras exporta los datos a S3, pero se le seguirán cobrando los costos de almacenamiento de esa instantánea hasta que se complete la tarea de exportación.
- No puede restaurar los datos de instantáneas exportados de S3 a una nueva instancia de base de datos ni importar datos de instantáneas de S3 a una instancia de base de datos existente.
- Puede tener hasta cinco tareas de exportación de instantáneas de base de datos en curso por Cuenta de AWS.
- Para exportar una instantánea de base de datos a un bucket de Amazon S3 en diversas cuentas, debe usar la AWS CLI o la API de RDS.
- Una vez que Amazon RDS complete una tarea de exportación, es posible que tenga que esperar un poco para iniciar otra tarea de exportación desde la misma instantánea de base de datos.
- No se pueden exportar vistas ni vistas materializadas.
- La exportación de RDS a S3 no admite el control de acceso basado en etiquetas para Malware Protection for S3 de GuardDuty.

Supervisión de las exportaciones de instantáneas para Amazon RDS

Puede monitorear las exportaciones de instantáneas de bases de datos mediante AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para monitorear las exportaciones de instantáneas de bases de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).

3. Para ver la lista de exportaciones de instantáneas, seleccione la pestaña Exports in Amazon S3 (Exportaciones en Amazon S3).
4. Para ver información acerca de la exportación de una instantánea específica, elija la tarea de exportación.

AWS CLI

Para monitorear exportaciones de instantáneas de bases de datos mediante la AWS CLI, ejecute el comando describe-export-tasks .

En el ejemplo siguiente se muestra cómo mostrar la información actual acerca de todas las exportaciones de instantáneas.

Example

```
aws rds describe-export-tasks

{
    "ExportTasks": [
        {
            "Status": "CANCELED",
            "TaskEndTime": "2019-11-01T17:36:46.961Z",
            "S3Prefix": "something",
            "ExportTime": "2019-10-24T20:23:48.364Z",
            "S3Bucket": "amzn-s3-demo-bucket",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/K7MDENG/
bPxRfiCYEXAMPLEKEY",
            "ExportTaskIdentifier": "anewtest",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
            "TaskStartTime": "2019-10-25T19:10:58.885Z",
            "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:parameter-
groups-test"
        },
{
            "Status": "COMPLETE",
            "TaskEndTime": "2019-10-31T21:37:28.312Z",
            "WarningMessage": "{\"skippedTables\":[],\"skippedObjectives\":[],\"general
\":[{\"reason\":\"FAILED_TO_EXTRACT_TABLES_LIST_FOR_DATABASE\"}]}",
            "S3Prefix": "",
            "ExportTime": "2019-10-31T06:44:53.452Z",
```

```
            "S3Bucket": "amzn-s3-demo-bucket1",
            "PercentProgress": 100,
            "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/2Zp9Utk/
h3yCo8nvbEXAMPLEKEY",
            "ExportTaskIdentifier": "thursday-events-test",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 263,
            "TaskStartTime": "2019-10-31T20:58:06.998Z",
            "SourceArn":
 "arn:aws:rds:AWS_Region:123456789012:snapshot:rds:example-1-2019-10-31-06-44"
        },
        {
            "Status": "FAILED",
            "TaskEndTime": "2019-10-31T02:12:36.409Z",
            "FailureCause": "The S3 bucket edgcuc-export isn't located in the current
 AWS Region. Please, review your S3 bucket name and retry the export.",
            "S3Prefix": "",
            "ExportTime": "2019-10-30T06:45:04.526Z",
            "S3Bucket": "amzn-s3-demo-bucket2",
            "PercentProgress": 0,
            "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/2Zp9Utk/
h3yCo8nvbEXAMPLEKEY",
            "ExportTaskIdentifier": "wednesday-afternoon-test",
            "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
            "TotalExtractedDataInGB": 0,
            "TaskStartTime": "2019-10-30T22:43:40.034Z",
            "SourceArn":
 "arn:aws:rds:AWS_Region:123456789012:snapshot:rds:example-1-2019-10-30-06-45"
        }
    ]
}
```

Para mostrar información sobre una exportación de instantáneas específica, incluya la opción `--export-task-identifier` con el comando `describe-export-tasks`. Para filtrar la salida, incluya la opción `--Filters`. Para obtener más opciones, consulte el comando describe-export-tasks.

API de RDS

Para mostrar información sobre las exportaciones de instantáneas de bases de datos mediante la API de Amazon RDS, ejecute la operación DescribeExportTasks.

Para realizar un seguimiento del flujo de trabajo de exportación o para iniciar otro flujo de trabajo, puede suscribirse a temas de Amazon Simple Notification Service. Para obtener más información sobre Amazon SNS, consulte Uso de notificaciones de eventos de Amazon RDS.

Cancelación de una tarea de exportación de instantáneas para Amazon RDS

Puede cancelar una tarea de exportación de instantáneas de bases de datos mediante AWS Management Console, la AWS CLI o la API de RDS.

> **Note**
>
> La cancelación de una tarea de exportación de instantáneas no elimina los datos exportados a Amazon S3. Para obtener información acerca de cómo eliminar los datos mediante la consola, consulte ¿Cómo se eliminan objetos de un bucket de S3? Para eliminar los datos mediante la CLI, ejecute el comando delete-object.

Consola

Para cancelar una tarea de exportación de una instantánea

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Seleccione la pestaña Exports in Amazon S3 (Exportaciones en Amazon S3).
4. Elija la tarea de exportación de instantáneas que desee cancelar.
5. Elija Cancel.
6. Seleccione Cancel export task (Cancelar tarea de exportación) en la página de confirmación.

AWS CLI

Para cancelar una tarea de exportación de instantáneas mediante la AWS CLI, ejecute el comando cancel-export-task . El comando requiere la opción `--export-task-identifier`.

Example

```
aws rds cancel-export-task --export-task-identifier my_export
{
    "Status": "CANCELING",
    "S3Prefix": "",
    "ExportTime": "2019-08-12T01:23:53.109Z",
    "S3Bucket": "amzn-s3-demo-bucket",
    "PercentProgress": 0,
    "KmsKeyId": "arn:aws:kms:AWS_Region:123456789012:key/K7MDENG/bPxRfiCYEXAMPLEKEY",
    "ExportTaskIdentifier": "my_export",
    "IamRoleArn": "arn:aws:iam::123456789012:role/export-to-s3",
    "TotalExtractedDataInGB": 0,
    "TaskStartTime": "2019-11-13T19:46:00.173Z",
    "SourceArn": "arn:aws:rds:AWS_Region:123456789012:snapshot:export-example-1"
}
```

API de RDS

Para cancelar una tarea de exportación de instantáneas mediante la API de Amazon RDS, ejecute la operación CancelExportTask con el parámetro `ExportTaskIdentifier`.

Mensajes de error para tareas de exportación de Amazon S3 para Amazon RDS

En la tabla siguiente se describen los mensajes que se devuelven cuando se producen errores en las tareas de exportación de Amazon S3.

Mensaje de error	Descripción
Se ha producido un error interno desconocido.	La tarea no se pudo completar debido a un error, excepción o falla desconocidos.
Ocurrió un error interno desconocido al escribir los metadatos de la tarea de exportación en el bucket de S3 [nombre del bucket].	La tarea no se pudo completar debido a un error, excepción o falla desconocidos.
La exportación de RDS no pudo escribir los metadatos de la tarea de exportaci	La tarea de exportación asume el rol de IAM para validar si está permitido escribir metadatos en el

Mensaje de error	Descripción
ón porque no puede asumir el rol de IAM [ARN de rol].	bucket de S3. Si la tarea no puede asumir su rol de IAM, muestra un error.
La exportación de RDS no pudo escribir los metadatos de la tarea de exportaci ón en el bucket de S3 [nombre del bucket] que utiliza el rol de IAM [ARN de rol] con la clave KMS [ID de clave]. Código de error: [código de error]	Faltan uno o más permisos, por lo que la tarea de exportación no puede acceder al bucket de S3. Este mensaje de error aparece cuando se recibe uno de los siguientes códigos de error: • `AWSSecurityTokenServiceException` con el código de error `AccessDenied` • `AmazonS3Exception` con el código de error `NoSuchBucket` , `AccessDenied` , `KMS.KMSInvalidStateException` , `403 Forbidden` , o `KMS.DisabledException` Estos códigos de error indican que la configuración del rol de IAM, el bucket de S3 o la clave KMS es incorrecta.
El rol de IAM [ARN de rol] no está autorizado para llamar a [acción de S3] en el bucket de S3 [nombre del bucket]. Revise sus permisos y vuelva a intentar la exportación.	La política de IAM está mal configurada. Falta el permiso para la acción específica de S3 en el bucket de S3, que provoca que falle la tarea de exportación.
Error en la verificación de claves KMS Verifique las credenciales de la clave KMS e inténtelo de nuevo.	Error en la verificación de credenciales de la clave KMS.
Error en la verificación de credencia les de S3. Verifique los permisos de su bucket de S3 y de la política de IAM.	Error en la verificación de credenciales de S3.

Mensaje de error	Descripción
El bucket de S3 [nombre del bucket] no es válido. O no se encuentra en la Región de AWS actual o no existe. Revise el nombre del bucket de S3 e intente hacer la exportación de nuevo.	El bucket de S3 no es válido.
El bucket de S3 [nombre del bucket] no se encuentra en la Región de AWS actual. Revise el nombre del bucket de S3 e intente hacer la exportación de nuevo.	El bucket de S3 está en la Región de AWS equivocada.

Solución de problemas de errores de permisos de RDS para PostgreSQL

Al exportar bases de datos PostgreSQL a Amazon S3, es posible que vea un error `PERMISSIONS_DO_NOT_EXIST` que indica que se omitieron ciertas tablas. Esto suele deberse a que el superusuario, que se especifica al crear la base de datos, no tiene permisos para acceder a dichas tablas.

Para corregir este error, ejecute el siguiente comando:

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA schema_name TO superuser_name
```

Para obtener más información sobre los privilegios de superusuario, consulte Privilegios de la cuenta de usuario maestro.

Convenciones de nomenclatura de archivos para exportaciones a Amazon S3 para Amazon RDS

Los datos exportados para tablas específicas se almacenan en el formato *base_prefix*/*files*, donde el prefijo base es el siguiente:

```
export_identifier/database_name/schema_name.table_name/
```

Por ejemplo:

```
export-1234567890123-459/rdststdb/rdststdb.DataInsert_7ADB5D19965123A2/
```

Hay dos convenciones para la forma en que se denominan los archivos.

- Convención actual:

  ```
  batch_index/part-partition_index-random_uuid.format-based_extension
  ```

  El índice de lote es un número secuencial que representa un lote de datos leídos desde la tabla. Si no podemos dividir su tabla en pequeños fragmentos para exportarlos en paralelo, habrá varios índices de lote. Lo mismo ocurre si la tabla está dividida en varias tablas. Habrá varios índices de lote, uno para cada una de las particiones de la tabla principal.

  Si podemos dividir su tabla en pequeños fragmentos para que se lean en paralelo, solo estará la carpeta de índices de lote 1.

  Dentro de la carpeta de índices de lote, habrá uno o varios archivos Parquet que contienen los datos de la tabla. El prefijo del nombre de archivo Parquet es `part-`*`partition_index`*. Si la tabla está particionada, habrá varios archivos que comiencen por el índice de partición `00000`.

  Puede haber huecos en la secuencia del índice de partición. Esto sucede porque cada partición se obtiene de una consulta por rangos de la tabla. Si no hay datos en el rango de esa partición, se omite ese número secuencial.

  Por ejemplo, supongamos que la columna `id` es la clave principal de la tabla y que sus valores mínimo y máximo son `100` y `1000`. Al intentar exportar esta tabla con nueve particiones, la leemos con consultas paralelas como las siguientes:

  ```
  SELECT * FROM table WHERE id <= 100 AND id < 200
  SELECT * FROM table WHERE id <= 200 AND id < 300
  ```

  Esto debería generar nueve archivos, del `part-00000-`*`random_uuid`*`.gz.parquet` al `part-00008-`*`random_uuid`*`.gz.parquet`. Sin embargo, si no hay filas con ID entre `200` y `350`, una de las particiones completadas estará vacía y no se creará ningún archivo para ella. En el ejemplo anterior, no se crea `part-00001-`*`random_uuid`*`.gz.parquet`.
- Convención anterior:

  ```
  part-partition_index-random_uuid.format-based_extension
  ```

Es igual a la convención actual, pero sin el prefijo *batch_index*, por ejemplo:

```
part-00000-c5a881bb-58ff-4ee6-1111-b41ecff340a3-c000.gz.parquet
part-00001-d7a881cc-88cc-5ab7-2222-c41ecab340a4-c000.gz.parquet
part-00002-f5a991ab-59aa-7fa6-3333-d41eccd340a7-c000.gz.parquet
```

La convención de nomenclatura de archivos está sujeta a cambios. Por lo tanto, cuando lea tablas de destino, recomendamos que lea todo lo que hay dentro del prefijo base de la tabla.

Conversión de datos al exportar a un bucket de Amazon S3 para Amazon RDS

Cuando exporta una instantánea de base de datos a un bucket de Amazon S3, Amazon RDS convierte los datos al formato Parquet, y exporta y almacena los datos en dicho formato. Para obtener más información sobre Parquet, consulte el sitio web de Apache Parquet.

Parquet almacena todos los datos como uno de los siguientes tipos primitivos:

- BOOLEANO
- INT32
- INT64
- INT96
- FLOAT
- DOUBLE
- BYTE_ARRAY: matriz de bytes de longitud variable, también conocida como binario.
- FIXED_LEN_BYTE_ARRAY. matriz de bytes de longitud fija utilizada cuando los valores tienen un tamaño constante.

Los tipos de datos Parquet son pocos para reducir la complejidad de leer y escribir el formato. Parquet proporciona tipos lógicos para ampliar los tipos primitivos. Un tipo lógico se implementa como una anotación con los datos en un campo de metadatos `LogicalType`. La anotación de tipo lógico explica cómo interpretar el tipo primitivo.

Cuando el tipo lógico `STRING` anota un tipo `BYTE_ARRAY`, indica que la matriz de bytes debe interpretarse como una cadena de caracteres codificada UTF-8. Cuando se complete la tarea de

exportación, Amazon RDS le notificará si se ha producido alguna conversión de cadena. Los datos subyacentes exportados siempre son los mismos que los datos del origen. Sin embargo, debido a la diferencia de codificación en UTF-8, algunos caracteres pueden parecer diferentes a los del origen cuando se leen en herramientas como Athena.

Para obtener más información, consulte Definiciones de tipos lógicos de Parquet en la documentación de Parquet.

Temas

- Mapeo del tipo de datos MySQL y MariaDB con Parquet
- Mapeo de tipos de datos PostgreSQL con Parquet

Mapeo del tipo de datos MySQL y MariaDB con Parquet

En la siguiente tabla se muestra el mapeo de los tipos de datos MySQL y MariaDB con los tipos de datos Parquet cuando los datos se convierten y se exportan a Amazon S3.

Tipo de datos de origen	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de conversión
Tipos de datos numéricos			
BIGINT	INT64		
BIGINT UNSIGNED	FIXED_LEN _BYTE_ARRAY(9)	DECIMAL(20,0)	Parquet solo admite tipos firmados, por lo que el mapeo requiere un byte adicional (8 más 1) para almacenar el tipo BIGINT_UNSIGNED.
BIT	BYTE_ARRAY		
DECIMAL	INT32	DECIMAL (p,s)	Si el valor de origen es inferior a 2^{31}, se almacena como INT32.

Tipo de datos de origen	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de conversión
	INT64	DECIMAL (p,s)	Si el valor de origen es 2^{31} o superior, pero inferior a 2^{63}, se almacena como INT64.
	FIXED_LEN _BYTE_ARRAY(N)	DECIMAL (p,s)	Si el valor de origen es 2^{63} o superior, se almacena como FIXED_LEN _BYTE_ARRAY(N).
	BYTE_ARRAY	STRING	Parquet no admite una precisión decimal superior a 38. El valor decimal se convierte en una cadena en un tipo BYTE_ARRAY y se codifica como UTF8.
DOUBLE	DOUBLE		
FLOAT	DOUBLE		
INT	INT32		
INT UNSIGNED	INT64		
MEDIUMINT	INT32		
MEDIUMINT UNSIGNED	INT64		

Tipo de datos de origen	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de conversión
NUMERIC	INT32	DECIMAL (p,s)	Si el valor de origen es inferior a 2^{31}, se almacena como INT32.
	INT64	DECIMAL (p,s)	Si el valor de origen es 2^{31} o superior, pero inferior a 2^{63}, se almacena como INT64.
	FIXED_LEN _ARRAY(N)	DECIMAL (p,s)	Si el valor de origen es 2^{63} o superior, se almacena como FIXED_LEN _BYTE_ARRAY(N).
	BYTE_ARRAY	STRING	Parquet no admite una precisión numérica superior a 38. Este valor numérico se convierte en una cadena en un tipo BYTE_ARRAY y se codifica como UTF8.
SMALLINT	INT32		
SMALLINT UNSIGNED	INT32		
TINYINT	INT32		
TINYINT UNSIGNED	INT32	INT(16, true)	

Tipo de datos de origen	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de conversión
Tipos de datos de cadena			
BINARY	BYTE_ARRAY		
BLOB	BYTE_ARRAY		
CHAR	BYTE_ARRAY		
ENUM	BYTE_ARRAY	STRING	
LINESTRING	BYTE_ARRAY		
LONGBLOB	BYTE_ARRAY		
LONGTEXT	BYTE_ARRAY	STRING	
MEDIUMBLOB	BYTE_ARRAY		
MEDIUMTEXT	BYTE_ARRAY	STRING	
MULTILINESTRING	BYTE_ARRAY		
SET	BYTE_ARRAY	STRING	
TEXT	BYTE_ARRAY	STRING	
TINYBLOB	BYTE_ARRAY		
TINYTEXT	BYTE_ARRAY	STRING	
VARBINARY	BYTE_ARRAY		
VARCHAR	BYTE_ARRAY	STRING	
Tipos de datos de fecha y hora			

Tipo de datos de origen	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de conversión
FECHA	BYTE_ARRAY	STRING	Una fecha se convierte en una cadena en un tipo BYTE_ARRAY y se codifica como UTF8.
DATETIME	INT64	TIMESTAMP_MICROS	
TIME	BYTE_ARRAY	STRING	Un tipo TIME se convierte en una cadena en un BYTE_ARRAY y se codifica como UTF8.
TIMESTAMP	INT64	TIMESTAMP_MICROS	
YEAR	INT32		
Tipos de datos geométricos			
GEOMETRY	BYTE_ARRAY		
GEOMETRYCOLLECTION	BYTE_ARRAY		
MULTIPOINT	BYTE_ARRAY		
MULTIPOLYGON	BYTE_ARRAY		
POINT	BYTE_ARRAY		
POLYGON	BYTE_ARRAY		
Tipos de datos de JSON			

Tipo de datos de origen	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de conversión
JSON	BYTE_ARRAY	STRING	

Mapeo de tipos de datos PostgreSQL con Parquet

En la tabla siguiente se muestra el mapeo de los tipos de datos PostgreSQL con los tipos de datos Parquet cuando los datos se convierten y se exportan a Amazon S3.

Tipos de datos de PostgreSQL	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de mapeo
Tipos de datos numéricos			
BIGINT	INT64		
BIGSERIAL	INT64		
DECIMAL	BYTE_ARRAY	STRING	Un tipo DECIMAL se convierte en una cadena en un tipo BYTE_ARRAY y se codifica como UTF8. Esta conversión se realiza para evitar complicaciones debidas a la precisión de los datos y los valores de datos que no son un número (NaN).
DOUBLE PRECISION	DOUBLE		
INTEGER	INT32		

Tipos de datos de PostgreSQL	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de mapeo
MONEY	BYTE_ARRAY	STRING	
REAL	FLOAT		
SERIAL	INT32		
SMALLINT	INT32	INT(16, true)	
SMALLSERIAL	INT32	INT(16, true)	
Tipos de datos de cadena y relacionados			
ARRAY	BYTE_ARRAY	STRING	Una matriz se convierte en una cadena y se codifica como BINARY (UTF8). Esta conversión se realiza para evitar complicaciones debido a la precisión de los datos, valores de datos que no son un número (NaN) y valores de datos de tiempo.
BIT	BYTE_ARRAY	STRING	
BIT VARYING	BYTE_ARRAY	STRING	
BYTEA	BINARY		
CHAR	BYTE_ARRAY	STRING	

Tipos de datos de PostgreSQL	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de mapeo
CHAR(N)	BYTE_ARRAY	STRING	
ENUM	BYTE_ARRAY	STRING	
NAME	BYTE_ARRAY	STRING	
TEXT	BYTE_ARRAY	STRING	
TEXT SEARCH	BYTE_ARRAY	STRING	
VARCHAR(N)	BYTE_ARRAY	STRING	
XML	BYTE_ARRAY	STRING	
Tipos de datos de fecha y hora			
FECHA	BYTE_ARRAY	STRING	
INTERVAL	BYTE_ARRAY	STRING	
TIME	BYTE_ARRAY	STRING	
TIME WITH TIME ZONE	BYTE_ARRAY	STRING	
TIMESTAMP	BYTE_ARRAY	STRING	
TIMESTAMP WITH TIME ZONE	BYTE_ARRAY	STRING	
Tipos de datos geométricos			
BOX	BYTE_ARRAY	STRING	
CIRCLE	BYTE_ARRAY	STRING	
LINE	BYTE_ARRAY	STRING	
LINESEGMENT	BYTE_ARRAY	STRING	

Tipos de datos de PostgreSQL	Tipo primitivo de Parquet	Anotación de tipo lógico	Notas de mapeo
PATH	BYTE_ARRAY	STRING	
POINT	BYTE_ARRAY	STRING	
POLYGON	BYTE_ARRAY	STRING	
Tipos de datos JSON			
JSON	BYTE_ARRAY	STRING	
JSONB	BYTE_ARRAY	STRING	
Otros tipos de datos			
BOOLEANO	BOOLEANO		
CIDR	BYTE_ARRAY	STRING	Tipo de datos de red
COMPOSITE	BYTE_ARRAY	STRING	
DOMAIN	BYTE_ARRAY	STRING	
INET	BYTE_ARRAY	STRING	Tipo de datos de red
MACADDR	BYTE_ARRAY	STRING	
OBJECT IDENTIFIER	N/A		
PG_LSN	BYTE_ARRAY	STRING	
RANGE	BYTE_ARRAY	STRING	
UUID	BYTE_ARRAY	STRING	

Utilización de AWS Backup para administrar copias de seguridad automatizadas para Amazon RDS

AWS Backup es un servicio de copia de seguridad completamente administrado que facilita la centralización y automatización de las copias de seguridad de datos en servicios de AWS en la nube y en las instalaciones. Puede administrar copias de seguridad de las bases de datos de Amazon RDS en AWS Backup.

> **Note**
>
> Las copias de seguridad administradas por AWS Backup se consideran instantáneas de base de datos manuales, pero no se cuentan para la cuota de instantáneas de base de datos para RDS. Las copias de seguridad que se crearon con AWS Backup tienen nombres que terminan en `awsbackup:backup-job-number`.

Para obtener más información sobre AWS Backup, consulte la Guía para desarrolladores de AWS Backup.

Para ver las copias de seguridad administradas por AWS Backup

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la pestaña Backup service (Servicio de copia de seguridad).

   Las copias de seguridad de AWS Backup se enumeran en Backup service snapshots (Instantáneas del servicio de copias de seguridad).

Supervisión de métricas en una instancia de Amazon RDS

En las secciones siguientes encontrará información general sobre la supervisión de Amazon RDS y una explicación sobre cómo acceder a las métricas. Para conocer cómo supervisar eventos, registros y flujos de actividad de bases de datos, consulte Supervisión de eventos, registros y flujos en una instancia de Amazon RDS.

Temas

- Plan de monitoreo
- Referencia de rendimiento
- Directrices de rendimiento
- Supervisión de herramientas de Amazon RDS
- Visualización del estado de la instancia
- Recomendaciones para Amazon RDS
- Consulta de métricas en la consola de Amazon RDS
- Visualización de las métricas combinadas en la consola de Amazon RDS
- Supervisión de métricas de Amazon RDS con Amazon CloudWatch
- Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch
- Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS
- Análisis de anomalías de rendimiento con Amazon DevOps Guru para Amazon RDS
- Supervisión de las métricas del sistema operativo con Supervisión mejorada
- Referencia de métricas para Amazon RDS

Plan de monitoreo

Antes de comenzar la monitorización Amazon RDS, cree un plan de monitorización. El plan debe responder a las siguientes preguntas:

- ¿Cuáles son los objetivos de la monitorización?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a monitorizar estos recursos?
- ¿Qué herramientas de monitorización va a utilizar?

- ¿Quién se encargará de realizar las tareas de monitorización?
- ¿Quién debe recibir una notificación cuando surjan problemas?

Referencia de rendimiento

Para lograr sus objetivos de monitoreo, debe establecer una referencia. Para ello, mida el rendimiento bajo distintas condiciones de carga en diferentes momentos en su entorno de Amazon RDS. Puede monitorear métricas como las siguientes:

- Network throughput
- Conexiones de clientes
- E/S para operaciones de lectura, escritura o metadatos
- Saldos de crédito de ráfagas para sus instancias de base de datos

Le recomendamos que almacene datos históricos de rendimiento para Amazon RDS. Utilizando los datos almacenados, puede comparar el rendimiento actual frente a las tendencias anteriores. También puede distinguir los patrones de rendimiento normales de las anomalías y diseñar técnicas para solucionar problemas.

Directrices de rendimiento

En general, los valores aceptables para las métricas de rendimiento dependen de lo que hace la aplicación respecto a la referencia. Investigue las variaciones coherentes o de las tendencias con respecto a la referencia. Las siguientes métricas suelen ser la fuente de problemas de rendimiento:

- Consumo elevado de CPU o RAM: unos valores elevados de consumo de CPU o RAM es posible que sean si se ajustan a los objetivos de su aplicación (de rendimiento o simultaneidad, por ejemplo) y son los esperados.
- Consumo de espacio en disco: investigue el consumo de espacio en el disco si el espacio utilizado está por sistema alrededor o por encima del 85 % del espacio total disponible en el disco. Compruebe si es posible eliminar datos de la instancia o archivar los datos en un sistema diferente para liberar espacio.
- Tráfico de red: para el tráfico de red, hable con el administrador de su sistema para saber cuál es el rendimiento esperado para la red de su dominio y para su conexión a Internet. Investigue el tráfico de red si el rendimiento es por sistema inferior al esperado.

- Conexiones a bases de datos: si ve que hay un alto número de conexiones de usuarios además de una reducción en el rendimiento y el tiempo de respuesta de la instancia, valore la posibilidad de restringir las conexiones a las bases de datos. El mejor número de conexiones de usuarios para su instancia de base de datos varía en función de la clase de instancia y de la complejidad de las operaciones que se estén llevando a cabo. Para determinar el número de conexiones a bases de datos, asocie la instancia de base de datos con un grupo de parámetros en el que el parámetro `User Connections` se haya establecido en un valor distinto de 0 (ilimitado). Puede utilizar un grupo de parámetros existente o crear uno nuevo. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
- Métricas de IOPS: los valores esperados para las métricas de IOPS dependen de la especificación del disco y la configuración del servidor, así que debe usar su referencia para conocer los valores típicos. Investigue si los valores son por sistema diferentes de los de la referencia. Para un rendimiento óptimo de IOPS, asegúrese de que el conjunto de trabajo típico se ajuste a la memoria para minimizar las operaciones de lectura y escritura.

Cuando el rendimiento está fuera del punto de referencia establecido, es posible que tenga que realizar cambios para optimizar la disponibilidad de la base de datos para la carga de trabajo. Por ejemplo, es posible que necesite cambiar la clase de instancia de su instancia de base de datos. O es posible que necesite cambiar el número de instancias de base de datos y réplicas de lectura disponibles para los clientes.

Supervisión de herramientas de Amazon RDS

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon RDS y de otras soluciones de AWS. AWS ofrece diversas herramientas de supervisión para vigilar a Amazon RDS, informar cuando algo no funciona y tomar medidas de manera automática cuando corresponda.

Temas

- Herramientas de monitoreo automatizadas
- Herramientas de monitoreo manuales

Herramientas de monitoreo automatizadas

Le recomendamos que automatice las tareas de supervisión en la medida de lo posible.

Temas

- Estado y recomendaciones de la instancia de Amazon RDS
- Métricas de Amazon CloudWatch para Amazon RDS
- Supervisión del sistema operativo e Información de rendimiento de Amazon RDS
- Servicios integrados

Estado y recomendaciones de la instancia de Amazon RDS

Puede utilizar las siguientes herramientas automatizadas para vigilar a Amazon RDS e informar cuando haya algún problema:

- Estado del clúster de Amazon RDS: vea los detalles sobre el estado actual del clúster mediante la consola de Amazon RDS, la AWS CLI o la API de RDS.
- Las Recomendaciones para Amazon RDS responden a recomendaciones automatizadas para recursos de base de datos, como instancias de base de datos, , réplicas de lectura y grupos de parámetros de de base de datos. Para obtener más información, consulte Recomendaciones para Amazon RDS.

Métricas de Amazon CloudWatch para Amazon RDS

Amazon RDS se integra con Amazon CloudWatch para proporcionar funciones de supervisión adicionales.

- Amazon CloudWatch: este servicio monitorea sus recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede utilizar las siguientes características de Amazon CloudWatch con Amazon RDS:
  - Métricas de Amazon CloudWatch–Amazon RDS envía métricas automáticamente a CloudWatch cada minuto para cada base de datos activos. No se cobran cargos adicionales por métricas de Amazon RDS en CloudWatch. Para obtener más información, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.
  - Alarmas de Amazon CloudWatch–: puede ver una sola Amazon RDSmétrica durante un periodo de tiempo específico. A continuación, puede realizar una o varias acciones en función del valor de la métrica en relación al umbral establecido. Para obtener más información, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.

Supervisión del sistema operativo e Información de rendimiento de Amazon RDS

Puede utilizar las siguientes herramientas automatizadas para supervisar el rendimiento de Amazon RDS:

- Información sobre rendimiento de Amazon RDS: evalúa la carga en su base de datos y determina cuándo y dónde realizar acciones. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.
- Supervisión mejorada de Amazon RDS: examine métricas en tiempo real para el sistema operativo. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Servicios integrados

Los siguientes servicios de AWS se integran con Amazon RDS:

- Amazon EventBridge: es un bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de varios orígenes. Para obtener más información, consulte Supervisión de eventos de Amazon RDS.

- Registros de Amazon Cloudwatch le ayuda a supervisar, almacenar y acceder a los archivos de registro desde instancias de Amazon RDS , CloudTrail y otros orígenes. Para obtener más información, consulte Supervisión de archivos de registro de Amazon RDS.
- AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o que se realizan en nombre de esta. Además, entrega los archivos de registro a un bucket de Amazon S3 especificado. Para obtener más información, consulte Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail.
- Los Flujos de actividad de la base de datos son una característica de Amazon RDS que proporciona un flujo casi en tiempo real de la actividad en su instancia de de base de datos de Oracle. Para obtener más información, consulte Supervisión de Amazon RDS con flujos de actividad de la base de datos.

Herramientas de monitoreo manuales

Tiene que monitorear manualmente aquellos elementos que las alarmas de CloudWatch no cubren. Los paneles de las consolas de Amazon RDS, CloudWatch, AWS Trusted Advisor y otras consolas de AWS proporcionan una vista rápida del entorno de AWS. Es recomendable que también compruebe los archivos de registro de su instancia de base de datos.

- En la consola de Amazon RDS, puede monitorizar los siguientes elementos para sus recursos:
  - Número de conexiones a una instancia de base de datos
  - La cantidad de operaciones de lectura y escritura de una instancia de base de datos
  - La cantidad de almacenamiento que utiliza actualmente una instancia de base de datos
  - La cantidad de memoria y de CPU que se utiliza para una instancia de base de datos
  - La cantidad de tráfico de red de entrada y salida de una instancia de base de datos
- Desde el panel de Trusted Advisor, puede revisar las siguientes comprobaciones de optimización del costo, seguridad, tolerancia a errores y mejora del rendimiento:
  - Amazon RDS Idle DB Instances
  - Amazon RDS Security Group Access Risk
  - Copias de seguridad de Amazon RDS
  - Amazon RDS Multi-AZ

  Para obtener más información acerca de estas comprobaciones, consulte Prácticas recomendadas de Trusted Advisor (verificaciones).

- La página de inicio de CloudWatch muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede utilizar CloudWatch para hacer lo siguiente:
  - Crear paneles personalizados para supervisar los servicios que le importan.
  - Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
  - Buscar y examinar todas sus métricas de recursos de AWS.
  - Crear y editar las alarmas de notificación de problemas.

Visualización del estado de la instancia

Con la consola de Amazon RDS, puede acceder rápidamente al estado de su instancia de base de datos.

Temas

- Visualización del estado de la instancia de base de datos de en un clúster de Aurora

Visualización del estado de la instancia de base de datos de en un clúster de Aurora

El estado de una instancia de base de datos indica la situación de la instancia de base de datos. Puede utilizar los siguientes procedimientos para ver el estado de la instancia de base de datos en la consola de Amazon RDS, el comando de la AWS CLI o la operación de la API.

> **Note**
>
> Amazon RDS también usa otro estado llamado estado de mantenimiento, que se muestra en la columna Mantenimiento de la consola de Amazon RDS. Este valor indica el estado de los parches de mantenimiento que se deben aplicar a una instancia de base de datos. El estado de mantenimiento es independiente del estado de la instancia de base de datos. Para obtener más información sobre el estado de mantenimiento, consulte Aplicación de actualizaciones a una instancia de base de datos.

Encuentre los valores de estado posibles para instancias de base de datos en la siguiente tabla. Esta tabla le muestra si se le facturará la instancia de base de datos y el almacenamiento, si se le facturará solo el almacenamiento o si no se le facturará. Para todos los estados de instancia de base de datos, se le factura siempre el uso de copia de seguridad.

Estado de la instancia de base de datos	Facturado	Descripción
available	Facturado	La instancia de base de datos funciona correctamente y está disponible.
backing-up	Facturado	Se está creando una copia de seguridad de la instancia de base de datos.
configuring-enhanced-monitoring	Facturado	La monitorización mejorada se está habilitando o deshabilitando para esta instancia de base de datos.
configuring-iam-database-auth	Facturado	La autenticación de base de datos en AWS Identity and Access Management (IAM) se está habilitando o desactivando para esta instancia de base de datos.

Estado de la instancia de base de datos	Facturado	Descripción
configuring-log-exports	Facturado	La publicación de archivos de registro en Amazon CloudWatch Logs se está habilitando o deshabili tando para esta instancia de base de datos.
converting-to-vpc	Facturado	La instancia de base de datos se está convirtiendo de una instancia de base de datos que no está en una Amazon Virtual Private Cloud (Amazon VPC) a una instancia de base de datos que está en una Amazon VPC.
creating	No facturado (no PITR) Facturado (solo PITR)	La instancia de base de datos se está creando. No se puede obtener acceso a la instancia de base de datos mientras se está creando. Si restaura una base de datos durante una recuperación en un momento dado (PITR), se le facturará mientras la base de datos esté en el estado creación. Este es el único escenario en el que el estado creación incurre en cargos.
delete-precheck	No facturado	Amazon RDS valida que las réplicas leídas estén en buen estado y se puedan eliminar de forma segura.
deleting	No facturado	Se está eliminando la instancia de base de datos.
error	No facturado	La instancia de base de datos ha generado un error y Amazon RDS no puede recuperarla. Realice una restauración al último momento restaurable de la instancia de base de datos para recuperar los datos.
inaccessible-encry ption-credentials	No facturado	No se puede obtener acceso ni recuperar la AWS KMS key utilizada para cifrar o descifrar la instancia de base de datos.

Estado de la instancia de base de datos	Facturado	Descripción
inaccessible-encryption-credentials-recoverable	Facturado para almacenamiento	No se puede acceder a la clave de KMS utilizada para cifrar o descifrar la instancia de base de datos. Sin embargo, si la clave de KMS está activada, reiniciar la instancia de base de datos puede ayudar a recuperarla. Para obtener más información, consulte Cifrar una instancia de base de datos.
incompatible-create	No facturado	Amazon RDS está intentando crear una instancia de base de datos, pero no puede hacerlo porque los recursos no son compatibles con la instancia de base de datos. Este estado puede darse si, por ejemplo, el perfil de instancia de su instancia de base de datos no tiene los permisos correctos.
incompatible-network	No facturado	Amazon RDS está intentando realizar una acción de recuperación en una instancia de base de datos, pero no puede hacerlo porque la VPC está en un estado que impide completar la acción. Este estado puede darse si, por ejemplo, todas las direcciones IP disponibles en una subred están en uso y Amazon RDS no puede obtener una dirección IP para la instancia de base de datos.
incompatible-option-group	Facturado	Amazon RDS ha intentado aplicar un cambio en el grupo de opciones, pero no puede hacerlo y no puede revertir al estado anterior del grupo de opciones. Para obtener información, consulte la lista Recent Events (Eventos recientes) para la instancia de base de datos. Este estado puede darse si, por ejemplo, el grupo de opciones contiene una opción como TDE y la instancia de base de datos no contiene información cifrada.

Estado de la instancia de base de datos	Facturado	Descripción
incompatible-parameters	Facturado	Amazon RDS no puede iniciar la instancia de base de datos porque los parámetros especificados en el grupo de parámetros de base de datos de la instancia de base de datos no son compatibles con la instancia de base de datos. Revierta los cambios de los parámetros o hágalos compatibles con la instancia de base de datos para recuperar el acceso a la instancia de base de datos. Para obtener más información acerca de los parámetros incompatibles, consulte la lista Recent Events (Eventos recientes) de la instancia de base de datos.
incompatible-restore	No facturado	Amazon RDS no puede realizar una restauración a un momento dado. Las causas habituales para este estado incluyen el uso de tablas temporales, el uso de tablas de MyISAM con MySQL o el uso de tablas de Aria con MariaDB.
insufficient-capacity	No facturado	Amazon RDS no puede crear la instancia porque actualmente no hay suficiente capacidad disponible. Para crear la instancia de base de datos en la misma zona de disponibilidad con el mismo tipo de instancia , elimine la instancia de base de datos, espere unas horas e intente crear de nuevo. Alternativamente, cree una nueva instancia utilizando una clase de instancia o zona de disponibilidad diferente.
maintenance	Facturado	Amazon RDS está aplicando una actualización de mantenimiento a la instancia de base de datos. Este estado se usa para el mantenimiento de nivel de instancia que RDS programa con mucha antelación.
modifying	Facturado	La instancia de base de datos se está modificando porque un cliente ha solicitado su modificación.

Estado de la instancia de base de datos	Facturado	Descripción
moving-to-vpc	Facturado	La instancia de base de datos se está moviendo a una nueva Amazon Virtual Private Cloud (Amazon VPC).
rebooting	Facturado	La instancia de base de datos se está reiniciando porque un cliente o un proceso de Amazon RDS que requiere el reinicio lo ha solicitado.
resetting-master-credentials	Facturado	Las credenciales maestras de la instancia de base de datos se están restableciendo porque un cliente lo ha solicitado.
renaming	Facturado	El nombre de la instancia de base de datos se está cambiando porque un cliente lo ha solicitado.
restore-error	Facturado	La instancia de base de datos ha registrado un error al intentar restaurar a un momento dado o a partir de una instantánea.
starting	Facturado para almacenamiento	La instancia de base de datos se está iniciando.
stopped	Facturado para almacenamiento	La instancia de base de datos se ha detenido.
deteniendo	Facturado para almacenamiento	La instancia de base de datos se está deteniendo.

Estado de la instancia de base de datos	Facturado	Descripción
storage-config-upgrade	Facturado	Se está actualizando la configuración del sistema de archivos de almacenamiento de la instancia de base de datos. Este estado solo es aplicable a las bases de datos verdes de una implementación azul/verde o a las réplicas de lectura de instancias de base de datos.
storage-full	Facturado	La instancia de base de datos ha alcanzado su asignación de capacidad de almacenamiento. Se trata de un estado crítico y le recomendamos que corrija este problema de inmediato. Para ello, aumente la escala del almacenamiento modificando la instancia de base de datos. Para evitar esta situación, defina las alarmas de Amazon CloudWatch para que se le advierta cuando el espacio de almacenamiento está bajando.
storage-initialization	Facturado	La instancia de base de datos carga bloques de datos de Amazon S3 para optimizar el rendimiento del volumen después de restaurarlo a partir de una instantánea. Sigue disponible para las operaciones, pero es posible que el rendimiento no esté al máximo hasta que se complete la inicialización.
storage-optimization	Facturado	Amazon RDS está optimizando el almacenamiento de su instancia de base de datos. El proceso de optimización del almacenamiento suele durar poco, pero a veces puede tardar 24 horas o más. Durante la optimización del almacenamiento, la instancia de base de datos permanece disponible. La optimización del almacenamiento es un proceso en segundo plano que no afecta a la disponibilidad de la instancia.

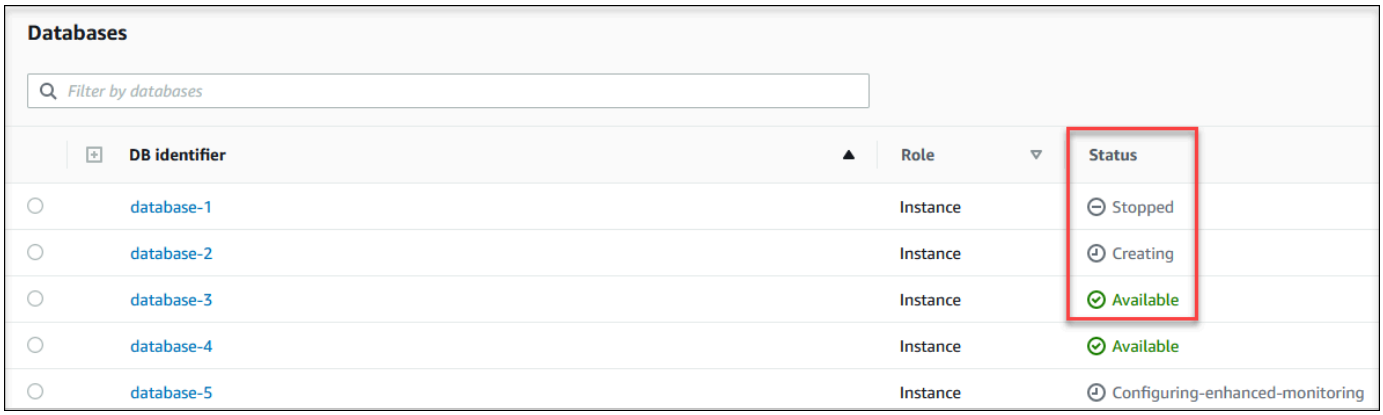
Estado de la instancia de base de datos	Facturado	Descripción
upgrading	Facturado	Se está actualizando la versión del motor de base de datos o del sistema operativo.

Consola

Para ver el estado de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).

   Se abre la página Databases (Bases de datos) con la lista de instancias de base de datos. Para cada clúster de base de datos , se muestra el valor del estado.



CLI

Para ver la instancia de base de datos y su información de estado usando el AWS CLI, utilice el comando describe-db-instances. Por ejemplo, el siguiente comando AWS CLI enumera toda la información de las instancias de base de datos.

```
aws rds describe-db-instances
```

Para ver una instancia de base de datos específica y su estado, llame al comando describe-db-instances con la siguiente opción:

- `DBInstanceIdentifier`: el nombre de la instancia de base de datos.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

Para ver solo el estado de todas las instancias de bases de datos, utilice la siguiente consulta en AWS CLI.

```
aws rds describe-db-instances --query 'DBInstances[*].
[DBInstanceIdentifier,DBInstanceStatus]' --output table
```

API

Para ver el estado de la instancia de base de datos usando la API de Amazon RDS, llame a la operación DescribeDBInstances.

Recomendaciones para Amazon RDS

Amazon RDS ofrece recomendaciones automatizadas para recursos de base de datos, como instancias de base de datos, réplicas de lectura y grupos de parámetros de bases de datos. Estas recomendaciones proporcionan instrucciones de las prácticas recomendadas mediante el análisis de la , la configuración de instancia de base de datos, el uso y los datos de rendimiento.

Información de rendimiento de Amazon RDS monitoriza automáticamente métricas específicas y crea umbrales mediante el análisis de qué niveles se consideran potencialmente problemáticos para un recurso específico. Cuando los nuevos valores de las métricas cruzan un umbral predefinido durante un período de tiempo determinado, Información de rendimiento genera una recomendación proactiva. Esta recomendación ayuda a evitar que el rendimiento de la base de datos se vea afectado en el futuro. Por ejemplo, la recomendación “Inactiva en la transacción” se genera para las instancias de RDS para PostgreSQL cuando las sesiones conectadas a la base de datos no están realizando un trabajo activo, pero pueden mantener bloqueados los recursos de la base de datos. Para recibir recomendaciones proactivas, debe activar Información de rendimiento con un período de retención de nivel de pago. Para obtener información acerca de la activación de Información de rendimiento, consulte Activación y desactivación de Información de rendimiento de Amazon RDS. Para obtener información sobre los precios y la retención de datos de Información de rendimiento, consulte Precios y retención de datos de Performance Insights.

DevOps Guru para RDS monitoriza determinadas métricas para detectar cuándo el comportamiento de una métrica se vuelve muy inusual o anómalo. Estas anomalías se presentan como información reactiva con recomendaciones. Por ejemplo, DevOps Guru para RDS podría recomendar que considere aumentar la capacidad de la CPU o investigar los eventos de espera que contribuyen a la carga de la base de datos. DevOps Guru para RDS también proporciona recomendaciones proactivas basadas en umbrales. Para ver estas recomendaciones, debe activar DevOps Guru para RDS. Para obtener información sobre cómo activar DevOps Guru para RDS, consulte Activación de DevOps Guru y especificación de la cobertura de recursos.

Las recomendaciones tendrán uno de los siguientes estados: activas, rechazadas, pendientes o resueltas. Las recomendaciones resueltas están disponibles durante 365 días.

Puede ver o descartar las recomendaciones. Puede aplicar una recomendación activa basada en la configuración de forma inmediata, programarla para el siguiente periodo de mantenimiento o descartarla. Para obtener recomendaciones proactivas basadas en umbrales y reactivas basadas en machine learning, debe revisar la causa sugerida del problema y, a continuación, realizar las acciones recomendadas para solucionarlo.

Las recomendaciones son compatibles en las siguientes:Regiones de AWS

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- América del Sur (São Paulo)

Aprenda a ver, aplicar, descartar y modificar recomendaciones de Amazon RDS en las siguientes secciones.

Temas

- Visualización Amazon RDS de recomendaciones
- Aplicación de recomendaciones para Amazon RDS
- Descarte de las recomendaciones de Amazon RDS
- Modificación de las recomendaciones de Amazon RDS descartadas a recomendaciones activas
- Recomendaciones de la referencia de Amazon RDS

Visualización Amazon RDS de recomendaciones

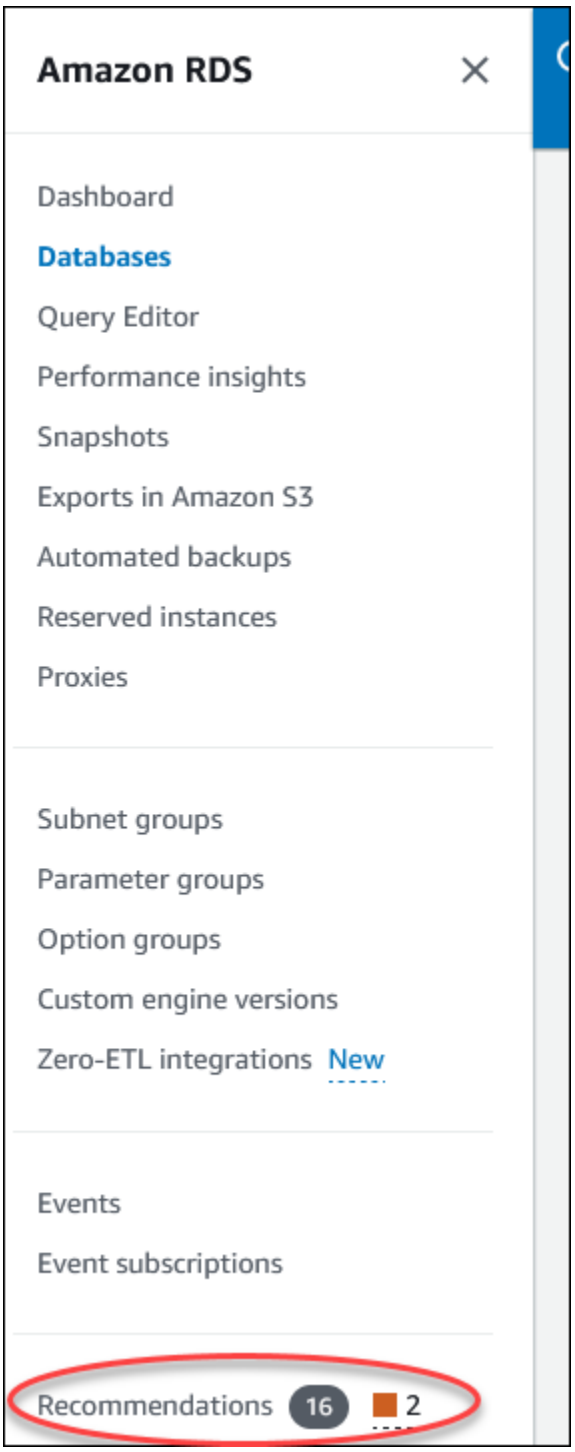
Con la consola de Amazon RDS, puede ver las recomendaciones de Amazon RDS para los recursos de su base de datos.

Consola

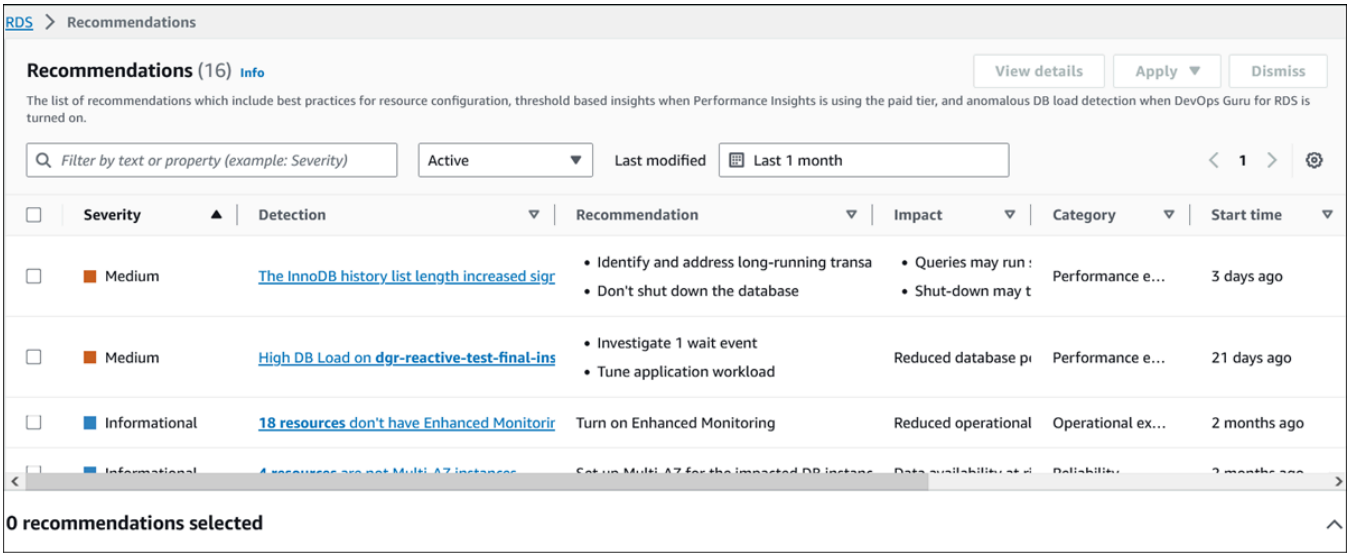
Para ver las recomendaciones de Amazon RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, realice cualquiera de las siguientes acciones:

   - Elija Recomendaciones. El número de recomendaciones activas para sus recursos y el número de recomendaciones con la mayor gravedad generadas en el último mes están disponibles junto a Recomendaciones. Para encontrar el número de recomendaciones activas para cada gravedad, seleccione el número que muestre la gravedad más alta.

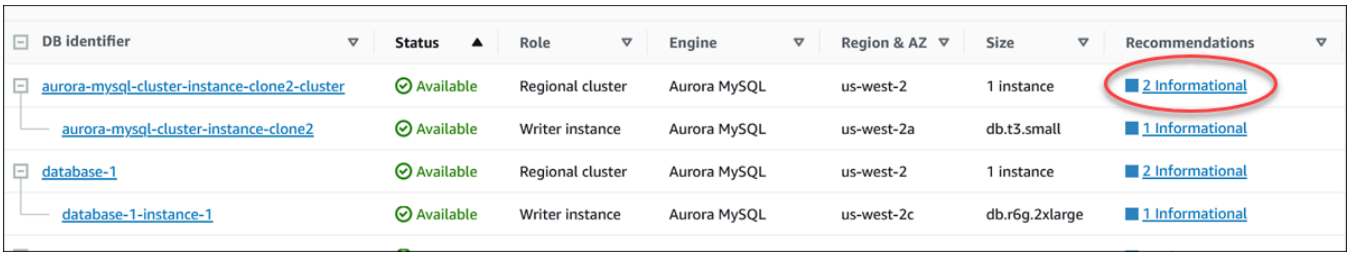


De forma predeterminada, la página de Recomendaciones muestra una lista de las nuevas recomendaciones en el mes pasado. Amazon RDS ofrece recomendaciones de todos los recursos de su cuenta y las clasifica por gravedad.

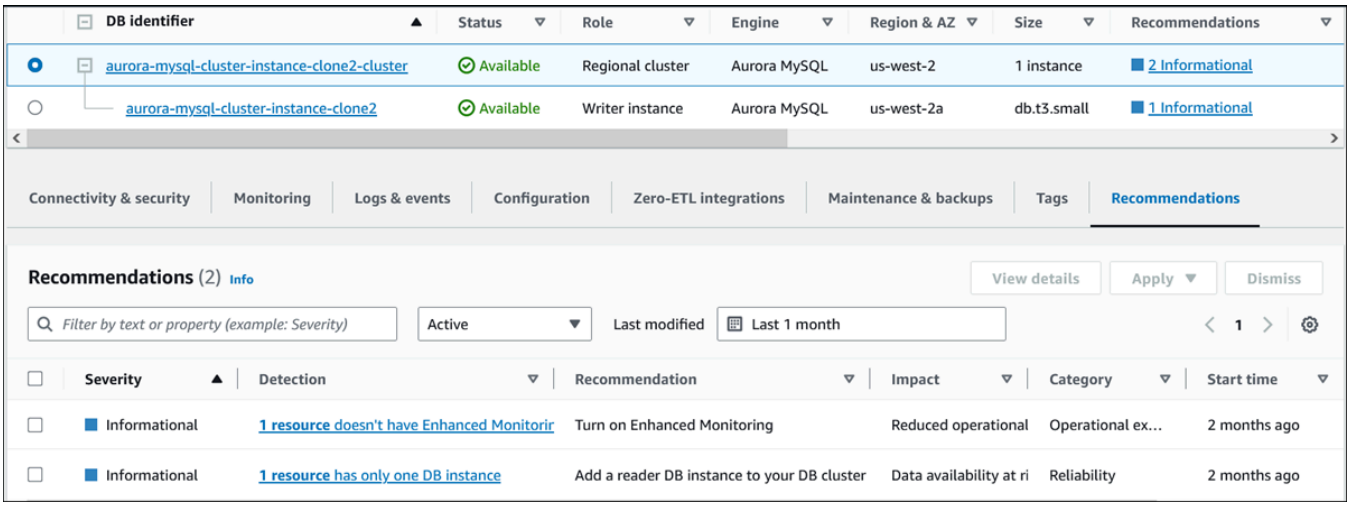


Puede elegir una recomendación para ver una sección en la parte inferior de la página que contiene los recursos afectados y los detalles sobre cómo se aplicará la recomendación.

- En la página Bases de datos, seleccione Recomendaciones para un recurso.



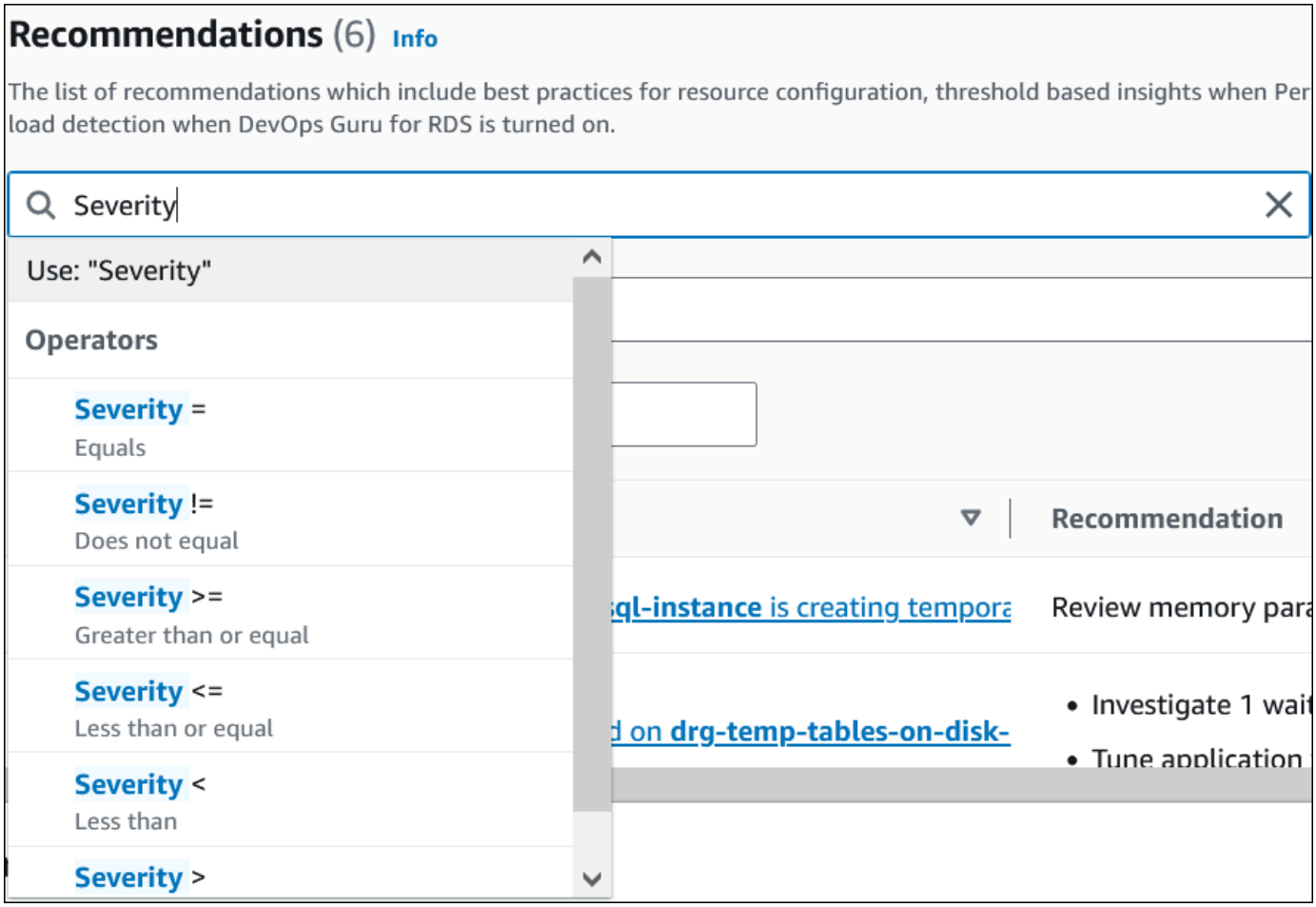
La pestaña Recomendaciones muestra las recomendaciones y sus detalles para el recurso seleccionado.



Están disponibles los siguientes detalles para las recomendaciones:

- Gravedad: el nivel de implicación del problema. Los niveles de gravedad son Alto, Medio, Bajo e Informativo.
- Detección: el número de recursos afectados y una breve descripción del problema. Haga clic en este enlace para ver la recomendación y los detalles del análisis.
- Recomendación: una breve descripción de la acción que se recomienda aplicar.
- Impacto: una breve descripción del posible impacto si no se aplica la recomendación.
- Categoría: el tipo de recomendación. Las categorías son Eficiencia de rendimiento, Seguridad, Fiabilidad, Optimización de costos, Excelencia operativa y Sostenibilidad.
- Estado: el estado actual de la recomendación. Los estados posibles son Todas, Activa, Descartada, Resuelta y Pendiente.
- Hora de inicio: hora a la que comenzó el problema. Por ejemplo, Hace 18 horas.
- Última modificación: la hora en que el sistema actualizó la recomendación por última vez debido a un cambio en la Gravedad, o la hora en que respondiera a la recomendación. Por ejemplo, Hace 10 horas.
- Hora de finalización: hora en la que finalizó el problema. La hora no se mostrará si hay problemas continuos.
- Identificador de recurso: el nombre de uno o más recursos.

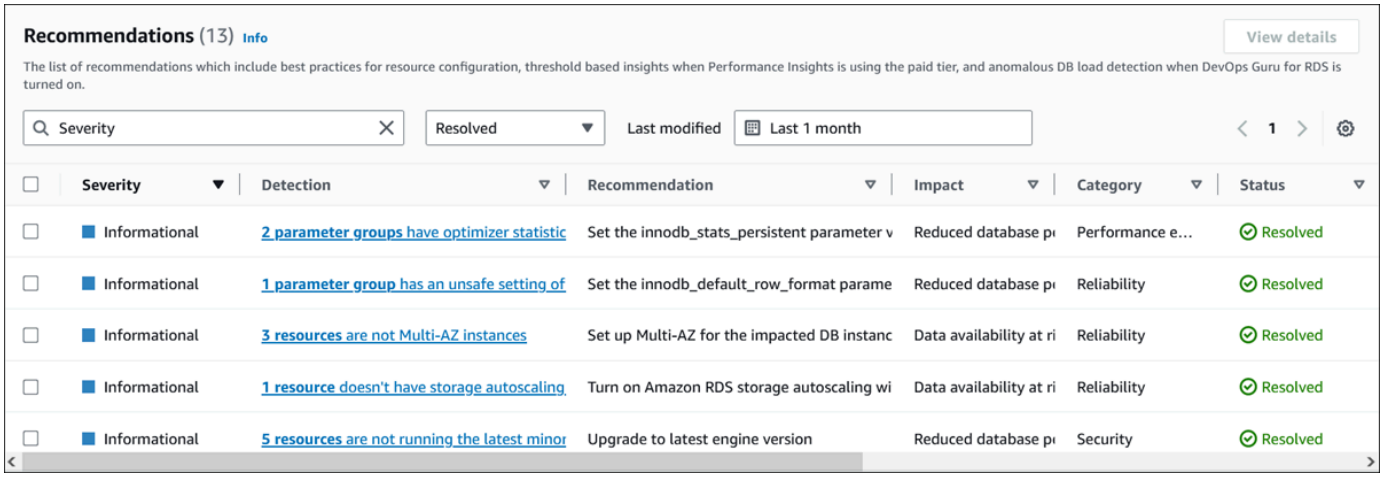
3. (Opcional) Elija los operadores Gravedad o Categoría en el campo para filtrar la lista de recomendaciones.



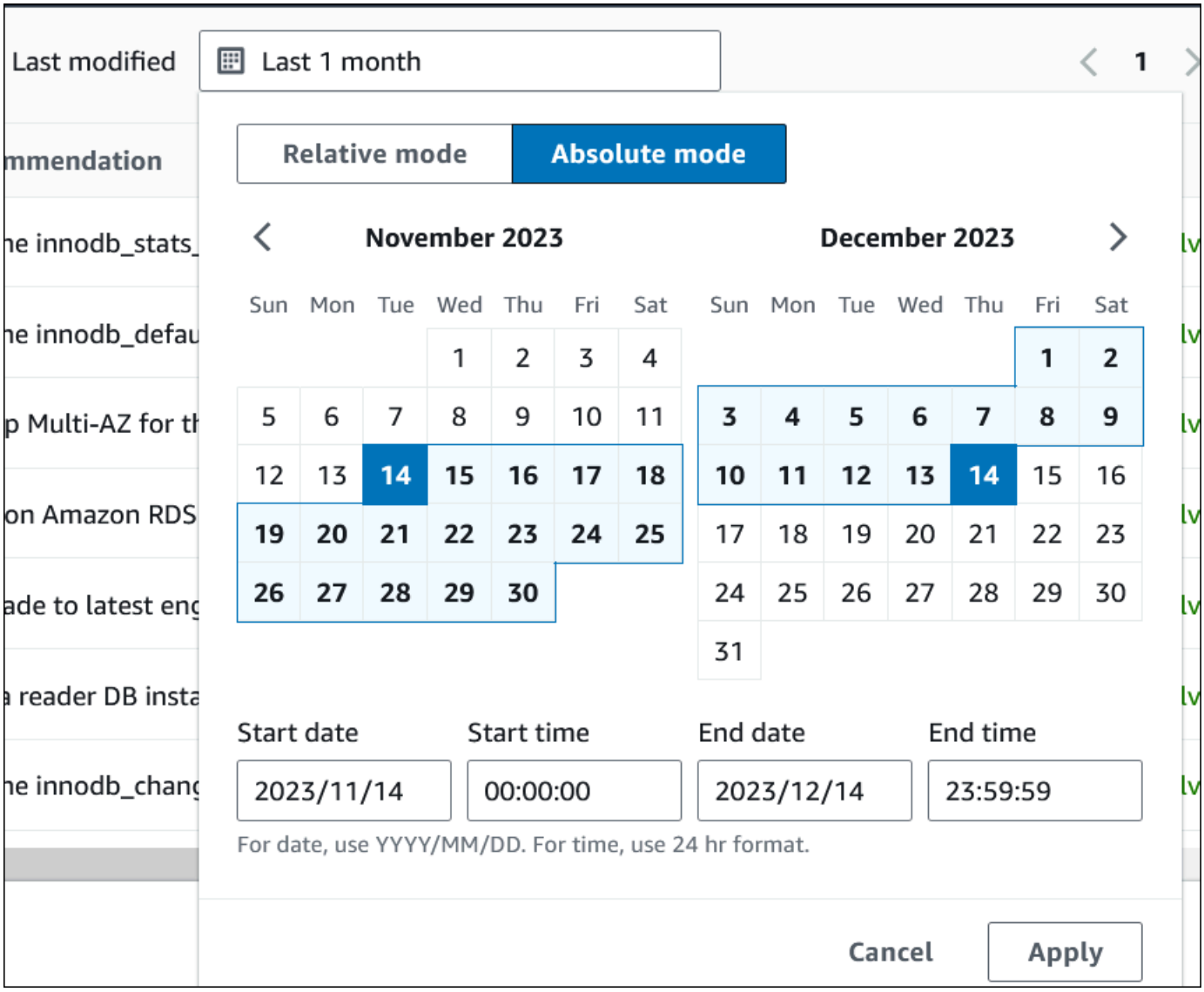
Aparecen las recomendaciones para la operación seleccionada.

4. (Opcional) Elija cualquiera de los siguientes estados de recomendación:

   - Activa: muestra las recomendaciones actuales que puede aplicar, programar para el próximo período de mantenimiento o descartar.
   - Todas: muestra todas las recomendaciones con el estado actual.
   - Descartada: muestra las recomendaciones rechazadas.
   - Resuelta: muestra las recomendaciones que se han resuelto.
   - Pendiente: muestra las recomendaciones cuyas acciones recomendadas están en curso o programadas para el siguiente período de mantenimiento.



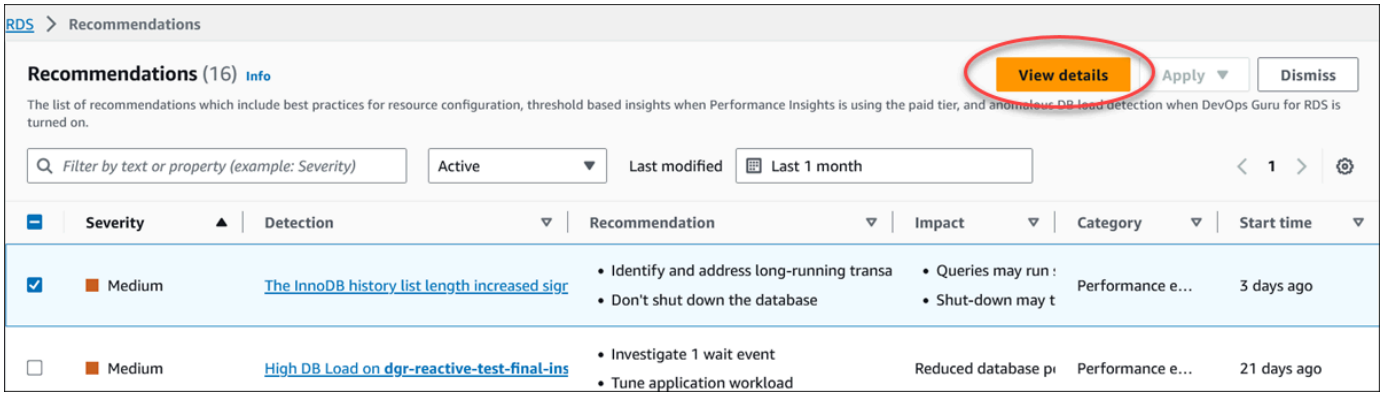
5. (Opcional) Seleccione Modo relativo o Modo absoluto en Última modificación para modificar el periodo de tiempo. La página de Recomendaciones muestra las recomendaciones generadas en el periodo de tiempo. El periodo de tiempo predeterminado es el mes pasado. En el Modo absoluto, puede elegir el período de tiempo o introducir la hora en los campos Fecha de inicio y Fecha de finalización.



Se muestran las recomendaciones para el período de tiempo establecido.

Tenga en cuenta que puede ver todas las recomendaciones de recursos de su cuenta si configura el rango en Todos.

6. (Opcional) Seleccione Preferencias en la parte derecha para personalizar los detalles que se van a mostrar. Puede elegir un tamaño de página, ajustar las líneas del texto y permitir u ocultar las columnas.
7. (Opcional) Elija una recomendación y, a continuación, seleccione Ver detalles.



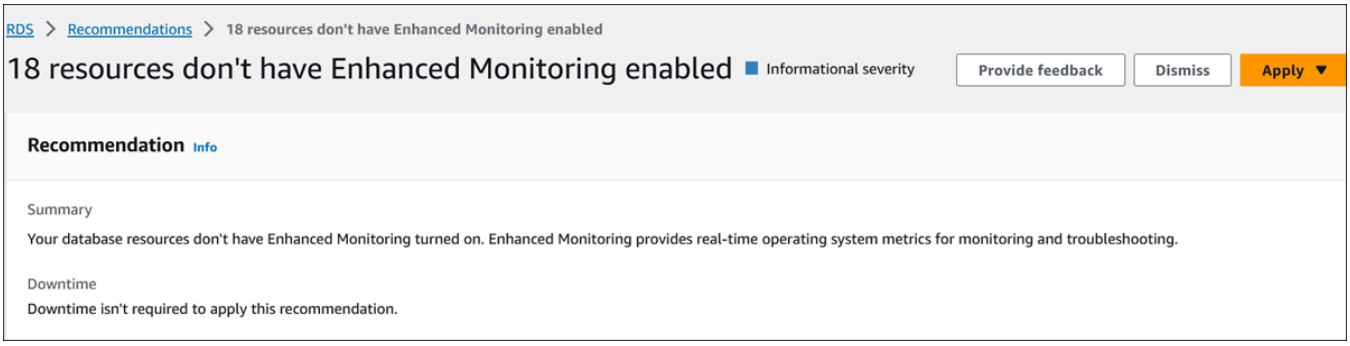
Aparece la página de detalles de la recomendación. En el título se indica el recuento total de los recursos con el problema detectado y su gravedad.

Para obtener información sobre los componentes de la página de detalles de una recomendación reactiva basada en anomalías, consulte Viewing reactive anomalies en la Guía del usuario de Amazon DevOps Guru.

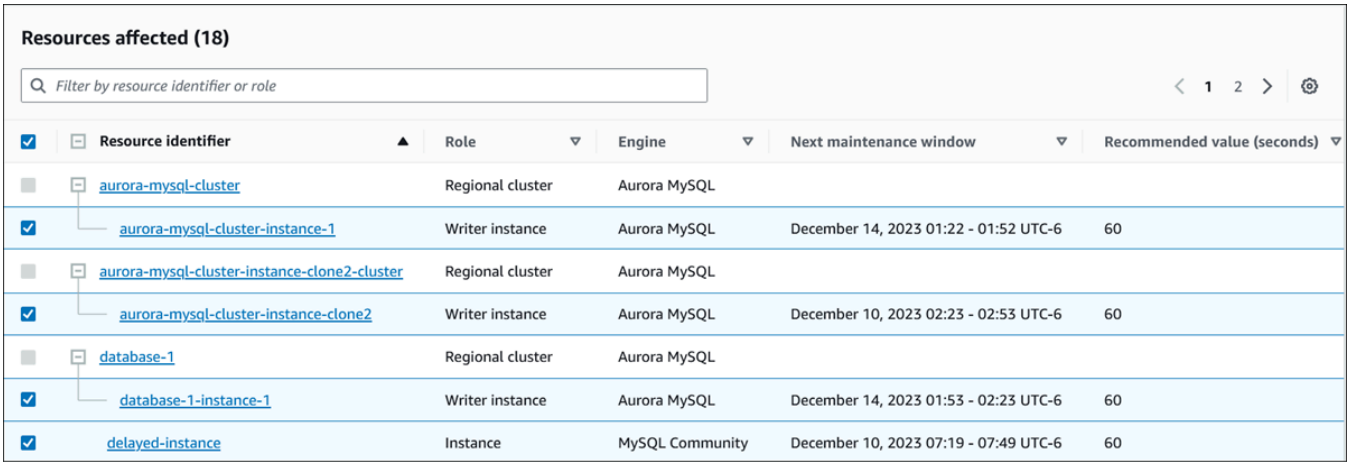
Para obtener información sobre los componentes en la página de detalles de una recomendación proactiva basada en un umbral, consulte Visualización de las recomendaciones proactivas de Información de rendimiento.

Las demás recomendaciones automatizadas muestran los siguientes componentes en la página de detalles de la recomendación:

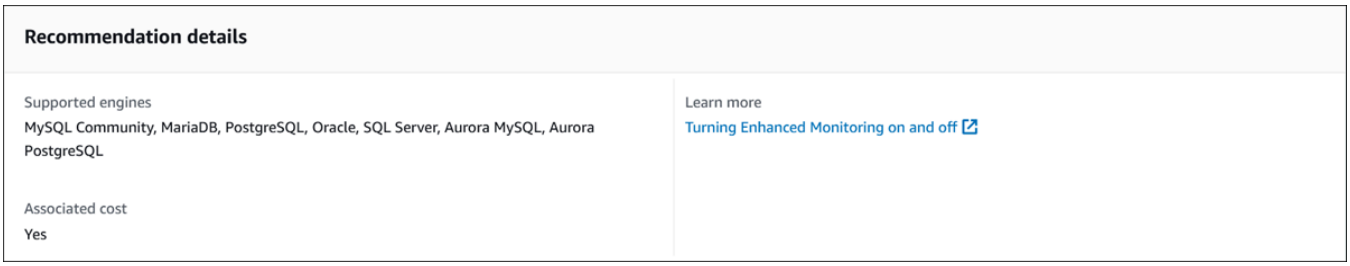
- Recomendación: un resumen de la recomendación y si se requiere un tiempo de inactividad para aplicarla.



- Recursos afectados: detalles de los recursos afectados.



- Detalles de la recomendación: información sobre los motores compatibles, cualquier costo asociado necesario para aplicar la recomendación y enlace a la documentación para obtener más información.



CLI

Para ver las recomendaciones de Amazon RDS sobre las instancias de base de datos , utilice el siguiente comando en AWS CLI.

```
aws rds describe-db-recommendations
```

API de RDS

Para ver las recomendaciones de Amazon RDS mediante la API de Amazon RDS, utilice la operación DescribeDBRecommendations.

Aplicación de recomendaciones para Amazon RDS

Para aplicar las recomendaciones de Amazon RDS mediante la consola de Amazon RDS, seleccione una recomendación basada en la configuración o un recurso afectado en la página de detalles. A continuación, seleccione si desea aplicar la recomendación inmediatamente o programarla para

el siguiente periodo de mantenimiento. Es posible que el recurso tenga que reiniciarse para que el cambio se aplique. Para obtener algunas recomendaciones sobre grupos de parámetros de bases de datos, es posible que deba reiniciar los recursos.

Las recomendaciones proactivas basadas en umbrales o las reactivas basadas en anomalías no tendrán la opción de aplicarse y es posible que necesiten una revisión adicional.

Consola

Para aplicar una recomendación basada en la configuración

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, realice una de las siguientes acciones:

   - Elija Recomendaciones.

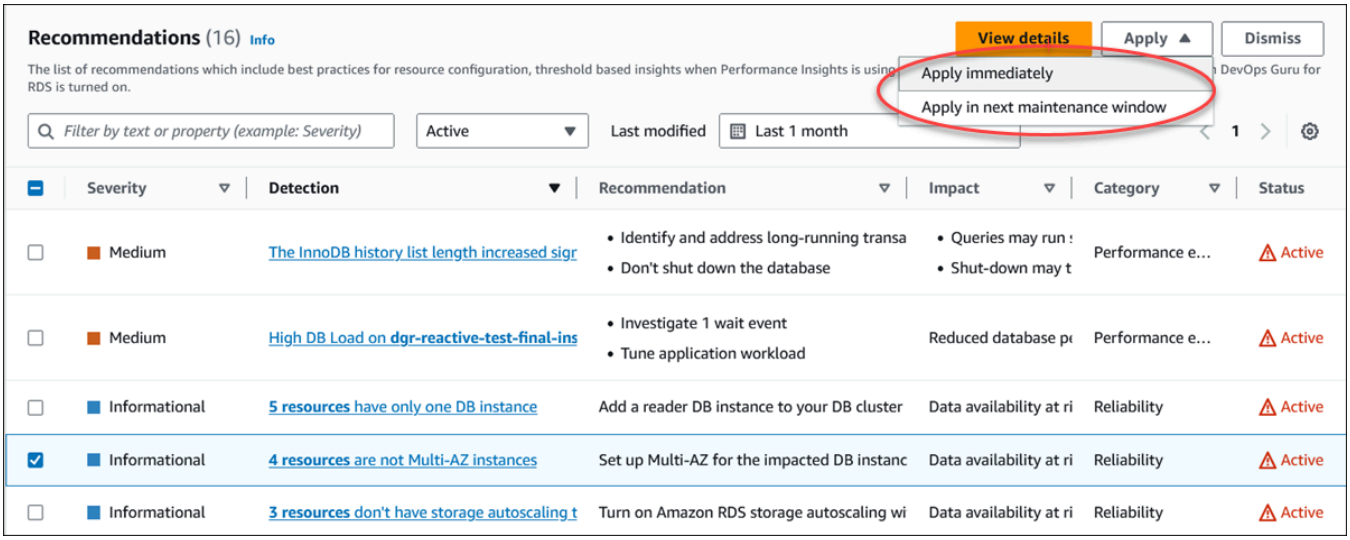
     Aparece la página de Recomendaciones con la lista de todas las recomendaciones.
   - Elija Bases de datos y, a continuación, elija Recomendaciones para un recurso en la página de bases de datos.

     Los detalles aparecen en la pestaña Recomendaciones de la recomendación seleccionada.
   - Seleccione Detección para ver una recomendación activa en la página Recomendaciones o en la pestaña Recomendaciones de la página Bases de datos.

     Aparece la página de detalles de la recomendación.
3. Elija una recomendación o uno o varios recursos afectados en la página de detalles de la recomendación y realice una de las siguientes acciones:

   - Seleccione Aplicar y, a continuación, seleccione Aplicar inmediatamente para aplicar la recomendación inmediatamente.
   - Seleccione Aplicar y elija Aplicar en el siguiente periodo de mantenimiento para programarlo en el siguiente periodo de mantenimiento.

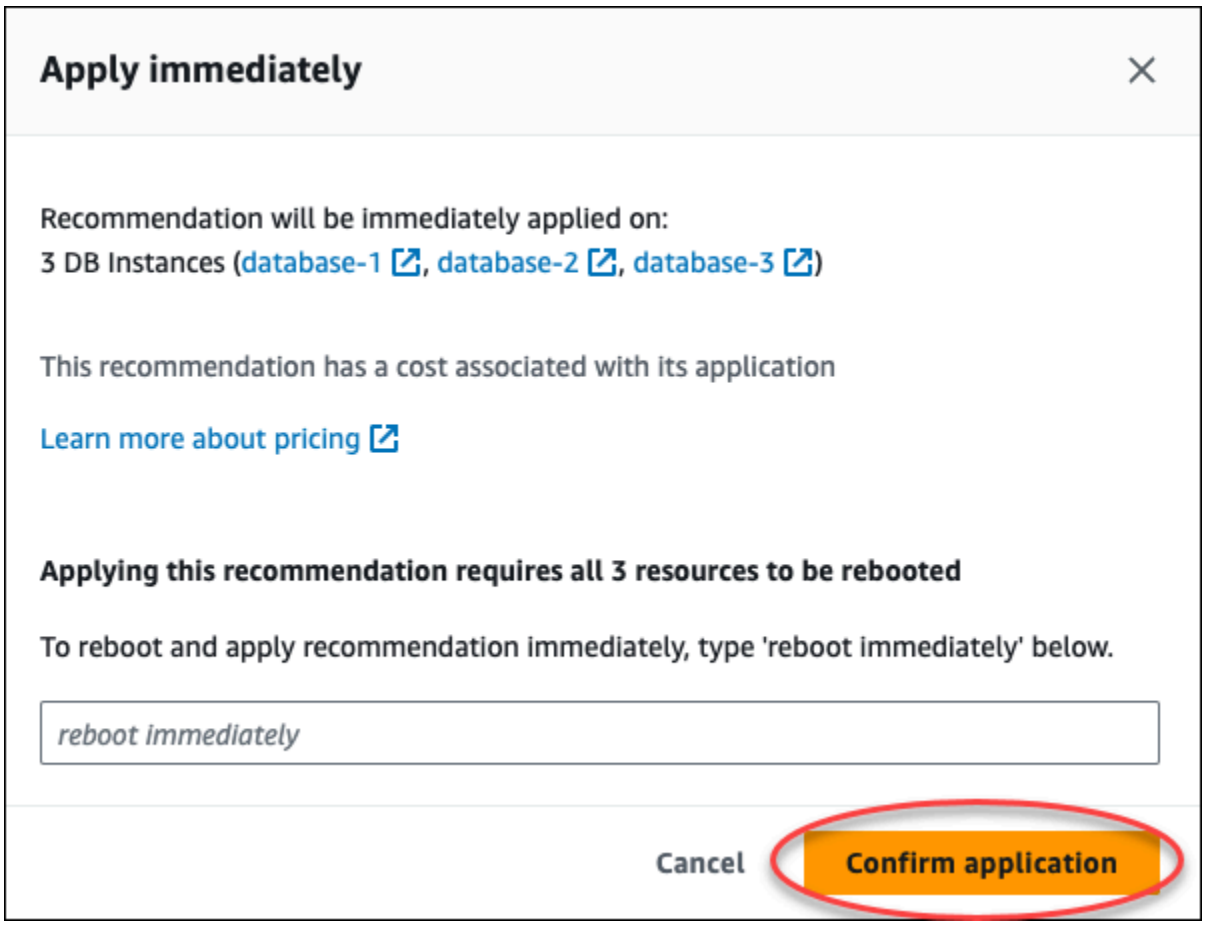
     El estado de la recomendación seleccionada se actualiza a pendiente hasta el siguiente período de mantenimiento.



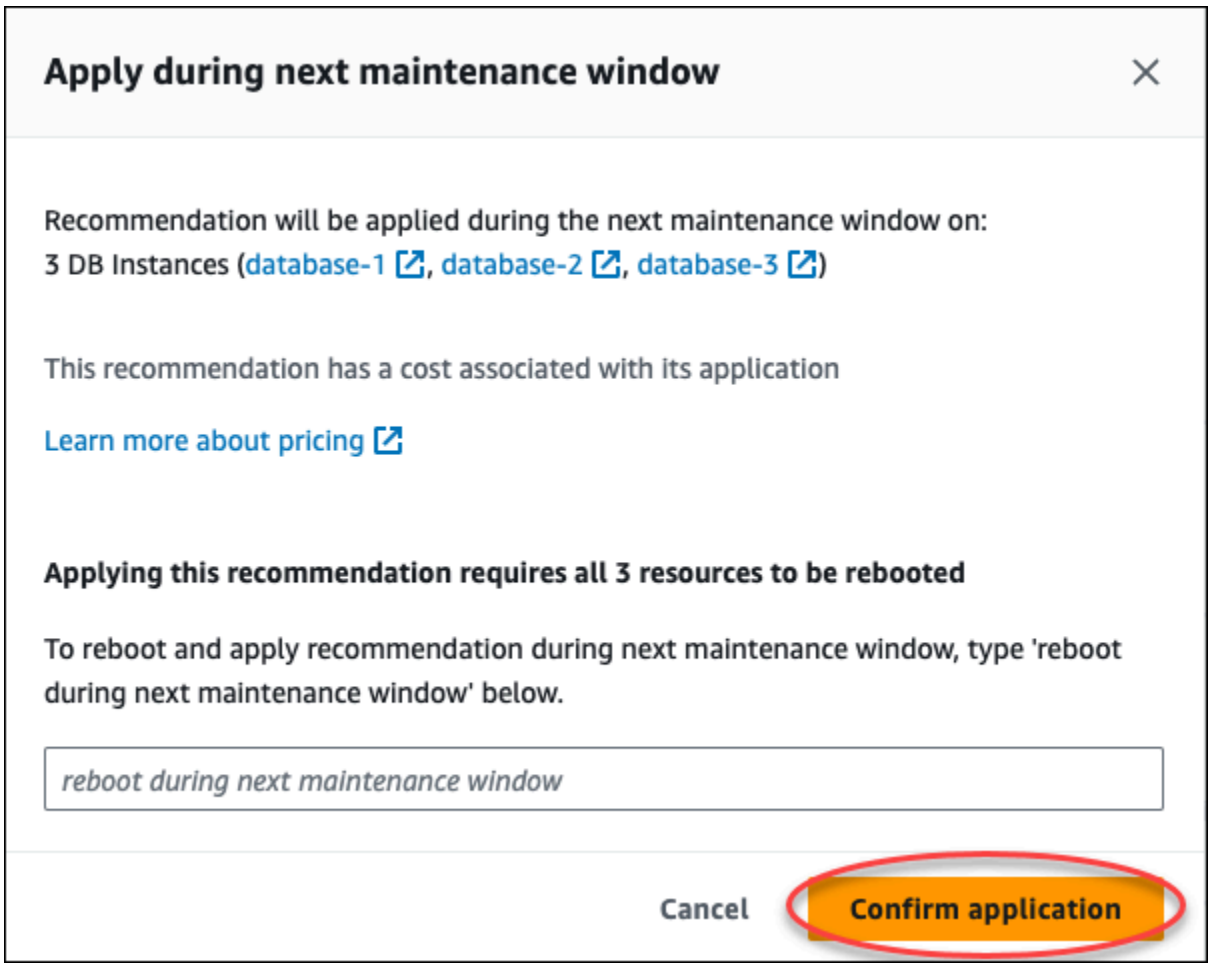
Aparece una ventana de confirmación.

4. Seleccione Confirmar aplicación para aplicar la recomendación. Esta ventana confirma si los recursos necesitan un reinicio automático o manual para que los cambios se apliquen.

   En el siguiente ejemplo, se muestra la ventana de confirmación para aplicar la recomendación inmediatamente.



El siguiente ejemplo muestra la ventana de confirmación para programar la aplicación de la recomendación en el siguiente período de mantenimiento.



Aparecerá un banner con un mensaje cuando la recomendación aplicada se haya aplicado correctamente o si no se ha podido aplicar.

En el siguiente ejemplo, se muestra el banner con el mensaje de aplicación correcta.



En el siguiente ejemplo, se muestra el banner con el mensaje de aplicación incorrecta.



API de RDS

Para aplicar una recomendación de RDS basada en la configuración mediante la API de Amazon RDS

1. Utilice la operación DescribeDBRecommendations. Las `RecommendedActions` de la salida pueden tener una o varias acciones recomendadas.
2. Use el objeto RecommendedAction para cada acción recomendada del paso 1. La salida contiene `Operation` y `Parameters`.

   En el siguiente ejemplo, se muestra el resultado con una acción recomendada.

```
   "RecommendedActions": [
       {
           "ActionId": "0b19ed15-840f-463c-a200-b10af1b552e3",
           "Title": "Turn on auto backup", // localized
           "Description": "Turn on auto backup for my-mysql-instance-1", //
localized
           "Operation": "ModifyDbInstance",
           "Parameters": [
               {
                   "Key": "DbInstanceIdentifier",
                   "Value": "my-mysql-instance-1"
               },
               {
                   "Key": "BackupRetentionPeriod",
                   "Value": "7"
               }
           ],
           "ApplyModes": ["immediately", "next-maintenance-window"],
           "Status": "applied"
       },
       ... // several others
   ],
```

3. Utilice la `operation` para cada acción recomendada del resultado del paso 2 e introduzca los valores de `Parameters`.
4. Cuando la operación del paso 2 se haya realizado correctamente, utilice la operación ModifyDBRecommendation para modificar el estado de la recomendación.

Descarte de las recomendaciones de Amazon RDS

Puede descartar una o más recomendaciones de Amazon RDS mediante la consola de Amazon RDS, la AWS CLI o la API de Amazon RDS.

Consola

Para descartar una o varias recomendaciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, realice una de las siguientes acciones:

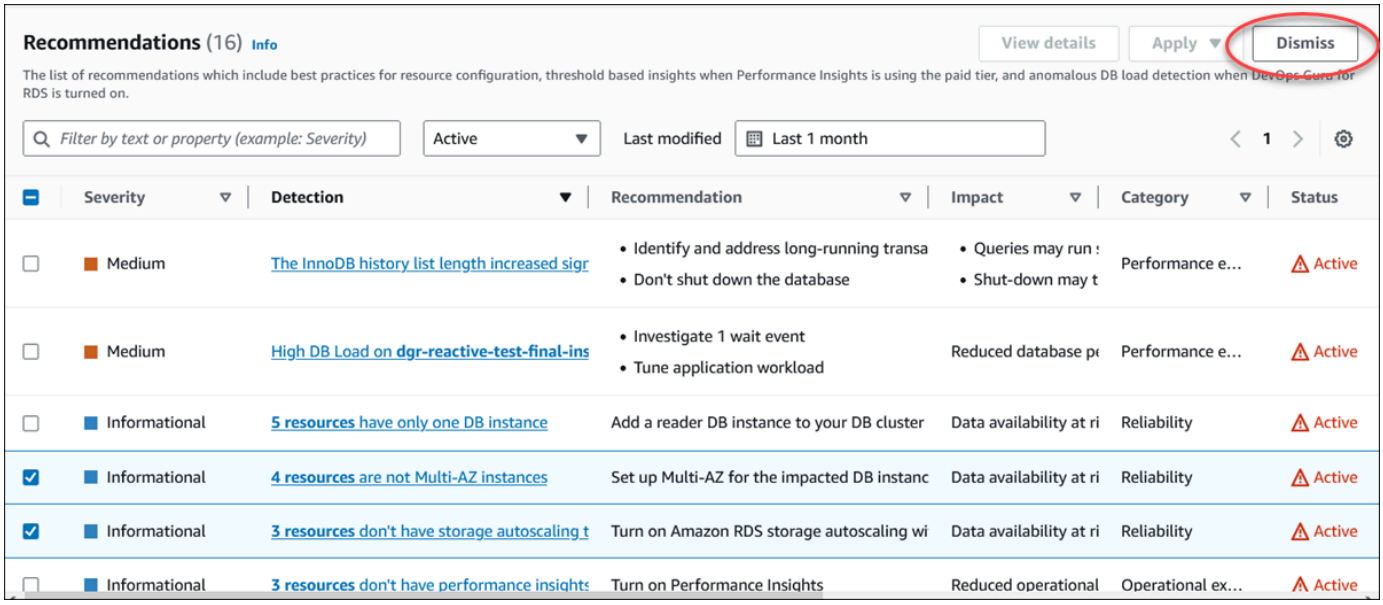
   - Elija Recomendaciones.

     Aparece la página de Recomendaciones con la lista de todas las recomendaciones.
   - Elija Bases de datos y, a continuación, elija Recomendaciones para un recurso en la página de bases de datos.

     Los detalles aparecen en la pestaña Recomendaciones de la recomendación seleccionada.
   - Seleccione Detección para ver una recomendación activa en la página Recomendaciones o en la pestaña Recomendaciones de la página Bases de datos.

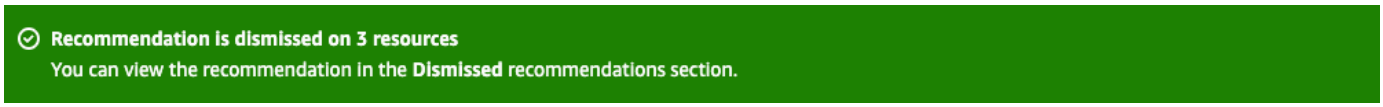
     La página de detalles de la recomendación muestra la lista de los recursos afectados.
3. Elija una o más recomendaciones o uno o más recursos afectados en la página de detalles de la recomendación y, a continuación, elija Descartar.

   En el siguiente ejemplo, se muestra la página Recomendaciones con varias recomendaciones activas seleccionadas para descartarlas.



Un banner muestra un mensaje cuando se descartan una o más recomendaciones seleccionadas.

En el siguiente ejemplo, se muestra el banner con el mensaje de aplicación correcta.



En el siguiente ejemplo, se muestra el banner con el mensaje de aplicación incorrecta.



CLI

Para descartar una recomendación de RDS utilizando la AWS CLI

1. Ejecute el comando `aws rds describe-db-recommendations --filters "Name=status,Values=active"`.

   En el resultado se proporciona una lista de recomendaciones en el estado `active`.
2. Busque el `recommendationId` para la recomendación que desee descartar en el paso 1.
3. Ejecute el comando `>aws rds modify-db-recommendation --status dismissed --recommendationId <ID>` con el `recommendationId` del paso 2 para descartar la recomendación.

API de RDS

Para descartar una recomendación de RDS mediante la API de Amazon RDS, utilice la operación ModifyDBRecommendation.

Modificación de las recomendaciones de Amazon RDS descartadas a recomendaciones activas

Puede cambiar una o más recomendaciones de Amazon RDS descartadas a activas mediante la consola de Amazon RDS, la AWS CLI o la API de Amazon RDS.

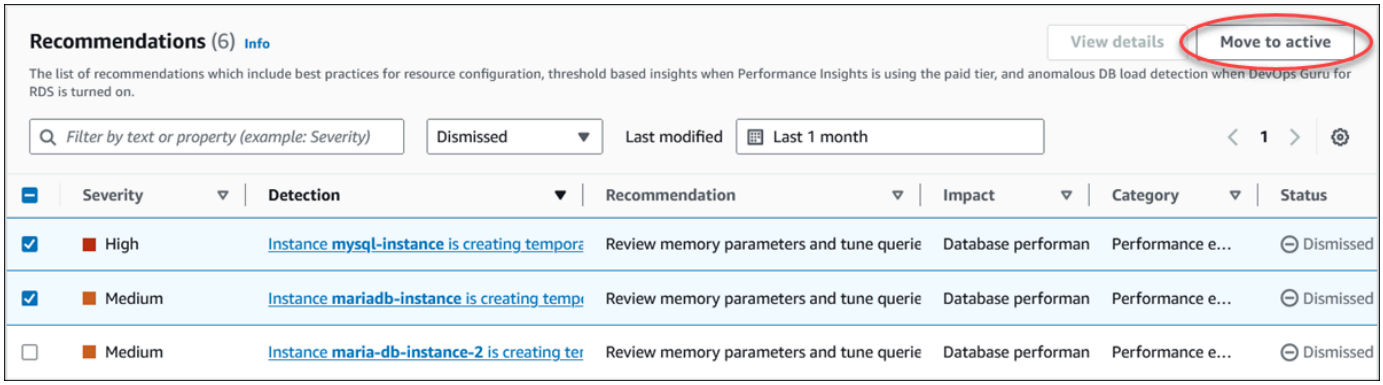
Consola

Para trasladar una o más recomendaciones descartadas a las recomendaciones activas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, realice una de las siguientes acciones:
   - Elija Recomendaciones.

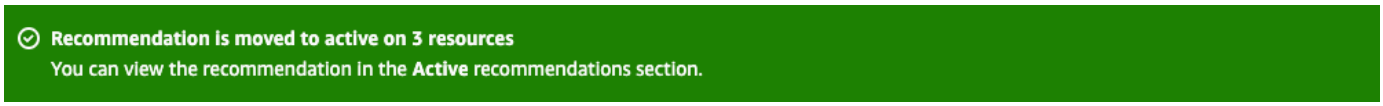
     En la página Recomendaciones, se muestra una lista de recomendaciones ordenadas por su gravedad para todos los recursos de su cuenta.
   - Elija Bases de datos y, a continuación, elija Recomendaciones para un recurso en la página de bases de datos.

     La pestaña Recomendaciones muestra las recomendaciones y sus detalles para el recurso seleccionado.
3. Elija una o más recomendaciones descartadas de la lista y, a continuación, elija Pasar a activas.



Un banner muestra un mensaje de éxito o fracaso al pasar las recomendaciones seleccionadas del estado descartado al estado activo.

En el siguiente ejemplo, se muestra el banner con el mensaje de aplicación correcta.



En el siguiente ejemplo, se muestra el banner con el mensaje de aplicación incorrecta.



CLI

Para convertir una recomendación de RDS descartada en una recomendación activa mediante la AWS CLI

1. Ejecute el comando `aws rds describe-db-recommendations --filters "Name=status,Values=dismissed"`.

   En el resultado se proporciona una lista de recomendaciones en el estado `dismissed`.
2. Busque el `recommendationId` de la recomendación para la que desee cambiar el estado desde el paso 1.
3. Ejecute el comando `>aws rds modify-db-recommendation --status active --recommendationId <ID>` con el `recommendationId` del paso 2 para cambiar la recomendación al estado activa.

API de RDS

Para convertir una recomendación de RDS descartada en una recomendación activa mediante la API de Amazon RDS, utilice la operación ModifyDBRecommendation.

Recomendaciones de la referencia de Amazon RDS

Amazon RDS genera recomendaciones para un recurso cuando se crea o modifica el recurso. Puede encontrar ejemplos de recomendaciones de Amazon RDS en la siguiente tabla.

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Volumen magnético en uso	Sus instancias de base de datos utilizan el almacenamiento magnético. El almacenamiento magnético no se recomienda para la mayoría de las instancias de base de datos. Elija un tipo de almacenamiento diferente: de uso general (SSD) o IOPS aprovisionadas.	Elija un tipo de almacenamiento diferente: de uso general (SSD) o IOPS aprovisionadas.	Sí	Volúmenes de generaciones anteriores en la documentación de Amazon EC2.
El recurso de copias de seguridad automatizadas está desactivado	Las copias de seguridad automatizadas no están activadas en sus instancias de base de datos. Se recomienda usar copias de seguridad automatizadas porque permiten la recuperación a un momento dado de su instancia de base de datos.	Active las copias de seguridad automatizadas con un período de retención de hasta 14 días.	Sí	Habilitar las copias de seguridad automatizadas Demystifying Amazon RDS backup storage costs en el blog de AWS Database
Debe efectuarse	Los recursos de su base de datos no	Actualícela a la última versión del motor.	Sí	Actualización de una versión del motor de

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
una mejora de la versión secundaria del motor	están ejecutando la última versión secundaria del motor de base de datos. La última versión secundaria contiene las últimas revisiones de seguridad y otras mejoras.			una instancia de base de datos
La monitorización mejorada está desactivada	Los recursos de la base de datos no tienen activada la monitorización mejorada. El monitoreo mejorado proporciona métricas del sistema operativo en tiempo real para el monitoreo y la solución de problemas.	Active la monitorización mejorada	No	Supervisión de las métricas del sistema operativo con Supervisión mejorada

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El cifrado de almacenamiento está desactivado	Amazon RDS admite el cifrado en reposo para todos los motores de bases de datos mediante las claves que administra en AWS Key Management Service (AWS KMS). En una instancia de base de datos activa con cifrado de Amazon RDS, los datos almacenados en reposo en el almacenamiento están cifrados, de forma similar a las copias de seguridad, las réplicas de lectura y las instantáneas automatizadas. Si el cifrado no está activado al crear una instancia de base de datos, tendrá que crear y restaurar una copia cifrada de la instantánea descifrada de la instancia de	Active el cifrado de los datos en reposo de su instancia de base de datos.	Sí	Seguridad en Amazon RDS Copia de una instantánea de base de datos para Amazon RDS

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
	base de datos antes de activar el cifrado.			
Información de rendimiento está desactivado	Información de rendimiento monitoriza la carga de la instancia de base de datos para ayudarle a analizar y solucionar los problemas de rendimiento de la base de datos. Le recomendamos que active Información de rendimiento.	Activar Información de rendimiento.	No	Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS
Las instancias de base de datos tienen desactivado el escalado automático del almacenamiento	El escalado automático de almacenamiento no está activado en su instancia de base de datos. El escalado automático del almacenamiento de RDS escala automáticamente la capacidad de almacenamiento cuando aumenta el tamaño de la carga de trabajo de la base de datos, sin tiempo de inactividad.	Active el escalado automático del almacenamiento de Amazon RDS con un umbral de almacenamiento máximo especificado	No	Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Es necesario actualizar las versiones principales de los recursos de RDS	No se admiten las bases de datos con la versión principal actual del motor de base de datos. Le recomendamos que actualice a la última versión principal, que incluye nuevas funciones y mejoras.	Actualización a la versión principal más reciente del motor de base de datos.	Sí	Actualización de una versión del motor de una instancia de base de datos Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Es necesaria la actualización de la clase de instancia de los recursos de RDS	Su instancia de base de datos se ejecuta en una clase de instancia de base de datos de generación anterior. Hemos sustituido las clases de instancia de base de datos de una generación anterior por clases de instancia de base de datos con mejor costo, rendimiento o ambos. Le recomendamos que ejecute su instancia de base de datos con una clase de instancia de base de datos de una generación más reciente.	Actualización de la clase de instancia de base de datos.	Sí	Motores de base de datos compatibles para clases de instancia de base de datos

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Los recursos de RDS utilizan una edición del motor al final del soporte con licencia incluida	Le recomendamos que actualice la versión principal a la última versión del motor compatible con Amazon RDS para continuar con el soporte de licencia actual. La versión del motor de su base de datos no será compatible con la licencia actual.	Le recomendamos que actualice su base de datos a la última versión compatible de Amazon RDS para seguir utilizando el modelo con licencia.	Sí	Actualizaciones principales de versiones de Oracle

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Instancias de base de datos que no utilizan la implement ación multi-AZ	Recomendamos usar la implement ación multi-AZ. Las implementaciones multi-AZ mejoran la disponibilidad y la durabilidad de la instancia de base de datos.	Configuración de multi-AZ para las instancias de base de datos afectadas	No No se produc un tiempo de inactividad durante este cambio Sin embarg existe un posible impact en el rendimiento. Para obtene más informa ón, consult Conver n de una	Precios de Amazon RDS Multi-AZ

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
			instanc de base de datos en una implem ación multi-AZ para Amazo RDS	

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Los parámetros de la memoria de la base de datos difieren de los predeterminados	Los parámetros de memoria de las instancias de base de datos difieren considerablemente de los valores predeterminados. Esta configuración puede afectar al rendimiento y provocar errores. Recomendamos restablecer los parámetros de memoria personalizados para la instancia de base de datos a sus valores predeterminados en el grupo de parámetros de la base de datos.	Restablezca los parámetros de memoria a sus valores predeterminados.	No	Best practices for configuring performance parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Parámetro `InnoDB_Change_Buffering` con un valor inferior al óptimo	El cambio de almacenamiento en búfer permite a una instancia de base de datos de MySQL aplazar algunas escrituras necesarias para mantener los índices secundarios. Esta característica era útil en entornos con discos lentos. El cambio en la configuración del almacenamiento en búfer mejoró ligeramente el rendimiento de la base de datos, pero provocó un retardo en la recuperación tras un fallo y prolongó los tiempos de apagado durante la actualización. Está establecido en `OFF` de forma predeterminada en MySQL versión 8.4	Establezca el valor del parámetro `InnoDB_Change_Buffering` en `NONE` en el grupo de parámetros de la base de datos.	No	Best practices for configuring performance parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro del caché de consultas está activado	Cuando los cambios requieran que se purgue la caché de consultas, parecerá que la instancia de base de datos se ha bloqueado. La mayoría de las cargas de trabajo no se benefician de una caché de consultas. La caché de consultas se ha quitado de la versión 8.0 de MySQL y posteriores. Es recomendable que establezca el parámetro query_cache_type en 0.	Establezca el valor del parámetro `query_cache_type` en `0` en el grupo de parámetros de su base de datos.	Sí	Best practices for configuring performance parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `log_output` está establecido en table	Cuando `log_output` se establece en `TABLE`, se utiliza más espacio de almacenamiento que cuando `log_output` se establece en `FILE`. Recomendamos que establezca el parámetro en `FILE` para evitar que se alcance el límite de tamaño de almacenamiento. Está establecido en `FILE` de forma predeterminada en MySQL versión 8.4 y superiores.	Establezca el valor del parámetro `log_output` en `FILE` en el grupo de parámetros de su base de datos.	No	Archivos de registro de base de datos de MySQL

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Los grupos de parámetros no utilizan páginas de gran tamaño	Las páginas grandes pueden aumentar la escalabilidad de la base de datos, pero la instancia de base de datos no utiliza páginas grandes. Le recomendamos que establezca el valor del parámetro `use_large_pages` en `ONLY` en el grupo de parámetros de base de datos de la instancia de base de datos.	Establezca el valor del parámetro `use_large_pages` en `ONLY` en el grupo de parámetros de su base de datos.	Sí	Activación de páginas de gran tamaño para una instancia de RDS para Oracle

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `autovacuum` está desactivado	El parámetro autovacuum está desactivado en sus instancias de base de datos. Desactivar autovacuum aumenta la sobrecarga de la tabla y del índice y afecta al rendimiento. Le recomendamos que active autovacuum en sus grupos de parámetros de base de datos.	Active el parámetro autovacuum en sus grupos de parámetros de de base de datos.	No	Understanding autovacuum in Amazon RDS for PostgreSQL environments en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `synchronous_commit` está desactivado	Cuando el parámetro `synchronous_commit` está desactivado, es posible que se pierdan datos si la base de datos se bloquea. La durabilidad de la base de datos está en riesgo. Le recomendamos que active el parámetro `synchronous_commit`.	Active el parámetro `synchronous_commit` en sus grupos de parámetros de la base de datos.	Sí	Amazon Aurora PostgreSQL parameters: Replication, security, and logging en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `track_counts` está desactivado	Si el parámetro `track_counts` está desactivado, la base de datos no recopila las estadísticas de actividad de la base de datos. Autovacuum necesita estas estadísticas para funcionar correctamente. Es recomendable que establezca el parámetro `track_counts` en 1.	Establezca el parámetro `track_counts` en 1.	No	Estadísticas de tiempo de ejecución para PostgreSQL
El parámetro `enable_indexonlyscan` está desactivado	El planificador u optimizador de consultas no puede usar el plan de análisis de solo índice si está desactivado. Es recomendable que establezca el valor del parámetro `enable_indexonlyscan` en 1.	Establezca el valor del parámetro `enable_indexonlyscan` en 1.	No	Configuración del método del planificador para PostgreSQL

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `enable_indexscan` está desactivado	El planificador u optimizador de consultas no puede usar el plan de análisis de índice si está desactivado. Es recomendable que defina el valor `enable_indexscan` en 1.	Establezca el valor del parámetro `enable_indexscan` en 1.	No	Configuración del método del planificador para PostgreSQL
El parámetro `innodb_flush_log_at_trx` está desactivado	El valor del parámetro `innodb_flush_log_at_trx` de la instancia de base de datos no es un valor seguro. Este parámetro controla la persistencia de las operaciones de confirmación en el disco. Es recomendable que establezca el parámetro `innodb_flush_log_at_trx` en 1.	Establezca el valor del parámetro `innodb_flush_log_at_trx` en 1.	No	Best practices for configuring performance parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `sync_binlog` está desactivado	La sincronización del registro binario con el disco no se aplica antes de que la confirmación de las transacciones se reconozca en la instancia de base de datos. Es recomendable que establezca el valor del parámetro `sync_binlog` en 1.	Establezca el valor del parámetro `sync_binlog` en 1.	No	Best practices for configuring replication parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `innodb_stats_persistent` está desactivado	Su instancia de base de datos no está configurada para conservar las estadísticas de InnoDB en el disco. Cuando las estadísticas no están almacenadas, se vuelven a calcular cada vez que la instancia se reinicia y se accede a la tabla. Esto provoca variaciones en el plan de ejecución de las consultas. Puede modificar el valor de este parámetro global a nivel de tabla. Es recomendable que establezca el valor del parámetro `innodb_stats_persistent` en `ON`.	Establezca el valor del parámetro `innodb_stats_persistent` en `ON`.	No	Best practices for configuring performance parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `innodb_open_files` es bajo	El parámetro `innodb_open_files` controla el número de archivos que InnoDB puede abrir a la vez. InnoDB abre todos los archivos de registro y de espacio de tablas del sistema cuando se ejecuta mysqld. Su instancia de base de datos tiene un valor bajo para la cantidad máxima de archivos que InnoDB puede abrir a la vez. Le recomendamos que establezca el parámetro `innodb_open_files` en un valor mínimo de 65.	Establezca el parámetro `innodb_open_files` en un valor mínimo de 65.	Sí	Archivos abiertos de InnoDB para MySQL

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `max_user_connections` es bajo	La instancia de base de datos tiene un valor bajo para el número máximo de conexiones simultáneas para cada cuenta de base de datos. Se recomienda aumentar el parámetro `max_user_connections` a un número superior a `5`.	Aumente el valor del parámetro `max_user_connections` a un número superior a `5`.	Sí	Establecimiento de límites de recursos de la cuenta para MySQL
Las réplicas de lectura están abiertas en modo de escritura	Su instancia de base de datos tiene la réplica de lectura en modo de escritura, lo que permite actualizaciones de los clientes. Se recomienda configurar el parámetro `read_only` en `TrueIfReplica` para que las réplicas de lectura no estén en modo de escritura.	Establezca el valor del parámetro `read_only` en `TrueIfReplica`.	No	Best practices for configuring replication parameters for Amazon RDS for MySQL en el blog de AWS Database

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
La configuración del parámetro `innodb_default_row_format` no es segura	Su instancia de base de datos encuentra un problema conocido: una tabla creada en una versión de MySQL anterior a la 8.0.26 con el valor `row_format` establecido en `COMPACT` o `REDUNDANT` será inaccesible e irrecuperable si el índice supera los 767 bytes. Es recomendable que establezca el valor del parámetro `innodb_default_row_format` en `DYNAMIC`.	Establezca el valor del parámetro `innodb_default_row_format` en `DYNAMIC`.	No	Cambios en MySQL 8.0.26

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
El parámetro `general_logging` está activado	El registro general está activado para su instancia de base de datos. Esta configuración es útil para solucionar los problemas de la base de datos. Sin embargo, la activación del registro general aumenta la cantidad de operaciones de E/S y el espacio de almacenamiento asignado, lo que puede provocar problemas de contención y una degradación del rendimiento. Compruebe sus requisitos para el uso del registro general. Es recomendable que establezca el valor del parámetro `general_logging` en `0`.	Compruebe sus requisitos para el uso del registro general. Si no es obligatorio, le recomendamos que establezca el valor del parámetro `general_logging` en `0`.	No	Información general de los registros de bases de datos de RDS para MySQL

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Instancia de RDS con aprovisionamiento insuficiente para la capacidad de memoria del sistema	Se recomienda ajustar las consultas para utilizar menos memoria o utilizar un tipo de instancia de base de datos con una mayor memoria asignada. Cuando la instancia se queda sin memoria, el rendimiento de la base de datos se ve afectado.	Utilice una instancia de base de datos con mayor capacidad de memoria	Sí	Scaling Your Amazon RDS Instance Vertically and Horizontally en el blog de AWS Database Tipos de instancia de Amazon RDS Precios de Amazon RDS
Instancia de RDS con aprovisionamiento insuficiente para la capacidad de CPU del sistema	Le recomendamos que ajuste las consultas para que usen menos CPU o que modifique la instancia de base de datos para que use una clase de instancia de base de datos con una asignación mayor de vCPU. El rendimiento de la base de datos puede disminuir cuando una instancia de base de datos se está quedando sin CPU.	Utilice una instancia de base de datos con mayor capacidad de CPU	Sí	Scaling Your Amazon RDS Instance Vertically and Horizontally en el blog de AWS Database Tipos de instancia de Amazon RDS Precios de Amazon RDS

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Los recursos de RDS no utilizan correctamente el grupo de conexiones	Le recomendamos que habilite Amazon RDS Proxy para agrupar y compartir de manera eficiente las conexiones de bases de datos existentes. Si ya utiliza un proxy para su base de datos, configúrelo correctamente para mejorar la agrupación de conexiones y el equilibrio de carga en varias instancias de base de datos. RDS Proxy puede ayudar a reducir el riesgo de agotamiento y tiempo de inactividad de la conexión, al mismo tiempo que mejora la disponibilidad y la escalabilidad.	Habilite RDS Proxy o modifique la configuración de proxy existente	No	Scaling Your Amazon RDS Instance Vertically and Horizontally en el blog de AWS Database Amazon RDS Proxy Precios de Amazon RDS Proxy

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Las instancias de RDS crean demasiados objetos temporales	Le recomendamos que ajuste la carga de trabajo para evitar la creación excesiva de objetos temporales o que cambie a clases de instancias de RDS que admitan lecturas optimizadas. Las lecturas optimizadas de RDS mejoran el rendimiento de la base de datos para cargas de trabajo que implican una gran cantidad de objetos temporales u objetos temporales de gran tamaño. Evalúe su carga de trabajo para determinar si el uso de una instancia con lecturas optimizadas de RDS beneficia a la carga de trabajo de la base de datos.	Utilice un tipo de instancia de base de datos con lecturas optimizadas de RDS	Sí	Tipos de instancia de Amazon RDS Mejora del rendimiento de las consultas de RDS para MySQL con lecturas optimizadas para Amazon RDS Mejora del rendimiento de las consultas de RDS para MariaDB con lecturas optimizadas para Amazon RDS Mejora del rendimiento de las consultas de RDS para PostgreSQL con lecturas optimizadas para Amazon RDS

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Instancias de RDS con aprovisionamiento insuficiente para la capacidad de IOPS del sistema	Recomendamos ajustar la carga de trabajo de la base de datos para reducir las IOPS o ampliar la instancia de base de datos a un tipo con un límite de IOPS predeterminado superior. La instancia de base de datos actual no admite las IOPS aprovisionadas o la carga de trabajo de la base de datos tiene un uso elevado de las IOPS.	Utilice un tipo de instancia de base de datos con límites de IOPS predeterminados más altos	Sí	Tipos de instancia de Amazon RDS Almacenamiento de instancias de base de datos de Amazon RDS Carga de base de datos

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Las instancias de RDS tienen volúmenes de Amazon EBS con poco aprovisionamiento	Recomendamos ajustar la carga de trabajo de la base de datos para reducir las IOPS o aumentar las IOPS aprovisionadas para la base de datos. Cuando la utilización de las IOPS se acerca a las IOPS aprovisionadas, es posible que el rendimiento de la base de datos disminuya.	Aprovisionamiento de más IOPS para la instancia de base de datos	Sí	Tipos de instancia de Amazon RDS Almacenamiento de instancias de base de datos de Amazon RDS Carga de base de datos
Las instancias de RDS tienen aprovisionamiento insuficiente para la capacidad de rendimiento	Recomendamos ajustar la carga de trabajo de la base de datos para reducir el rendimiento o aumentar el rendimiento aprovisionado para la base de datos. Cuando la utilización del rendimiento se acerca al rendimiento aprovisionado, el rendimiento de la base de datos puede verse afectado.	Aprovisionamiento de más rendimiento para la instancia de base de datos	Sí	Tipos de instancia de Amazon RDS Almacenamiento de instancias de base de datos de Amazon RDS Carga de base de datos

Tipo	Descripción	Recomendación	Tiempo de inactividad requeri	Información adicional
Instancias de RDS con aprovisionamiento insuficiente para E/S de EBS	Recomendamos ajustar la carga de trabajo de la base de datos para reducir las operaciones de E/S o modificar la instancia de base de datos para utilizar los volúmenes de io2 Block Express de Amazon RDS, que están diseñados para cargas de trabajo de bases de datos que requieren alto rendimiento, alta velocidad y baja latencia. Con la carga de trabajo actual, es posible que la base de datos no pueda procesar las operaciones de E/S a la velocidad requerida, lo que puede provocar una degradación del rendimiento.	Utilice los volúmenes de io2 Block Express de Amazon RDS para la instancia de RDS	No	Almacenamiento de instancias de base de datos de Amazon RDS Métricas de Amazon CloudWatch para Amazon RDS Provisioned IOPS SSD volumes en la guía del usuario de Amazon EBS

Consulta de métricas en la consola de Amazon RDS

Amazon RDS se integra con Amazon CloudWatch para mostrar una variedad de métricas de instancia de base de datos de RDS en la consola de RDS. Para obtener descripciones de estas métricas, así como también de las , consulte Referencia de métricas para Amazon RDS.

Para la instancia de base de datos de Aurora, se monitorizan las siguientes categorías de métricas:

- CloudWatch: muestra las métricas de Amazon CloudWatch para RDS a las que puede acceder desde la consola de RDS. También puede acceder a estas métricas desde la consola de CloudWatch. Cada métrica incluye un gráfico que muestra la métrica supervisada a lo largo de un periodo concreto. Para obtener una lista de las métricas de CloudWatch, consulte Métricas de Amazon CloudWatch para Amazon RDS.
- Enhanced monitoring (Supervisión mejorada): muestra un resumen de las métricas del sistema operativo cuando su instancia de base de datos de RDS activa la opción de Supervisión mejorada. RDS entrega las métricas de la supervisión mejorada a su cuenta de Amazon CloudWatch Logs. Cada métrica del sistema operativo incluye un gráfico que muestra la métrica supervisada a lo largo de un periodo concreto. Para obtener una descripción general, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada. Para ver una lista de métricas de Supervisión mejorada, consulte Métricas del sistema operativo en Supervisión mejorada.
- OS Process list (Lista de procesos de sistema operativo): muestra los detalles de cada proceso que se ejecuta en su instancia de base de datos.
- Performance Insights (Información sobre rendimiento): abre el panel de Información sobre rendimiento de la consola de Amazon RDS para una instancia de base de datos en el . Para obtener más detalles acerca de Información sobre rendimiento, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS. Para obtener una lista de las métricas de Información sobre rendimiento, consulte Métricas de Amazon CloudWatch para Información de rendimiento de Amazon RDS.

Amazon RDS ahora ofrece una vista consolidada de las métricas de Información de rendimiento y CloudWatch en el panel de Información de rendimiento. Debe activarse Información de rendimiento para que el clúster de base de datos pueda utilizar esta vista. Puede elegir la nueva vista de monitorización en la pestaña Monitorización o Información de rendimiento en el panel de navegación. Para ver las instrucciones para elegir esta vista, consulte Visualización de las métricas combinadas en la consola de Amazon RDS.

Visualización de las métricas combinadas en la consola de Amazon RDS

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch.
Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Amazon RDS ofrece una vista consolidada de las métricas de Información de rendimiento y CloudWatch de la instancia de base de datos en el panel de Información de rendimiento. Puede utilizar el panel preconfigurado o crear un panel personalizado. El panel preconfigurado proporciona las métricas más utilizadas para ayudar a diagnosticar problemas de rendimiento en un motor de base de datos. Asimismo, puede crear un panel personalizado con las métricas de un motor de base

de datos que cumpla sus requisitos de análisis. A continuación, utilice este panel para todas las instancias de base de datos de ese tipo de motor de base de datos en su cuenta de AWS.

Puede elegir la vista de monitorización en la pestaña Monitorización o Información de rendimiento en el panel de navegación.

Información de rendimiento debe estar activada para la instancia de base de datos para ver las métricas combinadas en el panel de Información de rendimiento. Para obtener más información acerca de la activación de Información de rendimiento, consulte Activación y desactivación de Información de rendimiento de Amazon RDS.

En las siguientes secciones, descubrirá cómo mostrar las métricas de Información de rendimiento y CloudWatch.

Temas

- Elección de la nueva vista de monitorización en la pestaña Monitorización
- Elección de la nueva vista de monitorización desde la página Información de rendimiento
- Creación de un panel personalizado con Información de rendimiento
- Elección del panel preconfigurado con Información de rendimiento

Elección de la nueva vista de monitorización en la pestaña Monitorización

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento.

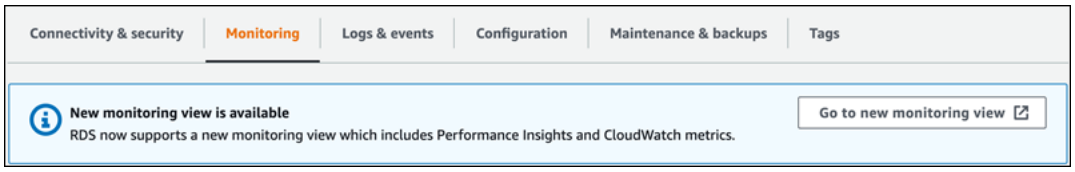
Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Desde la consola de Amazon RDS, puede elegir la nueva vista de monitorización a fin de consultar las métricas de Información de rendimiento y CloudWatch para su instancia de base de datos.

Para elegir la nueva vista de monitorización en la pestaña Monitorización

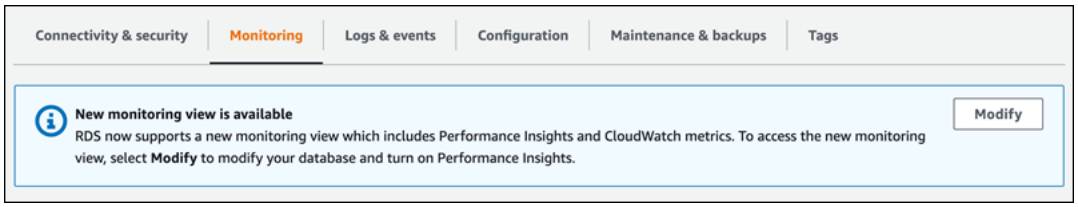
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, elija Bases de datos.
3. Elija la instancia de base de datos de Aurora que desee monitorizar.
4. Desplácese hacia abajo y elija Monitorización.

   Aparece un banner con la opción de elegir la nueva vista de monitorización. En el siguiente ejemplo muestra el banner para elegir la nueva vista de monitorización.



5. Elija Ir a la nueva vista de supervisión para abrir el panel de Información de rendimiento con las métricas de Información de rendimiento y CloudWatch para la instancia de base de datos.
6. (Opcional) Si Información de rendimiento está desactivada para la instancia de base de datos, aparece un banner con la opción de modificar el clúster de base de datos y activar Información de rendimiento

El siguiente ejemplo muestra el banner para modificar el clúster de base de datos en la pestaña Monitorización.



Elija Modificar para modificar el clúster de base de datos y activar Información de rendimiento. Para obtener más información acerca de la activación de Información de rendimiento, consulte Activación y desactivación de Información de rendimiento de Amazon RDS.

Elección de la nueva vista de monitorización desde la página Información de rendimiento

Important

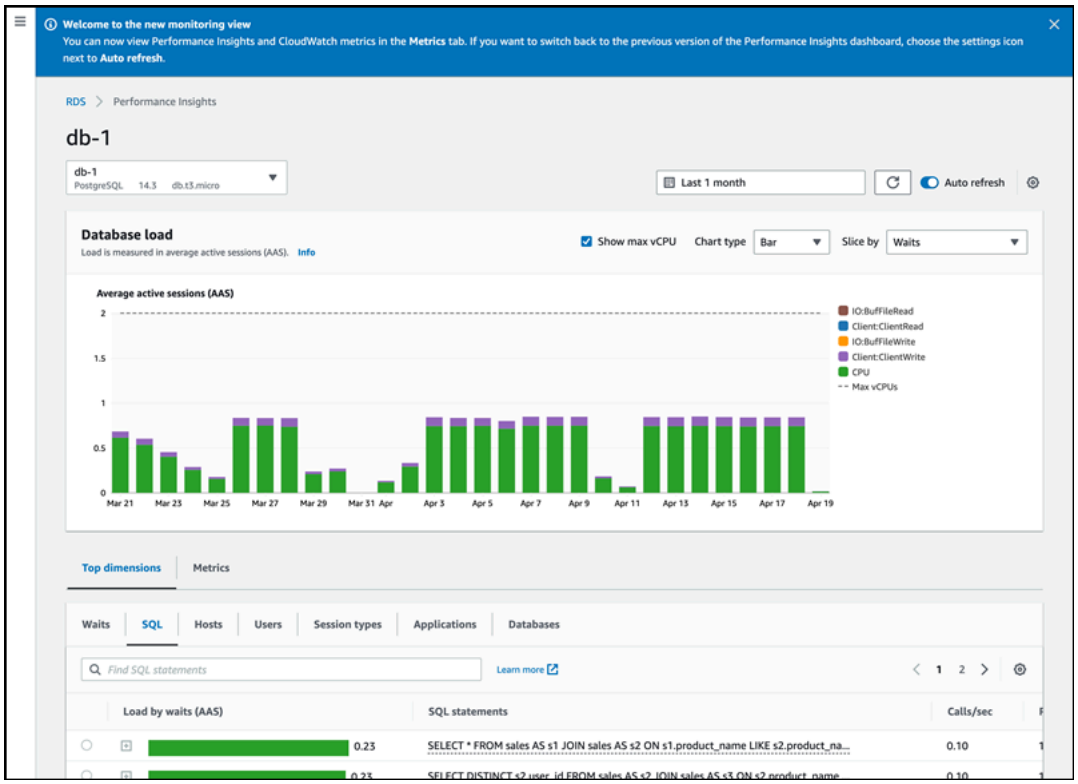
AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.

Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Desde la consola de Amazon RDS, puede elegir la nueva vista de monitorización a fin de consultar las métricas de Información de rendimiento y CloudWatch para su instancia de base de datos.

Elección de la nueva vista de monitorización con Información de rendimiento en el panel de navegación

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Seleccione una instancia de base de datos para ver el panel de Información de rendimiento donde aparecen las métricas de Información de rendimiento y CloudWatch para su instancia de base de datos.



Creación de un panel personalizado con Información de rendimiento

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

En la nueva vista de monitorización, puede crear un panel personalizado con las métricas que necesita para cumplir con los requisitos de análisis.

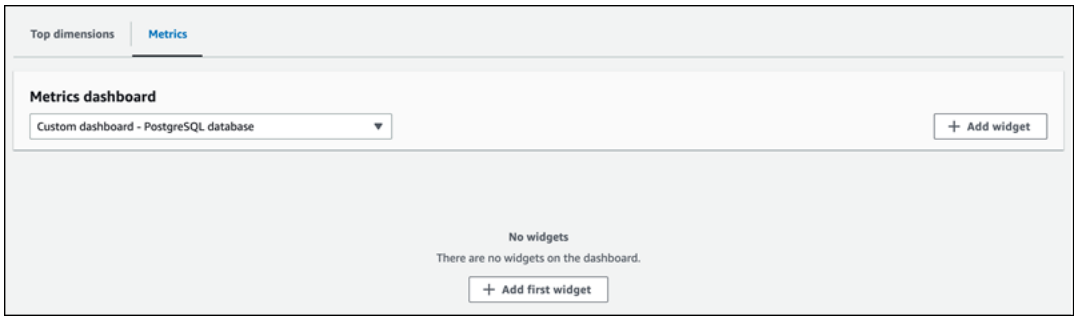
Puede crear un panel personalizado seleccionando las métricas de Información de rendimiento y CloudWatch para la instancia de base de datos. Puede utilizar este panel personalizado para otras instancias de base de datos del mismo tipo de motor de base de datos en su cuenta de AWS.

> **Note**
>
> El panel personalizado admite hasta 50 métricas.

Utilice el menú de configuración del widget para editar o eliminar el panel y mover o cambiar el tamaño de la ventana del widget.

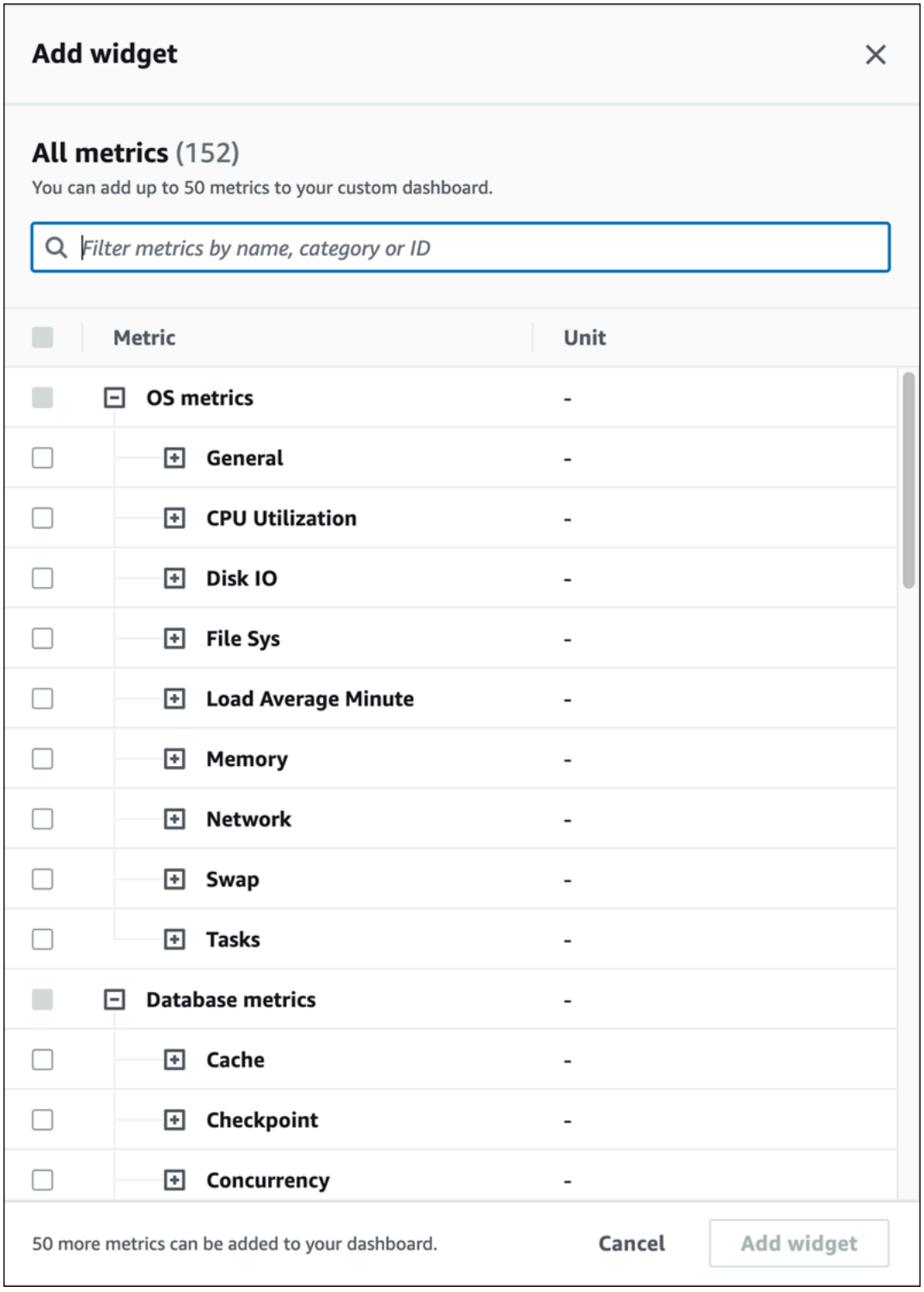
Creación de un panel personalizado con Información de rendimiento en el panel de navegación

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.
4. Desplácese hacia abajo hasta la pestaña Métricas de la ventana.
5. Seleccione el panel personalizado en la lista desplegable. En el siguiente ejemplo se muestra cómo se crea el panel personalizado.



6. Seleccione Agregar widget para abrir la ventana Agregar widget. Puede abrir y ver las métricas del sistema operativo (SO), las métricas de la base de datos y las métricas de CloudWatch disponibles en la ventana.

   El siguiente ejemplo muestra la ventana Agregar widget con las métricas.



7. Seleccione las métricas que desea ver en el panel y elija Agregar widget. Puede utilizar el campo de búsqueda para buscar una métrica específica.

   Las métricas seleccionadas aparecen en el panel.

8. (Opcional) Si quiere modificar o eliminar el panel, seleccione el icono de configuración en la parte superior derecha del widget y, a continuación, seleccione una de las siguientes acciones en el menú.

   - Editar: para modificar la lista de métricas de la ventana. Seleccione Actualizar widget después de seleccionar las métricas del panel.
   - Eliminar: para eliminar el widget. En la ventana de confirmación, elija Eliminar.

Elección del panel preconfigurado con Información de rendimiento

> **Important**
>
> AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
> Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
> Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

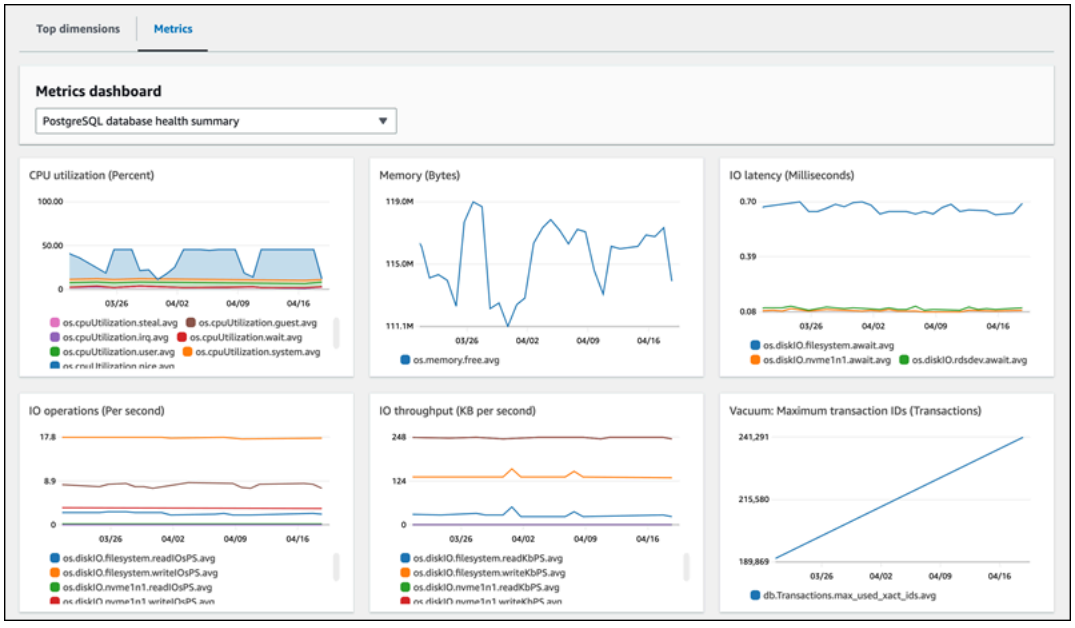
Puede ver las métricas más utilizadas en el panel preconfigurado. Este panel ayuda a diagnosticar problemas de rendimiento con un motor de base de datos y a reducir el tiempo medio de recuperación de horas a minutos.

> **Note**
>
> Este panel no se puede editar.

Elección del panel preconfigurado con Información de rendimiento en el panel de navegación

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.
4. Desplácese hacia abajo hasta la pestaña Métricas de la ventana.
5. Seleccione un panel preconfigurado de la lista desplegable.

   Puede ver las métricas de la instancia de base de datos en el panel. En el siguiente ejemplo se muestra un panel de control de métricas preconfigurado.



Supervisión de métricas de Amazon RDS con Amazon CloudWatch

Amazon CloudWatch es un repositorio de métricas. El repositorio recopila y procesa datos sin procesar de Amazon RDS en métricas legibles y casi en tiempo real. Para ver la lista completa de métricas de Amazon RDS enviadas a CloudWatch, consulte Referencia de métricas para Amazon RDS.

Para analizar y solucionar problemas del rendimiento de las bases de datos a escala, utilice Información sobre las bases de datos de CloudWatch.

Temas

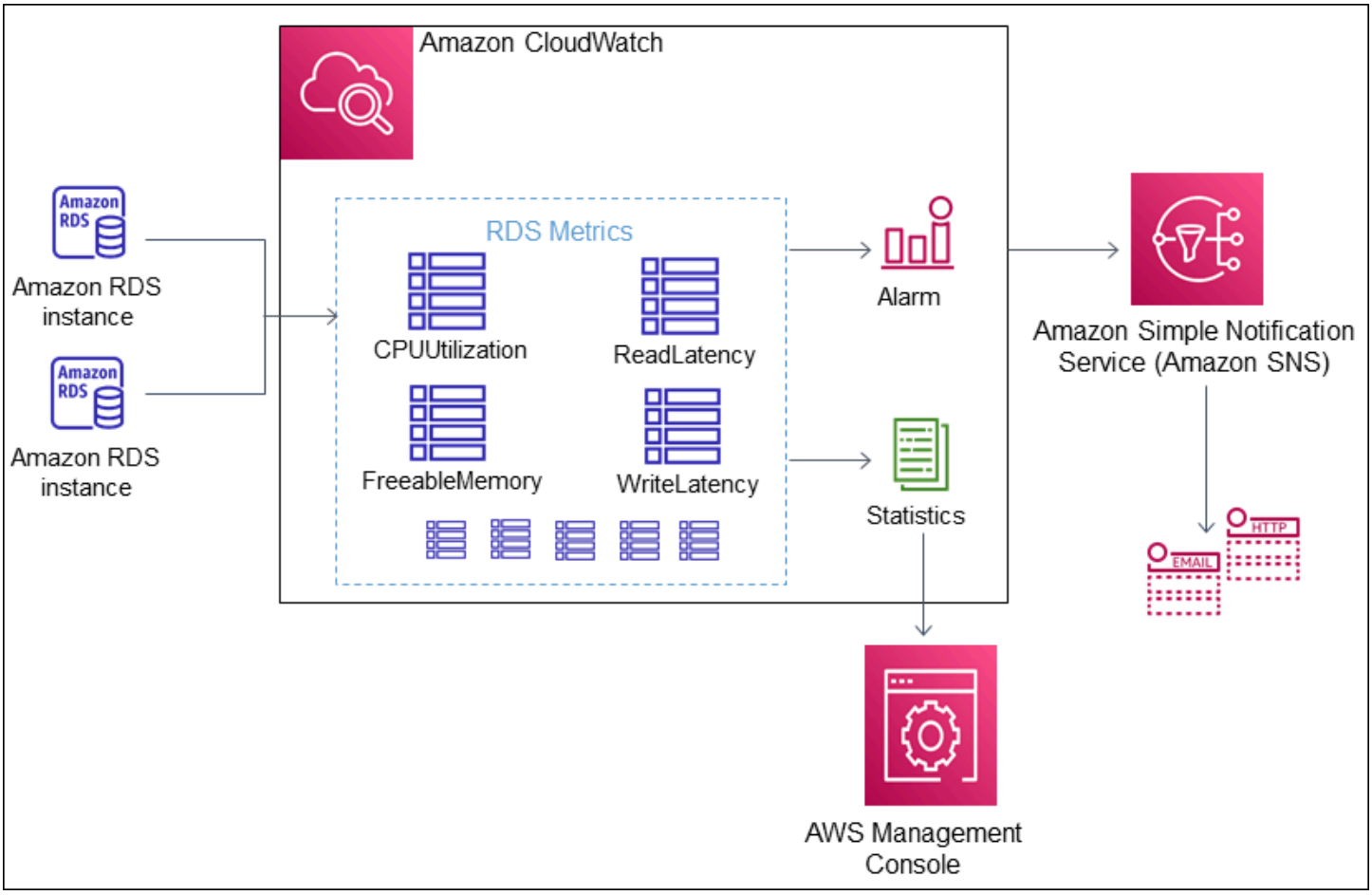
- Información general de Amazon RDS y Amazon CloudWatch
- Visualización de las métricas de la instancia de base de datos en la consola de CloudWatch y la AWS CLI
- Exportación de las métricas de Información sobre rendimiento a CloudWatch
- Creación de alarmas de CloudWatch para supervisar Amazon RDS
- Tutorial: creación de una alarma de Amazon CloudWatch para el retardo de réplica del clúster de base de datos multi-AZ para Amazon RDS

Información general de Amazon RDS y Amazon CloudWatch

De forma predeterminada, Amazon RDS envía datos de métricas a CloudWatch en periodos de 1 minuto. Por ejemplo, la métrica `CPUUtilization` registra el porcentaje de utilización de CPU para una instancia de base de datos a lo largo del tiempo. Los puntos de datos con un periodo de 60 segundos (1 minuto) están disponibles durante 15 días. Esto significa que puede acceder a información histórica y ver el rendimiento de su aplicación web o servicio.

Ahora puede exportar los paneles de métricas de Información de rendimiento desde Amazon RDS a Amazon CloudWatch. Puede exportar paneles de métricas personalizados o preconfigurados como un panel nuevo o añadirlos a un panel de CloudWatch existente. Los paneles de métricas exportados se pueden ver en la consola de CloudWatch. Para obtener más información sobre cómo exportar los paneles de métricas de Información de rendimiento a CloudWatch, consulte Exportación de las métricas de Información sobre rendimiento a CloudWatch.

Tal como se muestra en el siguiente diagrama, puede configurar alarmas para las métricas de CloudWatch. Por ejemplo, podría crear una alarma para cuando la utilización de la CPU para una instancia supere el 70 %. Puede configurar Amazon Simple Notification Service para que le envíe un correo electrónico cuando se supere el umbral.



Amazon RDS publica los siguientes tipos de métricas en Amazon CloudWatch:

- Métricas para las instancias de base de datos de RDS

  Para ver una tabla de estas métricas, consulte Métricas de Amazon CloudWatch para Amazon RDS.

- Métricas de Performance Insights

  Para ver una tabla de estas métricas, consulte Métricas de Amazon CloudWatch para Información de rendimiento de Amazon RDS y Métricas de contador de Información de rendimiento.

- Métricas de Supervisión mejorada (publicadas en registros de Amazon Cloudwatch)

  Para ver una tabla de estas métricas, consulte Métricas del sistema operativo en Supervisión mejorada.

- Métricas de uso de las cuotas de servicio de Amazon RDS en su Cuenta de AWS

Para ver una tabla de estas métricas, consulte Métricas de uso de Amazon CloudWatch para Amazon RDS. Para obtener más información acerca de las cuotas de Amazon RDS, consulte Cuotas y restricciones para Amazon RDS.

Para obtener más información acerca de CloudWatch, consulte ¿Qué es Amazon CloudWatch? en la Guía del usuario de Amazon CloudWatch. Para obtener más información acerca de la retención de métricas de CloudWatch, consulte Retención de métricas.

Visualización de las métricas de la instancia de base de datos en la consola de CloudWatch y la AWS CLI

A continuación, puede encontrar detalles sobre cómo consultar las métricas de su instancia de base de datos mediante CloudWatch. Para obtener información acerca del monitoreo de métricas para el sistema operativo de su instancia de base de datos en tiempo real mediante CloudWatch Logs, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Si utiliza recursos de Amazon RDS, Amazon RDS envía métricas y dimensiones a Amazon CloudWatch cada minuto.

Ahora puede exportar los paneles de métricas de Información de rendimiento desde Amazon RDS a Amazon CloudWatch y ver esas métricas en la consola de CloudWatch. Para obtener más información sobre cómo exportar los paneles de métricas de Información de rendimiento a CloudWatch, consulte Exportación de las métricas de Información sobre rendimiento a CloudWatch.

Utilice los siguientes procedimientos para consultar las métricas de Amazon RDS en la consola de CloudWatch y la CLI.

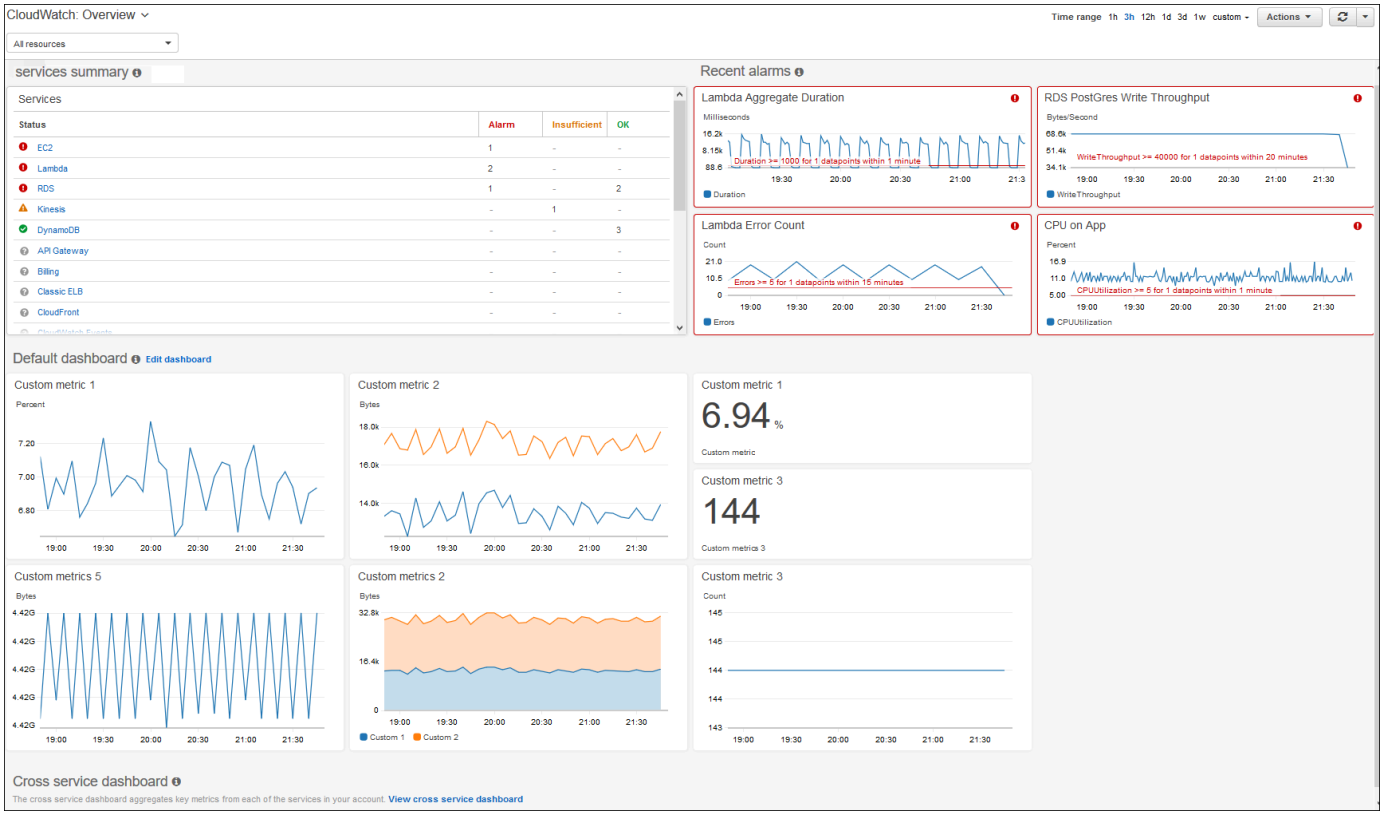
Consola

Para consultar las métricas desde la consola de Amazon CloudWatch

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

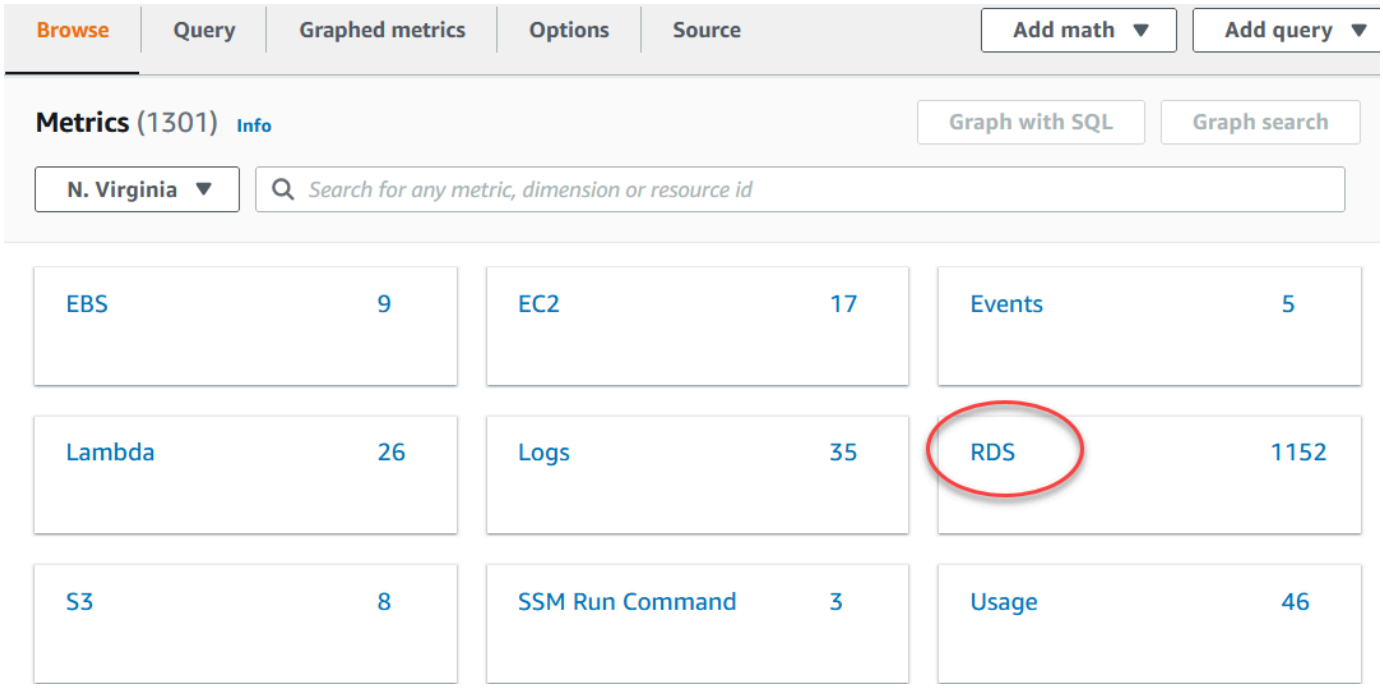
1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.

   Aparece la página de inicio de información general de CloudWatch.



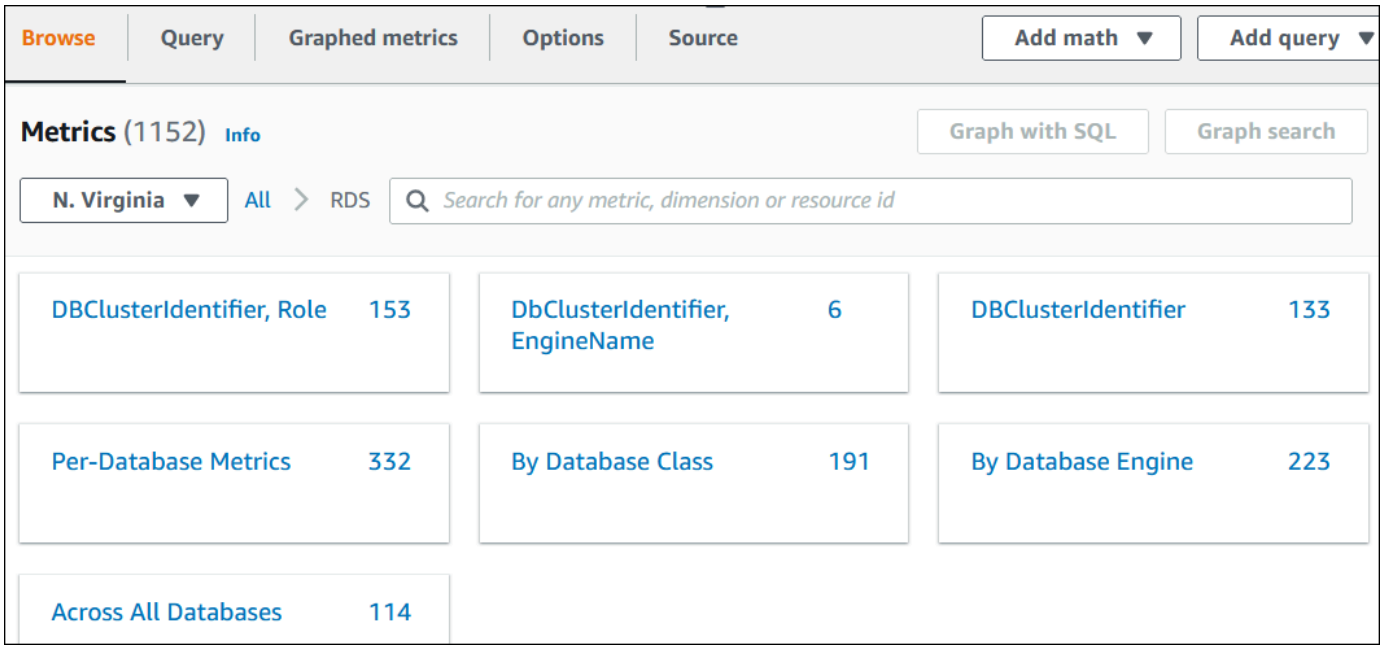
2. Si es necesario, cambie la Región de AWS. En la barra de navegación, elija la Región de AWS donde se encuentran los recursos de AWS. Para obtener más información, consulte Puntos de conexión y Regiones de .

3. En el panel de navegación, elija Metrics (Métricas) y, a continuación, All metrics (Todas las métricas).

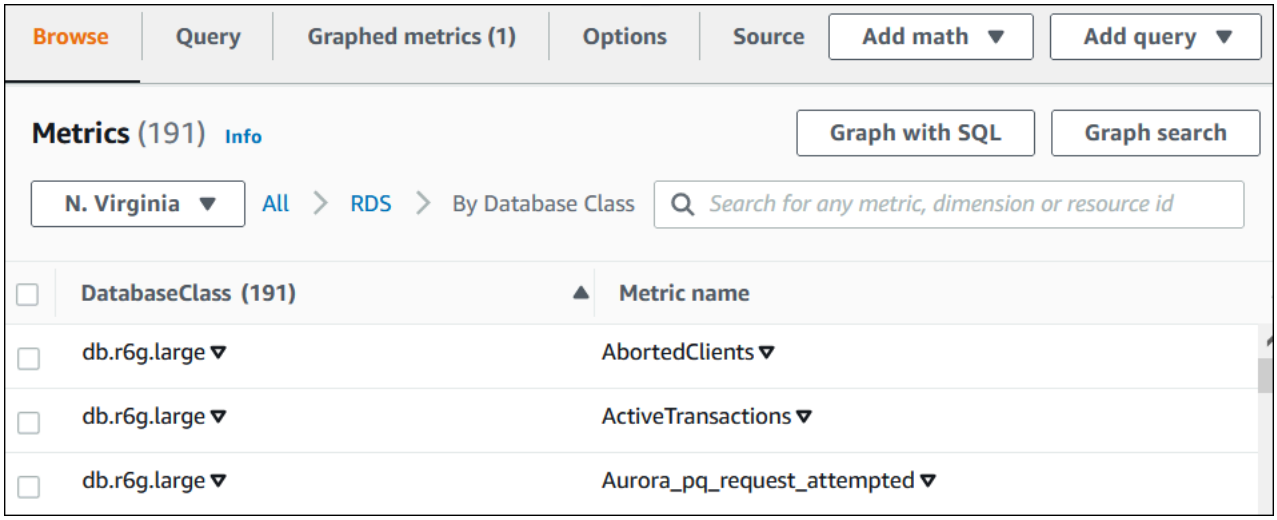


4. Desplácese hacia abajo y elija el espacio de nombres de la métrica de RDS.

   En la página, se muestran las dimensiones de Amazon RDS. Para obtener una descripción completa de estas dimensiones, consulte Dimensiones de Amazon CloudWatch para Amazon RDS..



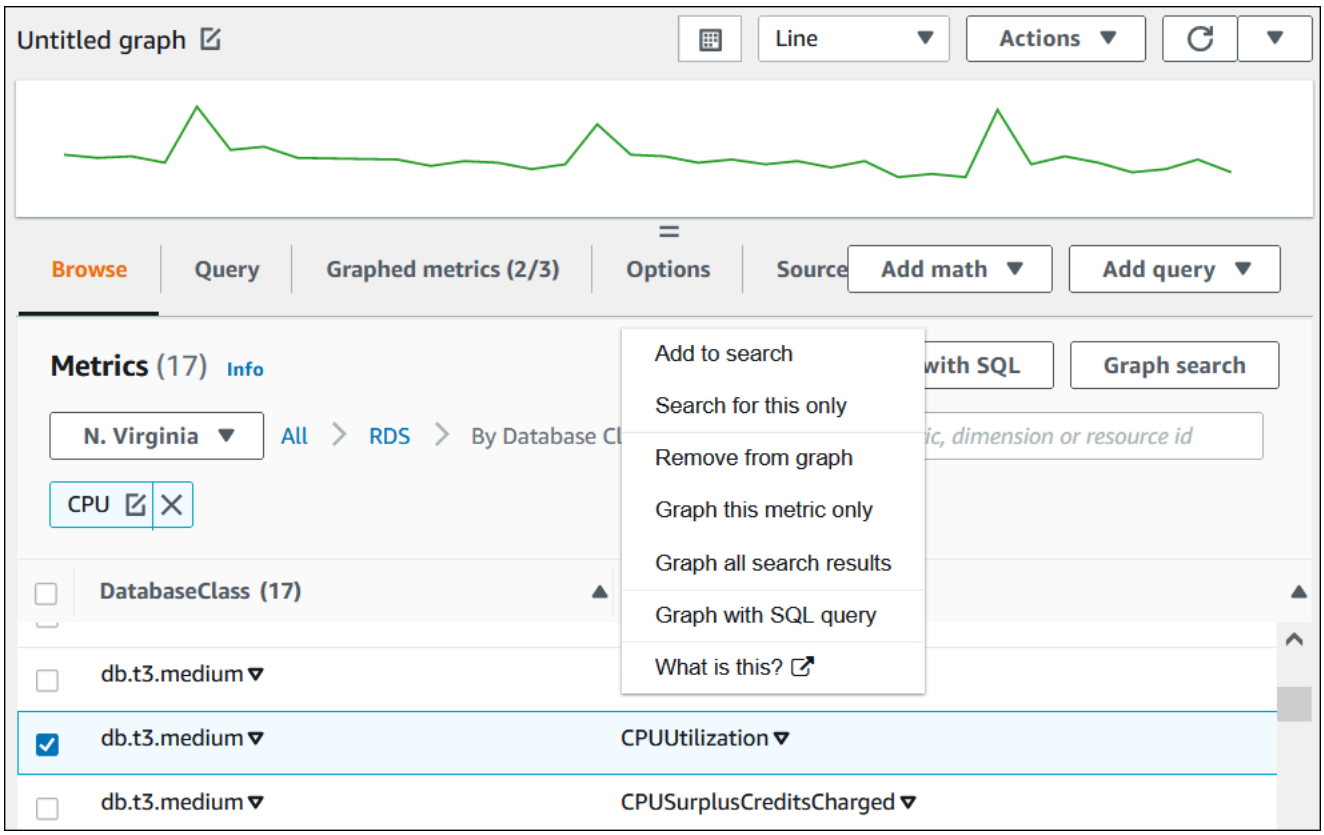
5. Seleccione una dimensión de métrica, por ejemplo, By Database Class (Por clase de base de datos).



6. Realice cualquiera de las siguientes acciones:

   - Para ordenar las métricas, utilice el encabezado de columna.
   - Para representar gráficamente una métrica, active la casilla de verificación situada junto a ella.
   - Para filtrar por recurso, elija el ID de recurso y, a continuación, elija Add to search (Añadir a la búsqueda).
   - Para filtrar por métrica, elija el nombre de la métrica y, a continuación, elija Add to search (Añadir a la búsqueda).

   En el siguiente ejemplo se filtra la clase db.t3.medium y se grafica la métrica CPUUtilization.



AWS CLI

Para obtener información sobre métricas con la AWS CLI, utilice el comando de CloudWatch `list-metrics`. En el siguiente ejemplo, se enumeran todas las métricas del espacio de nombres de `AWS/RDS`.

```
aws cloudwatch list-metrics --namespace AWS/RDS
```

Para obtener datos de métricas, utilice el comando `get-metric-data`.

El siguiente ejemplo obtiene estadísticas de `CPUUtilization` para la instancia `my-instance` en el periodo de 24 horas específico, con un nivel de detalle de 5 minutos.

Cree un archivo JSON denominado `CPU_metric.json` con el siguiente contenido.

```
{
   "StartTime" : "2023-12-25T00:00:00Z",
   "EndTime" : "2023-12-26T00:00:00Z",
   "MetricDataQueries" : [{
```

```
     "Id" : "cpu",
     "MetricStat" : {
    "Metric" : {
        "Namespace" : "AWS/RDS",
        "MetricName" : "CPUUtilization",
        "Dimensions" : [{ "Name" : "DBInstanceIdentifier" , "Value" : my-instance}]
    },
       "Period" : 360,
       "Stat" : "Minimum"
     }
   }]
}
```

Example

Para Linux, macOS o:Unix

```
aws cloudwatch get-metric-data \
    --cli-input-json file://CPU_metric.json
```

En:Windows

```
aws cloudwatch get-metric-data ^
     --cli-input-json file://CPU_metric.json
```

El resultado de ejemplo aparece como se muestra a continuación:

```
{
    "MetricDataResults": [
        {
            "Id": "cpu",
            "Label": "CPUUtilization",
            "Timestamps": [
                "2023-12-15T23:48:00+00:00",
                "2023-12-15T23:42:00+00:00",
                "2023-12-15T23:30:00+00:00",
                "2023-12-15T23:24:00+00:00",
                ...
            ],
            "Values": [
                13.299778337027714,
                13.677507543049558,
```

```
                14.24976250395827,
                13.02521708695145,
                ...
            ],
            "StatusCode": "Complete"
        }
    ],
    "Messages": []
}
```

Para obtener más información, consulte Obtención de estadísticas para una métrica en la Guía del usuario de Amazon CloudWatch.

Exportación de las métricas de Información sobre rendimiento a CloudWatch

Información sobre rendimiento le permite exportar los paneles de métricas preconfiguradas o personalizadas de su instancia de base de datos en Amazon CloudWatch. Puede exportar el panel de métricas como un panel nuevo o añadirlo a un panel de CloudWatch existente. Si decide añadir el panel a un panel de CloudWatch existente, puede crear una etiqueta de encabezado para que las métricas aparezcan en una sección independiente del panel de CloudWatch.

Puede ver el panel de métricas exportado en la consola de CloudWatch. Si añade nuevas métricas a un panel de métricas de Información sobre rendimiento después de exportarlo, debe exportar de nuevo ese panel para ver las nuevas métricas en la consola de CloudWatch.

También puede seleccionar un widget de métricas en el panel de Información sobre rendimiento y ver los datos de las métricas en la consola de CloudWatch.

Para obtener más información sobre cómo ver métricas en la consola de CloudWatch, consulte Visualización de las métricas de la instancia de base de datos en la consola de CloudWatch y la AWS CLI.

En las siguientes secciones, exporte las métricas de Información de rendimiento a CloudWatch como un nuevo panel o a un panel existente, y consulte las métricas de Información de rendimiento en CloudWatch.

Temas

- Exportación de métricas de Información sobre rendimiento como nuevo panel a CloudWatch

- Añadir métricas de Información sobre rendimiento a un panel de CloudWatch existente
- Visualización de un widget de métricas de Información sobre rendimiento en CloudWatch

Exportación de métricas de Información sobre rendimiento como nuevo panel a CloudWatch

Elija un panel de métricas preconfigurado o personalizado del panel de Información sobre rendimiento y expórtelo como un panel nuevo a CloudWatch. Puede ver el panel exportado en la consola de CloudWatch.

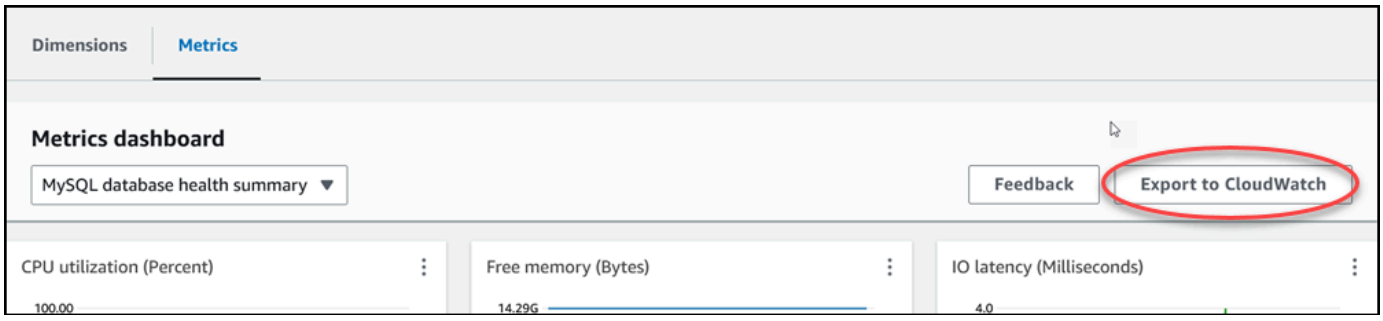
Exportación de un panel de métricas de Información sobre rendimiento como nuevo panel a CloudWatch

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.

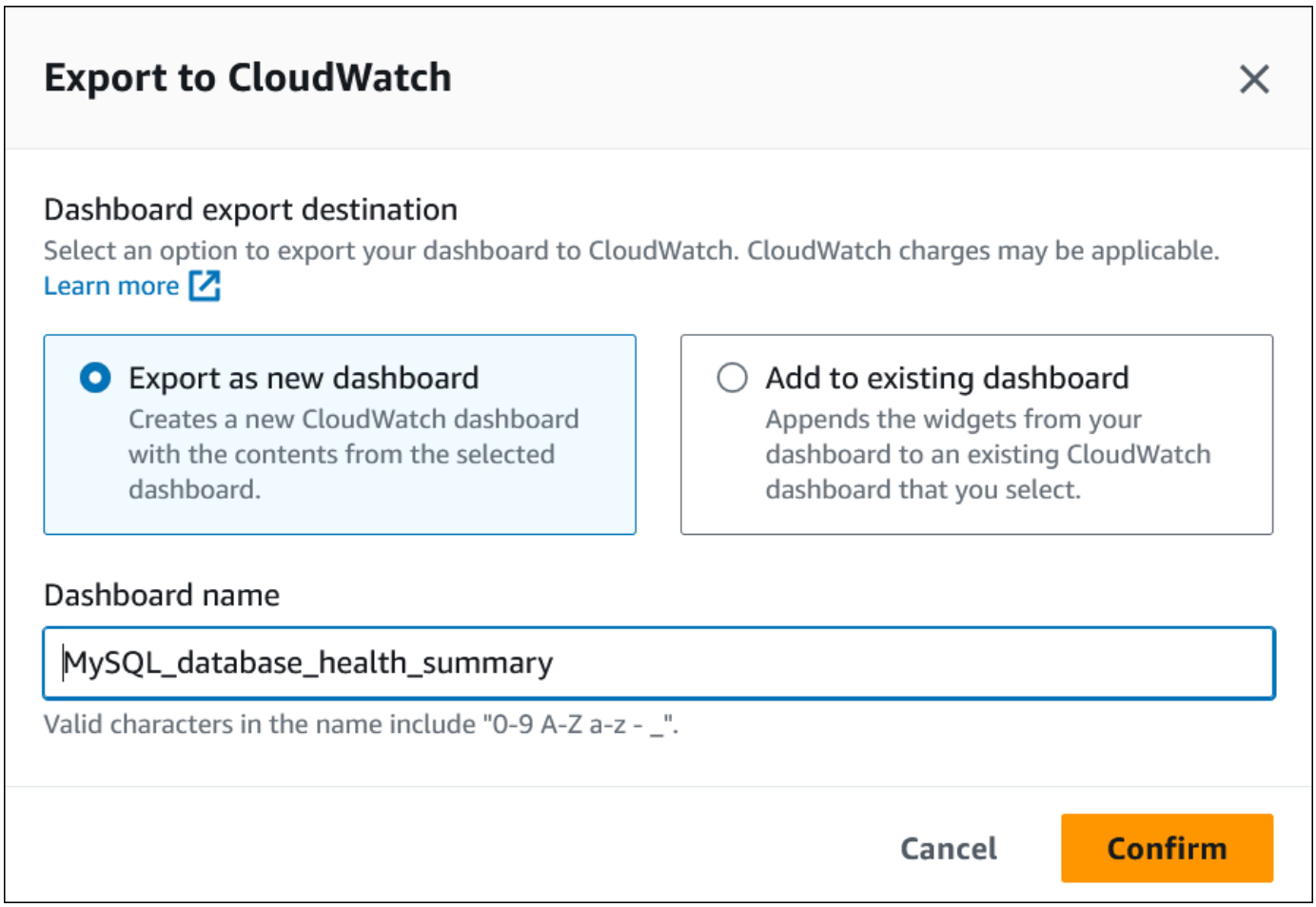
   Se muestra el panel de Información de rendimiento para la instancia de base de datos.
4. Vaya hacia abajo y seleccione Métricas.

   De forma predeterminada, aparece el panel preconfigurado con las métricas de Información sobre rendimiento.
5. Elija un panel preconfigurado o personalizado y, a continuación, seleccione Exportar a CloudWatch.

   Aparecerá la ventana Exportar a CloudWatch.

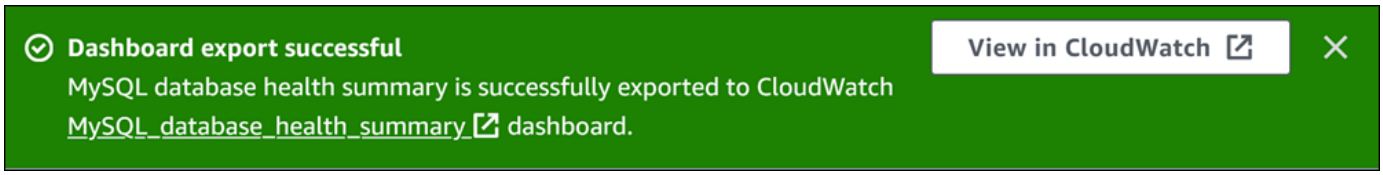


6. Seleccione Exportar como panel nuevo.



7. Introduzca un nombre para el nuevo panel en el campo Nombre del panel y seleccione Confirmar.

   Aparecerá un banner con un mensaje cuando el panel se haya exportado correctamente.



8. Seleccione el enlace o Ver en CloudWatch en el banner para ver el panel de métricas en la consola de CloudWatch.

Añadir métricas de Información sobre rendimiento a un panel de CloudWatch existente

Añada un panel de métricas preconfigurado o personalizado a un panel de CloudWatch existente. Puede añadir una etiqueta al panel de métricas para que aparezca en una sección independiente del panel de CloudWatch.

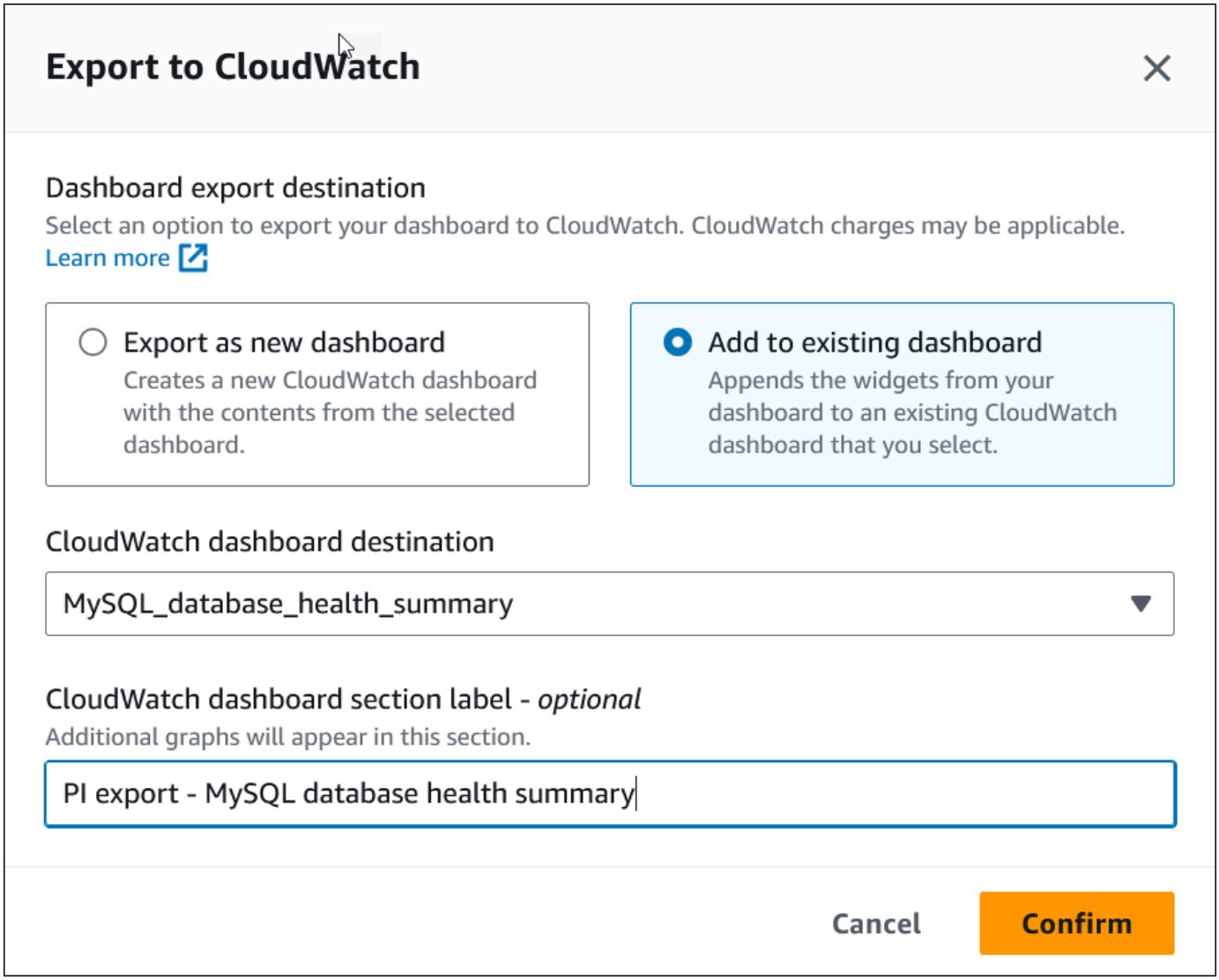
Exportación de métricas a un panel de CloudWatch existente

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.

   Se muestra el panel de Información de rendimiento para la instancia de base de datos.
4. Vaya hacia abajo y seleccione Métricas.

   De forma predeterminada, aparece el panel preconfigurado con las métricas de Información sobre rendimiento.
5. Elija un panel preconfigurado o personalizado y, a continuación, seleccione Exportar a CloudWatch.

   Aparecerá la ventana Exportar a CloudWatch.
6. Seleccione Agregar al panel existente.



7. Especifique el destino y la etiqueta del panel y, a continuación, elija Confirmar.

   - Destino del panel de CloudWatch: elija un panel de CloudWatch existente.
   - Etiqueta de la sección del panel de CloudWatch (opcional): introduzca un nombre para que las métricas de Información sobre rendimiento aparezcan en esta sección del panel de CloudWatch.

   Aparecerá un banner con un mensaje cuando el panel se haya exportado correctamente.

8. Seleccione el enlace o Ver en CloudWatch en el banner para ver el panel de métricas en la consola de CloudWatch.

Visualización de un widget de métricas de Información sobre rendimiento en CloudWatch

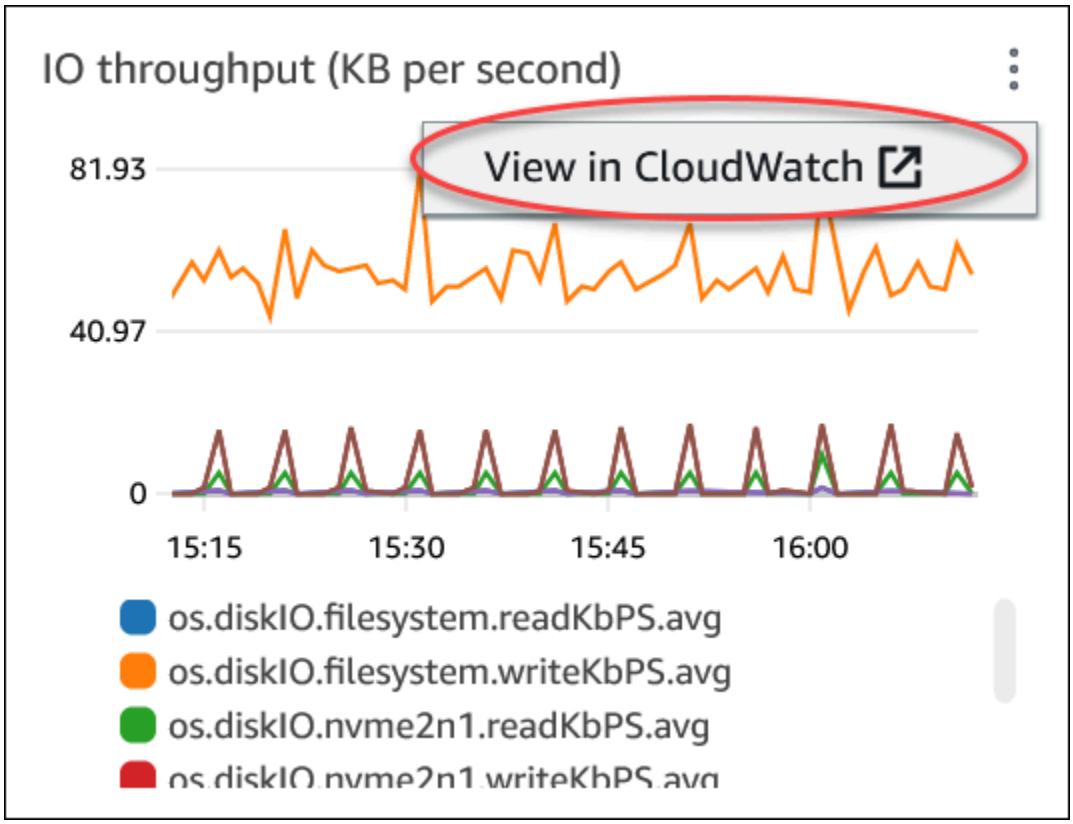
Seleccione un widget de métricas de Información sobre rendimiento en el panel de información de rendimiento de Amazon RDS y consulte los datos de métricas en la consola de CloudWatch.

Exportación de un widget de métricas y visualización de los datos de métricas en la consola de CloudWatch

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.

   Se muestra el panel de Información de rendimiento para la instancia de base de datos.
4. Vaya hacia abajo hasta llegar a Métricas.

   De forma predeterminada, aparece el panel preconfigurado con las métricas de Información sobre rendimiento.
5. Seleccione un widget de métricas y, a continuación, seleccione Ver en CloudWatch en el menú.



Los datos de métricas aparecen en la consola de CloudWatch.

Creación de alarmas de CloudWatch para supervisar Amazon RDS

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. La alarma realiza una o varias acciones en función del valor de la métrica con respecto a un umbral determinado durante varios periodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Amazon EC2 Auto Scaling.

Las alarmas invocan acciones únicamente para los cambios de estado prolongados. Las alarmas de CloudWatch no invocan acciones simplemente porque estén en un estado particular. El estado debe haber cambiado y debe haberse mantenido durante el número de periodos de tiempo especificado.

Puede utilizar la función matemática de métricas DB_PERF_INSIGHTS de la consola de CloudWatch para consultar Amazon RDS para conocer las métricas de los contadores de Información sobre rendimiento. La función DB_PERF_INSIGHTS también incluye la métrica DBLoad en intervalos de menos de un minuto. Puede establecer alarmas de CloudWatch sobre estas métricas.

Para obtener más información sobre cómo crear una alarma, consulte Create an alarm on Performance Insights counter metrics from an AWS database (Crear una alarma en las métricas de contador de Información sobre rendimiento desde una base de datos de AWS).

Para configurar una alarma mediante la AWS CLI

- Llame a `put-metric-alarm`. Para obtener más información, consulte la referencia de comandos de la AWS CLI.

Para configurar una alarma mediante la API de CloudWatch

- Llame a `PutMetricAlarm`. Para obtener más información, consulte la referencia de la API de Amazon CloudWatch.

Para obtener más información sobre la configuración de los temas de Amazon SNS y la creación de alarmas, consulte Uso de las alarmas de Amazon CloudWatch.

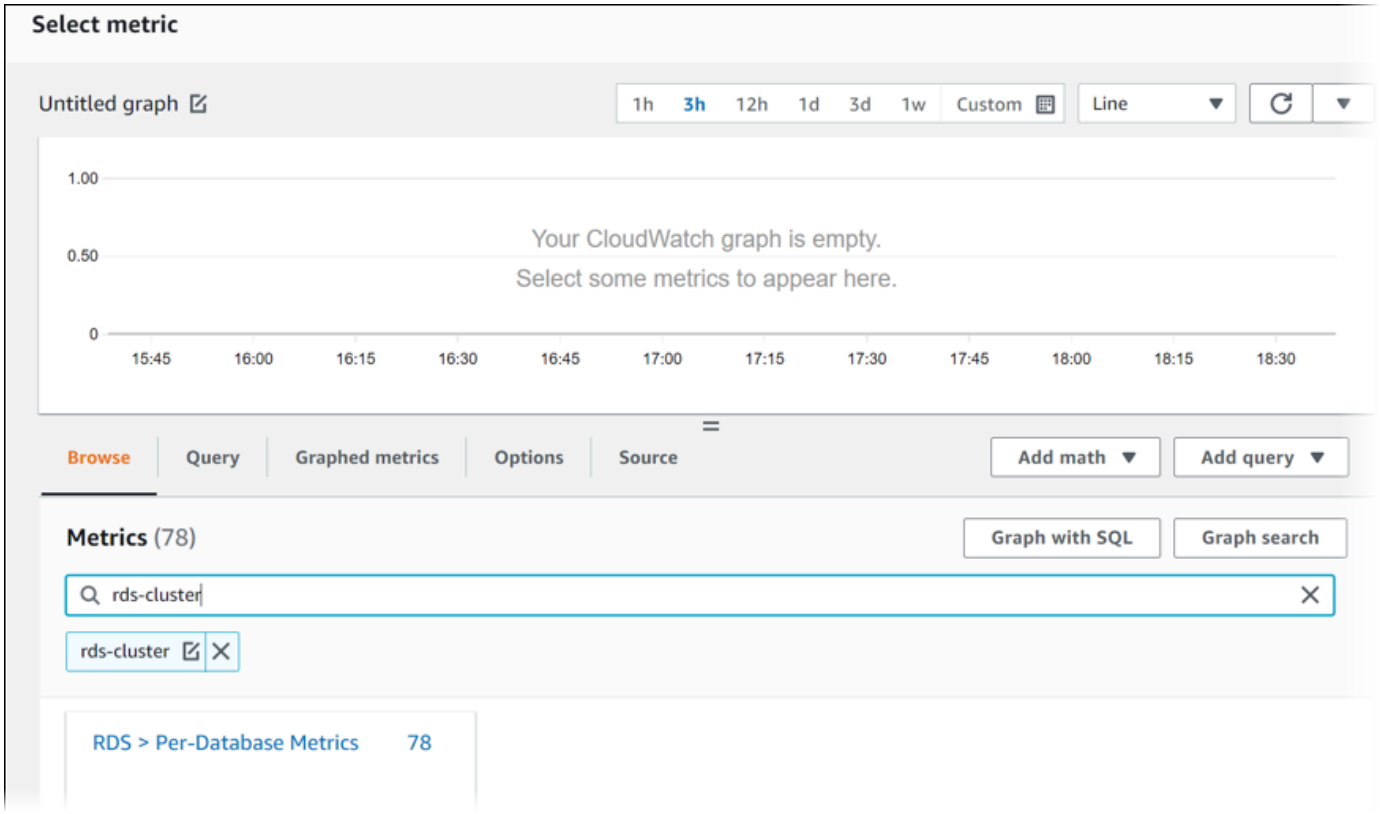
Tutorial: creación de una alarma de Amazon CloudWatch para el retardo de réplica del clúster de base de datos multi-AZ para Amazon RDS

Puede crear una alarma de Amazon CloudWatch que envíe un mensaje de Amazon SNS cuando el retraso de la réplica de un clúster de una base de datos Multi-AZ supere un límite. Una alarma vigila la métrica de `ReplicaLag` durante el periodo especificado. La acción es una notificación que se envía a un tema de Amazon SNS o a una política de Amazon EC2 Auto Scaling.

Para configurar una alarma de CloudWatch para el retraso de réplica de un clúster de bases de datos Multi-AZ

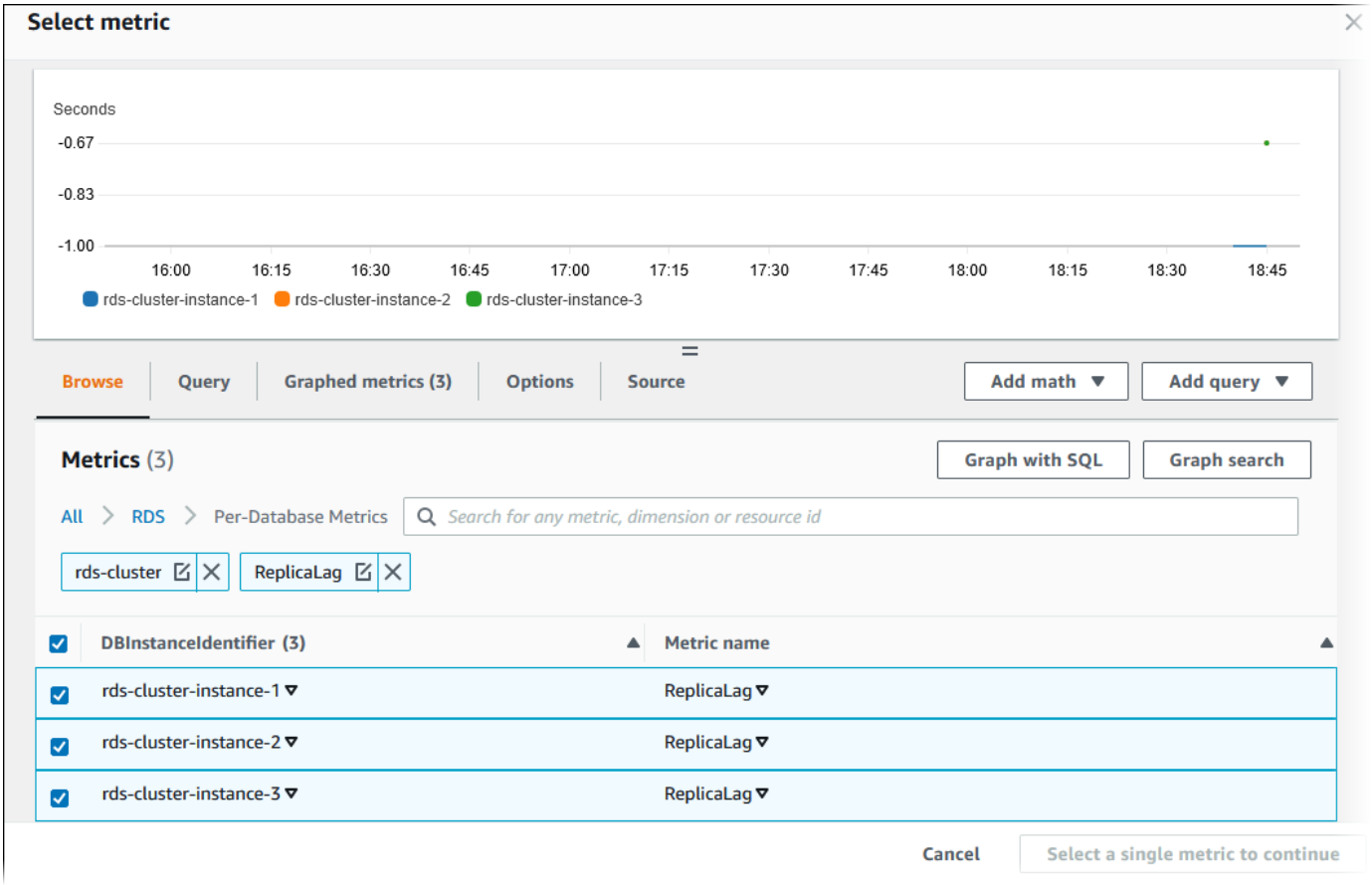
1. Inicie sesión en la AWS Management Console y abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas) y, luego, Create Alarm (Crear alarma).
3. Elija Create alarm (Crear alarma).
4. En la página Especificar métricas y condiciones, elija Seleccionar métrica.
5. En el cuadro de búsqueda, ingrese el nombre del clúster de bases de datos Multi-AZ y presione Enter (Ingresar).

   En la siguiente imagen, se muestra la página Select metric (Seleccionar métrica) con un clúster de bases de datos Multi-AZ denominado `rds-cluster` que ya está ingresado.



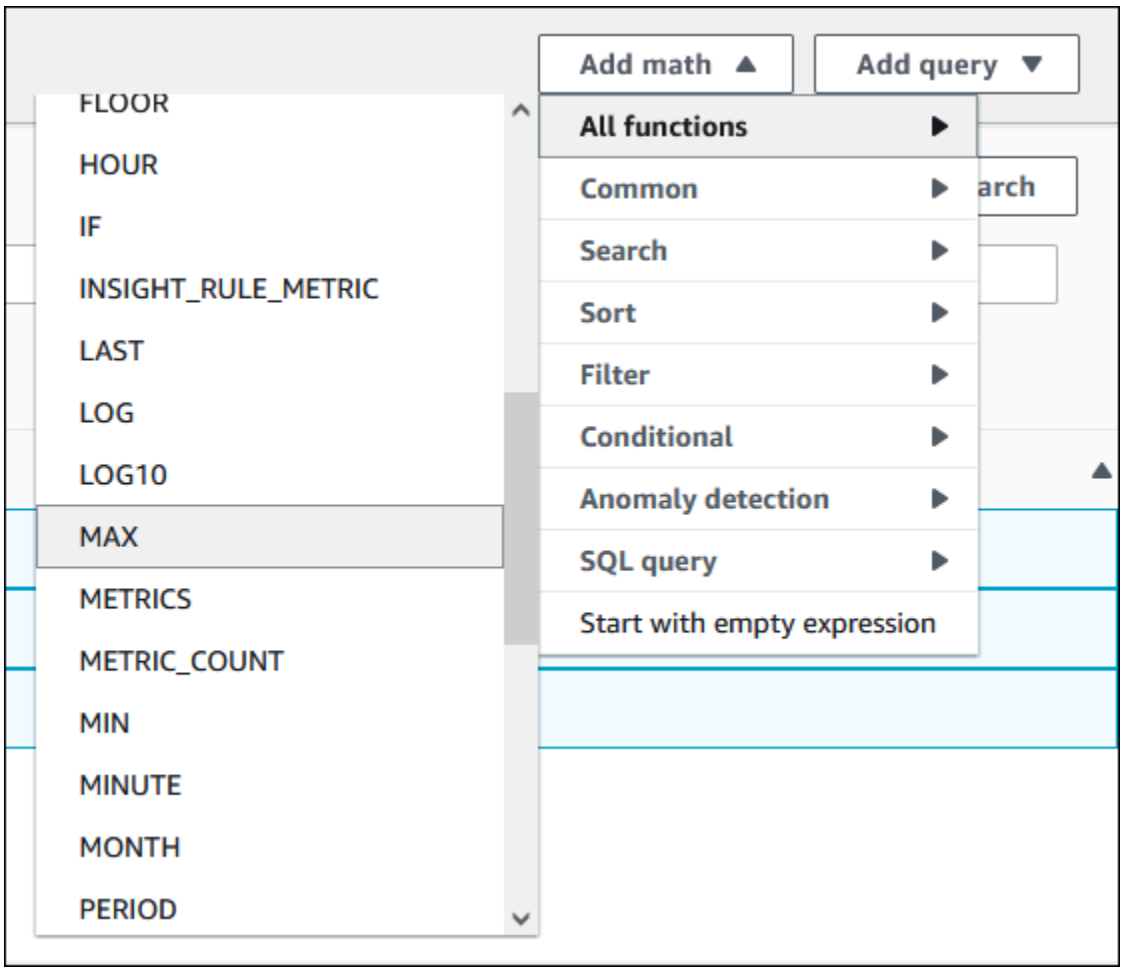
6. Elija RDS, Per-Database Metrics (Métricas por base de datos).
7. En el cuadro de búsqueda, ingrese **`ReplicaLag`** y presione Enter (Ingresar) y, a continuación, seleccione cada instancia de base de datos del clúster en el clúster de bases de datos.

   En la siguiente imagen, se muestra la página Select metric (Seleccionar métrica) con las instancias de base de datos seleccionadas para la métrica ReplicaLag.



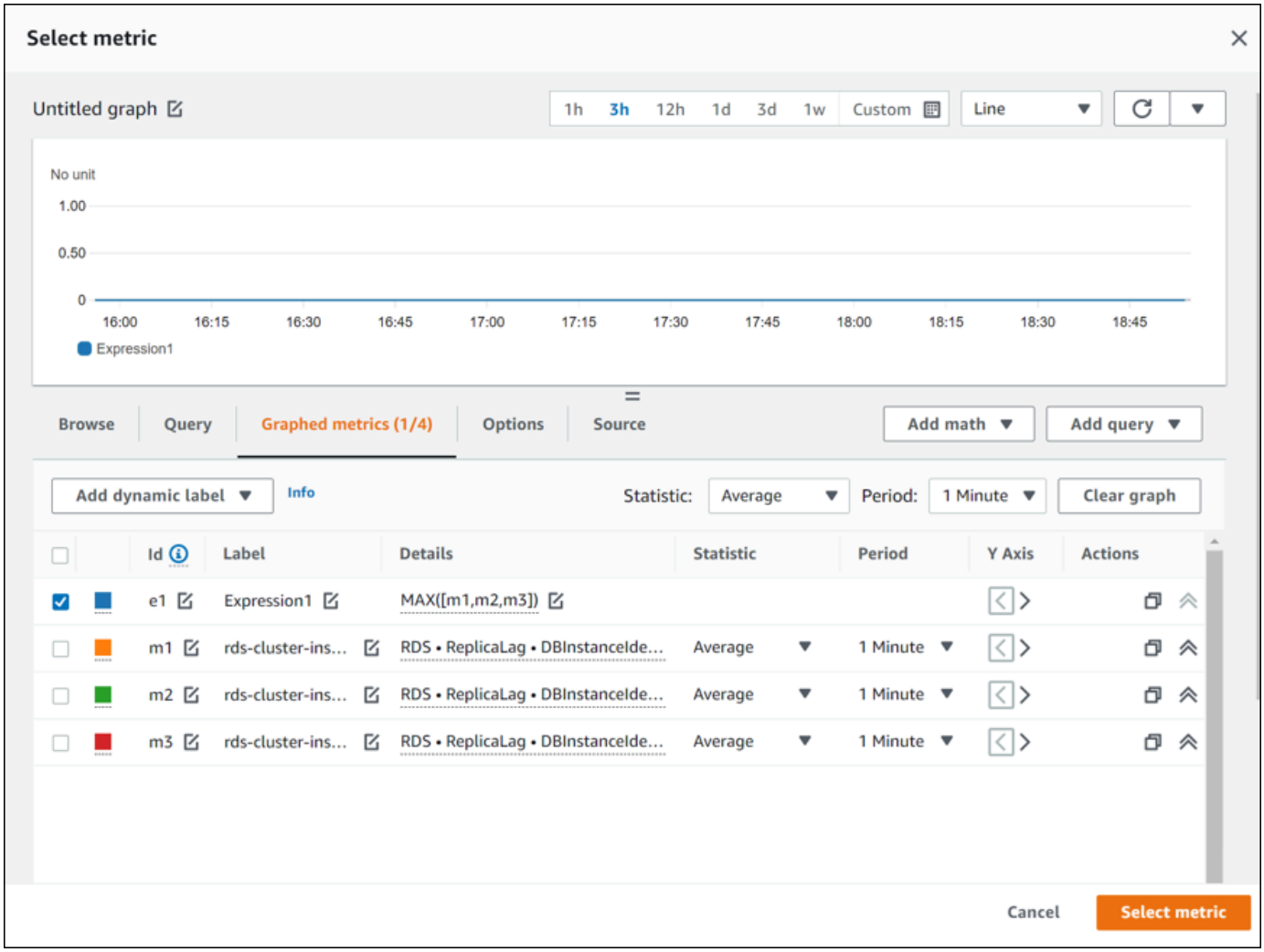
Esta alarma considera el retraso de réplica de las tres instancias de base de datos del clúster de bases de datos Multi-AZ. La alarma reacciona cuando cualquier instancia de base de datos supera el límite. Utiliza una expresión matemática que devuelve el valor máximo de las tres métricas. Clasifique por nombre de métrica y, a continuación, elija las tres métricas de ReplicaLag.

8. En Add math (Agregar matemáticas), elija All functions (Todas las funciones), MAX.



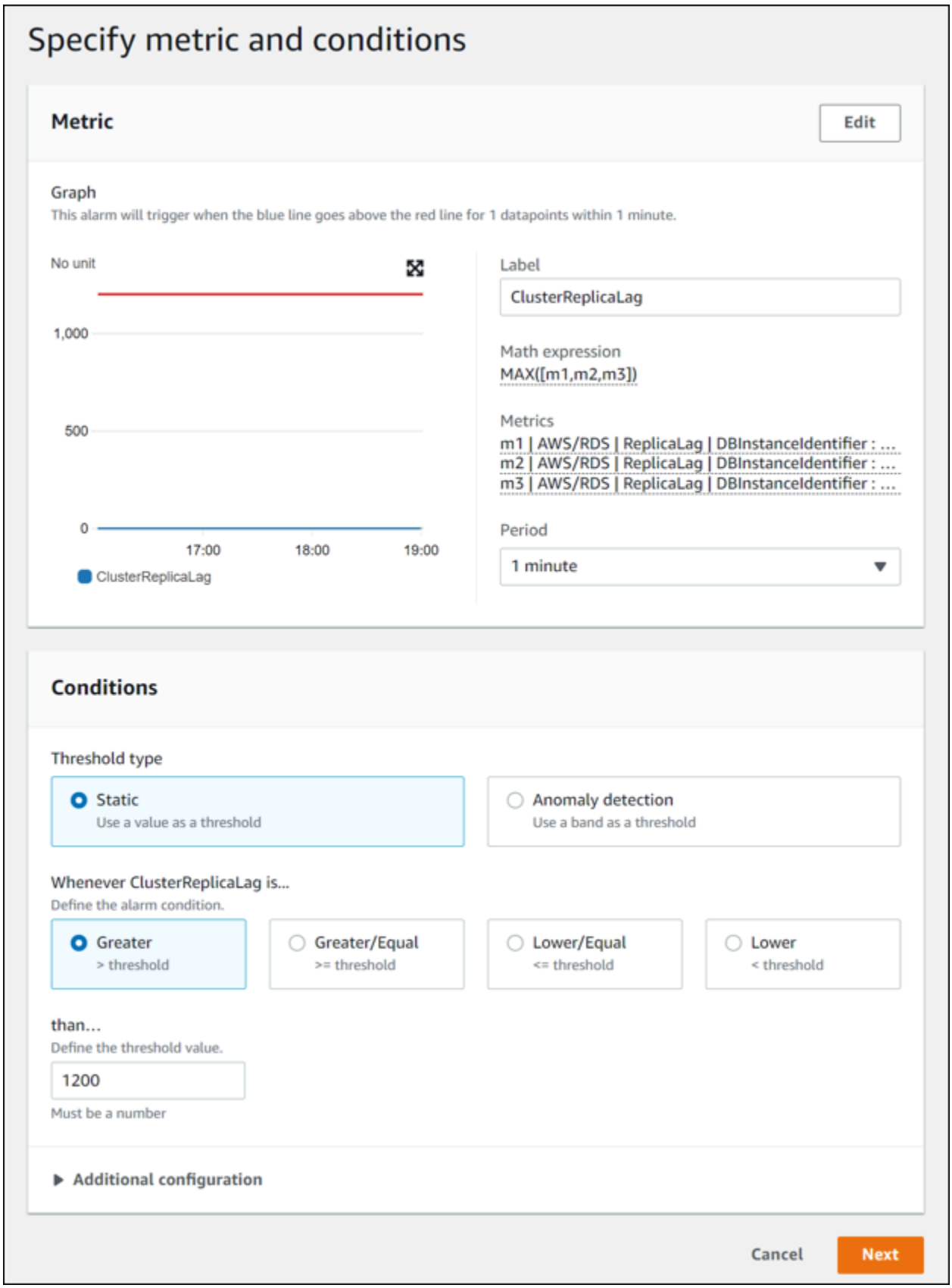
9. Elija la pestaña Graphed metrics (Representación gráfica de las métricas) y cambie los datos de Expression1 a **`MAX([m1,m2,m3])`**.
10. Para las tres métricas de ReplicaLag, cambie el Period (Periodo) a 1 minute (1 minuto).
11. Borre la selección de todas las métricas excepto la de Expression1.

    La página Select metric (Seleccionar métrica) debería tener un aspecto similar al de la siguiente imagen.



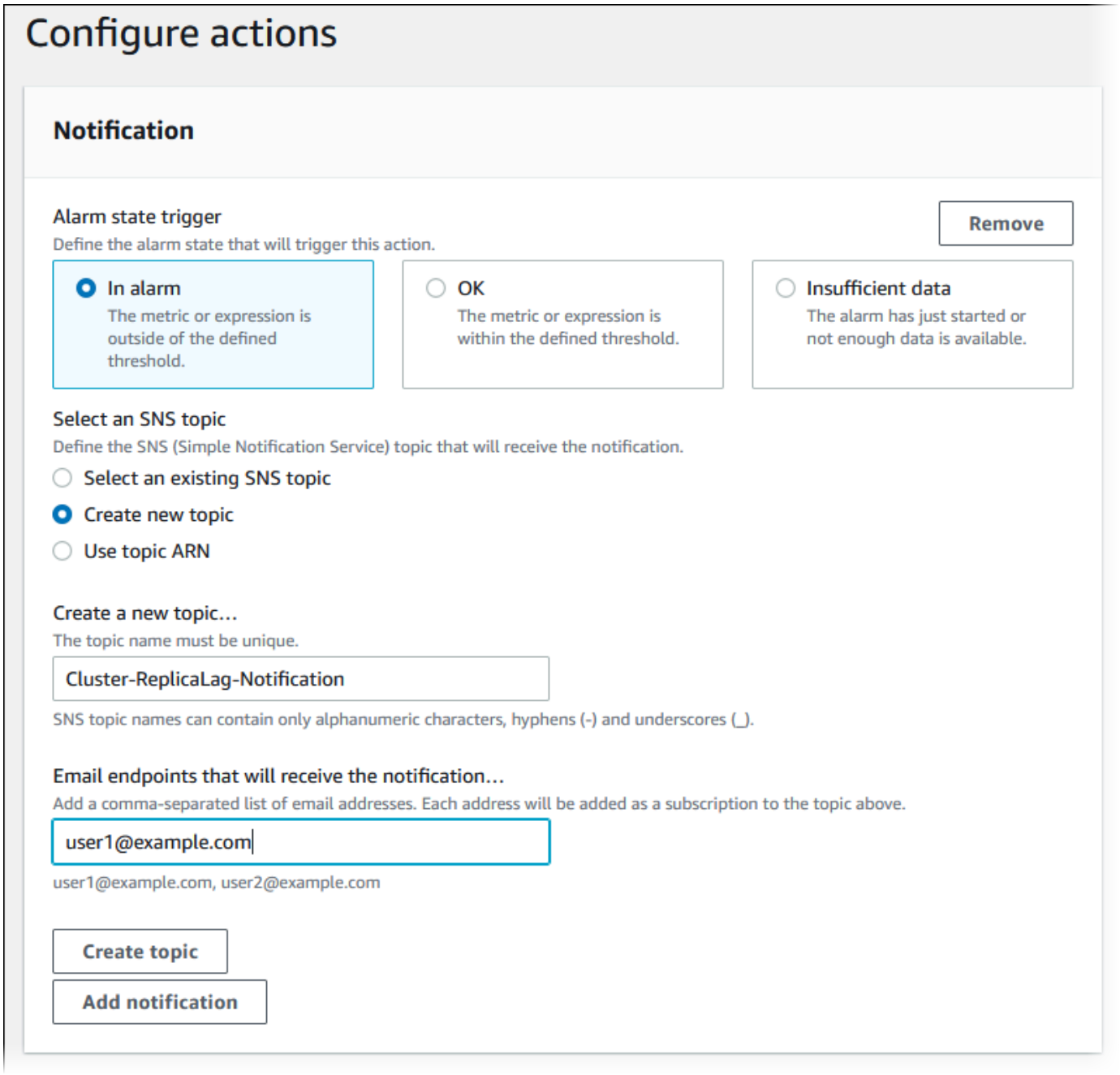
12. Elija Seleccionar métrica.
13. En la página Specify metric and conditions (Especificar métrica y condiciones), cambie la etiqueta por un nombre significativo, por ejemplo **`ClusterReplicaLag`** e ingrese un número de segundos en Define the threshold value (Definir el valor del límite). En este tutorial, seleccione **`1200`** segundos (20 minutos). Puede ajustar este valor para los requisitos de la carga de trabajo.

    La página Specify metric and conditions (Especificar métrica y condiciones) debería tener un aspecto similar al de la siguiente imagen.

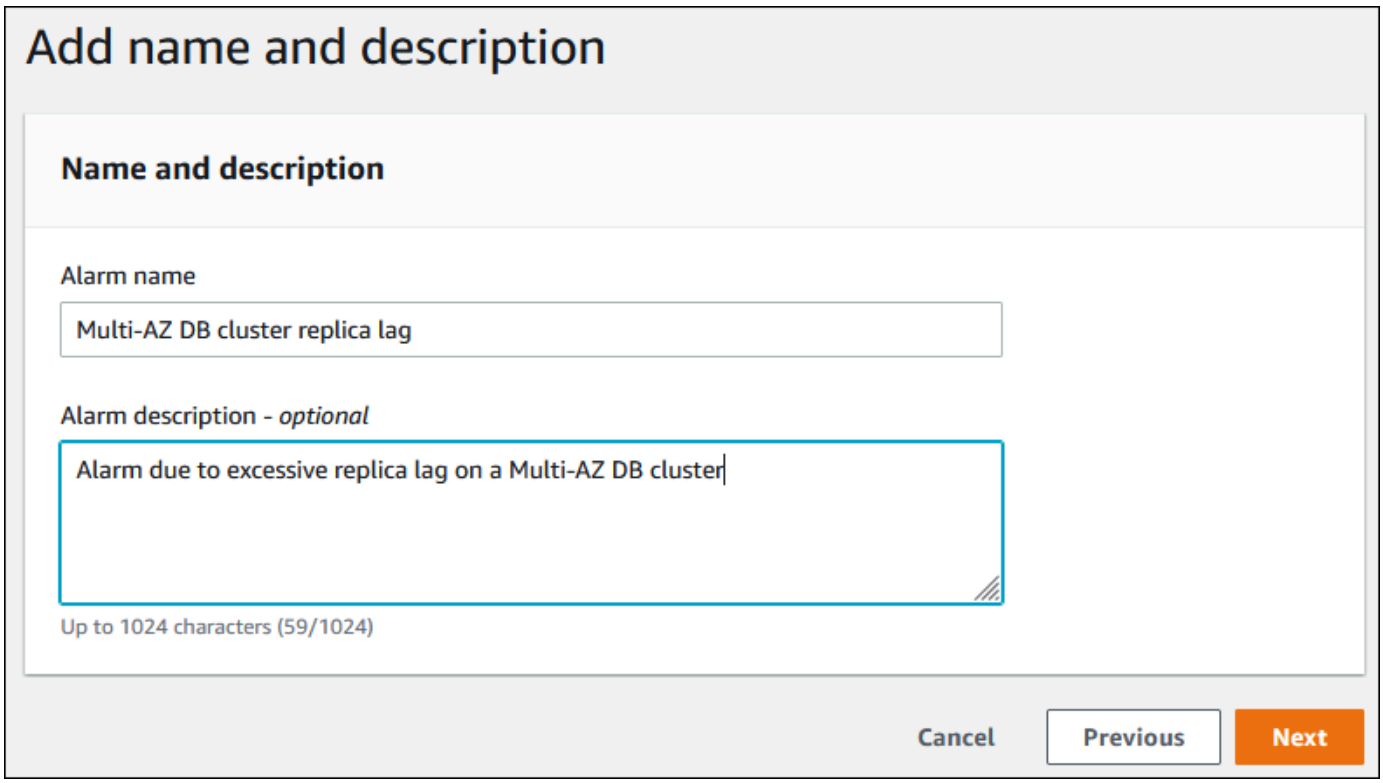


14. Elija Next (Siguiente) para abrir la página Configure actions (Configurar acciones).

15. Mantenga seleccionado In alarm (En alarma), elija Create new topic (Crear tema nuevo) e ingrese el nombre del tema y una dirección de email.



16. Elija Create topic (Crear tema) y después Next (Siguiente).
17. En la página Add name and description (Agregar nombre y descripción), ingrese un Alarm name (Nombre de alarma) y una Alarm description (Descripción de alarma) y, a continuación, elija Next (Siguiente).



18. Previsualice la alarma que va a crear en la página Preview and create (Previsualizar y crear) y, a continuación, elija Create alarm (Crear alarma).

Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch

Supervise la carga de la base de datos (carga de DB) de su flota de instancias de bases de datos de Amazon RDS con Información sobre las bases de datos. La carga de la base de datos mide el nivel de actividad de la sesión en la base de datos. Puede utilizar Información sobre las bases de datos para analizar y solucionar problemas del rendimiento de las bases de datos de Amazon RDS a escala.

Con Información sobre las bases de datos, puede visualizar la carga de la base de datos en su flota de bases de datos y filtrar la carga por esperas, instrucciones SQL, hosts o usuarios.

De forma predeterminada, RDS habilita el modo estándar de Información sobre las bases de datos para las bases de datos de Amazon RDS.

Para obtener información sobre el uso de Información sobre las bases de datos en la consola de Amazon CloudWatch, consulte Información sobre bases de datos de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Precios

Para obtener información acerca de los precios, consulte Precios de Amazon CloudWatch.

Temas

- Compatibilidad con el motor de base de datos de Amazon RDS, la región y la clase de instancia para Información sobre las bases de datos
- Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS
- Activación del modo estándar de Información sobre las bases de datos para Amazon RDS
- Configuración de la base de datos para supervisar las consultas SQL lentas con Información sobre las bases de datos para Amazon RDS
- Consideraciones acerca de Información sobre las bases de datos para Amazon RDS

Compatibilidad con el motor de base de datos de Amazon RDS, la región y la clase de instancia para Información sobre las bases de datos

Las siguiente tabla indica los motores de base de datos de Amazon RDS que admiten la Información sobre las bases de datos.

Motor de base de datos de Amazon RDS	Versiones de motor y regiones compatibles	Restricciones de clase de instancia
Amazon RDS para MariaDB	Para obtener más informaci ón sobre la disponibilidad en versiones y regiones de Informaci ón sobre las bases de datos con RDS para MariaDB, consulte Regiones y motores de base de datos admitidos para Informaci ón sobre rendimiento en Amazon RDS.	Información sobre las bases de datos no es compatible con las siguientes clases de instancia: • db.t2.micro • db.t2.small • db.t3.micro • db.t3.small • db.t4g.micro • db.t4g.small
RDS para MySQL	Para obtener más informaci ón sobre la disponibilidad en versiones y regiones de Informaci ón sobre las bases de datos con RDS para MySQL, consulte Regiones y motores de base de datos admitidos para Informaci ón sobre rendimiento en Amazon RDS.	Información sobre las bases de datos no es compatible con las siguientes clases de instancia: • db.t2.micro • db.t2.small • db.t3.micro • db.t3.small • db.t4g.micro • db.t4g.small

Motor de base de datos de Amazon RDS	Versiones de motor y regiones compatibles	Restricciones de clase de instancia
Amazon RDS for Microsoft SQL Server	Para obtener más informaci ón sobre la disponibilidad en versiones y regiones de Informaci ón sobre las bases de datos con RDS para SQL Server, consulte Regiones y motores de base de datos admitidos para Informaci ón sobre rendimiento en Amazon RDS.	N/A
Amazon RDS para PostgreSQL	Para obtener más informaci ón sobre la disponibilidad en versiones y regiones de Informaci ón sobre las bases de datos con RDS para PostgreSQL, consulte Regiones y motores de base de datos admitidos para Informaci ón sobre rendimiento en Amazon RDS.	N/A
Amazon RDS para Oracle	Para obtener más informaci ón sobre la disponibilidad en versiones y regiones de Informaci ón sobre las bases de datos con RDS para Oracle, consulte Regiones y motores de base de datos admitidos para Informaci ón sobre rendimiento en Amazon RDS.	N/A

Compatibilidad con el motor de base de datos de Amazon RDS, la región y la clase de instancia para características de información sobre las bases de datos

Las siguiente tabla indica los motores de base de datos de Amazon RDS que admiten las características de la información sobre las bases de datos.

Característica	Niveles de precios	Regiones admitidas	Motores de bases de datos compatibles	Clases de instancias admitidas
Estadísticas de SQL para Performance Insights	Todos	Todos	Todos	Todos
Análisis de planes de ejecución de Oracle mediante el panel de Información de rendimiento para Amazon RDS	Todos	Todos	RDS para Oracle	Todos
Análisis del rendimiento de la base de datos durante un período de tiempo	Solo nivel de pago	Todos	• RDS para MariaDB • RDS para MySQL • RDS para PostgreSQL	Todos
Visualización de las recomendaciones proactivas de Información de rendimiento	Solo nivel de pago	• Este de EE. UU. (Ohio) • Este de EE. UU. (Norte de Virginia)	Todos	Todos

Característica	Niveles de precios	Regiones admitidas	Motores de bases de datos compatibles	Clases de instancias admitidas
		• Oeste de EE. UU. (Norte de California) • Oeste de EE. UU. (Oregón) • Asia-Pacífico (Bombay) • Asia-Pacífico (Seúl) • Asia-Pacífico (Singapur) • Asia-Pacífico (Sídney) • Asia-Pacífico (Tokio) • Canadá (centro) • Europa (Fráncfort) • Europa (Irlanda) • Europa (Londres) • Europa (París) • Europa (Estocolmo) • América del Sur (São Paulo)		

Compatibilidad con la región de Amazon RDS para información sobre las bases de datos

Amazon RDS admite Información sobre las bases de datos en las siguientes Regiones de AWS.

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Oeste de Canadá (Calgary)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milán)
- Europa (París)
- Europa (España)
- Europa (Estocolmo)
- Europa (Zúrich)

- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Oeste de EE. UU.)

Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS

Para activar el modo avanzado de Información sobre las bases de datos para Amazon RDS, use estos procedimientos.

Activación del modo avanzado de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos multi-AZ

Active el modo avanzado de Información sobre las bases de datos al crear una base de datos para Amazon RDS.

Console

En la consola, puede activar el modo avanzado de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos Multi-AZ.

Activación del modo avanzado de Información sobre las bases de datos al crear una instancia de base de datos o una implementación multi-AZ de un clúster de bases de datos con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione Bases de datos.
3. Elija Creación de base de datos.
4. En la sección Información sobre bases de datos, seleccione el Modo avanzado. A continuación, elija las siguientes opciones:

    - Retención: el número de días durante los que se conservan los datos de Información de rendimiento. El periodo de retención debe ser de 15 meses para el modo avanzado de información sobre las bases de datos.

- AWS KMS key: especifique su clave de KMS. Performance Insights cifra todos los datos potencialmente confidenciales con su propia clave de KMS. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.

5. Elija Creación de base de datos.

AWS CLI

Para activar el modo avanzado de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos Multi-AZ, llame al comando create-db-instance o create-db-cluster de la AWS CLI e introduzca los siguientes valores:

- `--database-insights-mode advanced` para activar el modo avanzado de Información sobre las bases de datos.
- `--engine`: el motor de base de datos para la instancia de base de datos.
- `--db-instance-identifier`: el identificador de la instancia de base de datos o `--db-cluster-identifier`: el identificador del clúster de bases de datos Multi-AZ.
- `--enable-performance-insights` para activar Información sobre rendimiento para Información sobre las bases de datos.
- `--performance-insights-retention-period`: es el periodo de retención de los datos de la instancia de base de datos o del clúster de bases de datos Multi-AZ. Para activar Información sobre las bases de datos, el período de retención debe ser de al menos 465 días.

En el siguiente ejemplo se habilita el modo avanzado de Información sobre las bases de datos al crear una instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --database-insights-mode advanced \
    --engine postgresql \
    --db-instance-identifier sample-db-identifier \
    --enable-performance-insights \
    --performance-insights-retention-period 465
```

Para Windows:

```
aws rds create-db-instance ^
    --database-insights-mode advanced ^
    --engine postgresql ^
    --db-instance-identifier sample-db-identifier ^
    --enable-performance-insights ^
    --performance-insights-retention-period 465
```

RDS API

Para activar el modo avanzado de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos multi-AZ, especifique los siguientes parámetros para la operación de la API CreateDBInstance o CreateDBCluster de Amazon RDS.

- De `DatabaseInsightsMode` a `advanced`
- De `EnablePerformanceInsights` a `True`
- `PerformanceInsightsRetentionPeriod` en al menos 465 días

Activación del modo avanzado de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de bases de datos multi-AZ

Active Información sobre las bases de datos al modificar una base de datos para Amazon RDS. La modificación de una instancia de base de datos para habilitar el modo avanzado de información de bases de datos no provoca tiempo de inactividad.

> **Note**
>
> Para habilitar Información sobre las bases de datos, cada instancia de base de datos de un clúster de bases de datos Multi-AZ debe tener la misma configuración de Información de rendimiento y Supervisión mejorada.

Console

En la consola, puede activar el modo avanzado de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de bases de datos Multi-AZ.

Activación del modo avanzado de Información sobre las bases de datos al modificar una base de datos o una implementación multi-AZ de un clúster de bases de datos con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione Bases de datos.
3. Elija una instancia de base de datos o una implementación multi-AZ de un clúster de bases de datos y elija Modificar.
4. En la sección Información sobre bases de datos, seleccione el Modo avanzado. A continuación, elija las siguientes opciones:
   - Retención: el número de días durante los que se conservan los datos de Información de rendimiento. El periodo de retención debe ser de 15 meses para el modo avanzado de información sobre las bases de datos.
   - AWS KMS key: especifique su clave de KMS. Performance Insights cifra todos los datos potencialmente confidenciales con su propia clave de KMS. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
5. Elija Continuar.
6. En Programación de modificaciones, elija Aplicar inmediatamente. Si elige Aplicar durante el próximo periodo de mantenimiento programado, la base de datos ignora esta configuración y activa de inmediato el modo avanzado de Información sobre las bases de datos.
7. Seleccione Modificar clúster.

AWS CLI

Para activar el modo avanzado de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de bases de datos Multi-AZ, llame al comando modify-db-instance o modify-db-cluster de la AWS CLI e introduzca los siguientes valores:

- `--database-insights-mode advanced` para activar el modo avanzado de Información sobre las bases de datos.
- `--db-instance-identifier`: el identificador de la instancia de base de datos o `--db-cluster-identifier`: el identificador del clúster de bases de datos Multi-AZ.
- `--enable-performance-insights` para activar Información sobre rendimiento para Información sobre las bases de datos.

- `--performance-insights-retention-period`: es el periodo de retención de los datos de la instancia de base de datos. Para activar el modo avanzado de Información sobre las bases de datos, el período de retención debe ser de al menos 465 días.

En el siguiente ejemplo se habilita el modo avanzado de Información sobre las bases de datos al modificar una instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --database-insights-mode advanced \
    --db-instance-identifier sample-db-identifier \
    --enable-performance-insights \
    --performance-insights-retention-period 465
```

Para Windows:

```
aws rds modify-db-instance ^
    --database-insights-mode advanced ^
    --db-instance-identifier sample-db-identifier ^
    --enable-performance-insights ^
    --performance-insights-retention-period 465
```

RDS API

Para activar el modo avanzado de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de base de datos multi-AZ, especifique los siguientes parámetros para la operación de la API ModifyDBInstance o ModifyDBCluster de Amazon RDS.

- De `DatabaseInsightsMode` a `advanced`
- De `EnablePerformanceInsights` a `True`
- `PerformanceInsightsRetentionPeriod` en al menos 465 días

Activación del modo estándar de Información sobre las bases de datos para Amazon RDS

Para activar el modo estándar de Información sobre las bases de datos para Amazon RDS, use estos procedimientos.

Activación del modo estándar de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos multi-AZ

Active el modo estándar de Información sobre las bases de datos al crear una base de datos para Amazon RDS.

Console

En la consola, puede activar el modo estándar de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos Multi-AZ.

Activación del modo estándar de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de base de datos multi-AZ con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione Bases de datos.
3. Elija Creación de base de datos.
4. En la sección Información sobre las bases de datos, seleccione el Modo estándar. A continuación, seleccione una de las siguientes opciones para activar o desactivar la Información de rendimiento:
   - Para desactivar la Información de rendimiento, anule la selección de Habilitar Información sobre rendimiento.
   - Para activar la Información de rendimiento, seleccione Habilitar Información sobre rendimiento. Para configurar la Información sobre rendimiento, especifique las siguientes opciones:
     - Retención: el tiempo durante el que se conservan los datos de la Información de rendimiento. El período de retención debe ser de al menos 7 días.
     - AWS KMS key: especifique su clave de KMS. Performance Insights cifra todos los datos potencialmente confidenciales con su propia clave de KMS. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
5. Elija Creación de base de datos.

AWS CLI

Para activar el modo estándar de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de bases de datos Multi-AZ, llame al comando create-db-instance o create-db-cluster de la AWS CLI e introduzca los siguientes valores:

- `--database-insights-mode standard` para activar el modo estándar de Información sobre las bases de datos.
- `--engine`: el motor de base de datos para la instancia de base de datos.
- `--db-instance-identifier`: el identificador de la instancia de base de datos o `--db-cluster-identifier`: el identificador del clúster de bases de datos Multi-AZ.
- `--enable-performance-insights` o `--no-enable-performance-insights` para habilitar o deshabilitar Información sobre rendimiento. Si especifica `--enable-performance-insights`, también debe especificar el `--performance-insights-retention-period`: el periodo de retención de los datos de la instancia de base de datos. El período de retención debe ser de al menos 7 días.

En el siguiente ejemplo se habilita el modo estándar de Información sobre las bases de datos e Información de rendimiento al crear una instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --database-insights-mode standard \
    --engine postgresql \
    --db-instance-identifier sample-db-identifier \
    --enable-performance-insights \
    --performance-insights-retention-period 7
```

Para Windows:

```
aws rds create-db-instance ^
    --database-insights-mode standard ^
    --engine postgresql ^
    --db-instance-identifier sample-db-identifier ^
    --enable-performance-insights ^
    --performance-insights-retention-period 7
```

En el siguiente ejemplo se habilita el modo estándar de Información sobre las bases de datos y se deshabilita Información de rendimiento al crear una instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --database-insights-mode standard \
    --engine postgresql \
    --db-instance-identifier sample-db-identifier \
    --no-enable-performance-insights
```

Para Windows:

```
aws rds create-db-instance ^
    --database-insights-mode standard ^
    --engine postgresql ^
    --db-instance-identifier sample-db-identifier ^
    --no-enable-performance-insights
```

RDS API

Para activar el modo estándar de Información sobre las bases de datos al crear una instancia de base de datos o un clúster de base de datos multi-AZ, especifique los siguientes parámetros para la operación de la API CreatedBInstance o CreatedBCluster de Amazon RDS.

- De `DatabaseInsightsMode` a `standard`
- De `EnablePerformanceInsights` a `True` o `False`. Si configura `EnablePerformanceInsights` como `True`, debe configurar `PerformanceInsightsRetentionPeriod` como al menos 7 días.

Activación del modo estándar de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de bases de datos multi-AZ

Active el modo estándar de Información sobre las bases de datos al modificar una base de datos para Amazon RDS. La modificación de una instancia de base de datos para habilitar el modo estándar de información de base de datos no provoca tiempo de inactividad.

> **Note**
>
> Para habilitar Información sobre las bases de datos, cada instancia de base de datos de un clúster de bases de datos Multi-AZ debe tener la misma configuración de Información de rendimiento y Supervisión mejorada.

Console

En la consola, puede activar el modo estándar de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de bases de datos Multi-AZ.

Activación del modo estándar de Información sobre las bases de datos al modificar una instancia de base de datos o una implementación multi-AZ de un clúster de bases de datos con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione Bases de datos.
3. Elija una instancia de base de datos o una implementación multi-AZ de un clúster de bases de datos y elija Modificar.
4. En la sección Información sobre las bases de datos, seleccione el Modo estándar. A continuación, elija entre las siguientes opciones:
   - Para desactivar la Información de rendimiento, anule la selección de Habilitar Información sobre rendimiento.
   - Para activar la Información de rendimiento, seleccione Habilitar Información sobre rendimiento. Para configurar la Información sobre rendimiento, especifique las siguientes opciones:
     - Retención: el tiempo durante el que se conservan los datos de la Información de rendimiento. El período de retención debe ser de al menos 7 días.
     - AWS KMS key: especifique su clave de KMS. Performance Insights cifra todos los datos potencialmente confidenciales con su propia clave de KMS. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
5. Elija Continuar.

6. En Programación de modificaciones, elija Aplicar inmediatamente. Si elige Aplicar durante el próximo periodo de mantenimiento programado, la base de datos ignora esta configuración y activa de inmediato el modo estándar de Información sobre las bases de datos.
7. Seleccione Modificar clúster.

AWS CLI

Para activar el modo estándar de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de bases de datos Multi-AZ, llame al comando modify-db-instance o modify-db-cluster de la AWS CLI e introduzca los siguientes valores:

- `--database-insights-mode standard` para activar el modo estándar de Información sobre las bases de datos.
- `--db-instance-identifier`: el identificador de la instancia de base de datos o `--db-cluster-identifier`: el identificador del clúster de bases de datos Multi-AZ.
- `--enable-performance-insights` o `--no-enable-performance-insights` para habilitar o deshabilitar Información sobre rendimiento. Si especifica `--enable-performance-insights`, también debe especificar el `--performance-insights-retention-period`: el periodo de retención de los datos de la instancia de base de datos o del clúster de bases de datos Multi-AZ. El período de retención debe ser de al menos 7 días.

En el siguiente ejemplo se habilita el modo estándar de Información sobre las bases de datos y se habilita la Información de rendimiento al modificar una instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --database-insights-mode standard \
    --db-instance-identifier sample-db-identifier \
    --enable-performance-insights \
    --performance-insights-retention-period 7
```

Para Windows:

```
aws rds modify-db-instance ^
    --database-insights-mode standard ^
    --db-instance-identifier sample-db-identifier ^
    --enable-performance-insights ^
```

```
    --performance-insights-retention-period 7
```

En el siguiente ejemplo se habilita el modo estándar de Información sobre las bases de datos y se deshabilita la Información de rendimiento al modificar una instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --database-insights-mode standard \
    --db-instance-identifier sample-db-identifier \
    --no-enable-performance-insights
```

Para Windows:

```
aws rds modify-db-instance ^
    --database-insights-mode standard ^
    --db-instance-identifier sample-db-identifier ^
    --no-enable-performance-insights
```

RDS API

Para activar el modo estándar de Información sobre las bases de datos al modificar una instancia de base de datos o un clúster de base de datos multi-AZ, especifique los siguientes parámetros para la operación de la API ModifyDBInstance o ModifyDBCluster de Amazon RDS.

- De `DatabaseInsightsMode` a `standard`
- De `EnablePerformanceInsights` a `True` o `False`. Si configura `EnablePerformanceInsights` como `True`, debe configurar `PerformanceInsightsRetentionPeriod` como al menos 7 días.

Configuración de la base de datos para supervisar las consultas SQL lentas con Información sobre las bases de datos para Amazon RDS

Para supervisar las consultas SQL lentas de la base de datos, puede utilizar la sección Consultas SQL lentas del panel de Información sobre las bases de datos. Antes de configurar la base de datos para supervisar consultas SQL lentas, la sección Consultas SQL lentas está en blanco.

Para obtener más información sobre cómo supervisar consultas SQL lentas en el panel de Información sobre las bases de datos, consulte Visualización del panel de instancia de base de

datos para Información sobre las bases de datos de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Para configurar la base de datos para supervisar las consultas de SQL lentas con información de las bases de datos, complete los siguiente pasos:

1. Habilite la exportación de registros a registros de CloudWatch.
2. Cree o modifique el grupo de parámetros de base de datos para la instancia de base de datos.

Para obtener información sobre la configuración de las exportaciones de registros, consulte Publicación de registros de bases de datos en Registros de Amazon CloudWatch en la Guía del usuario de Amazon RDS.

Para crear o modificar el grupo de parámetros de base de datos, consulte los temas siguientes.

- Creación de un grupo de parámetros de base de datos en Amazon RDS
- Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS

RDS for MariaDB

Para configurar la instancia de base de datos de RDS para MariaDB a fin de supervisar consultas SQL lentas, establezca los siguientes parámetros.

- `log_slow_query`: se establece como `1`.
- `log_slow_query_time`: se establece como `1.0`.
- `log_output`: se establece como `FILE`.

RDS for MySQL

Para configurar la instancia de base de datos de RDS para MySQL a fin de supervisar consultas SQL lentas, establezca los siguientes parámetros.

- `slow_query_log`: se establece como `1`.
- `long_query_time`: se establece como `1.0`.
- `log_output`: se establece como `FILE`.

RDS for PostgreSQL

Para configurar la instancia de base de datos de PostgreSQL para MySQL a fin de supervisar consultas SQL lentas, establezca los siguientes parámetros. Tenga en cuenta que la configuración de estos parámetros puede reducir el rendimiento de la instancia de base de datos.

- `log_min_duration_statement`: se establece como `1000`.
- `log_statement`: se establece como `none`.
- `log_destination`: se establece como `stderr`.

> **Note**
>
> Para RDS para MySQL, puede configurar el parámetro `long_query_time` con un detalle de 1 microsegundo. Por ejemplo, puede establecer este parámetro en `0.000001`. Dependiendo de la cantidad de consultas en la instancia de la base de datos, el valor del parámetro `long_query_time` puede reducir el rendimiento. Comience con el valor `1.0` y ajústelo en función de la carga de trabajo. Cuando establece este parámetro en `0`, Información sobre las bases de datos registra todas las consultas.

Para obtener información sobre los registros de RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL, consulte lo siguiente.

- Archivos de registro de base de datos de MariaDB
- Archivos de registro de base de datos de MySQL
- Archivos de registro de bases de datos de RDS para PostgreSQL

Consideraciones acerca de Información sobre las bases de datos para Amazon RDS

A continuación, presentamos algunas consideraciones acerca de Información sobre las bases de datos para Amazon RDS.

- No puede administrar Información sobre las bases de datos para una instancia de base de datos en un clúster de bases de datos Multi-AZ.

- Para habilitar el modo avanzado de Información sobre las bases de datos, debe habilitar Información de rendimiento y establecer el período de retención de Información de rendimiento en 465 días (15 meses) como mínimo. No hay ningún costo adicional por establecer el periodo de retención de información sobre rendimiento en 15 meses, aparte del costo de la información de la base de datos. Para obtener más información sobre los precios de Database Insights, consulte Precios de Amazon CloudWatch.
- Para habilitar Información sobre las bases de datos, cada instancia de base de datos de un clúster de bases de datos Multi-AZ debe tener la misma configuración de Información de rendimiento y Supervisión mejorada.
- La modificación de una instancia de base de datos para habilitar el modo de información de base de datos no provoca tiempo de inactividad.

Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch.
Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Performance Insights amplía las características de supervisión existentes de Amazon RDS para ilustrar y ayudarlo a analizar el rendimiento de la base de datos. En el panel de Performance Insights puede visualizar la carga de la base de datos en su carga de instancia de base de datos de Amazon RDS y filtrarla por esperas, instrucciones SQL, hosts o usuarios. Para obtener más información sobre

el uso de Performance Insights con Amazon DocumentDB, consulte la Guía para desarrolladores de Amazon DocumentDB.

Temas

- Uso de Performance Insights en Amazon RDS
- Activación y desactivación de Información de rendimiento de Amazon RDS
- Descripción general de Performance Schema para Información de rendimiento en Amazon RDS para MariaDB o MySQL
- Configuración de directivas de acceso para información sobre rendimiento
- Análisis de métricas mediante el panel de Información sobre rendimiento
- Visualización de las recomendaciones proactivas de Información de rendimiento
- Recuperación de métricas con la API de Información sobre rendimiento para Amazon RDS
- Registro de llamadas de Performance Insights mediante el uso de AWS CloudTrail
- API de Información de rendimiento y puntos de conexión de VPC de interfaz (AWS PrivateLink)

Uso de Performance Insights en Amazon RDS

> **Important**
>
> AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
>
> Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS.

Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

De forma predeterminada, RDS habilita Información sobre rendimiento en el asistente de creación de la consola para todos los motores de Amazon RDS. Si tiene más de una base de datos en una instancia de base de datos, Performance Insights agrega datos de rendimiento.

Encontrará información general sobre Performance Insights para Amazon RDS en el siguiente vídeo.

Uso de Performance Insights para analizar el rendimiento de Amazon Aurora PostgreSQL

Important

Los siguientes temas describen cómo usar la característica de Performance Insights de Amazon RDS con motores de base de datos que no son de Aurora. Para obtener información sobre el uso de Performance Insights de Amazon RDS con Amazon Aurora, consulte Uso de Performance Insights de Amazon RDS en la guía del usuario de Amazon Aurora.

Temas

- Carga de base de datos
- Máximo de la CPU
- El motor de base de datos de Amazon RDS, la región y la clase de instancia son compatibles con Información de rendimiento
- Precios y retención de datos de Performance Insights

Carga de base de datos

La carga de base de datos mide el nivel de actividad de la sesión en la base de datos. `DBLoad` es la métrica clave de Información sobre rendimiento y Información sobre rendimiento recopila la carga de la base de datos cada segundo.

Temas

- Sesiones activas
- Sesiones activas promedio
- Ejecuciones activas promedio
- Dimensiones

Sesiones activas

Una sesión de base de datos representa el diálogo de una aplicación con una base de datos relacional. Una sesión activa es una conexión que ha enviado trabajo al motor de base de datos y está esperando una respuesta.

Una sesión está activa cuando se ejecuta en la CPU o a la espera de que un recurso esté disponible para que pueda continuar. Por ejemplo, una sesión activa puede esperar a que se lea una página (o bloque) en la memoria y, a continuación, consumir CPU mientras lee los datos de la página.

Sesiones activas promedio

El promedio de sesiones activas (AAS) es la unidad para la métrica de `DBLoad` en Performance Insights. Mide cuántas sesiones están activas simultáneamente en la base de datos.

Cada segundo, Información de rendimiento muestra el número de sesiones que ejecutan una consulta simultáneamente. Para cada sesión activa, Información de rendimiento recopila los siguientes datos:

- Instrucción SQL
- Estado de la sesión (en ejecución en la CPU o en espera)
- Host
- Usuario que ejecuta el SQL

Información de rendimiento calcula el AAS que se obtiene dividiendo el número total de sesiones entre el número total de ejemplos de un periodo de tiempo específico. Por ejemplo, en la tabla

siguiente se muestran 5 ejemplos consecutivos de una consulta en ejecución realizada a intervalos de 1 segundo.

Ejemplo	Número de sesiones que ejecutan una consulta	AAS	Cálculo
1	2	2.	2 sesiones en total / 1 ejemplo
2	0	1	2 sesiones en total / 2 ejemplos
3	4	2	6 sesiones en total / 3 ejemplos
4	0	1.5	6 sesiones en total / 4 ejemplos
5	4	2	10 sesiones en total / 5 ejemplos

En el ejemplo anterior, la carga de base de datos para el intervalo de tiempo es de 2 AAS. Esta medición significa que, de media, 2 sesiones han estado activas a la vez durante el plazo en que se han tomado las 5 muestras.

Ejecuciones activas promedio

Las ejecuciones activas promedio (AAE) por segundo están relacionadas con las sesiones activas promedio. Para calcular el AAE, Performance Insights divide el tiempo total de ejecución de una consulta por el intervalo de tiempo. En la tabla siguiente se muestra el cálculo de AAE para la misma consulta de la tabla anterior.

Tiempo transcurrido (en segundos)	Tiempo total de ejecución (en segundos)	AAE	Cálculo
60	120	2	120 segundos de ejecución/60 segundos transcurridos
120	120	1	120 segundos de ejecución/120 segundos transcurridos
180	380	2.11	380 segundos de ejecución/180 segundos transcurridos
240	380	1.58	380 segundos de ejecución/240 segundos transcurridos
300	600	2	600 segundos de ejecución/300 segundos transcurridos

En la mayoría de los casos, el AAS y el AAE de una consulta dan aproximadamente lo mismo. Sin embargo, dado que las entradas de los cálculos son diferentes orígenes de datos, los cálculos suelen variar ligeramente.

Dimensiones

La métrica `db.load` es distinta de las demás métricas de series temporales porque puede desglosarla en subcomponentes llamados dimensiones. Las dimensiones son una especie de categorías “dividir por” de las diferentes características de la métrica `DBLoad`.

Cuando se diagnostican problemas de rendimiento, las siguientes dimensiones suelen ser las más útiles:

Temas

- Eventos de espera
- SQL principal
- Planes

Para obtener una lista completa de las dimensiones de los motores de Amazon RDS, consulte Carga de base de datos dividida por dimensiones.

Eventos de espera

Un evento de espera hace que una instrucción SQL espere a que ocurra un evento específico antes de que pueda continuar ejecutándose. Los eventos de espera son una dimensión o categoría importante de la carga de base de datos, porque indican dónde se ve obstaculizado el trabajo.

Cada sesión activa se ejecuta en la CPU o en espera. Por ejemplo, las sesiones consumen CPU cuando buscan memoria para un búfer, llevan a cabo un cálculo o ejecutan código de procedimiento. Cuando las sesiones no consumen CPU, pueden estar en espera de que se libere un búfer de memoria, se lea un archivo de datos o se escriba un registro. Cuanto más tiempo espere una sesión por los recursos, menos tiempo se ejecutará en la CPU.

Cuando ajusta una base de datos, a menudo intenta averiguar los recursos que esperan las sesiones. Por ejemplo, dos o tres eventos de espera podrían representar el 90 por ciento de la carga de base de datos. Esta medida significa que, en promedio, las sesiones activas pasan la mayor parte del tiempo en espera de un pequeño número de recursos. Si puede averiguar la causa de estas esperas, puede intentar una solución.

Los eventos de espera varían en función del motor de base de datos:

- Para obtener más información sobre todos los eventos de espera de MariaDB y MySQL, consulte Wait Event Summary Tables (Tablas de resumen de eventos de espera) en la documentación de MySQL.
- Para obtener más información sobre todos los eventos de espera de PostgreSQL, consulte Ecentos de espera de PostgreSQL en la documentación de PostgreSQL.
- Para obtener más información sobre todos los eventos de espera de Oracle, consulte Descriptions of Wait Events (Descripciones de los eventos de espera) en la documentación de Oracle.
- Para obtener información sobre todos los eventos de espera de SQL Server, consulte Types of Waits (Tipos de espera) en la documentación de SQL Server.

> **Note**
>
> Para Oracle, los procesos en segundo plano a veces funcionan sin una instrucción SQL asociada. En estos casos, Performance Insights informa del tipo de proceso en segundo plano concatenado con un punto y coma y la clase de espera asociada a ese proceso en segundo plano. Entre los tipos de procesos en segundo plano se incluyen `LGWR`, `ARC0`, `PMON`, etc.
> Por ejemplo, cuando el archivador está realizando E/S, el informe de Performance Insights correspondiente es similar a `ARC1:System I/O`. Ocasionalmente, también falta el tipo de proceso en segundo plano y Performance Insights solo informa sobre la clase de espera, por ejemplo, `:System I/O`.

SQL principal

Mientras que los eventos de espera muestran los cuellos de botella, la dimensión SQL principal indica qué consultas contribuyen más a la carga de base de datos. Por ejemplo, es posible que, aunque haya muchas consultas ejecutándose actualmente en la base de datos, una de ellas consuma el 99 % de la carga de base de datos. En este caso, es posible que la carga alta indique un problema con la consulta.

De forma predeterminada, en la consola de Performance Insights se muestran las principales consultas SQL que contribuyen a la carga de la base de datos. En la consola se muestran también estadísticas importantes sobre cada instrucción. Para diagnosticar los problemas de rendimiento de una instrucción específica, puede examinar su plan de ejecución.

Planes

Un plan de ejecución, también llamado simplemente plan, es una secuencia de pasos que acceden a los datos. Por ejemplo, un plan para unir las tablas `t1` y `t2` podría recorrer en bucle todas las filas de `t1` y comparar cada fila con una fila de `t2`. En una base de datos relacional, un optimizador es un código integrado que determina el plan más eficiente para una consulta de SQL.

Para las instancias de base de datos, Información de rendimiento recopila planes de ejecución automáticamente. Para diagnosticar problemas de rendimiento de SQL, examine los planes capturados para consultas de SQL de altos recursos. Los planes muestran cómo la base de datos ha analizado y ha ejecutado consultas.

Para obtener información sobre cómo analizar la carga de la base de datos mediante planes, consulte:

- Oracle: Análisis de planes de ejecución de Oracle mediante el panel de Información de rendimiento para Amazon RDS
- SQL Server: Análisis de planes de ejecución de SQL Server mediante el panel de Información de rendimiento para Amazon RDS

Captura del plan

Cada cinco minutos, Información de rendimiento identifica las consultas que requieren más recursos y captura sus planes. Por lo tanto, no es necesario recopilar ni administrar manualmente una gran cantidad de planes. En su lugar, puede usar la pestaña Top SQL (SQL principal) para centrarse en los planes de las consultas más problemáticas.

> **Note**
>
> Performance Insights no captura planes para consultas cuyo texto supere el límite máximo de texto de consulta recopilable. Para obtener más información, consulte Acceso a más texto SQL en el panel de Performance Insights.

El período de retención de los planes de ejecución es el mismo que el de todos los datos de Performance Insights. La configuración de retención en la capa gratuita es Default (7 days) (Predeterminado [7 días]). Para retener los datos de rendimiento durante más tiempo, especifique de 1 a 24 meses. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.

Consultas de resumen

La pestaña Top SQL (SQL principal) muestra las consultas de resumen de forma predeterminada. Una consulta de resumen no tiene por sí misma un plan, pero todas las consultas que utilizan valores literales sí tienen planes. Por ejemplo, una consulta de resumen podría incluir el texto `WHERE \`email\`=?`. El resumen podría contener dos consultas, una con el texto `WHERE email=user1@example.com` y otra con `WHERE email=user2@example.com`. Cada una de estas consultas literales podría incluir varios planes.

Al seleccionar una consulta de resumen, la consola muestra todos los planes para las instrucciones secundarias del resumen seleccionado. Por lo tanto, no es necesario revisar todas las instrucciones

secundarias para encontrar el plan. Es posible que vea planes que no están en la lista mostrada de las 10 principales instrucciones secundarias. La consola muestra los planes de todas las consultas secundarias para las que se han recopilado planes, independientemente de si las consultas se encuentran entre las 10 principales.

Máximo de la CPU

En el panel, el gráfico de Carga de base de datos recopila, agrega y muestra información de la sesión. Para ver si las sesiones activas superan el máximo de la CPU, observe su relación con la línea Máximo de la CPU virtual. Información sobre rendimiento determina el valor Máximo de la CPU virtual mediante el número de núcleos de vCPU (CPU virtual) de la instancia de base de datos.

Se puede ejecutar un proceso en una vCPU a la vez. Si el número de procesos supera el número de vCPU, los procesos comienzan a ponerse en cola. Cuando las colas aumentan, el rendimiento de la base de datos disminuye. Si la carga de base de datos suele estar por encima de la línea Máximo de la CPU virtual y el estado de espera principal es CPU, la CPU del sistema está sobrecargada. En este caso, quizá sea conveniente limitar las conexiones con la instancia, ajustar las consultas SQL con una carga de CPU alta o pensar en la posibilidad de usar una clase de instancia de mayor tamaño. Si hay instancias altas y uniformes en cualquier estado de espera, eso indica que es posible que haya problemas de contención de recursos o cuellos de botella que hay que resolver. Esto puede ser así aunque la carga de base de datos no cruce la línea de Máximo de la CPU virtual.

El motor de base de datos de Amazon RDS, la región y la clase de instancia son compatibles con Información de rendimiento

> **Important**
>
> AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.

Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Las siguiente tabla indica los motores de base de datos de Amazon RDS que admiten la Información de rendimiento.

> **Note**
>
> Para Amazon Aurora, consulte El motor de base de datos de Amazon Aurora admite Performance Insightsen Guía del usuario de Amazon Aurora.

Motor de base de datos de Amazon RDS	Versiones de motor y regiones compatibles	Restricciones de clase de instancia
Amazon RDS para MariaDB	Para obtener más informaci ón sobre la disponibilidad en versiones y regiones de Performan ce Insights con RDS para MariaDB, consulte Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS.	Performance Insights no es compatible con las siguientes clases de instancia: • db.t2.micro • db.t2.small • db.t3.micro

Motor de base de datos de Amazon RDS	Versiones de motor y regiones compatibles	Restricciones de clase de instancia
		• db.t3.small • db.t4g.micro • db.t4g.small
RDS para MySQL	Para obtener más información sobre la disponibilidad en versiones y regiones de Performance Insights con RDS para MySQL, consulte Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS.	Performance Insights no es compatible con las siguientes clases de instancia: • db.t2.micro • db.t2.small • db.t3.micro • db.t3.small • db.t4g.micro • db.t4g.small
Amazon RDS for Microsoft SQL Server	Para obtener más información sobre la disponibilidad en versiones y regiones de Performance Insights con RDS para SQL Server, consulte Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS.	N/A

Motor de base de datos de Amazon RDS	Versiones de motor y regiones compatibles	Restricciones de clase de instancia
Amazon RDS para PostgreSQL	Para obtener más información sobre la disponibilidad en versiones y regiones de Performance Insights con RDS para PostgreSQL, consulte Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS.	N/A
Amazon RDS para Oracle	Para obtener más información sobre la disponibilidad en versiones y regiones de Performance Insights con RDS para Oracle, consulte Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS.	N/A

Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento

Las siguiente tabla indica los motores de base de datos de Amazon RDS que admiten características de Información de rendimiento.

Característica	Niveles de precios	Regiones admitidas	Motores de bases de datos compatibles	Clases de instancias admitidas
Estadísticas de SQL para Performance Insights	Todos	Todos	Todos	Todos

Característica	Niveles de precios	Regiones admitidas	Motores de bases de datos compatibles	Clases de instancias admitidas
Análisis de planes de ejecución de Oracle mediante el panel de Información de rendimiento para Amazon RDS	Todos	Todos	RDS para Oracle	Todos
Análisis del rendimiento de la base de datos durante un período de tiempo	Solo nivel de pago	Todos	RDS para PostgreSQL	Todos

Característica	Niveles de precios	Regiones admitidas	Motores de bases de datos compatibles	Clases de instancias admitidas
Visualización de las recomendaciones proactivas de Información de rendimiento	Solo nivel de pago	• Este de EE. UU. (Ohio) • Este de EE. UU. (Norte de Virginia) • Oeste de EE. UU. (Norte de California) • Oeste de EE. UU. (Oregón) • Asia-Pacífico (Bombay) • Asia-Pacífico (Seúl) • Asia-Pacífico (Singapur) • Asia-Pacífico (Sídney) • Asia-Pacífico (Tokio) • Canadá (centro) • Europa (Fráncfort) • Europa (Irlanda) • Europa (Londres) • Europa (París)	Todos	Todos

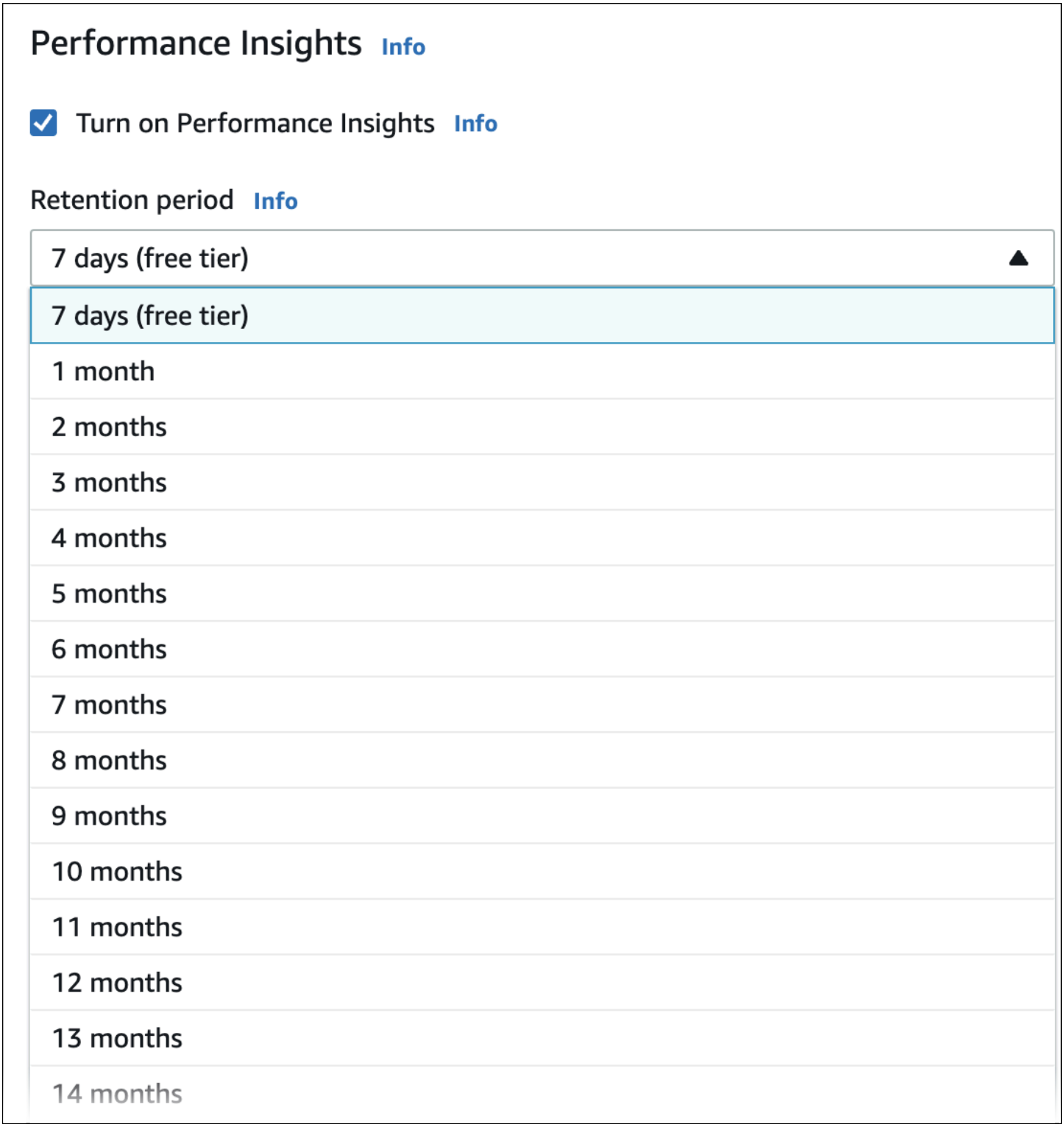
Característica	Niveles de precios	Regiones admitidas	Motores de bases de datos compatibles	Clases de instancias admitidas
		• Europa (Estocolmo) • América del Sur (São Paulo)		

Precios y retención de datos de Performance Insights

De forma predeterminada, Performance Insights ofrece una capa gratuita que incluye 7 días de historial de datos de rendimiento y 1 millón de solicitudes de API al mes. También puede comprar períodos de retención más largos. Para obtener información completa sobre los precios, consulte los precios de Performance Insights.

En la consola de RDS, puede elegir cualquiera de los siguientes períodos de retención de sus datos de Performance Insights:

- Predeterminado (7 días)
- ***n***meses, donde***n***es un número del 1 al 24



Para obtener información para configurar un período de retención con AWS CLI, consulte ???.

Activación y desactivación de Información de rendimiento de Amazon RDS

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.

Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de Información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.

Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Puede activar la información sobre rendimiento para el instancia o clúster de base de datos multi-AZ de base de datos durante su creación. Si es necesario, puede desactivarlo más adelante. Para ello, modifique el instancia de base de datos en la consola. La activación y desactivación de Información de rendimiento no provoca tiempo de inactividad, un reinicio ni una conmutación por error.

> **Note**
>
> Performance Schema es una herramienta de rendimiento opcional utilizada por Amazon RDS para MariaDB o MySQL. Si activa o desactiva Esquema de rendimiento, debe reiniciar. Sin embargo, si activa o desactiva Performance Insights, no es necesario que se reinicie. Para obtener más información, consulte Descripción general de Performance Schema para Información de rendimiento en Amazon RDS para MariaDB o MySQL.

El agente Performance Insights consume CPU y memoria limitadas en el host de base de datos. Cuando la carga de la base de datos es alta, el agente limita el impacto en el rendimiento mediante la recopilación de datos con menos frecuencia.

Console

En la consola, puede activar o desactivar Información sobre rendimiento al crear o modificar una instancia de base de datos o un clúster de bases de datos multi-AZ.

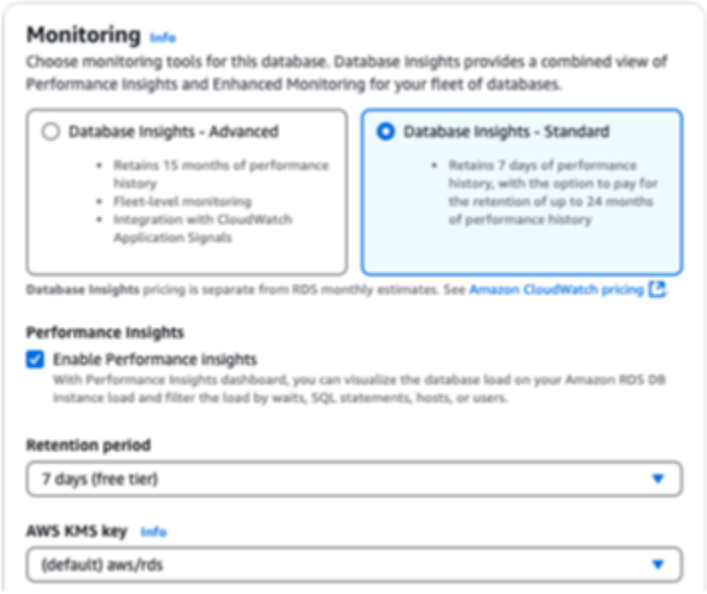
Activación o desactivación de Performance Insights al crear una instancia de base de datos o un clúster de bases de datos Multi-AZ

Tras crear una nueva instancia de base de datos o un clúster de base de datos Multi-AZ, Amazon RDS habilita información sobre rendimiento de forma predeterminada. Para desactivar información sobre rendimiento, elija la opción Información de base de datos: estándar y desmarque la opción Habilitar información sobre rendimiento.

Para obtener más información, consulte los siguientes temas.

- Para crear una instancia de base de datos, siga las instrucciones del motor de base de datos específico que se indican en Creación de una instancia de base de datos de Amazon RDS.
- Para crear un clúster de bases de datos Multi-AZ, siga las instrucciones para su motor de base de datos en Creación de un clúster de base de datos multi-AZ para Amazon RDS.

La siguiente captura de pantalla muestra la sección Información de rendimiento.



Si elige Activar Información de rendimiento, dispondrá de las siguientes opciones:

- Retención (solo para el modo estándar de información sobre rendimiento): la cantidad de tiempo durante el que se retienen los datos de información sobre rendimiento. La configuración de retención en la capa gratuita es Predeterminado (7 días). Para retener los datos de rendimiento durante más tiempo, especifique de 1 a 24 meses. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.
- AWS KMS key: especifique su AWS KMS key. Performance Insights cifra todos los datos potencialmente confidenciales con su propia clave de KMS. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cambio de una política de AWS KMS para Información de rendimiento.

Activación o desactivación de información sobre rendimiento al modificar un instancia de base de datos o clúster de base de datos multi-AZ

En la consola, puede modificar una instancia de base de datos o clúster de base de datos multi-AZ para administrar información sobre rendimiento.

Para administrar información sobre rendimiento para una instancia de base de datos o clúster de base de datos multi-AZ mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. Seleccione Bases de datos.
3. Elija un instancia de base de datos o clúster de base de datos multi-AZ y elija Modificar.
4. Para activar la Información de rendimiento, seleccione Habilitar Información sobre rendimiento. Para desactivar información sobre rendimiento, elija la opción Información de base de datos: estándar y desmarque la opción Habilitar información sobre rendimiento.

   Si elige Activar Información de rendimiento, dispondrá de las siguientes opciones:

   - Retención (solo para el modo estándar de información sobre rendimiento): la cantidad de tiempo durante el que se retienen los datos de información sobre rendimiento. La configuración de retención en la capa gratuita es Predeterminado (7 días). Para retener los datos de rendimiento durante más tiempo, especifique de 1 a 24 meses. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.
   - AWS KMS key: especifique su clave de KMS. Performance Insights cifra todos los datos potencialmente confidenciales con su propia clave de KMS. Las datos se cifran en reposo y en tránsito. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
5. Elija Continuar.
6. En Scheduling of Modifications (Programación de modificaciones) (Programación de modificaciones), elija Apply immediately (Aplicar inmediatamente). Si elige Apply during the next scheduled maintenance window (Aplicar durante la próxima ventana de mantenimiento programada), la instancia ignora esta configuración y activa de inmediato Performance Insights.
7. Elija Modificar instancia.

AWS CLI

Cuando utilice el comando create-db-instance de la AWS CLI, active información sobre rendimiento especificando `--enable-performance-insights` y estableciendo `--database-insights-mode` en `advanced` o `standard`. Para desactivar información sobre rendimiento, especifique `--no-enable-performance-insights` y establezca `database-insights-mode` en `standard`.

Estos valores también pueden especificarse con los siguientes comandos de AWS CLI:

- create-db-cluster

- modify-db-cluster
- create-db-instance-read-replica
- modify-db-instance
- restore-db-instance-from-s3

Al activar Información de rendimiento en la CLI, puede especificar, si lo desea, el tiempo en días que se retienen los datos de Información de rendimiento mediante la opción `--performance-insights-retention-period`. Puede especificar7, *`mes`** 31 (donde *`mes`* es un número comprendido entre 1 y 23), o 731. Por ejemplo, si desea retener los datos de rendimiento durante 3 meses, especifique 93, que es 3 * 31. El valor predeterminado es 7 días. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.

El ejemplo siguiente activa Información de rendimiento para `sample-db-cluster` y especifica que los datos de Información de rendimiento se retengan durante 93 días (3 meses).

Para Linux, macOS o Unix:

```
aws rds modify-db-cluster \
 --database-insights-mode standard \
    --db-cluster-identifier sample-db-instance \
    --enable-performance-insights \
    --performance-insights-retention-period 93
```

Para Windows:

```
aws rds modify-db-cluster ^
 --database-insights-mode standard ^
    --db-cluster-identifier sample-db-instance ^
    --enable-performance-insights ^
    --performance-insights-retention-period 93
```

Si especifica un período de retención, como 94 días, que no es un valor válido, RDS emitirá un error.

```
An error occurred (InvalidParameterValue) when calling the CreateDBInstance
 operation:
Invalid Performance Insights retention period. Valid values are: [7, 31, 62, 93,
 124, 155, 186, 217,
```

```
248, 279, 310, 341, 372, 403, 434, 465, 496, 527, 558, 589, 620, 651, 682, 713, 731]
```

> **Note**
>
> Solo puede activar Información de rendimiento para una instancia de un clúster de base de datos en la que Información de rendimiento no se administre en el clúster.

RDS API

Si crea una nueva instancia de base de datos mediante la operación CreateDBInstance de la operación de la API de Amazon RDS, active Información de rendimiento configurando `EnablePerformanceInsights` como `True`. Para desactivar información sobre rendimiento, establezca `EnablePerformanceInsights` en `False` y establezca `DatabaseInsightsMode` en `standard`.

También puede especificar el valor `EnablePerformanceInsights` utilizando las siguientes operaciones de la API:

- CreateDBCluster (Clúster de base de datos multi-AZ)
- ModifyDBCluster (Clúster de base de datos multi-AZ)
- ModifyDBInstance
- CreateDBInstanceReadReplica
- RestoreDBInstanceFromS3

Cuando activa Información de rendimiento, puede especificar, si lo desea, la cantidad de tiempo en días que se retienen los datos de Información de rendimiento con el parámetro `PerformanceInsightsRetentionPeriod`. Puede especificar7, *`mes`** 31 (donde *`mes`* es un número comprendido entre 1 y 23), o `731`. Por ejemplo, si desea retener los datos de rendimiento durante 3 meses, especifique 93, que es 3 * 31. El valor predeterminado es 7 días. Para obtener más información acerca de los periodos de retención, consulte Precios y retención de datos de Performance Insights.

Descripción general de Performance Schema para Información de rendimiento en Amazon RDS para MariaDB o MySQL

Performance Schema es una característica opcional para supervisar el rendimiento de tiempo de ejecución de Amazon RDS para MariaDB o MySQL con un nivel bajo de detalle. Performance Schema está diseñado para tener un impacto mínimo en el rendimiento de la base de datos. Performance Insights es una característica distinta que puede utilizar con o sin Performance Schema.

Temas

- Información general de Performance Schema
- Performance Insights y Performance Schema
- Administración automática de Performance Schema mediante Performance Insights
- Qué ocurre al activar Performance Schema
- Determinación de si Performance Insights está administrando Performance Schema
- Activación de Performance Schema para Amazon RDS para MariaDB o MySQL

Información general de Performance Schema

Performance Schema supervisa los eventos en las bases de datos MariaDB y MySQL. Un evento es una acción de servidor de base de datos que consume tiempo y se ha instrumentado para que se pueda recopilar información de tiempo. A continuación, se muestran ejemplos de eventos:

- Llamadas a funciones
- Esperas del sistema operativo
- Etapas de la ejecución de SQL
- Grupos de instrucciones SQL

El motor de almacenamiento `PERFORMANCE_SCHEMA` es un mecanismo para implementar la característica Performance Schema. El motor recopila datos de eventos mediante la instrumentación en el código fuente de la base de datos. El motor almacena eventos en tablas solo en la memoria en la base de datos de `performance_schema`. Puede consultar `performance_schema` al igual que puede consultar cualquier otra tabla. Para obtener más información, consulte MySQL Performance Schema en el Manual de referencia de MySQL.

Performance Insights y Performance Schema

Performance Insights y Performance Schema son características independientes, pero están conectadas. El comportamiento de Performance Insights para Amazon RDS para MariaDB o MySQL depende de si Performance Schema está activado y, de ser así, de si Performance Insights administra el Performance Schema automáticamente. La tabla siguiente describe el comportamiento.

Performance Schema activado	Modo de administración de Performance Insights	Comportamiento de Performance Insights
Sí	Automático	• Recopila información detallada de supervisión de bajo nivel • Recopila métricas de sesión activas cada segundo • Muestra la carga de base de datos categorizada por eventos de espera detallados, que puede utilizar para identificar cuellos de botella
Sí	Manual	• Recopila eventos de espera y métricas por SQL • Recopila métricas de sesión activas cada segundo • Informa sobre estados de usuario, como insertar y enviar, que no ayudan a identificar cuellos de botella
No	N/A	• No recopila eventos de espera, métricas por SQL ni otra información de supervisión detallada y de bajo nivel • Recopila métricas de sesión activas cada cinco segundos en lugar de cada segundo • Informa sobre estados de usuario, como insertar y enviar, que no ayudan a identificar cuellos de botella

Administración automática de Performance Schema mediante Performance Insights

Al crear una instancia de base de datos de Amazon RDS para MariaDB o MySQL con Performance Insights activado, también se activa Performance Schema. En este caso, la Performance Insights administra automáticamente sus parámetros de Esquema de rendimiento. Esta es la configuración recomendada.

Si es así, Información de rendimiento administra automáticamente el Esquema de rendimiento, el Origen de `performance_schema` es `System default`.

> **Note**
>
> La clase de instancia t4g.medium no admite la administración automática del esquema de rendimiento.

Si cambia el valor del parámetro `performance_schema` manualmente y, más tarde, desea volver a la gestión automática, consulte Activación de Performance Schema para Amazon RDS para MariaDB o MySQL.

> **Important**
>
> Cuando Performance Insights activa Performance Schema, no cambia los valores del grupo de parámetros. Sin embargo, los valores se cambian en las instancias de base de datos que se están ejecutando. La única forma de ver los valores modificados es ejecutar elcomando `SHOW GLOBAL VARIABLES`.

Qué ocurre al activar Performance Schema

Performance Insights y Performance Schema tienen requisitos distintos para los reinicios de instancias de base de datos:

Performance Schema

Para activar o desactivar esta característica, debe reiniciar la instancia de base de datos.

Información de rendimiento

Para activar o desactivar esta característica, no es necesario reiniciar la instancia de base de datos.

Si Performance Schema no está activado actualmente y activa Performance Insights sin reiniciar la instancia de base de datos, Performance Schema no se activará.

Determinación de si Performance Insights está administrando Performance Schema

Para saber si Información de rendimiento está administrando actualmente Performance Schema en todas las versiones principales del motor, consulte la siguiente tabla.

Configuración del parámetro performance_schema	Configuración de la columna Source (Origen)	¿Performance Insights está administrando Performance Schema?
`0`	`System default`	Sí
`0` o `1`	`Modified`	No

En el siguiente procedimiento, determinará si Información de rendimiento está administrando Performance Schema de forma automática.

Para determinar si Performance Insights está administrando Performance Schema automáticamente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Parameter groups (Grupos de parámetros).
3. Seleccione el grupo de parámetros para la instancia de base de datos.
4. Escriba **`performance_schema`** en la barra de búsqueda.
5. Compruebe si Origen es el valor predeterminado del sistema y si Valor es 0. Si es así, la Performance Insights administra automáticamente Performance Schema.

   En este ejemplo, Información de rendimiento no está administrando Performance Schema de forma automática.



Activación de Performance Schema para Amazon RDS para MariaDB o MySQL

Supongamos que Performance Insights está activado para su instancia de base de datos o clúster de base de datos Multi-AZ pero no está administrando actualmente Performance Schema. Si desea permitir que Performance Insights administre Performance Schema automáticamente, complete los siguientes pasos.

Para configurar Performance Schema para la administración automática

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Grupos de parámetros.
3. Seleccione el nombre del grupo de parámetros para la instancia de base de datos o el clúster de bases de datos Multi-AZ.
4. Seleccione Editar.
5. Escriba **`performance_schema`** en la barra de búsqueda.
6. Seleccione el parámetro `performance_schema`.
7. Seleccione Establecer en el valor predeterminado.
8. Para confirmar, seleccione Establecer los valores en su forma predeterminada.
9. Elija Guardar cambios.
10. Reinicie la instancia de base de datos o el clúster de bases de datos multi-AZ.

> **Important**
>
> Al activar o desactivar Performance Schema, deberá reiniciar la instancia de base de datos o el clúster de bases de datos Multi-AZ.

Para obtener información sobre cómo modificar los parámetros de la instancia de base de datos, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS. Para obtener más información acerca del panel, consulte Análisis de métricas mediante el panel de Información sobre rendimiento. Para obtener más información sobre el esquema de rendimiento de MySQL, consulte MySQL Performance Schema (para 8.0) y MySQL Performance Schema (para 8.4) en la documentación de MySQL.

Configuración de directivas de acceso para información sobre rendimiento

Para acceder a Performance Insights, la entidad principal deberá tener los permisos adecuados de AWS Identity and Access Management (IAM). Puede otorgar acceso de las siguientes formas:

- Adjunte la política administrada `AmazonRDSPerformanceInsightsReadOnly` a un conjunto de permisos o rol para acceder a todas las operaciones de solo lectura de la API de Información de rendimiento. Asocie los siguientes permisos de CloudWatch: `GetMetricStatistics`, `ListMetrics` y `GetMetricData`. Para obtener más información sobre los permisos de CloudWatch, consulte la referencia de permisos de Amazon CloudWatch.
- Adjunte la política administrada `AmazonRDSPerformanceInsightsFullAccess` a un conjunto de permisos o rol para acceder a todas las operaciones de la API de Información de rendimiento. Asocie los siguientes permisos de CloudWatch: `GetMetricStatistics`, `ListMetrics` y `GetMetricData`. Para obtener más información sobre los permisos de CloudWatch, consulte la referencia de permisos de Amazon CloudWatch.
- Cree una política de IAM personalizada y asóciela a un conjunto de permisos o a un rol.

Si especificó una clave administrada por cliente al activar Información de rendimiento, asegúrese de que los usuarios de su cuenta tengan los permisos `kms:Decrypt` y `kms:GenerateDataKey` en la AWS KMS key.

En las siguientes secciones, asocie una política administrada de AWS a una entidad principal de IAM, cree una política de IAM personalizada, cambie una política de AWS KMS y conceda un acceso detallado a Información de rendimiento.

Temas

- Asociación de la política AmazonRDSPerformanceInsightsReadOnly a una entidad principal de IAM
- Asociación de la política AmazonRDSPerformanceInsightsFullAccess a una entidad principal de IAM
- Creación de una política de IAM personalizada para la información sobre rendimiento
- Cambio de una política de AWS KMS para Información de rendimiento
- Concesión de acceso preciso para Información sobre rendimiento

Asociación de la política AmazonRDSPerformanceInsightsReadOnly a una entidad principal de IAM

`AmazonRDSPerformanceInsightsReadOnly` es una política administrada de AWS que concede acceso a todas las operaciones de solo lectura de la API de Información sobre rendimiento de Amazon RDS.

Si asocia `AmazonRDSPerformanceInsightsReadOnly` a un conjunto de permisos o a un rol, el destinatario puede utilizar Información de rendimiento con las demás características de la consola.

Para obtener más información, consulte Política administrada por:AWS AmazonRDSPerformanceInsightsReadOnly.

Asociación de la política AmazonRDSPerformanceInsightsFullAccess a una entidad principal de IAM

`AmazonRDSPerformanceInsightsFullAccess` es una política administrada de AWS que concede acceso a todas las operaciones de la API de Información sobre rendimiento de Amazon RDS.

Si asocia `AmazonRDSPerformanceInsightsFullAccess` a un conjunto de permisos o a un rol, el destinatario puede utilizar Información de rendimiento con las demás características de la consola.

Para obtener más información, consulte Política administrada por AWS: AmazonRDSPerformanceInsightsFullAccess.

Creación de una política de IAM personalizada para la información sobre rendimiento

En el caso de usuarios que no tengan la política `AmazonRDSPerformanceInsightsReadOnly` o `AmazonRDSPerformanceInsightsFullAccess`, puede conceder acceso a Información sobre rendimiento a través de la creación o modificación de una política de IAM administrada por el usuario. Al asociar la política a un conjunto de permisos o a un rol, el destinatario puede utilizar Información de rendimiento.

Creación de una política personalizada

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).

4. En la página Crear política, elija la opción JSON.
5. Copie y pegue el texto proporcionado en la sección Documento de política de JSON en la Guía de referencia de las políticas administradas de AWS para la política AmazonRDSPerformanceInsightsReadOnly o AmazonRDSPerformanceInsightsFullAccess.
6. Elija Review policy (Revisar política).
7. Proporcione un nombre para la política y, opcionalmente, una descripción, a continuación, elija Create policy (Crear política).

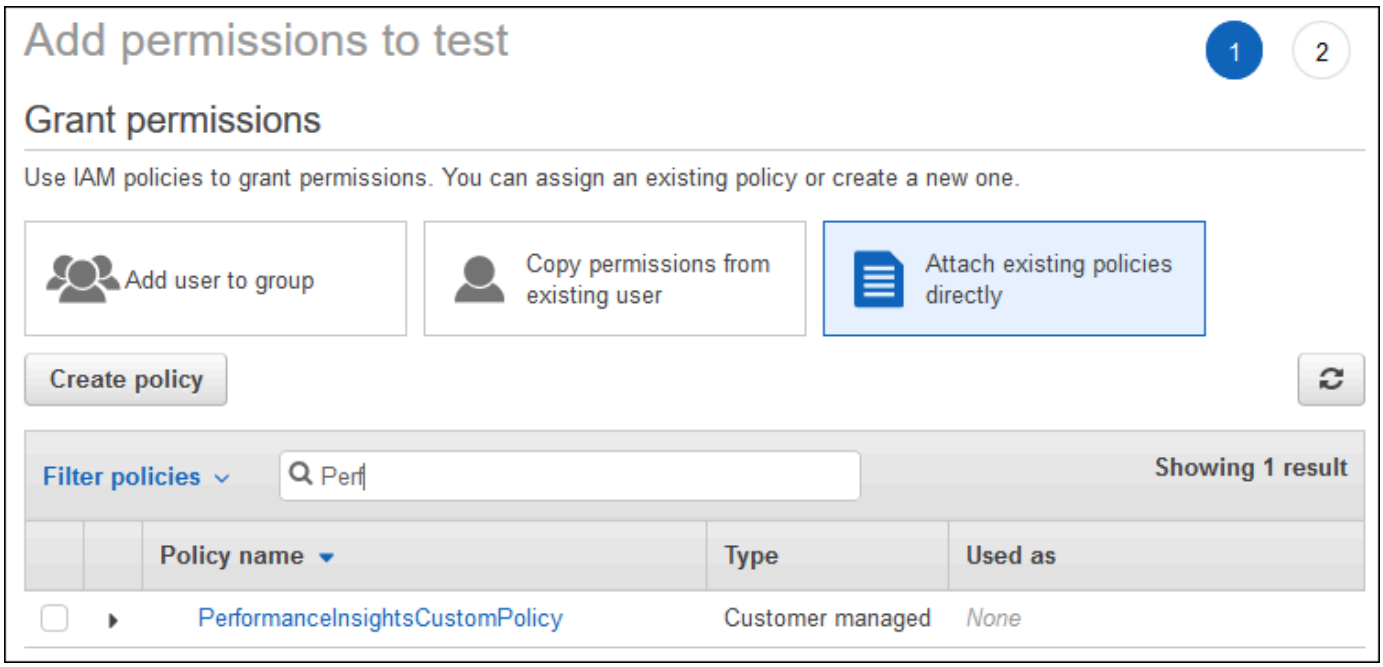
Ahora ya puede asociar la política a un conjunto de permisos o a un rol. En el procedimiento siguiente, se presupone que ya tiene un usuario para este fin.

Asociación de la política a un usuario

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Users.
3. Elija en la lista un usuario existente.

> **Important**
>
> Para utilizar Performance Insights, asegúrese de tener acceso a Amazon RDS además de la política personalizada. Por ejemplo, la política predefinida `AmazonRDSPerformanceInsightsReadOnly` ofrece acceso de solo lectura a Amazon RDS. Para obtener más información, consulte Administración de acceso mediante políticas.

4. En la página Summary, elija Add permissions.
5. Elija Asociar políticas existentes directamente. En Buscar, escriba los primeros caracteres del nombre de la política, como se muestra en la siguiente imagen.



6. Elija la política y, a continuación, elija Next: Review.
7. Elija Add permissions (Agregar permisos).

Cambio de una política de AWS KMS para Información de rendimiento

Performance Insights utiliza una AWS KMS key para cifrar información confidencial. Cuando active Performance Insights a través de la API o de la consola, podrá hacer una de las siguientes cosas:

- Elegir la Clave administrada de AWS predeterminada.

  Amazon RDS utiliza la Clave administrada de AWS para su nueva instancia de base de datos. Amazon RDS crea una Clave administrada de AWS para su cuenta de Cuenta de AWS. Su cuenta de Cuenta de AWS tiene una Clave administrada de AWS diferente para Amazon RDS para cada Región de AWS.
- Elija una clave administrada por el cliente.

  Si especifica una clave administrada por el cliente, los usuarios de su cuenta que llamen a la API de Performance Insights necesitarán los permisos `kms:Decrypt` y `kms:GenerateDataKey` sobre la clave de KMS. Puede configurar estos permisos a través de directivas de IAM. Sin embargo, le recomendamos que administre estos permisos a través de su directiva de clave KMS. Para obtener más información, consulte Políticas de claves en AWS KMS en la Guía para desarrolladores de AWS Key Management Service.

Example

En el siguiente ejemplo se muestra cómo agregar instrucciones a la política de claves de KMS. Estas instrucciones permiten el acceso a la información sobre rendimiento. Dependiendo de cómo utilice la clave KMS, es posible que desee cambiar algunas restricciones. Antes de agregar sentencias a la directiva, elimine todos los comentarios.

```
{
"Version" : "2012-10-17",
 "Id" : "your-policy",
 "Statement" : [ {
    //This represents a statement that currently exists in your policy.
 }
 ....,
 //Starting here, add new statement to your policy for Performance Insights.
 //We recommend that you add one new statement for every RDS instance
{
    "Sid" : "Allow viewing RDS Performance Insights",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            //One or more principals allowed to access Performance Insights
            "arn:aws:iam::444455556666:role/Role1"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition" : {
        "StringEquals" : {
            //Restrict access to only RDS APIs (including Performance Insights).
            //Replace region with your AWS Region.
            //For example, specify us-west-2.
            "kms:ViaService" : "rds.region.amazonaws.com"
        },
        "ForAnyValue:StringEquals": {
            //Restrict access to only data encrypted by Performance Insights.
            "kms:EncryptionContext:aws:pi:service": "rds",
            "kms:EncryptionContext:service": "pi",

            //Restrict access to a specific RDS instance.
```

```
            //The value is a DbiResourceId.
           "kms:EncryptionContext:aws:rds:db-id": "db-AAAAABBBBBCCCCDDDDDEEEEE"
        }
    }
}
```

Cómo Información de rendimiento utiliza la clave administrada por el cliente de AWS KMS

Información de rendimiento utiliza claves administradas por el cliente para cifrar datos confidenciales. Al activar Información de rendimiento, puede proporcionar una clave de AWS KMS a través de la API. Información de rendimiento crea permisos de KMS en esta clave. Utiliza la clave y realiza las operaciones necesarias para procesar los datos confidenciales. Los datos confidenciales incluyen campos como el usuario, la base de datos, la aplicación y el texto de la consulta SQL. Información de rendimiento garantiza que los datos permanezcan cifrados tanto en reposo como en tránsito.

Funcionamiento de la IAM de Información de rendimiento con AWS KMS

IAM otorga permisos a API específicas. Información de rendimiento tiene las siguientes API públicas, que puede restringir mediante políticas de IAM:

- `DescribeDimensionKeys`
- `GetDimensionKeyDetails`
- `GetResourceMetadata`
- `GetResourceMetrics`
- `ListAvailableResourceDimensions`
- `ListAvailableResourceMetrics`

Puede utilizar las siguientes solicitudes de API para obtener datos confidenciales.

- `DescribeDimensionKeys`
- `GetDimensionKeyDetails`
- `GetResourceMetrics`

Cuando utiliza la API para obtener datos confidenciales, Información de rendimiento utiliza las credenciales del intermediario. Esta comprobación garantiza que el acceso a los datos confidenciales esté limitado a quienes tengan acceso a la clave de KMS.

Al llamar a estas API, necesita permisos para llamar a la API a través de la política de IAM y permisos para invocar la acción `kms:decrypt` a través de la política de claves de AWS KMS.

La API `GetResourceMetrics` puede devolver datos confidenciales y no confidenciales. Los parámetros de la solicitud determinan si la respuesta debe incluir datos confidenciales. La API devuelve datos confidenciales cuando la solicitud incluye una dimensión confidencial en los parámetros del filtro o de grupo.

Para obtener más información acerca de las dimensiones que puede utilizar con la API `GetResourceMetrics`, consulte DimensionGroup.

Example Ejemplos

En el siguiente ejemplo se solicitan los datos confidenciales del grupo:`db.user`

```
POST / HTTP/1.1
Host: <Hostname>
Accept-Encoding: identity
X-Amz-Target: PerformanceInsightsv20180227.GetResourceMetrics
Content-Type: application/x-amz-json-1.1
User-Agent: <UserAgentString>
X-Amz-Date: <Date>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
 Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
  "ServiceType": "RDS",
  "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
  "MetricQueries": [
    {
      "Metric": "db.load.avg",
      "GroupBy": {
        "Group": "db.user",
        "Limit": 2
      }
    }
  ],
  "StartTime": 1693872000,
  "EndTime": 1694044800,
  "PeriodInSeconds": 86400
}
```

Example

En el siguiente ejemplo se solicitan los datos no confidenciales de la métrica:`db.load.avg`

```
POST / HTTP/1.1
Host: <Hostname>
Accept-Encoding: identity
X-Amz-Target: PerformanceInsightsv20180227.GetResourceMetrics
Content-Type: application/x-amz-json-1.1
User-Agent: <UserAgentString>
X-Amz-Date: <Date>
Authorization: AWS4-HMAC-SHA256 Credential=<Credential>, SignedHeaders=<Headers>,
 Signature=<Signature>
Content-Length: <PayloadSizeBytes>
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "MetricQueries": [
        {
            "Metric": "db.load.avg"
        }
    ],
    "StartTime": 1693872000,
    "EndTime": 1694044800,
    "PeriodInSeconds": 86400
}
```

Concesión de acceso preciso para Información sobre rendimiento

El control de acceso preciso ofrece formas adicionales de controlar el acceso a Información sobre rendimiento. Este control de acceso puede permitir o denegar el acceso a dimensiones individuales para acciones de Información sobre rendimiento `GetResourceMetrics`, `DescribeDimensionKeys` y `GetDimensionKeyDetails`. Para utilizar el acceso preciso, especifique las dimensiones en la política de IAM mediante claves de condición. La evaluación del acceso sigue la lógica de evaluación de la política de IAM. Para obtener más información, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM. Si la instrucción de la política de IAM no especifica ninguna dimensión, entonces la instrucción controla el acceso a todas las dimensiones de la acción especificada. Para ver la lista de dimensiones disponibles, consulte DimensionGroup.

Para averiguar las dimensiones a las que están autorizadas a acceder sus credenciales, utilice el parámetro `AuthorizedActions` en `ListAvailableResourceDimensions` y especifique la acción. Los valores permitidos para `AuthorizedActions` son los siguientes:

- `GetResourceMetrics`
- `DescribeDimensionKeys`
- `GetDimensionKeyDetails`

Por ejemplo, si especifica `GetResourceMetrics` para el parámetro `AuthorizedActions`, `ListAvailableResourceDimensions` devuelve la lista de dimensiones a las que la acción `GetResourceMetrics` está autorizada a acceder. Si especifica varias acciones en el parámetro `AuthorizedActions`, `ListAvailableResourceDimensions` devuelve una intersección de las dimensiones a las que esas acciones están autorizadas a acceder.

Example

El siguiente ejemplo proporciona acceso a las dimensiones especificadas para las acciones `GetResourceMetrics` y `DescribeDimensionKeys`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowToDiscoverDimensions",
            "Effect": "Allow",
            "Action": [
                "pi:ListAvailableResourceDimensions"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ]
        },
        {
            "Sid": "SingleAllow",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": [
```

```
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    // only these dimensions are allowed. Dimensions not included in
                    // a policy with "Allow" effect will be denied
                    "pi:Dimensions": [
                        "db.sql_tokenized.id",
                        "db.sql_tokenized.statement"
                    ]
                }
            }
        }


    ]
}
```

A continuación se muestra la respuesta para la dimensión solicitada:

```
 // ListAvailableResourceDimensions API
// Request
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "Metrics": [ "db.load" ],
    "AuthorizedActions": ["DescribeDimensionKeys"]
}

// Response
{
    "MetricDimensions": [ {
        "Metric": "db.load",
        "Groups": [
            {
                "Group": "db.sql_tokenized",
                "Dimensions": [
                    { "Identifier": "db.sql_tokenized.id" },
                  //  { "Identifier": "db.sql_tokenized.db_id" }, // not included
 because not allows in the IAM Policy
```

```
                    { "Identifier": "db.sql_tokenized.statement" }
                ]
            }

        ] }
    ]
}
```

El siguiente ejemplo especifica un acceso permitido y dos denegados para las dimensiones.

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
            "Sid": "AllowToDiscoverDimensions",
            "Effect": "Allow",
            "Action": [
                "pi:ListAvailableResourceDimensions"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ]
          },

          {
            "Sid": "O01AllowAllWithoutSpecifyingDimensions",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ]
        },

        {
            "Sid": "O01DenyAppDimensionForAll",
            "Effect": "Deny",
            "Action": [
                "pi:GetResourceMetrics",
```

```
                "pi:DescribeDimensionKeys"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "pi:Dimensions": [
                        "db.application.name"
                    ]
                }
            }
        },

        {
            "Sid": "O01DenySQLForGetResourceMetrics",
            "Effect": "Deny",
            "Action": [
                "pi:GetResourceMetrics"
            ],
            "Resource": [
                "arn:aws:pi:us-east-1:123456789012:metrics/rds/db-
ABC1DEFGHIJKL2MNOPQRSTUV3W"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "pi:Dimensions": [
                        "db.sql_tokenized.statement"
                    ]
                }
            }
        }
    ]
}
```

A continuación se muestran las respuestas para las dimensiones solicitadas:

```
   // ListAvailableResourceDimensions API
// Request
{
```

```
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "Metrics": [ "db.load" ],
    "AuthorizedActions": ["GetResourceMetrics"]
}

// Response
{
    "MetricDimensions": [ {
        "Metric": "db.load",
        "Groups": [
            {
                "Group": "db.application",
                "Dimensions": [

                  // removed from response because denied by the IAM Policy
                  //  { "Identifier": "db.application.name" }
                ]
            },
            {
                "Group": "db.sql_tokenized",
                "Dimensions": [
                    { "Identifier": "db.sql_tokenized.id" },
                    { "Identifier": "db.sql_tokenized.db_id" },

                  // removed from response because denied by the IAM Policy
                  //  { "Identifier": "db.sql_tokenized.statement" }
                ]
            },
            ...
        ] }
    ]
}
```

```
// ListAvailableResourceDimensions API
// Request
{
    "ServiceType": "RDS",
    "Identifier": "db-ABC1DEFGHIJKL2MNOPQRSTUV3W",
    "Metrics": [ "db.load" ],
    "AuthorizedActions": ["DescribeDimensionKeys"]
}
```

```
// Response
{
    "MetricDimensions": [ {
        "Metric": "db.load",
        "Groups": [
            {
                "Group": "db.application",
                "Dimensions": [
                  // removed from response because denied by the IAM Policy
                  //  { "Identifier": "db.application.name" }
                ]
            },
            {
                "Group": "db.sql_tokenized",
                "Dimensions": [
                    { "Identifier": "db.sql_tokenized.id" },
                    { "Identifier": "db.sql_tokenized.db_id" },

                  // allowed for DescribeDimensionKeys because our IAM Policy
                  // denies it only for GetResourceMetrics
                    { "Identifier": "db.sql_tokenized.statement" }
                ]
            },
            ...
        ] }
    ]
}
```

Análisis de métricas mediante el panel de Información sobre rendimiento

Important

AWS ha anunciado la fecha de fin de la vida útil de Información de rendimiento: el 30 de noviembre de 2025. Después de esta fecha, Amazon RDS dejará de admitir la experiencia de la consola de Información de rendimiento, los periodos de retención flexibles (de 1 a 24 meses) y los precios asociados. La API de Información de rendimiento seguirá existiendo sin cambios en los precios. Los costos de la API de Información de rendimiento aparecerán en la factura de AWS junto con el costo de información de la base de datos de CloudWatch. Le recomendamos que actualice cualquier instancia de base de datos que utilice el nivel de pago de Información de rendimiento al modo avanzado de la información de la base de

datos antes del 30 de noviembre de 2025. Para obtener información sobre la actualización al modo avanzado de Información de rendimiento, consulte Activación del modo avanzado de Información sobre las bases de datos para Amazon RDS.
Si no realiza ninguna acción, las instancias de base de datos que utilizan Información de rendimiento pasarán por defecto a utilizar el modo estándar de información de rendimiento. Con el modo estándar de Información de base de datos, es posible que pierda el acceso al historial de datos de rendimiento de más de 7 días y que no pueda utilizar los planes de ejecución y las características de análisis bajo demanda en la consola de Amazon RDS. Después del 30 de noviembre de 2025, solo el modo avanzado de la información de base de datos admitirá los planes de ejecución y el análisis bajo demanda.
Con la información de la base de datos de CloudWatch, puede supervisar la carga de base de datos de la flota de bases de datos y analizar y solucionar problemas de rendimiento a escala. Para obtener más detalles acerca de Información de base de datos, consulte Supervisión de las bases de datos de Amazon RDS con Información sobre las bases de datos de CloudWatch. Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

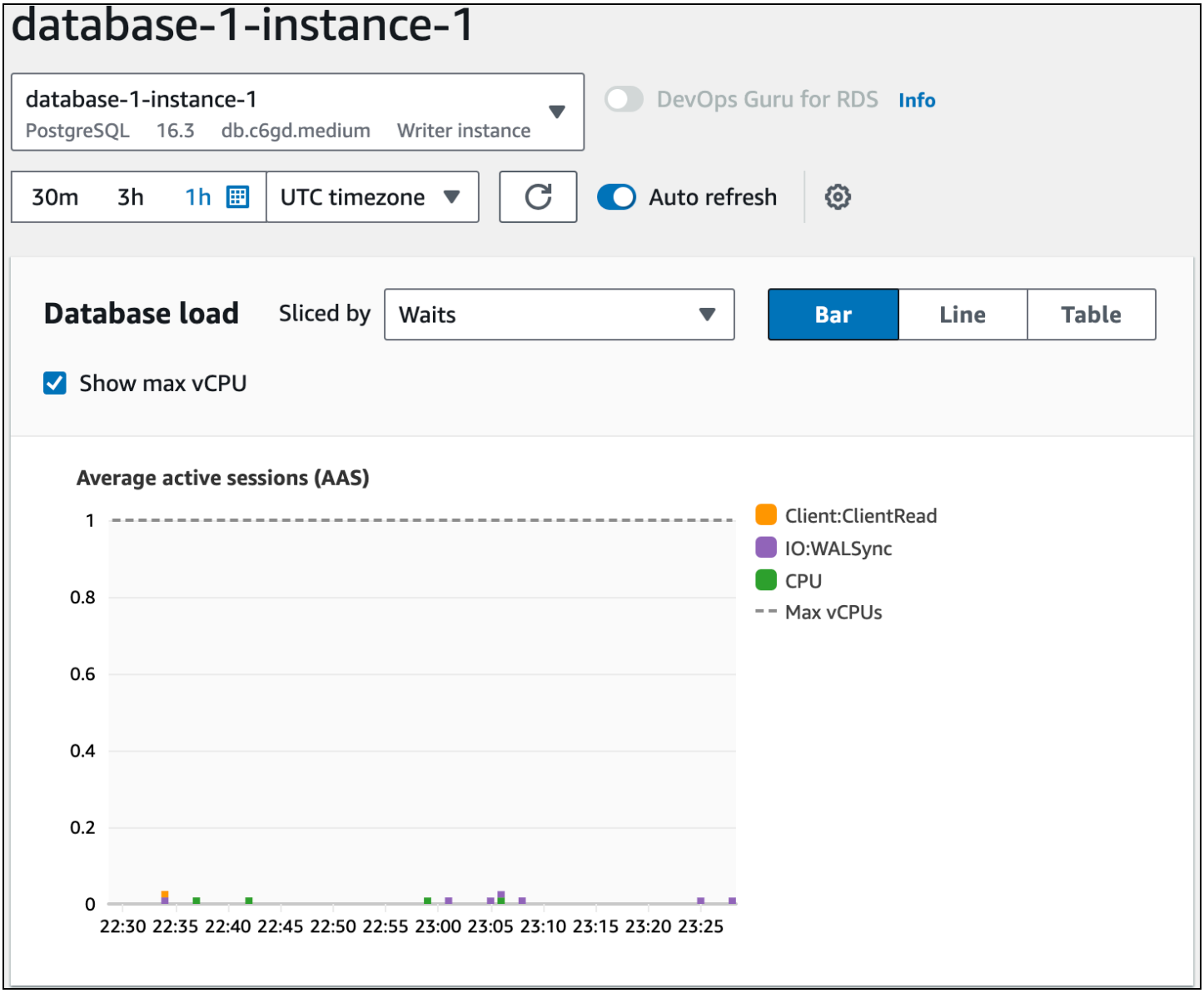
El panel de Performance Insights contiene información de desempeño de la base de datos para ayudarle a analizar y solucionar los problemas de desempeño. En la página del panel principal, encontrará información sobre la carga de la base de datos. Puede “dividir” la carga de la base de datos por dimensiones, como eventos de espera o SQL.

Panel de Performance Insights

- Información general del panel de Performance Insights
- Acceso al panel Información de rendimiento
- Análisis de carga de base de datos mediante eventos de espera
- Análisis del rendimiento de la base de datos durante un período de tiempo
- Análisis de consultas con la pestaña Top SQL en Información de rendimiento
- Análisis de la carga de PDB principal de Oracle
- Análisis de planes de ejecución mediante el panel de Información de rendimiento para Amazon RDS

Información general del panel de Performance Insights

El panel es la forma más sencilla de interactuar con Performance Insights. En el siguiente ejemplo, se muestra el panel de una instancia de base de datos de PostgreSQL.

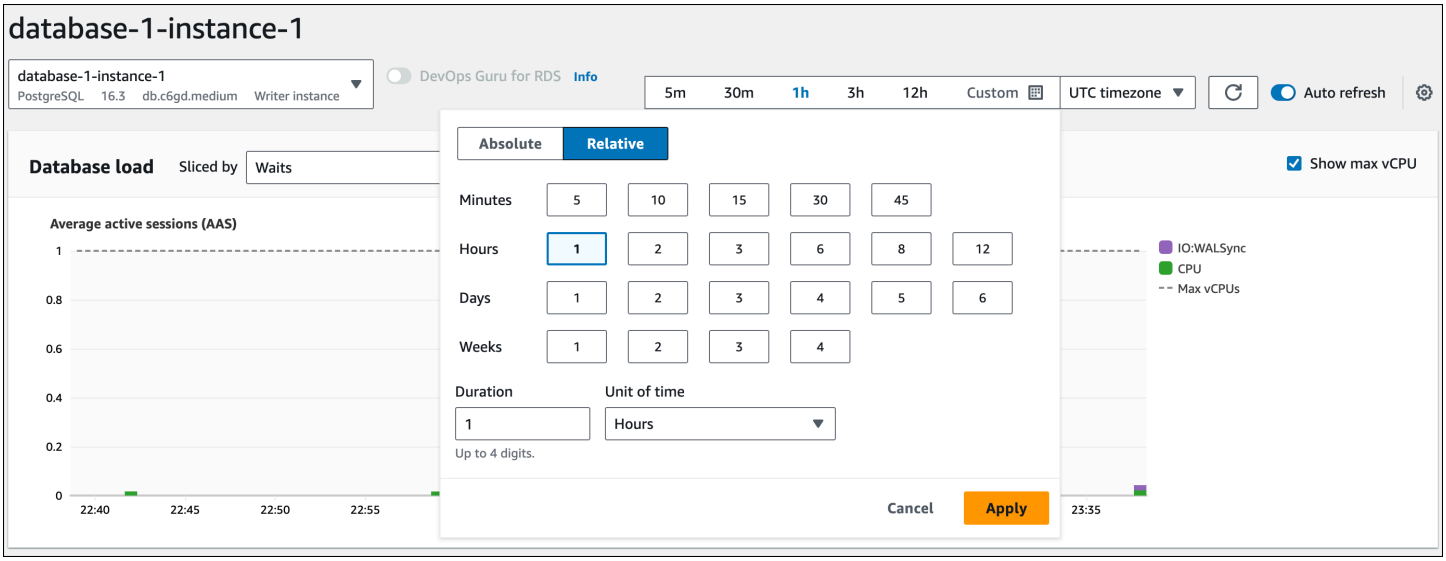


Temas

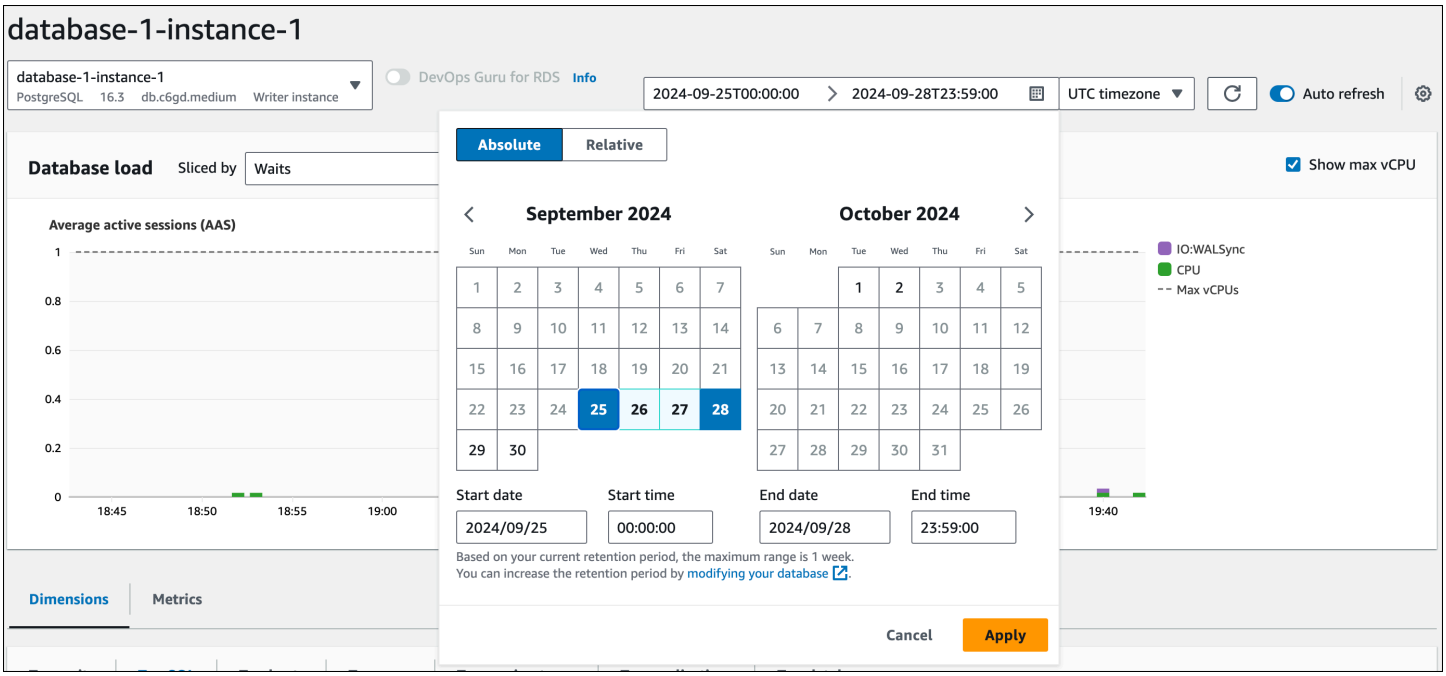
- Filtro de intervalo de tiempo
- Gráfico Counter metrics (Métricas de contador)
- Gráfico Database load (Carga de base de datos)
- Tabla de dimensiones principales

Filtro de intervalo de tiempo

De forma predeterminada, el panel de Performance Insights muestra los datos de carga de la base de datos de la última hora. Puede ajustar este rango de modo que sea tan corto como 5 minutos o tan largo como 2 años. También puede seleccionar un rango relativo personalizado.



Puede seleccionar un rango absoluto con fecha y hora de inicio y fin. En el siguiente ejemplo, se muestra el intervalo de tiempo que comienza a medianoche del 25/09/24 y termina a las 23:59 del 28/09/24.



De forma predeterminada, la zona horaria para el panel de Información de rendimiento es el horario universal coordinado (UTC). También puede elegir la zona horaria local.

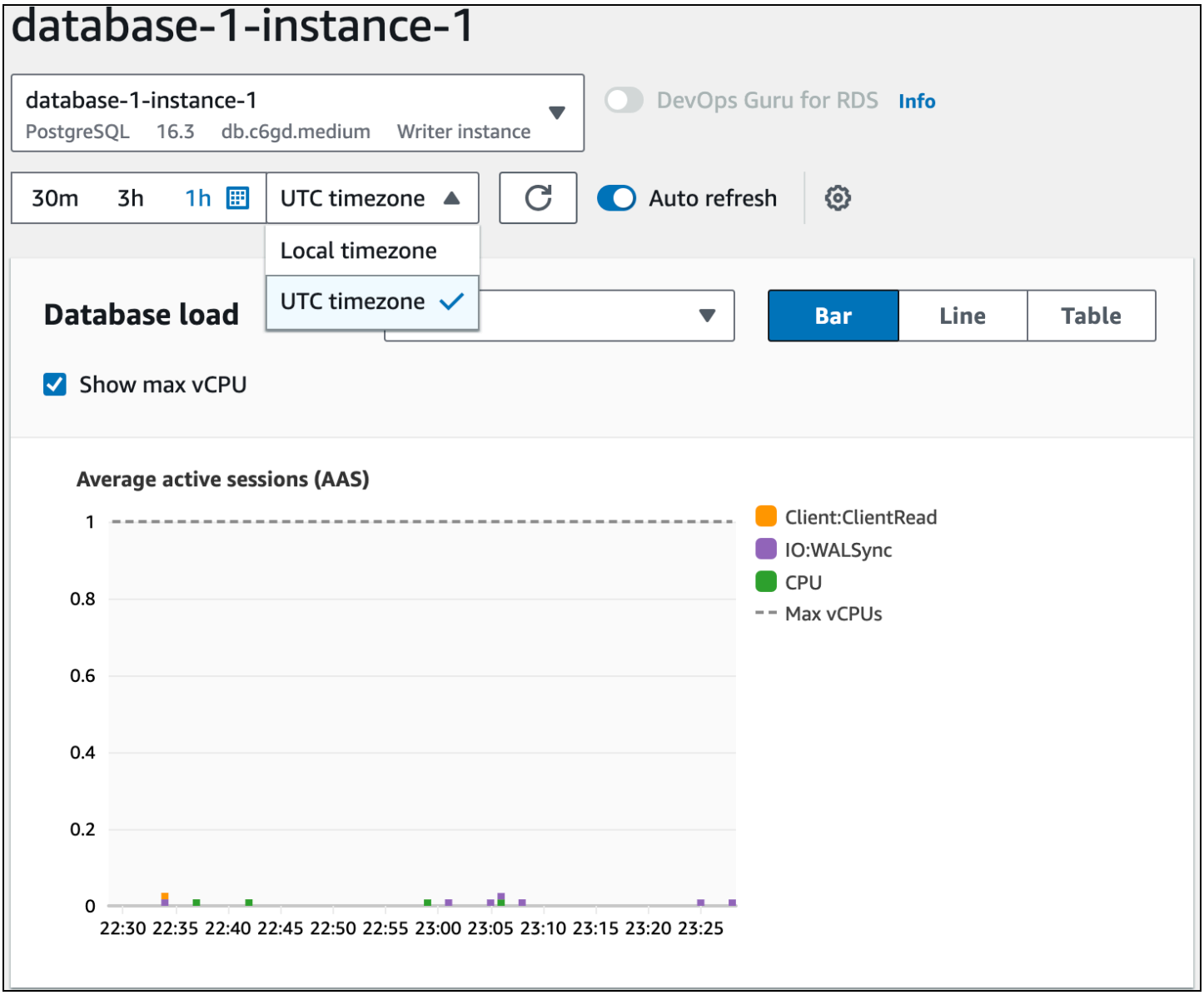
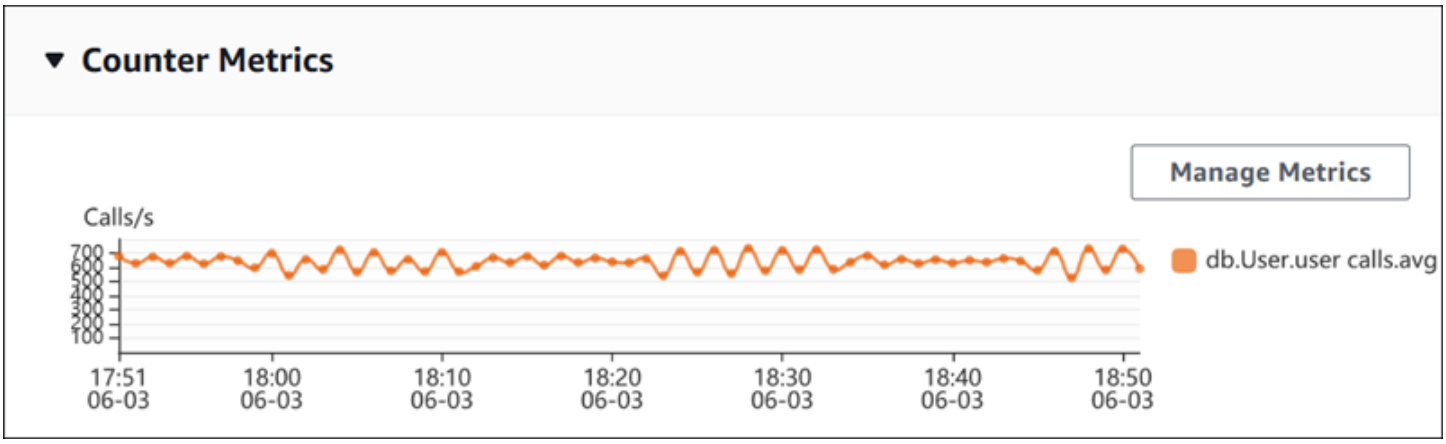


Gráfico Counter metrics (Métricas de contador)

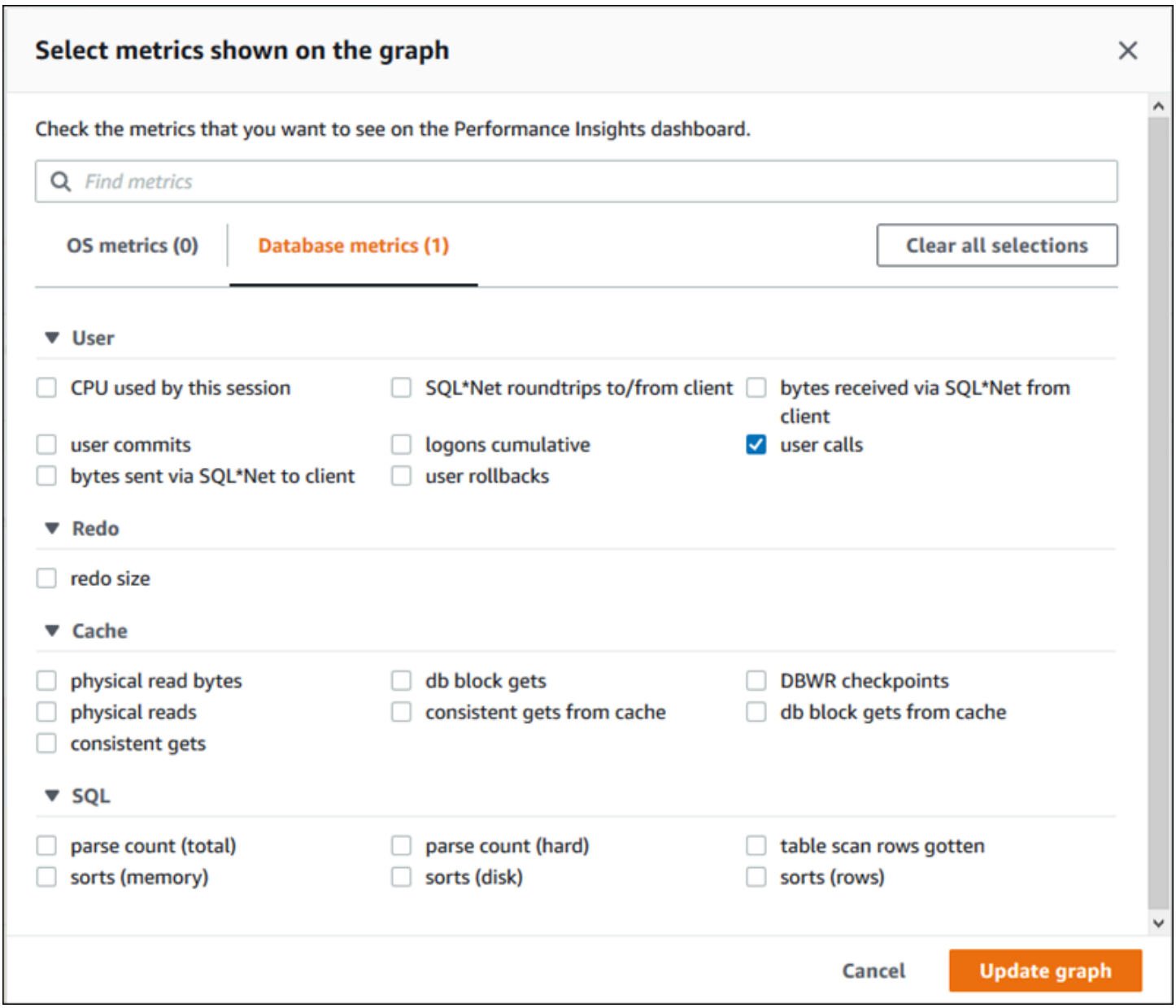
Con las métricas de contador, puede personalizar el panel de Información sobre rendimiento para que incluya hasta 10 gráficos adicionales. Estos gráficos muestran una selección de docenas de métricas de rendimiento de sistemas operativos y bases de datos. Esta información se puede correlacionar con la carga de base de datos para ayudar a identificar y analizar problemas de rendimiento.

El gráfico Counter metrics (Métricas de contador) muestra los datos para los contadores de rendimiento. Las métricas predeterminadas dependen del motor de base de datos:

- MySQL y MariaDB: `db.SQL.Innodb_rows_read.avg`
- Oracle – `db.User.user calls.avg`
- Microsoft SQL Server – `db.Databases.Active Transactions(_Total).avg`
- PostgreSQL – `db.Transactions.xact_commit.avg`



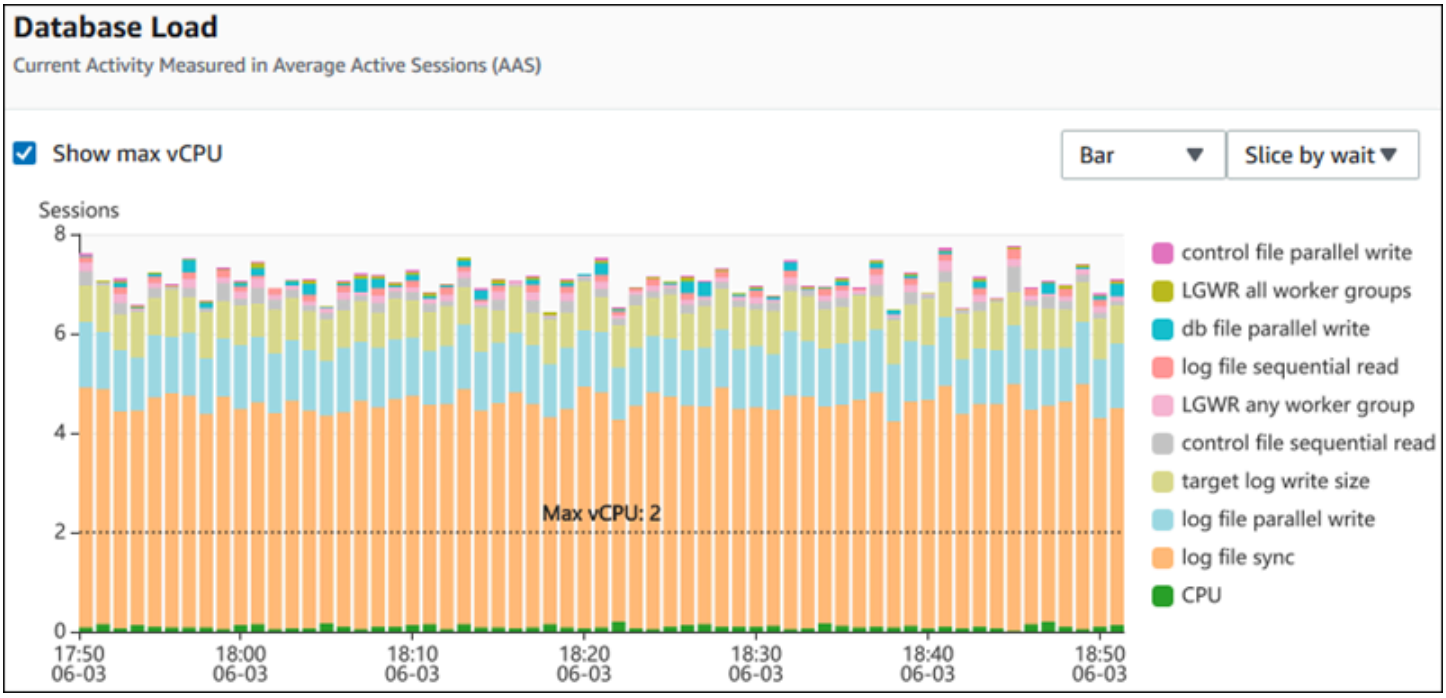
Para cambiar los contadores de rendimiento, elija Manage Metrics (Administrar métricas). Puede seleccionar varias métricas del sistema operativo o métricas de la base de datos, como se muestra en la siguiente captura de pantalla. Para ver los detalles de cualquier métrica, sitúe el cursor sobre el nombre de la métrica.



Para obtener descripciones de las métricas de contador que puede agregar para cada motor de base de datos, consulte Métricas de contador de Información de rendimiento.

Gráfico Database load (Carga de base de datos)

El gráfico Database load (Carga de base de datos) muestra cómo se compara la carga de base de datos con la capacidad de la instancia de base de datos representada por la línea Max vCPU (Máximo de vCPU). De forma predeterminada, el gráfico de líneas apilado representa la carga de base de datos como promedio de sesiones activas por unidad de tiempo. La carga de base de datos está dividida (agrupada) por estados de espera.

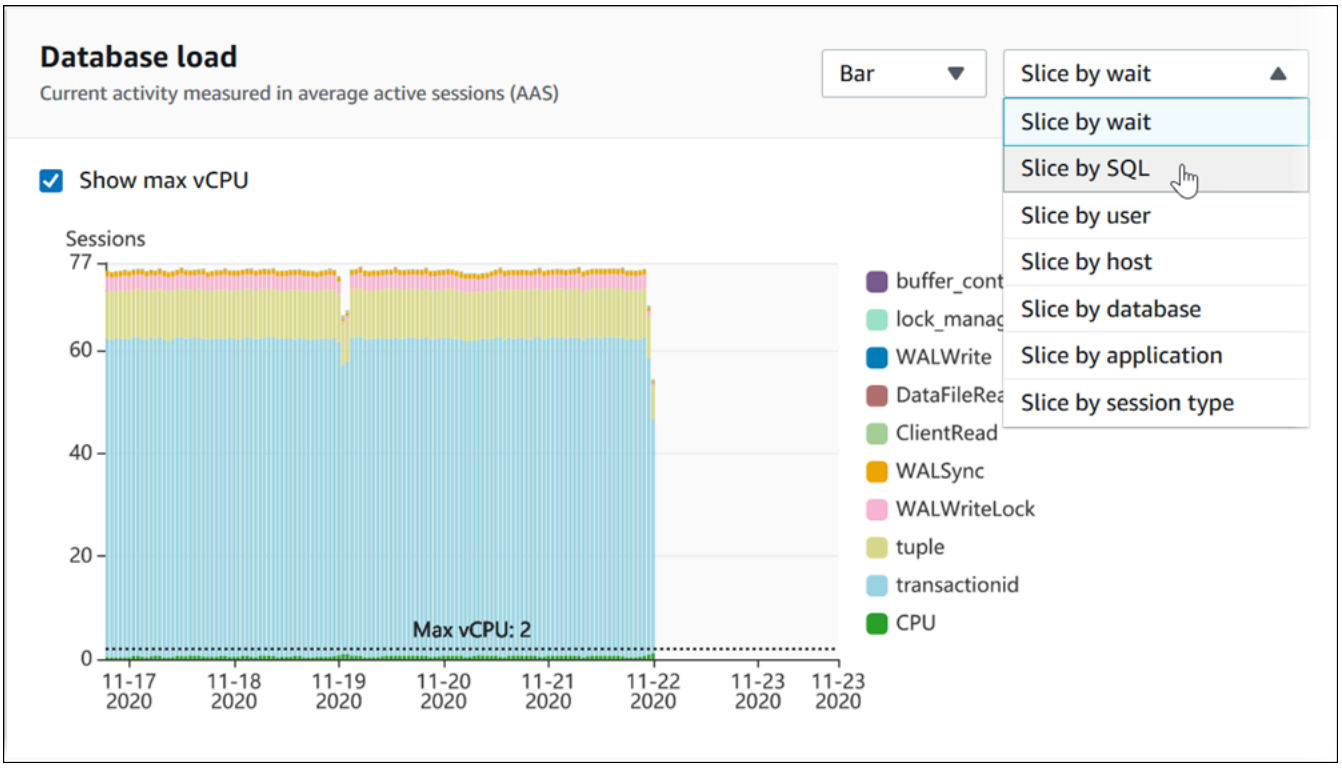


Carga de base de datos dividida por dimensiones

Puede elegir ver la carga como sesiones activas agrupadas por cualquier dimensión admitida. En la tabla siguiente se muestran las dimensiones admitidas para los distintos motores.

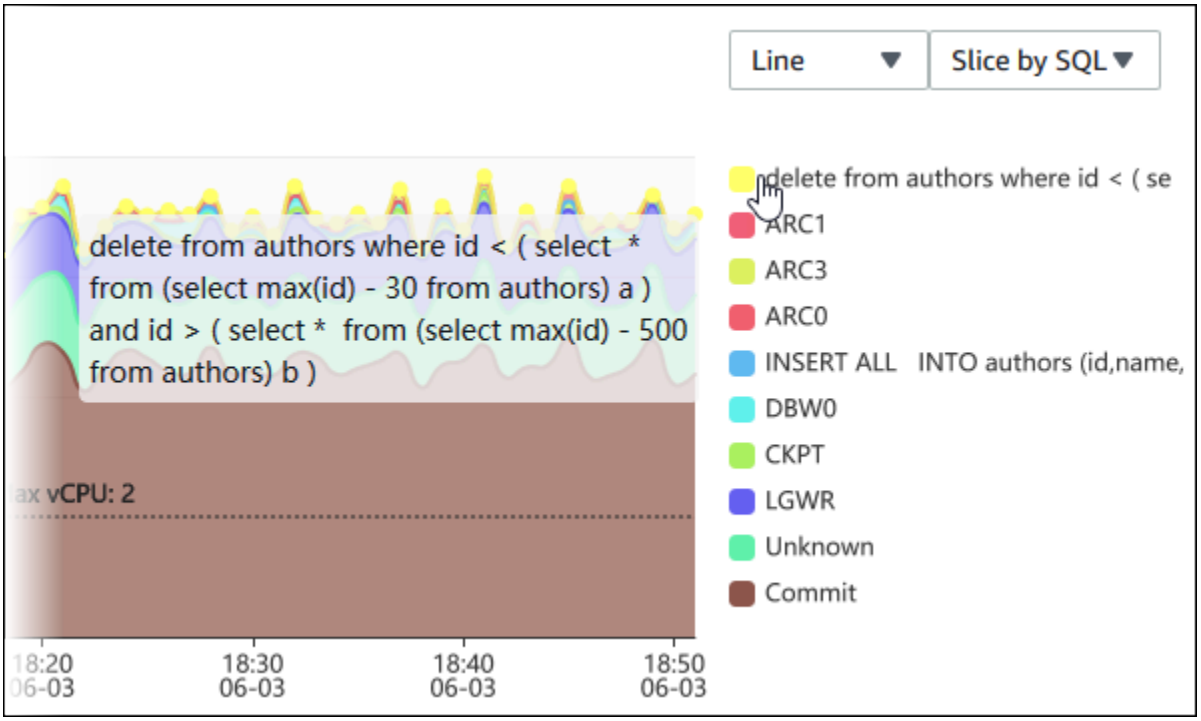
Dimensión	Oracle	SQL Server	PostgreSQL	MySQL
Host	Sí	Sí	Sí	Sí
SQL	Sí	Sí	Sí	Sí
User	Sí	Sí	Sí	Sí
Esperas	Sí	Sí	Sí	Sí
Planes	Sí	No	No	No
Aplicación	No	No	Sí	No
Base de datos	No	No	Sí	Sí
Tipo de sesión	No	No	Sí	No

En la imagen siguiente, se muestran las dimensiones de una instancia de base de datos de PostgreSQL.



Detalles de carga de base de datos de un elemento de dimensión

Para consultar los detalles de un elemento de carga de base de datos dentro de una dimensión, pase el cursor sobre el nombre de elemento. En la imagen siguiente, se muestran los detalles de una instrucción de SQL.



Para consultar los detalles de cualquier elemento para el periodo de tiempo seleccionado en la leyenda, coloque el cursor sobre ese elemento.

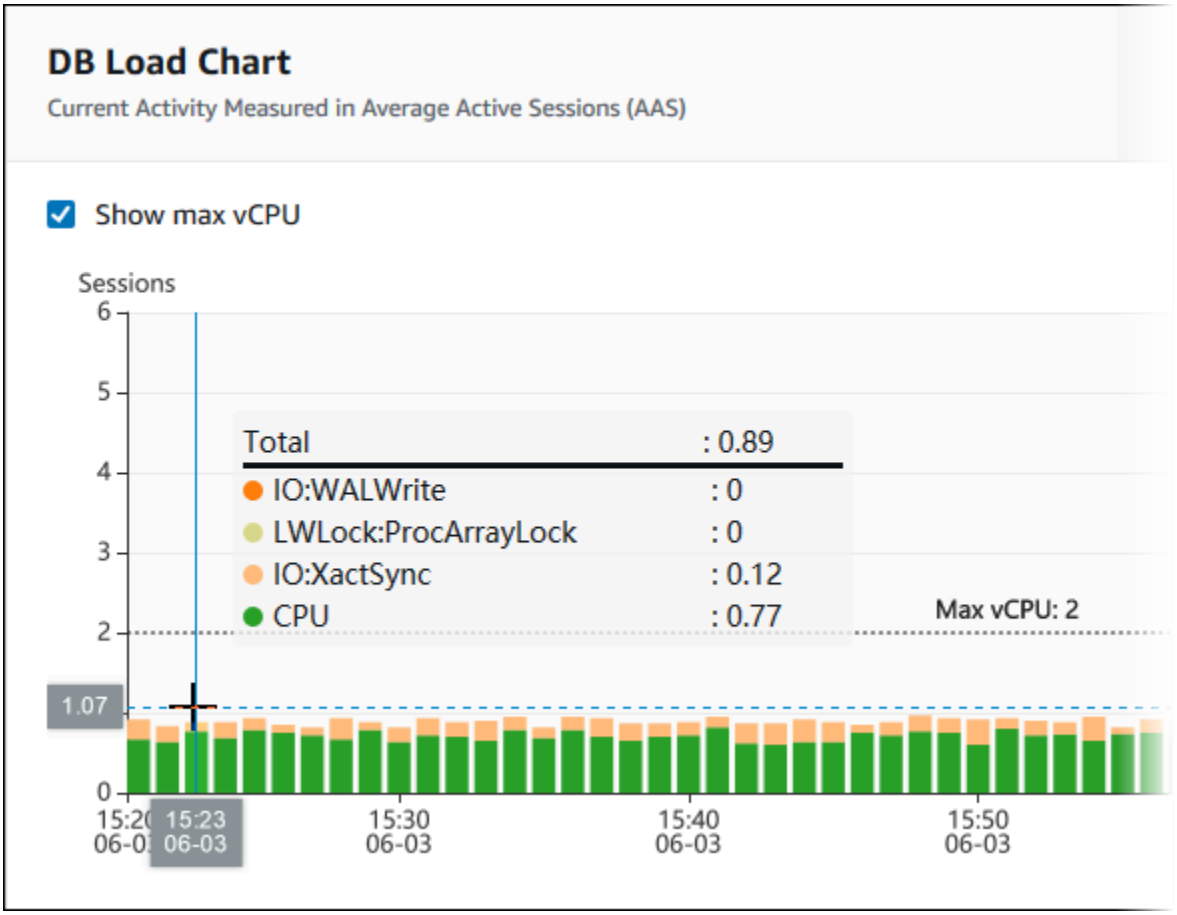
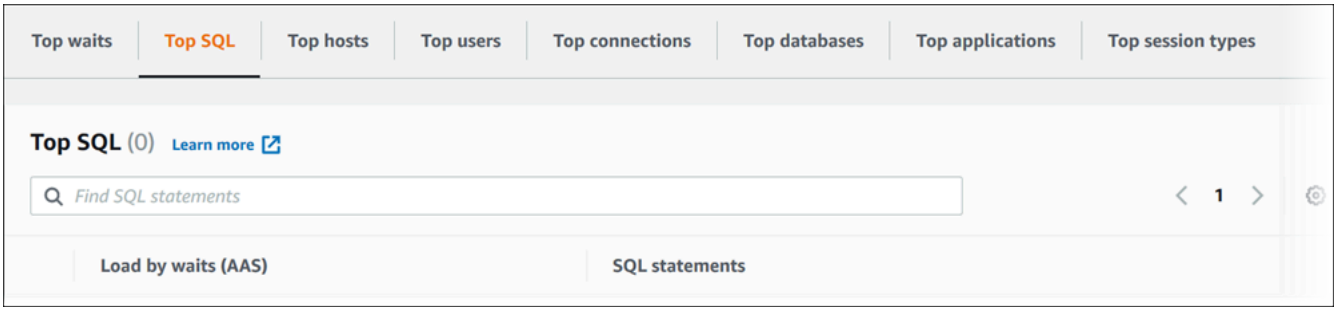


Tabla de dimensiones principales

La tabla de dimensiones principales divide la carga de base de datos por diferentes dimensiones. Una dimensión es una categoría o “dividir por” para diferentes características de la carga de base de datos. Si la dimensión es SQL, Top SQL (SQL principal) muestra las instrucciones SQL que más contribuyen a la carga de bases de datos.



Elija cualquiera de las siguientes pestañas de dimensión.

Tab	Descripción	Motores admitidos
SQL principal	Las instrucciones SQL que se están ejecutando	Todos
Esperas principales	El evento por el que la base de datos de backend está esperando.	Todos
Hosts principales	El nombre del host del cliente conectado.	Todos
Usuarios principales	El usuario que ha iniciado sesión en la base de datos.	Todos
Bases de datos principales	El nombre de la base de datos a la que está conectado el cliente.	PostgreSQL, MySQL, MariaDB y SQL Server solamente
Aplicaciones principales	El nombre de la aplicación que está conectada a la base de datos.	PostgreSQL y SQL Server solamente
Tipos de sesiones principales	El tipo de la sesión actual	PostgreSQL únicamente

Para obtener más información sobre cómo analizar las consultas mediante la pestaña Top SQL (SQL principal), consulte Información general sobre la pestaña Top SQL (SQL principal).

Acceso al panel Información de rendimiento

Amazon RDS ofrece una vista consolidada de las métricas de Información de rendimiento y CloudWatch en el panel Información de rendimiento.

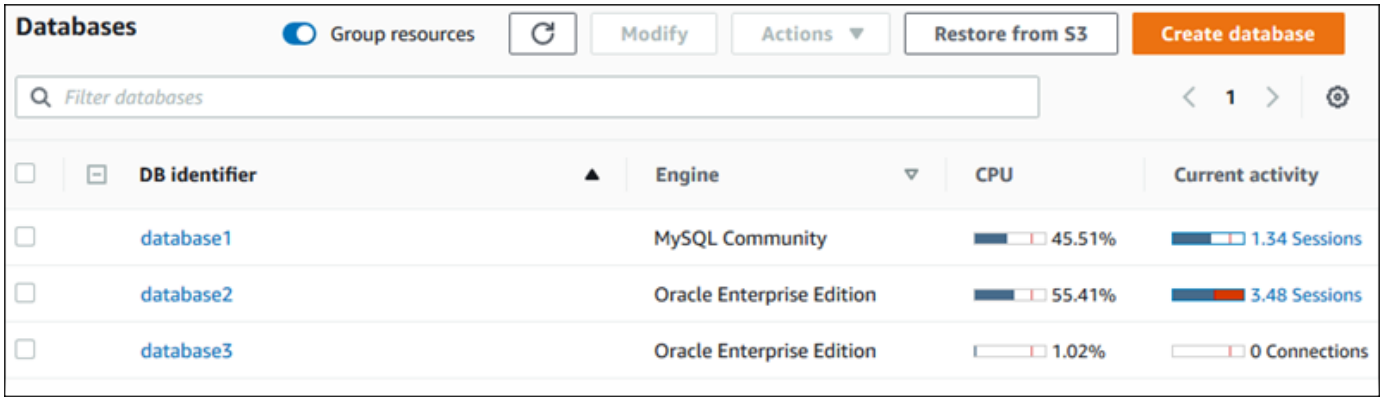
Para acceder al panel Información de rendimiento, lleve a cabo el siguiente procedimiento.

Para ver el panel de Performance Insights en la consola de administración de AWS

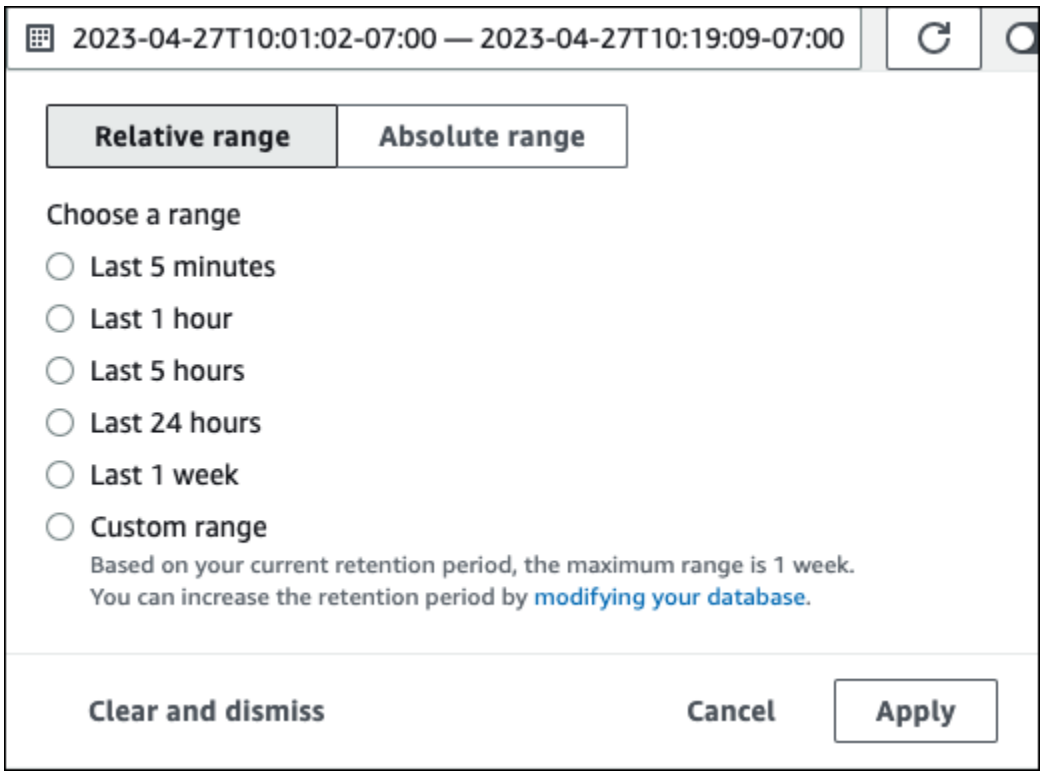
1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.

3. Elija una instancia de base de datos.

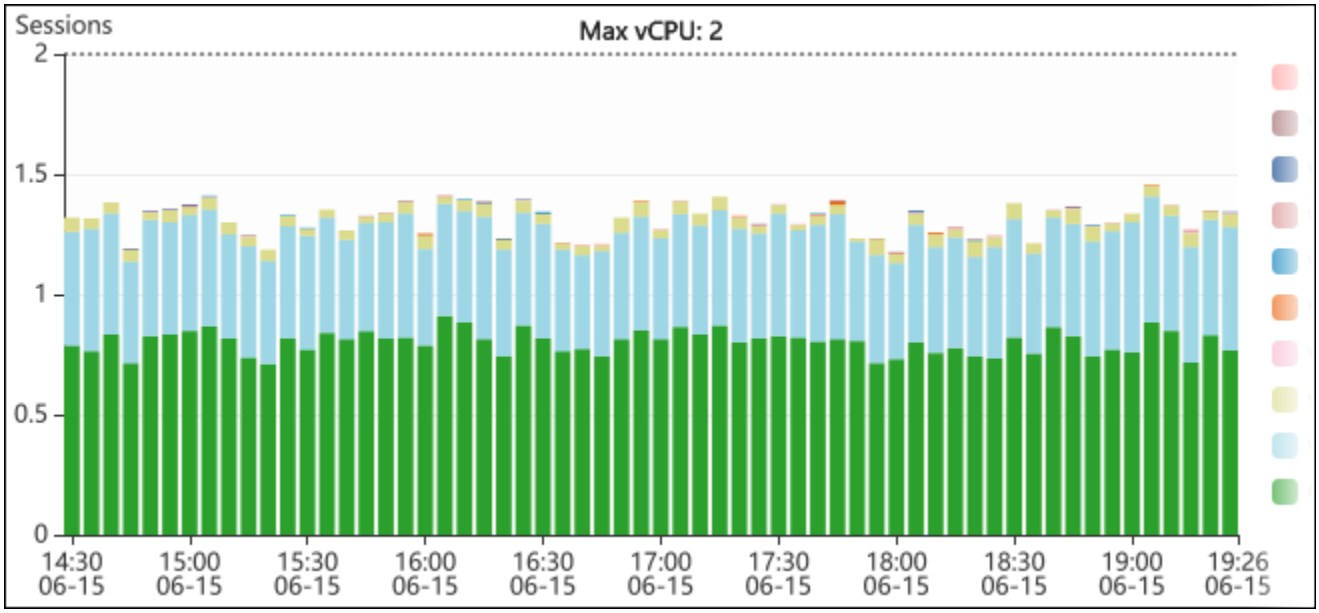
   En instancias de base de datos con Información de rendimiento activado, también puede acceder al panel Información de rendimiento eligiendo el elemento Sesiones en la lista de instancias de bases de datos. En Actividad actual, el elemento Sesiones muestra la carga de la base de datos en el como promedio de sesiones activas en los últimos cinco minutos. La barra muestra gráficamente la carga. Cuando la barra está vacía, la instancia de base de datos está inactiva. Conforme aumenta la carga, la barra se va completando en azul. Cuando la carga supera el número de CPU virtuales (vCPU) en la clase de instancia de base de datos, la barra cambia a rojo, lo cual indica un posible cuello de botella.



4. (Opcional) Elija el intervalo de fecha o tiempo en la parte superior derecha y especifique un intervalo de tiempo relativo o absoluto diferente. Ahora puede especificar un período de tiempo y generar un informe de análisis del rendimiento de la base de datos. El informe proporciona información identificada y recomendaciones. Para obtener más información, consulte Creación de un informe de análisis de rendimiento en Información de rendimiento.

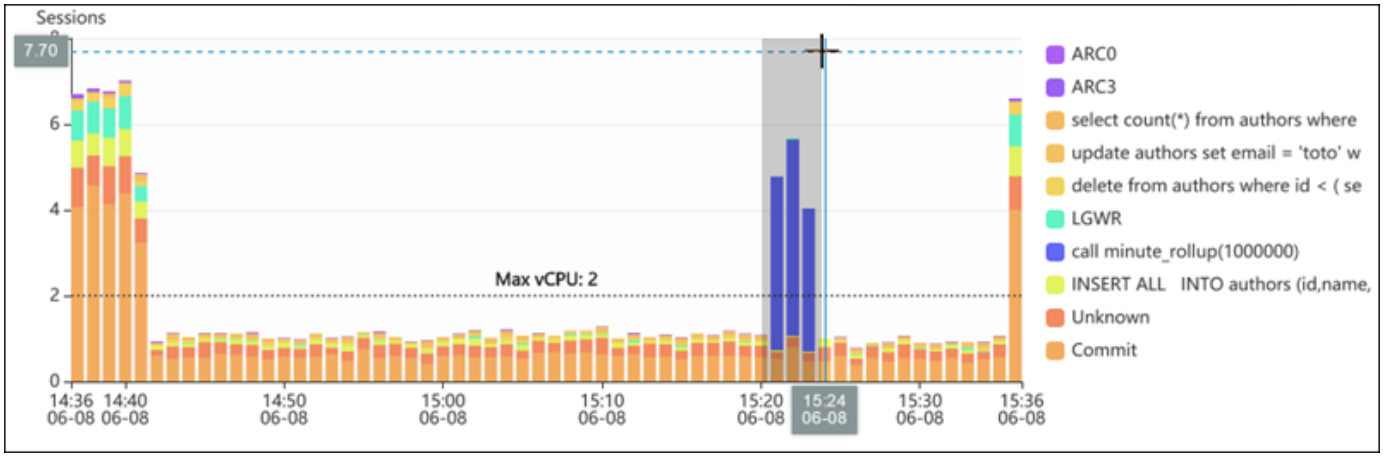


En la siguiente captura de pantalla, el intervalo de carga de la base de datos es de 5 horas.

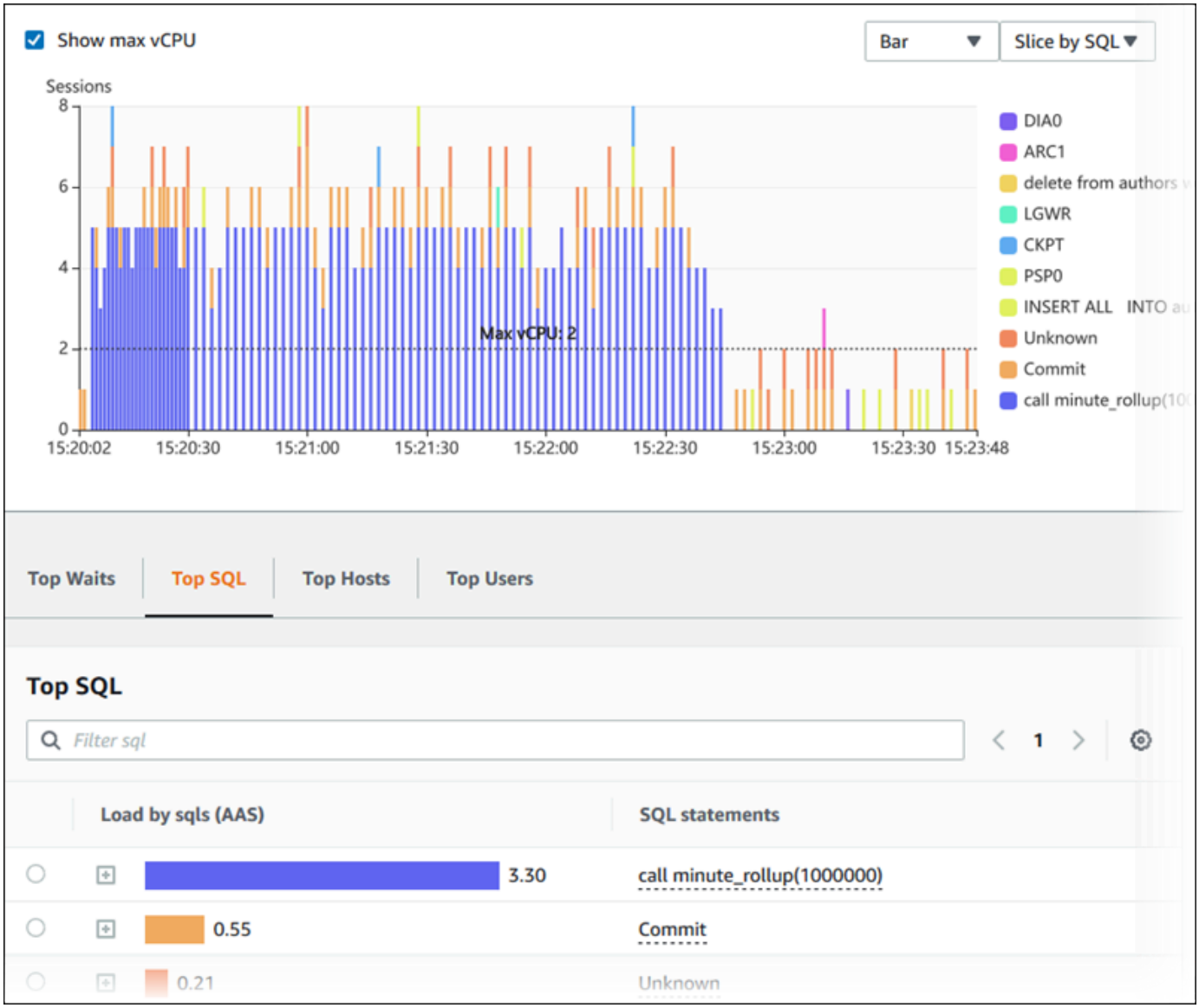


5. (Opcional) Para ampliar una parte del gráfico de carga de base de datos, elija la hora de inicio y arrástrela hasta el final del período que desee.

   El área seleccionada se resalta en el gráfico de carga de base de datos.



Cuando suelte el ratón, el gráfico de carga de base de datos ampliará la región de AWS seleccionada y se volverá a calcular la tabla de las dimensiones principales.



6. (Opcional) Para actualizar los datos automáticamente, habilite Actualización automática.



El panel de Información de rendimiento se actualiza automáticamente con nuevos datos. La frecuencia de actualización depende de la cantidad de datos mostrados:

- 5 minutos actualiza cada 10 segundos.
- 1 hora actualiza cada 5 minutos.
- 5 horas actualiza cada 5 minutos.
- 24 horas actualiza cada 30 minutos.
- 1 semana actualiza cada día.

- 1 mes actualiza cada día.

Análisis de carga de base de datos mediante eventos de espera

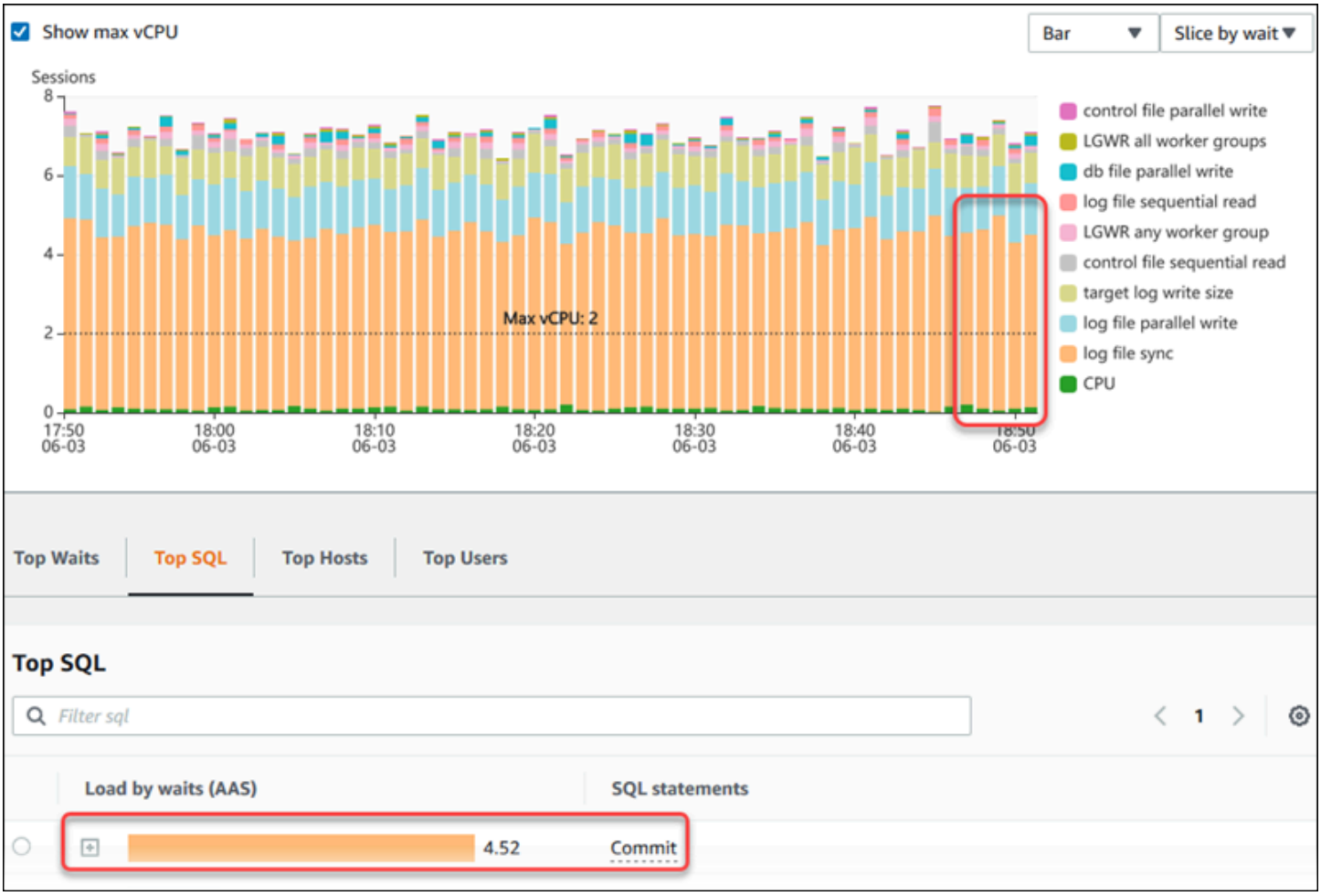
Si el gráfico Database load (Carga de base de datos) indica que hay un cuello de botella, puede averiguar de dónde procede la carga. Para ello, fíjese en la tabla de elementos de carga principales situada debajo del gráfico Database load (Carga de base de datos). Elija un elemento en particular, como una consulta SQL o un usuario, para ampliar la información de ese elemento y ver los detalles.

La carga de base de datos agrupada por esperas y principales consultas de SQL es la vista predeterminada del panel de Performance Insights. Esta combinación normalmente ofrece la máxima información sobre problemas de desempeño. La carga de la base de datos agrupada por esperas indica si hay algún cuello de botella de simultaneidad o recursos en la base de datos. En este caso, la pestaña SQL de la tabla de elementos de carga principales indica qué consultas están contribuyendo a esa carga.

Este es el flujo de trabajo típico para diagnosticar los problemas de desempeño:

1. Revise el gráfico Carga de base de datos para ver si hay algún incidente de carga de base de datos que sobrepase la línea Máximo de CPU.
2. De ser así, fíjese en el gráfico Database load (Carga de base de datos) e identifique qué estado o estados de espera son los principales responsables.
3. Para identificar las consultas de resumen que están provocando la carga, consulte qué consultas de la pestaña SQL de la tabla de elementos de carga principales están contribuyendo más a esos estados de espera. Para identificarlas, utilice la columna DB Load by Wait (Carga de base de datos por espera).
4. Elija una de estas consultas de resumen en la pestaña SQL para ampliarla y ver las consultas secundarias que contiene.

Por ejemplo, en el panel que se muestra a continuación, la espera de la sincronización de archivos de registro se corresponde con la mayor parte de la carga de base de datos. La espera de todos los nodos de trabajo de LGWR también es alta. El gráfico Top SQL (SQL principal) muestra lo que provoca las esperas de sincronización de archivos de registro: instrucciones `COMMIT` frecuentes. En este caso, confirmar con menos frecuencia reducirá la carga de la base de datos.



Análisis del rendimiento de la base de datos durante un período de tiempo

Analice el rendimiento de la base de datos con análisis bajo demanda mediante la creación de un informe de análisis de rendimiento durante un periodo de tiempo. Vea informes de análisis de rendimiento para detectar problemas de rendimiento, como cuellos de botella de recursos o cambios en una consulta en la instancia de base de datos. El panel de Información de rendimiento le permite seleccionar un período de tiempo específico y crear un informe de análisis de rendimiento. También puede añadir una o varias etiquetas al informe.

Para utilizar esta característica, debe utilizar el período de retención del nivel de pago. Para obtener más información, consulte Precios y retención de datos de Performance Insights

Puede seleccionar y ver el informe en la pestaña Informes de análisis de rendimiento: nuevo. El informe contiene la información, las métricas relacionadas y las recomendaciones para resolver el problema de rendimiento. Puede ver el informe durante el período de retención de Información de rendimiento.

El informe se elimina si la hora de inicio del período de análisis del informe está fuera del período de retención. También puede eliminar el informe antes de que finalice el período de retención.

Para detectar los problemas de rendimiento y generar el informe de análisis para su instancia de base de datos, debe activar Información de rendimiento. Para obtener más información acerca de la activación de Información de rendimiento, consulte Activación y desactivación de Información de rendimiento de Amazon RDS.

Para obtener información sobre la compatibilidad de esta característica por región, motor de base de datos y clase de instancia, consulte Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento.

En las siguientes secciones, puede crear, ver y eliminar informes de análisis de rendimiento, así como añadir etiquetas.

Temas

- Creación de un informe de análisis de rendimiento en Información de rendimiento
- Visualización de un informe de análisis de rendimiento en Información de rendimiento
- Cómo añadir etiquetas a un informe de análisis de rendimiento en Información de rendimiento
- Eliminación de un informe de análisis de rendimiento en Información de rendimiento

Creación de un informe de análisis de rendimiento en Información de rendimiento

Puede crear un informe de análisis de rendimiento para un período específico en el panel de Información de rendimiento. Puede seleccionar un período de tiempo y añadir una o más etiquetas al informe de análisis.

El período de análisis puede oscilar entre 5 minutos y 6 días. Debe haber al menos 24 horas de datos de rendimiento antes de la hora de inicio del análisis.

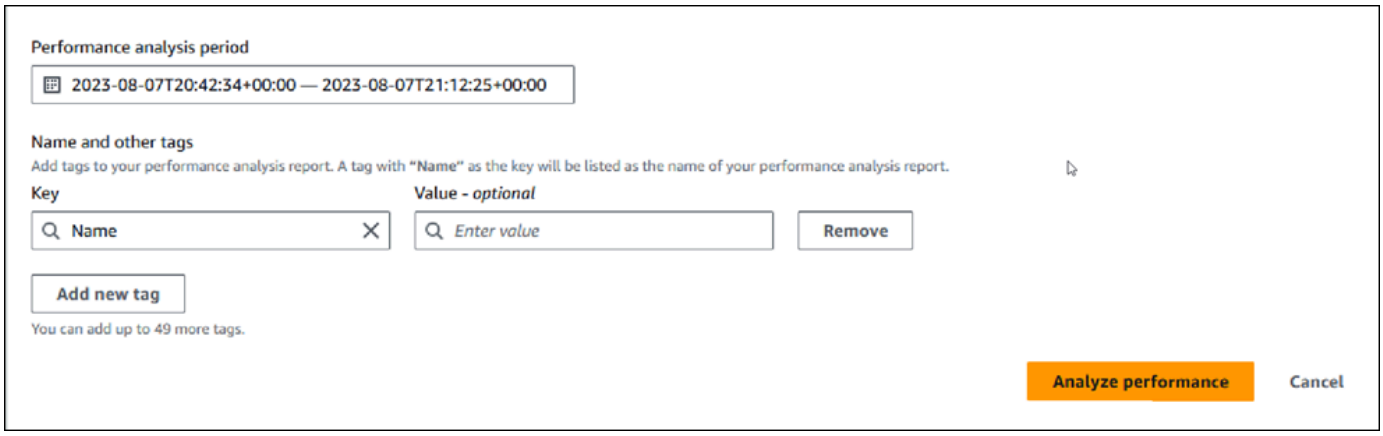
Para obtener información sobre la compatibilidad de esta característica por región, motor de base de datos y clase de instancia, consulte Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento.

Para crear un informe de análisis de rendimiento para un período de tiempo

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.

3. Elija una instancia de base de datos.
4. Elija Analizar rendimiento en la sección Carga de base de datos del panel de Información de rendimiento.

   Se muestran los campos para establecer el período de tiempo y añadir una o más etiquetas al informe de análisis de rendimiento.

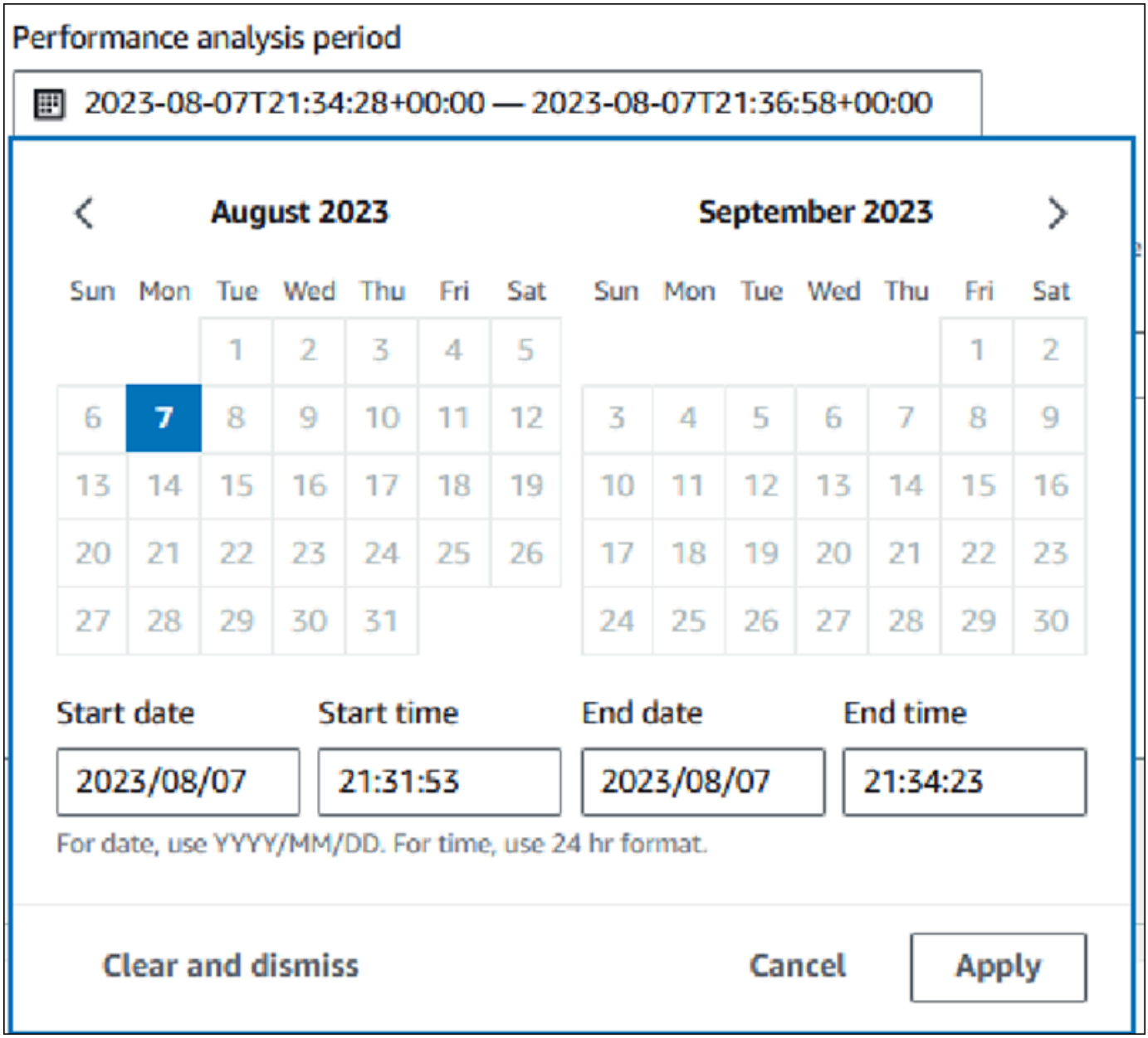


5. Elija un período de tiempo. Si establece un período de tiempo en el Intervalo relativo o Intervalo absoluto en la esquina superior derecha, solo puede introducir o seleccionar la fecha y la hora del informe de análisis dentro de este período de tiempo. Si selecciona un período de análisis fuera de este período de tiempo, aparece un mensaje de error.

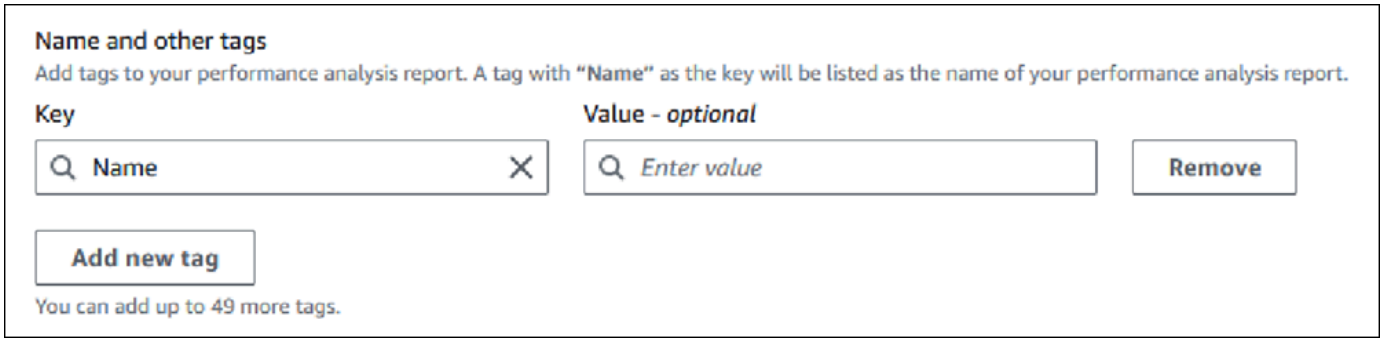
   Para establecer el período de tiempo, puede realizar una de las siguientes acciones:

   - Pulse y arrastre cualquiera de los controles deslizantes del gráfico de carga de la base de datos.

     El cuadro Período de análisis de rendimiento muestra el período de tiempo seleccionado y el gráfico de carga de la base de datos resalta el período de tiempo seleccionado.
   - Elija la Fecha de inicio, la Hora de inicio, la Fecha de finalización y la Hora de finalización en el cuadro Período de análisis de rendimiento.



6. (Opcional) Introduzca la Clave y el Valor-opcional para añadir una etiqueta al informe.



7. Elija Analizar rendimiento.

   Un banner muestra un mensaje que indica si el informe se ha generado correctamente o no ha tenido éxito. El mensaje también proporciona el enlace para ver el informe.

   En el siguiente ejemplo, se muestra el banner con el mensaje de creación correcta del informe.



   Puede ver el informe en la pestaña Informes de análisis de rendimiento: nuevo.

Puede crear un informe de análisis de rendimiento con la AWS CLI. Para ver un ejemplo sobre cómo crear un informe con la AWS CLI, consulte Creación de un informe de análisis de rendimiento para un período de tiempo.

Visualización de un informe de análisis de rendimiento en Información de rendimiento

La pestaña Informes de análisis de rendimiento: nuevo muestra todos los informes que se crean para la instancia de base de datos. En cada informe, se muestra lo siguiente:

- ID: identificador único del informe.
- Nombre: clave de etiqueta añadida al informe.
- Tiempo de creación del informe: hora en que creó el informe.
- Hora de inicio del análisis: hora de inicio del análisis en el informe.
- Hora de finalización del análisis: hora de finalización del análisis en el informe.

Para ver un informe de análisis de rendimiento

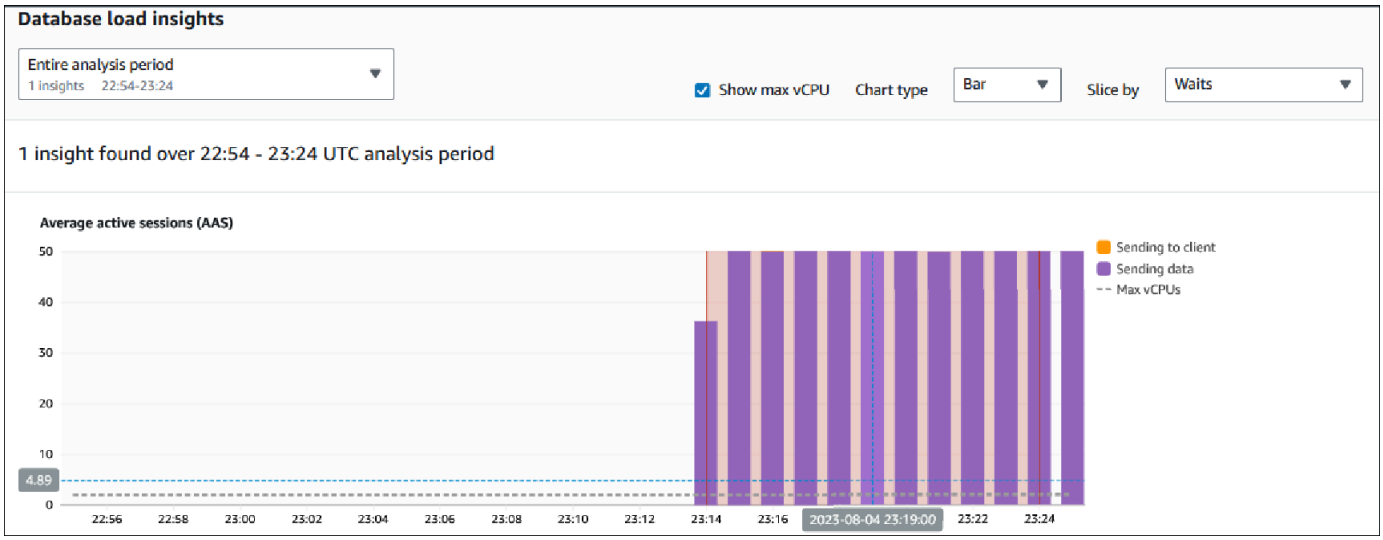
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija la instancia de base de datos para la que desee ver el informe de análisis.
4. Desplácese hacia abajo y elija la pestaña Informes de análisis de rendimiento: nuevo en el panel de Información de rendimiento.

   Se muestran todos los informes de análisis de los diferentes períodos de tiempo.
5. Elija el ID del informe que desea ver.

El gráfico de carga de la base de datos muestra todo el período de análisis de forma predeterminada si se identifica más de una información. Si el informe ha identificado una información, el gráfico de carga de la base de datos muestra la información de forma predeterminada.

El panel también muestra las etiquetas del informe en la sección Etiquetas.

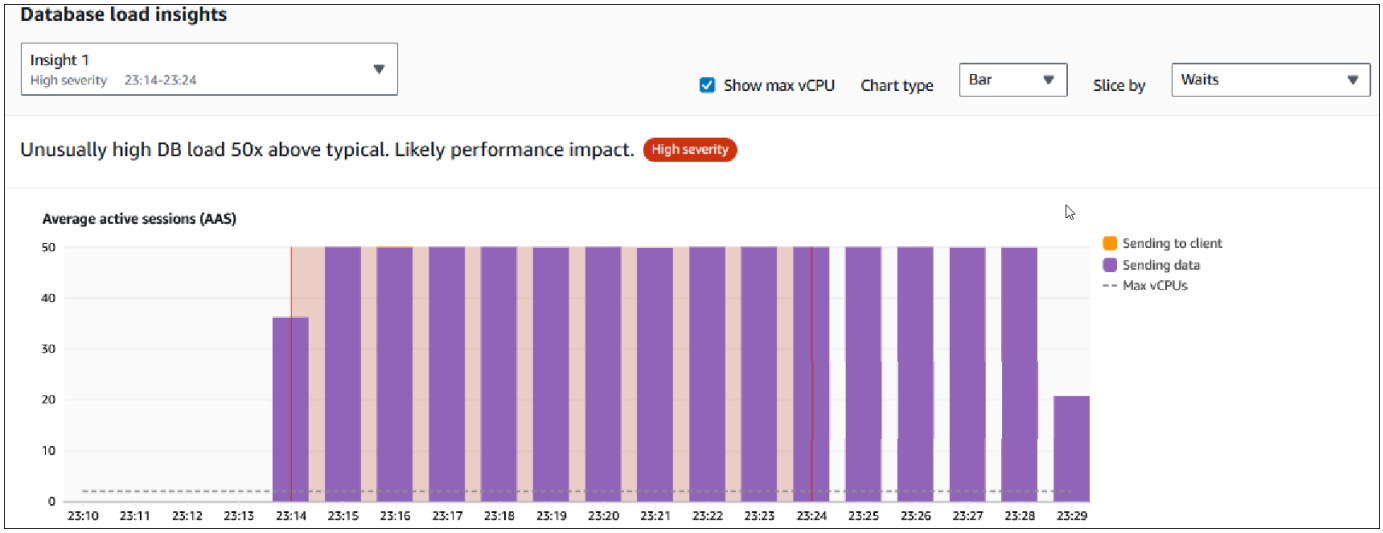
En el siguiente ejemplo se muestra todo el período de análisis del informe.

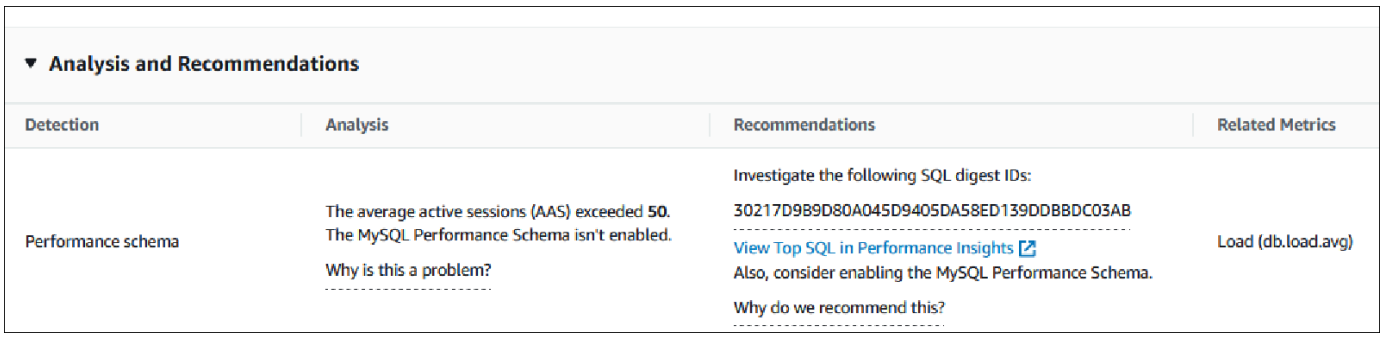


6. Elija la información en la lista Información de carga de la base de datos que desee ver si se identifica más de una información en el informe.

   El panel muestra el mensaje de información, el gráfico de carga de la base de datos que destaca el período de tiempo de la información, los análisis, las recomendaciones y la lista de etiquetas del informe.

   En el siguiente ejemplo se muestra la información de carga de la base de datos en el informe.





Cómo añadir etiquetas a un informe de análisis de rendimiento en Información de rendimiento

Puede añadir una etiqueta al crear o ver un informe. Puede añadir un máximo de 50 etiquetas a un informe.

Debe tener los permisos para añadir las etiquetas. Para obtener más información sobre las políticas de acceso para la Información de rendimiento, consulte Configuración de directivas de acceso para información sobre rendimiento

Para añadir una o más etiquetas al crear un informe, consulte el paso 6 del procedimiento Creación de un informe de análisis de rendimiento en Información de rendimiento.

Para añadir una o más etiquetas al ver un informe

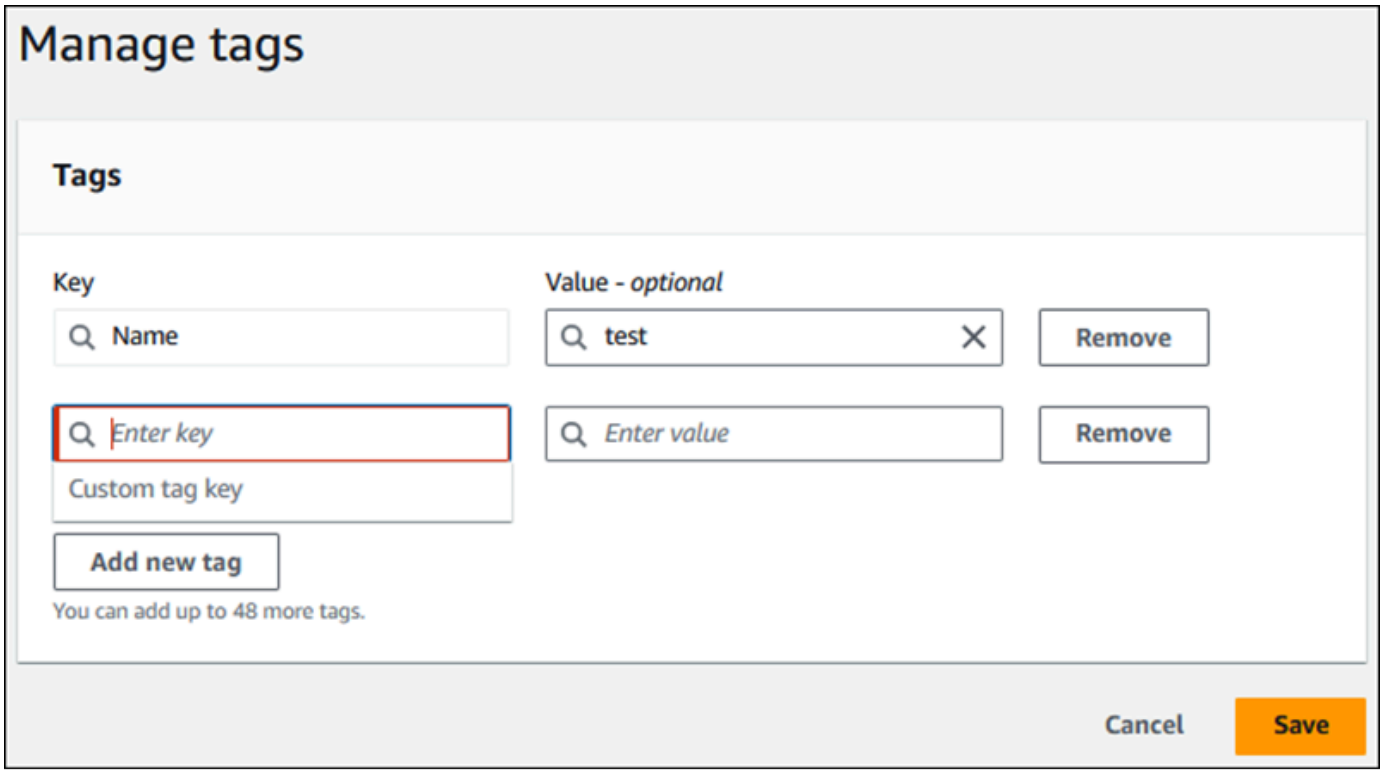
1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.

Se muestra el panel de Información de rendimiento para la instancia de base de datos.

4. Desplácese hacia abajo y elija la pestaña Informes de análisis de rendimiento: nuevo.
5. Elija el informe al que desee añadir las etiquetas.

   El panel muestra el informe.
6. Desplácese hacia abajo hasta Etiquetas y elija Administrar etiquetas.
7. Elija Añadir nueva etiqueta.
8. Introduzca la Clave y el Valor - opcional, y elija Agregar nueva etiqueta.

   En el ejemplo siguiente se ofrece la opción de añadir una etiqueta nueva en el informe seleccionado.



Se crea una etiqueta nueva para el informe.

La lista de etiquetas del informe se muestra en la sección Etiquetas del panel. Si desea eliminar una etiqueta del informe, elija Eliminar junto a la etiqueta.

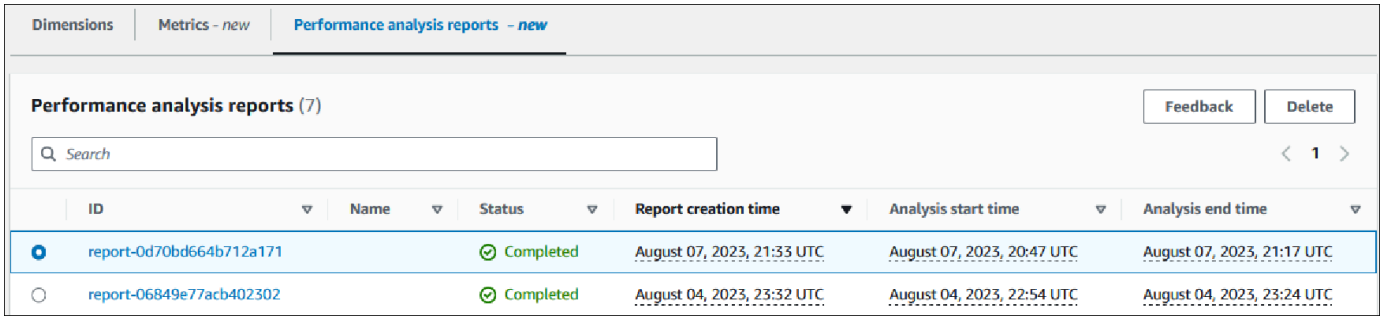
Eliminación de un informe de análisis de rendimiento en Información de rendimiento

Puede eliminar un informe de la lista de informes que se muestra en la pestaña Informes de análisis de rendimiento o mientras visualiza un informe.

Para eliminar un informe

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. Elija una instancia de base de datos.

   Se muestra el panel de Información de rendimiento para la instancia de base de datos.
4. Desplácese hacia abajo y elija la pestaña Informes de análisis de rendimiento: nuevo.
5. Seleccione el informe que quiera eliminar y elija Eliminar en la esquina superior derecha.



   Aparece una ventana de confirmación. El informe se elimina después de que seleccione confirmar.
6. (Opcional) Elija el ID del informe que desea eliminar.

   En la página del informe, elija Eliminar en la esquina superior derecha.

   Aparece una ventana de confirmación. El informe se elimina después de que seleccione confirmar.

Análisis de consultas con la pestaña Top SQL en Información de rendimiento

En el panel de Performance Insights de Amazon RDS, puede encontrar información sobre las consultas recientes y en ejecución en la pestaña Top SQL (SQL principal) en la tabla Top dimensions (Dimensiones principales). Puede utilizar esta información para ajustar sus consultas.

Temas

- Información general sobre la pestaña Top SQL (SQL principal)
- Acceso a más texto SQL en el panel de Performance Insights
- Visualización de estadísticas de SQL en el panel de Performance Insights

Información general sobre la pestaña Top SQL (SQL principal)

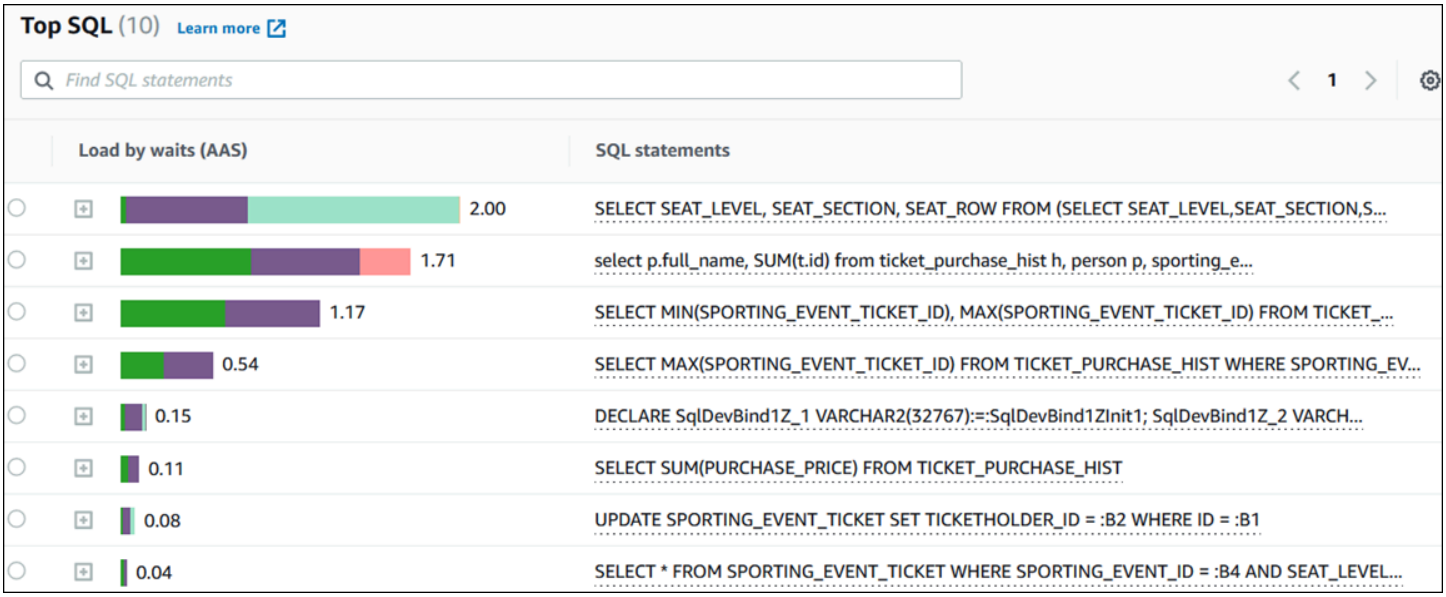
De forma predeterminada, la pestaña Top SQL (SQL principal) muestra las 25 consultas que contribuyen a la carga de base de datos. Para ayudar a ajustar las consultas, puede analizar información como el texto de la consulta y las estadísticas de SQL. También puede elegir las estadísticas que quiere que aparezcan en la pestaña Top SQL (SQL principal).

Temas

- Texto SQL
- Estadísticas de SQL
- Load by waits (AAS) (Carga por esperas [AAS])
- Ver información de SQL
- Escoger preferencias de estadísticas

Texto SQL

De forma predeterminada, cada fila de la tabla Top SQL (SQL principal) muestra 500 bytes de texto de ara cada instrucción.

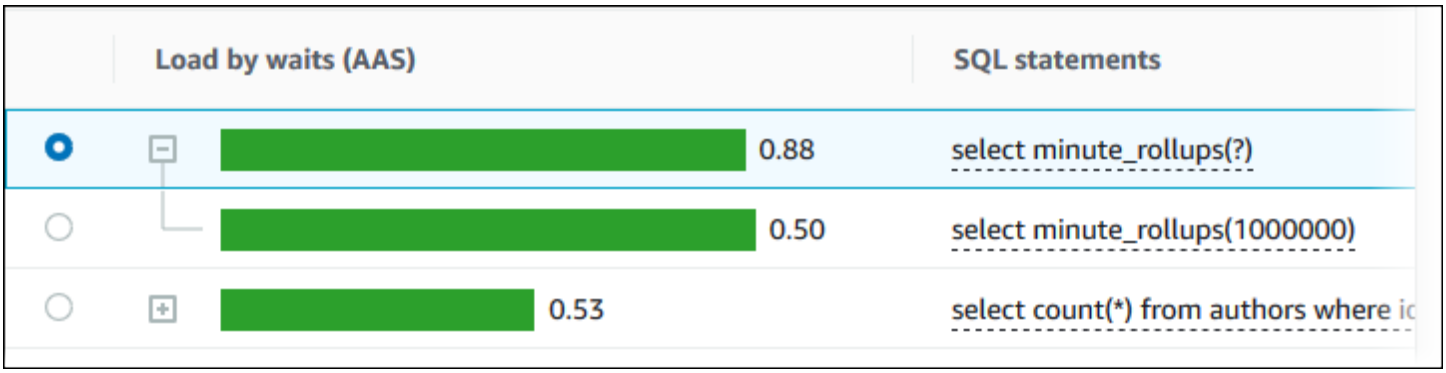


Para obtener información sobre cómo ver más de los 500 bytes predeterminados de texto SQL, consulte Acceso a más texto SQL en el panel de Performance Insights.

Un resumen de SQL es un compuesto de múltiples consultas reales que son similares en estructura, pero que pueden tener diferentes valores literales. El resumen reemplaza los valores codificados por un signo de interrogación. Por ejemplo, un resumen podría ser `SELECT * FROM emp WHERE lname= ?`. Este resumen podría incluir las siguientes consultas secundarias:

```
SELECT * FROM emp WHERE lname = 'Sanchez'
SELECT * FROM emp WHERE lname = 'Olagappan'
SELECT * FROM emp WHERE lname = 'Wu'
```

Para ver las instrucciones SQL literales de un resumen, seleccione la consulta y, a continuación, elija el símbolo más (+). En el siguiente ejemplo, la consulta seleccionada es un resumen.



> **Note**
>
> Un resumen de SQL agrupa instrucciones SQL similares, pero no redacta información confidencial.

Performance Insights puede mostrar el texto de Oracle SQL como Unknown (Desconocido). El texto tiene este estado en las siguientes situaciones:

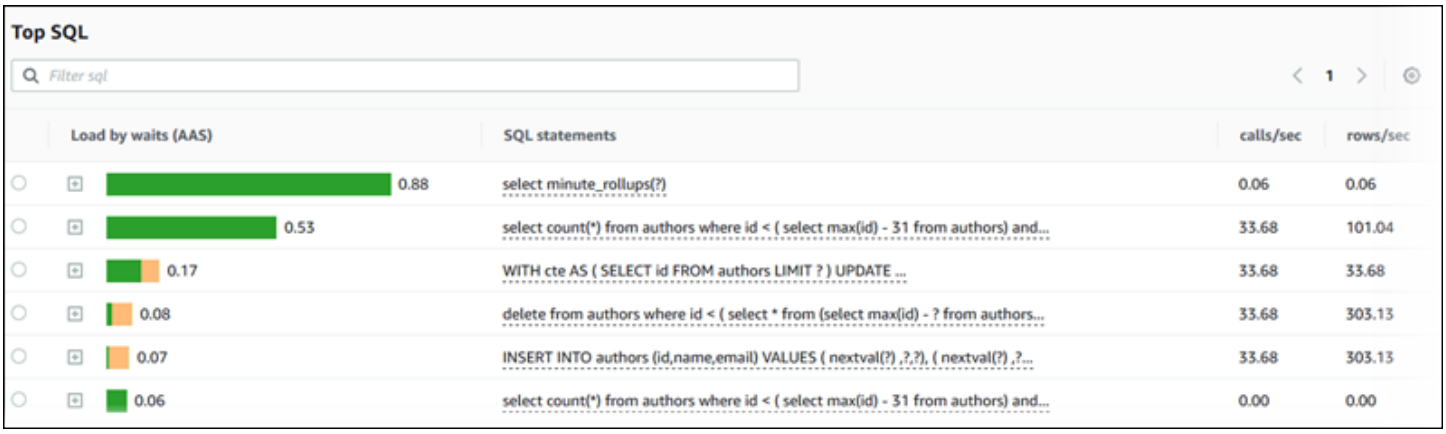
- Un usuario de base de datos de Oracle distinto de SYS está activo pero no ejecuta SQL actualmente. Por ejemplo, cuando se completa una consulta paralela, el coordinador de consultas espera a que los procesos auxiliares envíen sus estadísticas de sesión. Durante la espera, el texto de la consulta muestra Unknown (Desconocido).

- Para una instancia de RDS para Oracle en Standard Edition 2, el Administrador de recursos de Oracle limita el número de subprocesos paralelos. El proceso en segundo plano que realiza este trabajo hace que el texto de la consulta se muestre como Unknown (Desconocido).

Estadísticas de SQL

Las estadísticas de SQL son métricas relacionadas con el rendimiento de las consultas SQL. Por ejemplo, Performance Insights podría mostrar ejecuciones por segundo o filas procesadas por segundo. Performance Insights recopila estadísticas solo para las consultas más comunes. Normalmente, coinciden con las consultas principales por carga mostradas en el panel de Performance Insights.

Todas las líneas de la tabla Top SQL (SQL principal) muestra estadísticas relevantes de la instrucción o resumen de SQL, como se muestra en el ejemplo siguiente.



Performance Insights puede informar `0.00` y `-` (desconocido) para las estadísticas de SQL. Esta situación se produce en las siguientes condiciones:

- Solo existe una muestra. Por ejemplo, Performance Insights calcula las tasas de cambio para las consultas de RDS PostgreSQL basadas en varios ejemplos de la vista `pg_stat_statements`. Cuando una carga de trabajo se ejecuta durante un breve período de tiempo, es posible que Performance Insights solo recopile una muestra, lo que significa que no puede calcular una tasa de cambio. El valor desconocido se representa con un guion (`-`).
- Dos muestras tienen los mismos valores. Performance Insights no puede calcular una tasa de cambio porque no se ha producido ningún cambio, por lo que informa la tasa como `0.00`.
- Una instrucción de RDS PostgreSQL carece de identificador válido. PostgreSQL crea un identificador para una instrucción solo después de analizar. Por lo tanto, puede existir una instrucción en las estructuras internas en memoria de PostgreSQL sin identificador. Dado que

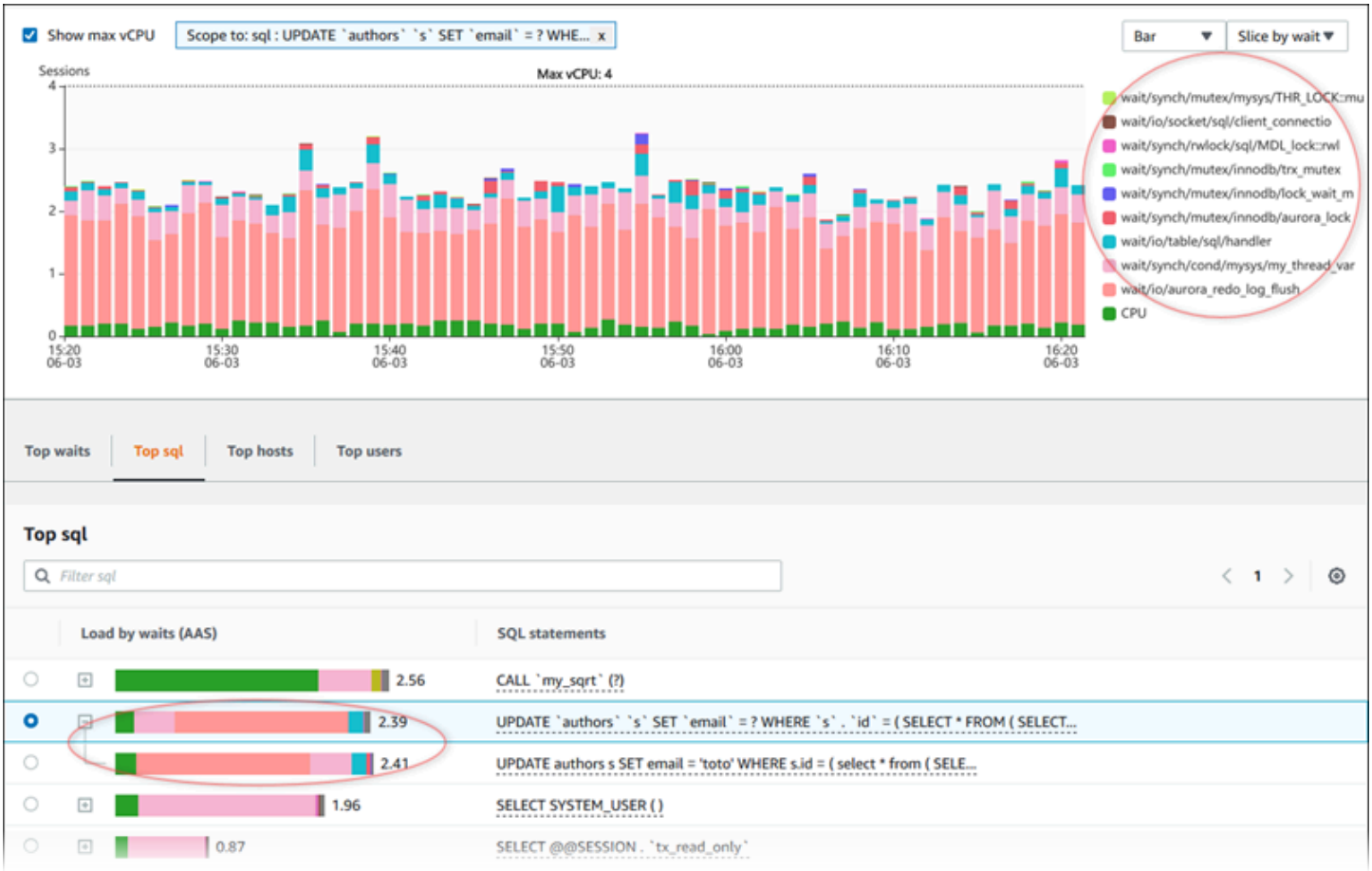
Performance Insights realiza muestras de estructuras internas en memoria una vez por segundo, pueden aparecer consultas de baja latencia para una sola muestra. Si el identificador de consulta no está disponible para esta muestra, Performance Insights no puede asociar esta instrucción a sus estadísticas. El valor desconocido se representa con un guion (-).

Para obtener una descripción de las estadísticas de SQL de los motores de Amazon RDS, consulte Estadísticas de SQL para Performance Insights.

Load by waits (AAS) (Carga por esperas [AAS])

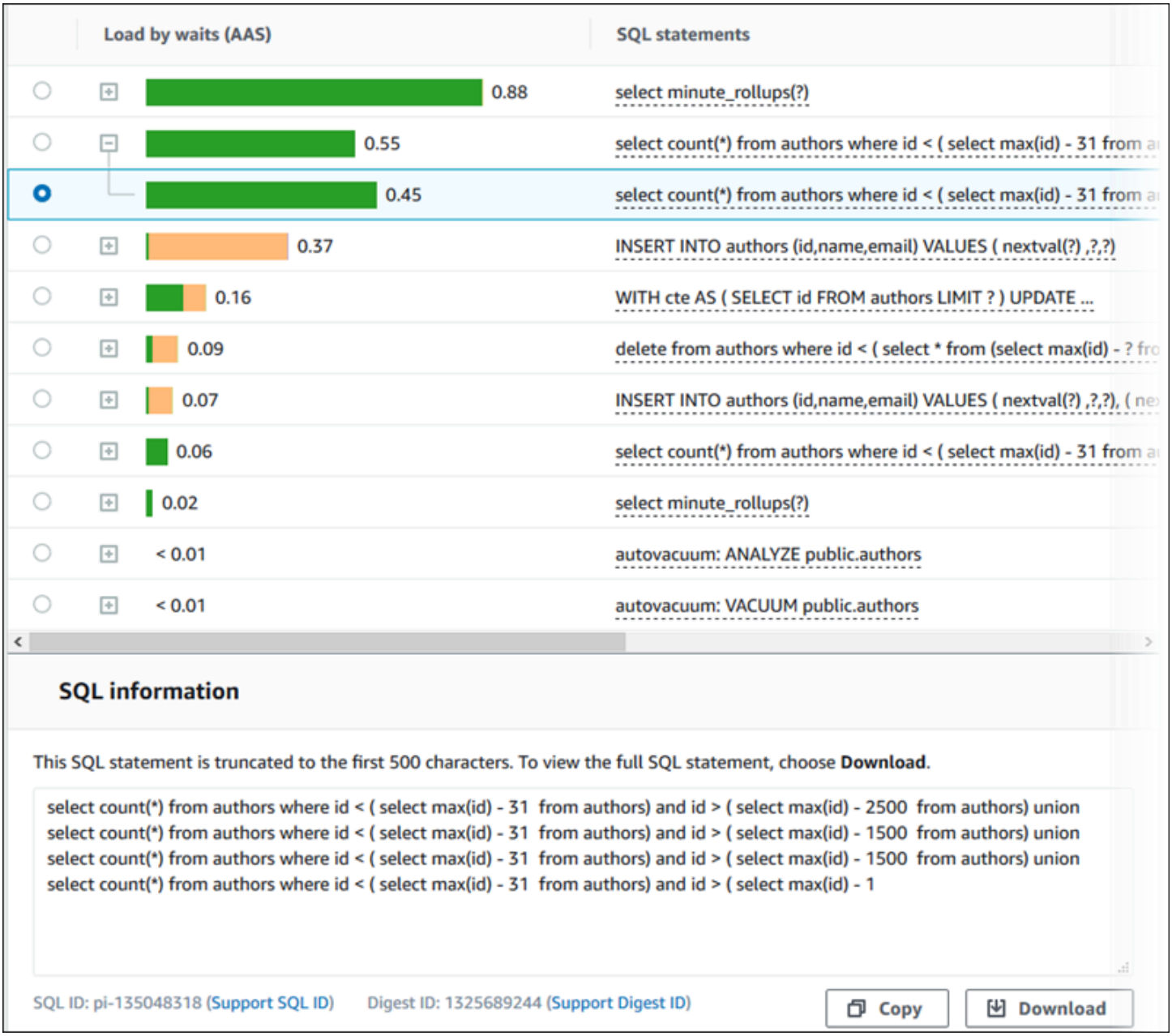
En Top SQL (SQL principal), la columna Load by waits (AAS) (Carga por espera [AAS]) ilustra el porcentaje de carga de la base de datos asociada con cada elemento de carga principal. Esta columna refleja la carga de ese elemento por cualquier agrupación que se haya seleccionado actualmente en el gráfico de carga de base de datos. Para obtener más información acerca de las sesiones activas de Average (AAS), consulte Sesiones activas promedio.

Por ejemplo, es posible que pueda agrupar el gráfico DB load (Carga de base de datos) por estados de espera. Puede examinar consultas SQL en la tabla de elementos de carga principal. En este caso, la barra DB Load by Waits (Carga de base de datos por esperas) estaría dimensionada, segmentada y dividida por colores para mostrar en qué proporción contribuye esa consulta a un estado de espera. También muestra qué estados de espera afectan a la consulta seleccionada.



Ver información de SQL

En la tabla Top SQL (SQL principal), puede abrir una instrucción para consultar su información. La información aparece en el panel inferior.

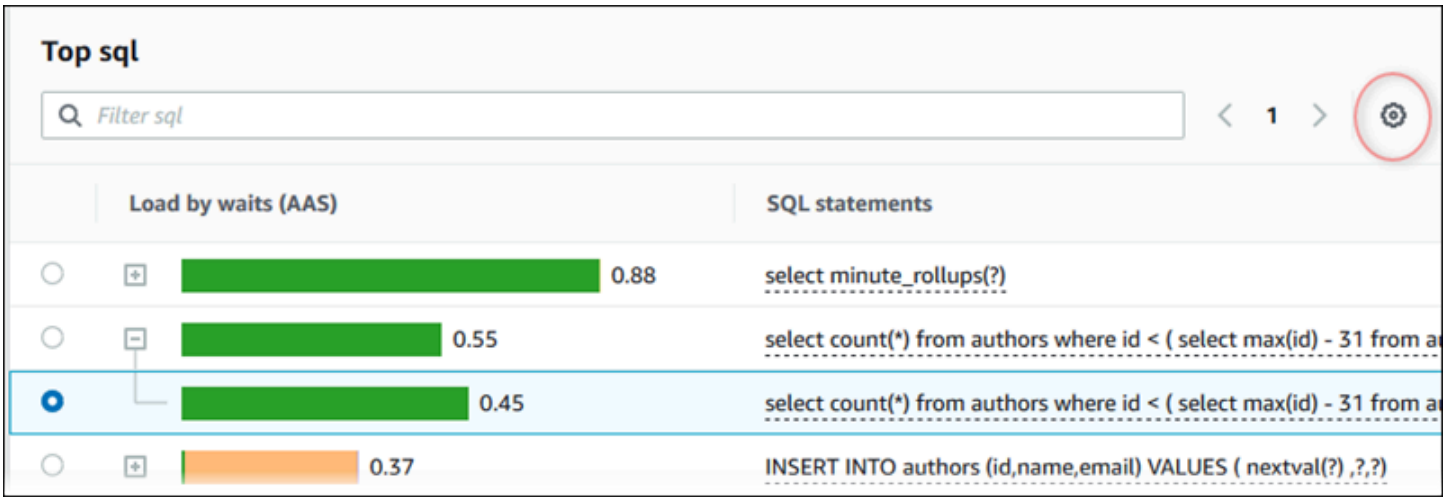


Los siguientes tipos de identificadores (ID) asociados con instrucciones SQL:

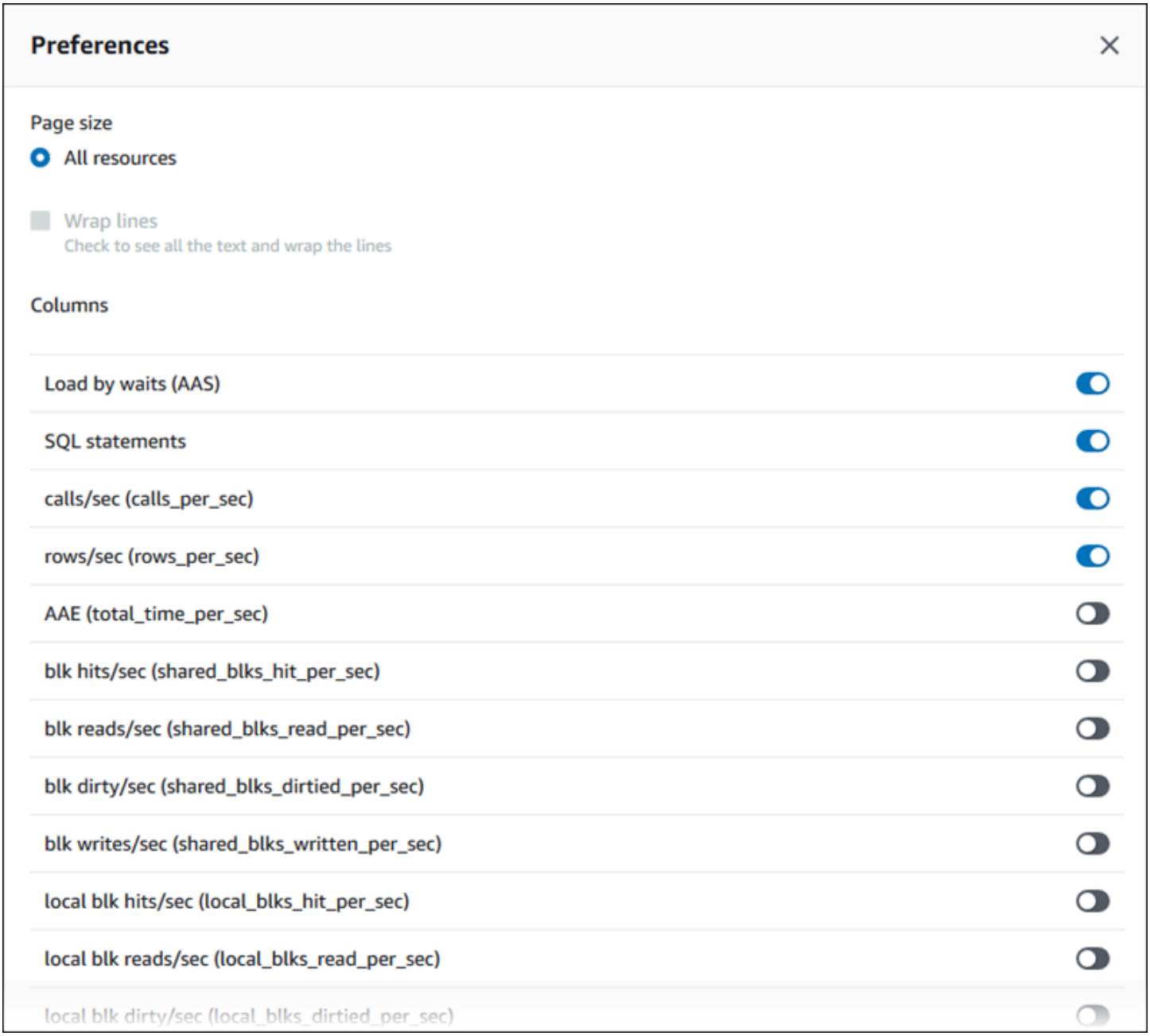
- Support SQL ID (Compatibilidad con ID SQL): un valor hash del ID de SQL. Este valor sirve solo para hacer referencia a un ID de SQL al trabajar con AWS Support. AWS Support no tiene acceso a sus ID de SQL y texto SQL reales.
- Support Digest ID (Compatibilidad con ID de resumen): un valor hash del ID de resumen. Este valor sirve solo para hacer referencia a un ID de resumen al trabajar con AWS Support. AWS Support no tiene acceso a sus ID de resumen y texto SQL reales.

Escoger preferencias de estadísticas

Para controlar las estadísticas mostradas en la pestaña Top SQL (SQL principal), puede elegir el icono Preferences (Preferencias).



Al seleccionar el icono Preferences (Preferencias), se abrirá la ventana Preferences (Preferencias). La siguiente captura de pantalla es un ejemplo de la ventana Preferences (Preferencias).



Para habilitar las estadísticas que desea que estén visibles en la pestaña Top SQL (SQL principal), utilice el ratón para desplazarse hasta la parte inferior de la ventana y, a continuación, elija Continue (Continuar).

Para obtener más información sobre las estadísticas por segundo o por llamada de los motores Amazon RDS, consulte la sección de estadísticas SQL específicas del motor en Estadísticas de SQL para Performance Insights.

Acceso a más texto SQL en el panel de Performance Insights

De forma predeterminada, cada fila de la tabla Top SQL (SQL principal) muestra 500 bytes de texto SQL para cada instrucción SQL.



Cuando una instrucción SQL supera los 500 bytes, puede ver más texto en la sección SQL text (Texto SQL), bajo la tabla Top SQL (SQL principal). En este caso, la longitud máxima del texto que se muestra SQL text (Texto SQL) es de 4 KB. Este límite lo introduce la consola y está sujeto a los límites establecidos por el motor de base de datos. Para guardar el texto que se muestra en SQL text (Texto SQL), elija Download (Descargar).

Temas

- Límites de tamaño del texto para los motores de Amazon RDS
- Ajuste del limite de texto SQL para las instancias de base de datos de Amazon RDS para PostgreSQL
- Ver y descargar texto SQL en el panel de Performance Insights

Límites de tamaño del texto para los motores de Amazon RDS

Cuando se descarga un texto SQL, el motor de la base de datos determina su longitud máxima. Puede descargar texto SQL hasta los siguientes límites por motor:

Motor de base de datos	Longitud máxima del texto descargado
Amazon RDS para MySQL y MariaDB	La longitud se fija en 4096 bytes cuando se habilita Performance Schema. Si Performance Schema no está habilitado, la longitud se fija en 65 535 bytes.
Amazon RDS for Microsoft SQL Server	4,096 caracteres
Amazon RDS para Oracle	1000 bytes

En la sección SQL text (Texto SQL) de la consola de Performance Insights, se muestra el máximo que devuelve el motor. Por ejemplo, si MySQL devuelve como máximo 1 kB a Performance Insights,

solo puede recopilar y mostrar 1 kB, incluso si la consulta original es de mayor longitud. Así, cuando se visualiza la consulta en SQL text (Texto SQL) o se descarga, Performance Insights devuelve el mismo número de bytes.

Si utiliza la AWS CLI o la API, Información de rendimiento no tiene el límite de 4 KB aplicado por la consola. `DescribeDimensionKeys` y `GetResourceMetrics` devuelven como máximo 500 bytes.

> **Note**
>
> `GetDimensionKeyDetails` devuelve la consulta completa, pero el tamaño está sujeto al límite del motor.

Ajuste del limite de texto SQL para las instancias de base de datos de Amazon RDS para PostgreSQL

Amazon RDS para PostgreSQL maneja el texto de manera diferente. Puede establecer el límite de tamaño del texto con el parámetro de instancia de base de datos `track_activity_query_size`. Este parámetro incluye las siguientes características:

Tamaño de texto predeterminado

En la versión 9.6 de Amazon RDS for PostgreSQL, la configuración predeterminada del parámetro `track_activity_query_size` es de 1024 bytes. En la versión 10 o superior de Amazon RDS for PostgreSQL, la configuración predeterminada del parámetro es de 4096 bytes.

Tamaño máximo del texto

El límite de `track_activity_query_size` para la versión 12 o inferior de Amazon RDS for PostgreSQL es de 102 400 bytes. El máximo es de 1 MB para la versión 13 y superior.

Si el motor devuelve 1 MB a Performance Insights, la consola muestra solo los primeros 4 kB. Si descarga la consulta, obtendrá 1 MB completo. En este caso, la visualización y la descarga devuelven diferentes cantidades de bytes. Para obtener más información sobre el parámetro de instancia de base de datos `track_activity_query_size`, consulte Run-time Statistics (Estadísticas de tiempo de ejecución) en la documentación de PostgreSQL.

Para aumentar el tamaño del texto SQL, aumente el límite de `track_activity_query_size`. Para modificar el parámetro, cambie el ajuste en el grupo de parámetros asociado a la instancia de base de datos de Amazon RDS para PostgreSQL.

Para cambiar la configuración cuando la instancia utiliza el grupo de parámetros predeterminado

1. Cree un nuevo grupo de parámetros de instancia de base de datos para el motor de base de datos y la versión del motor de base de datos adecuados.
2. Establezca el parámetro en el nuevo grupo de parámetros.
3. Asocie el nuevo grupo de parámetros a la instancia de base de datos.

Para obtener más información sobre configurar un parámetro de instancia de base de datos, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

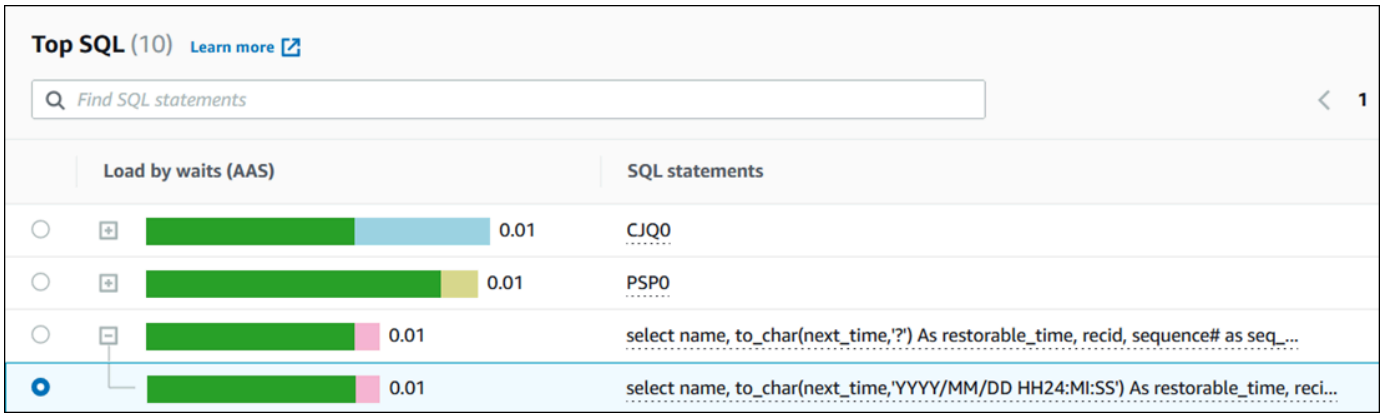
Ver y descargar texto SQL en el panel de Performance Insights

Puede ver o descargar texto SQL en el panel de Performance Insights.

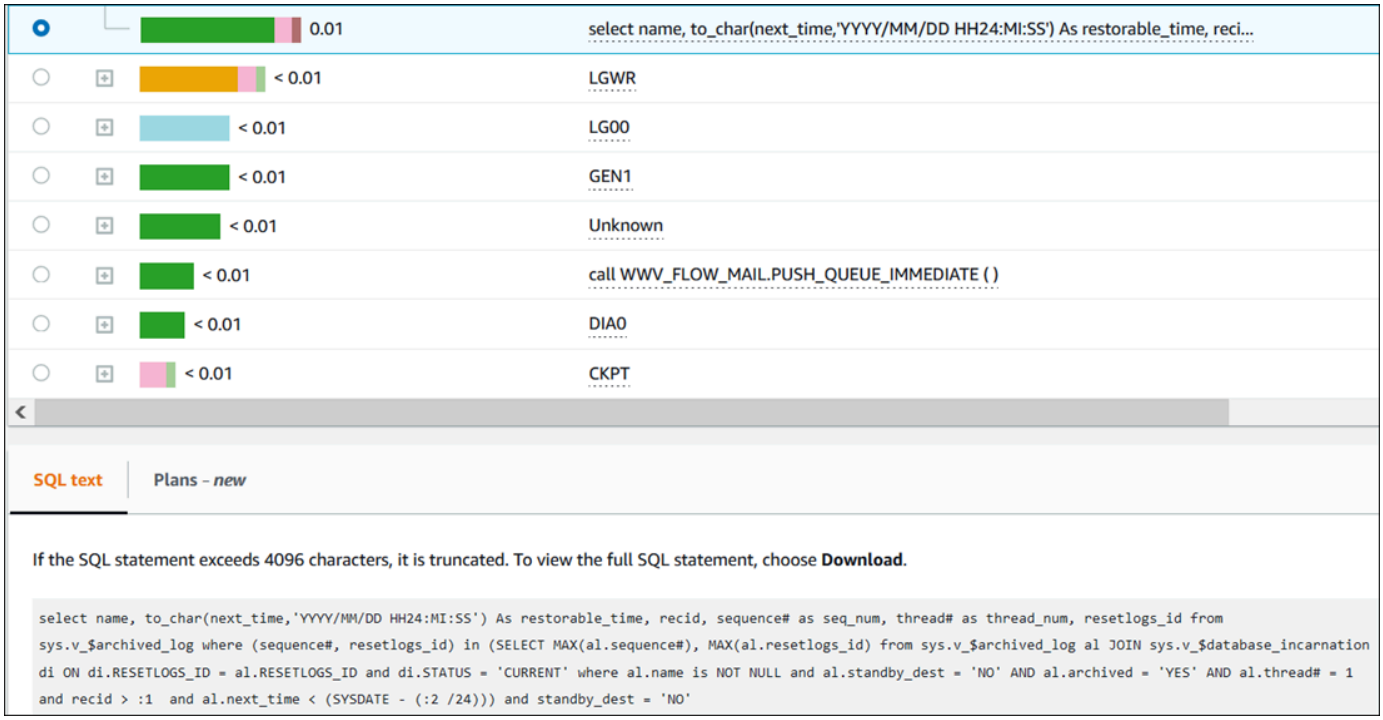
Para ver más texto SQL en el panel de Performance Insights

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Performance Insights.
3. Elija una instancia de base de datos.
4. Baje hasta la pestaña Top SQL en el panel de Información de rendimiento.
5. Elija el signo más para expandir un resumen de SQL y elija una de las consultas secundarias del resumen.

   Las instrucciones SQL con texto superior a 500 bytes son similares a las que se indican en la siguiente imagen.



6. Desplácese hasta la pestaña SQL text (Texto SQL).



El panel de Performance Insights puede mostrar hasta 4096 bytes por cada instrucción SQL.

7. (Opcional) Elija Copiar para copiar la instrucción SQL mostrada o elija Descargar para descargar la instrucción SQL para consultar el texto SQL hasta el límite del motor de base de datos.

> **Note**
>
> Para copiar o descargar la instrucción SQL, deshabilite los bloqueadores de pantallas emergentes.

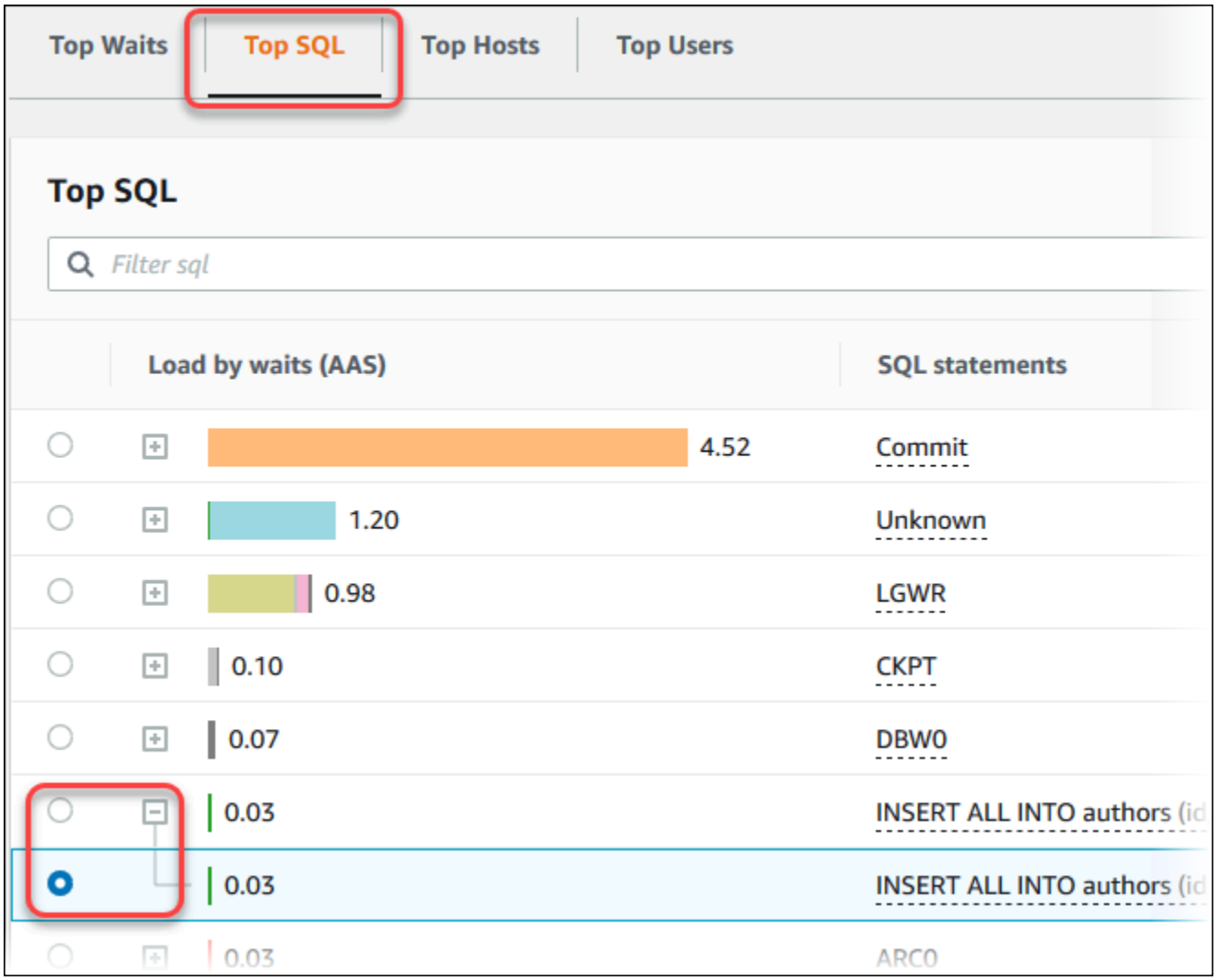
Visualización de estadísticas de SQL en el panel de Performance Insights

En el panel de Performance Insights, las estadísticas de SQL están disponibles en la pestaña Top SQL (SQL principal) del gráfico Database load (Carga de base de datos).

Para ver las estadísticas de SQL

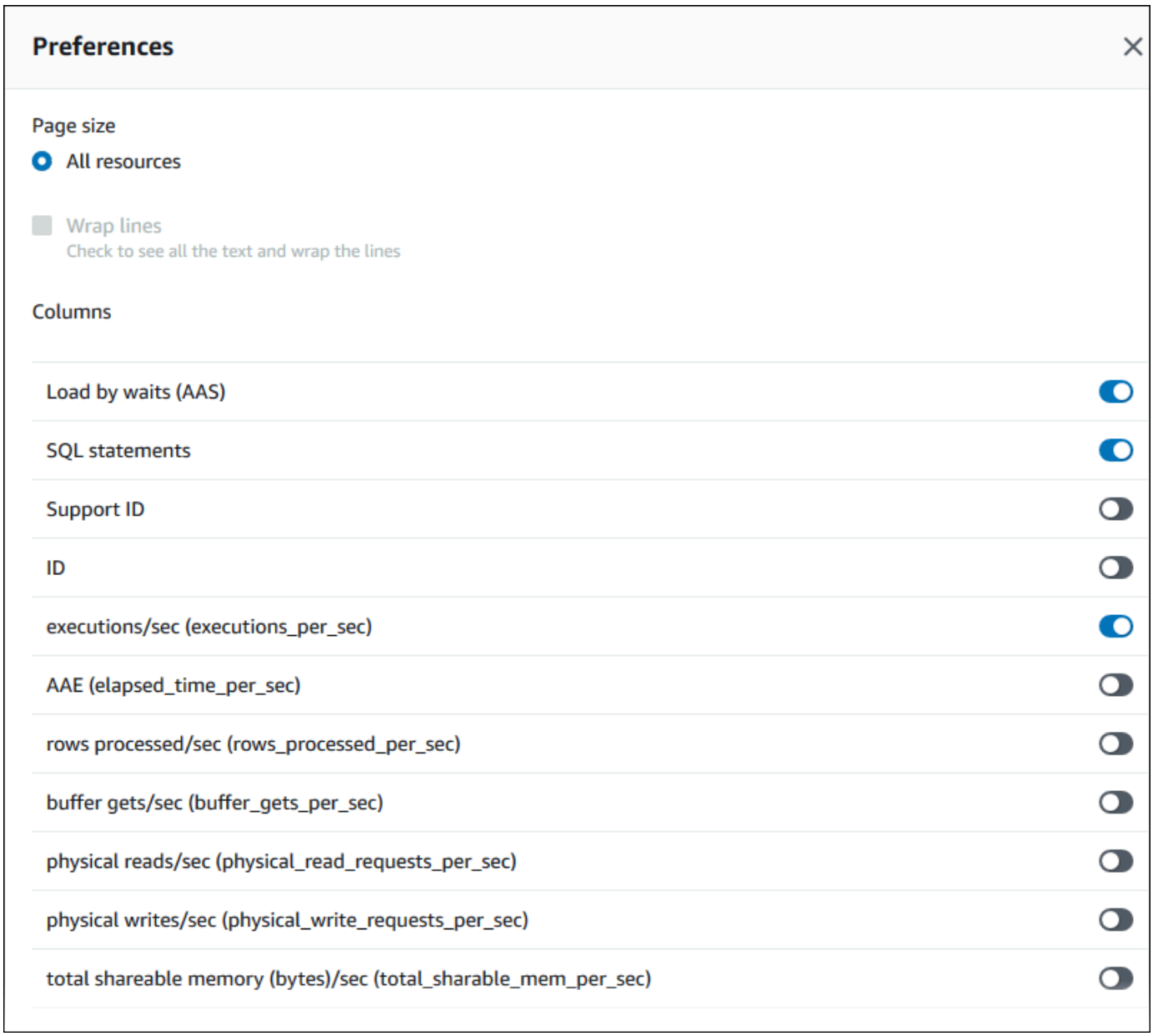
1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Performance Insights.
3. En la parte superior de la página, elija la base de datos cuyas estadísticas de SQL desea ver.
4. Desplácese a la parte inferior de la página y seleccione Top SQL (SQL principal).

5. Elija una instrucción individual o consulte el resumen.

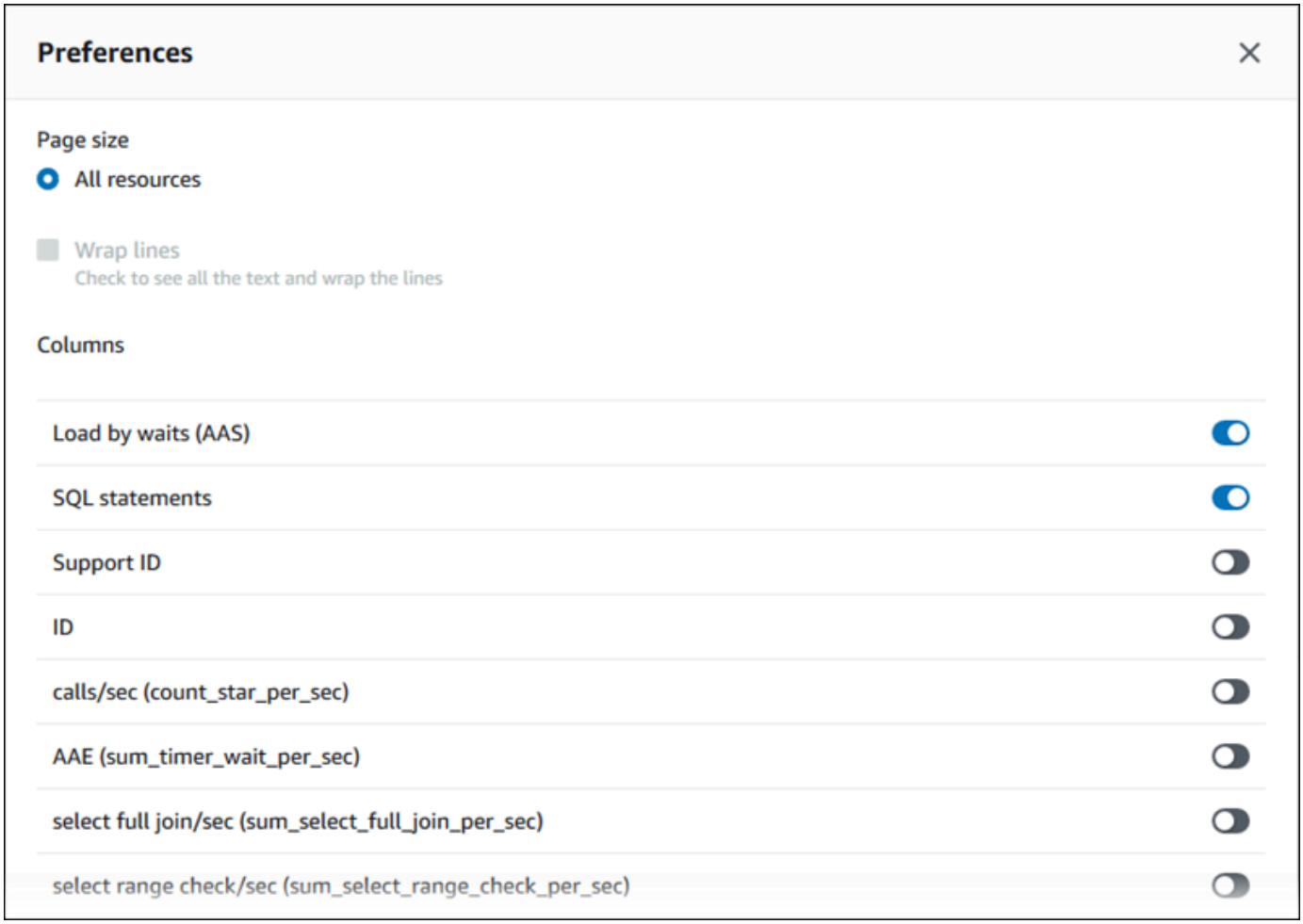


6. Seleccione qué estadísticas mostrar seleccionando el icono de engranaje de la esquina superior derecha del gráfico. Para obtener descripciones de las estadísticas de SQL de los motores de Amazon RDS, consulte Estadísticas de SQL para Performance Insights.

   El siguiente ejemplo muestra las preferencias para las instancias de base de datos de Oracle.



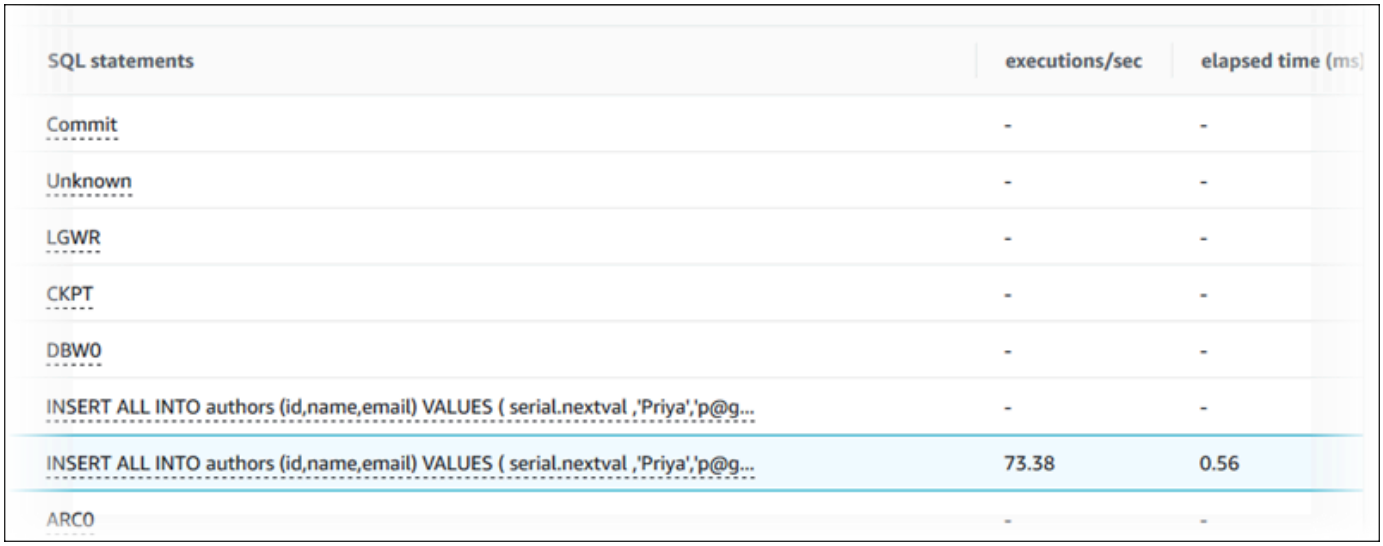
El siguiente ejemplo muestra las preferencias para las instancias de base de datos de MariaDB y MySQL.



7. Elija Save (Guardar) para guardar las preferencias.

   Se actualiza la tabla Top SQL (SQL principal).

   En el siguiente ejemplo se muestran las estadísticas de una consulta SQL de Oracle.



SQL statements	executions/sec	elapsed time (ms)
Commit	-	-
Unknown	-	-
LGWR	-	-
CKPT	-	-
DBW0	-	-
INSERT ALL INTO authors (id,name,email) VALUES (serial.nextval ,'Priya','p@g...	-	-
INSERT ALL INTO authors (id,name,email) VALUES (serial.nextval ,'Priya','p@g...	73.38	0.56
ARC0	-	-

Análisis de la carga de PDB principal de Oracle

Al analizar la carga en una base de datos de contenedor de Oracle (CDB), es posible que quiera identificar qué bases de datos conectables (PDB) contribuyen más a la carga de la base de datos. También puede comparar el rendimiento de PDB individuales que ejecutan consultas similares para ajustar el rendimiento. Para obtener más información acerca de las CDB de Oracle, consulte Arquitectura de base de datos de RDS para Oracle.

En el panel de Información sobre rendimiento de Amazon RDS, puede encontrar información sobre las bases de datos conectables (PDB) en la pestaña PDB principal en la pestaña Dimensiones.

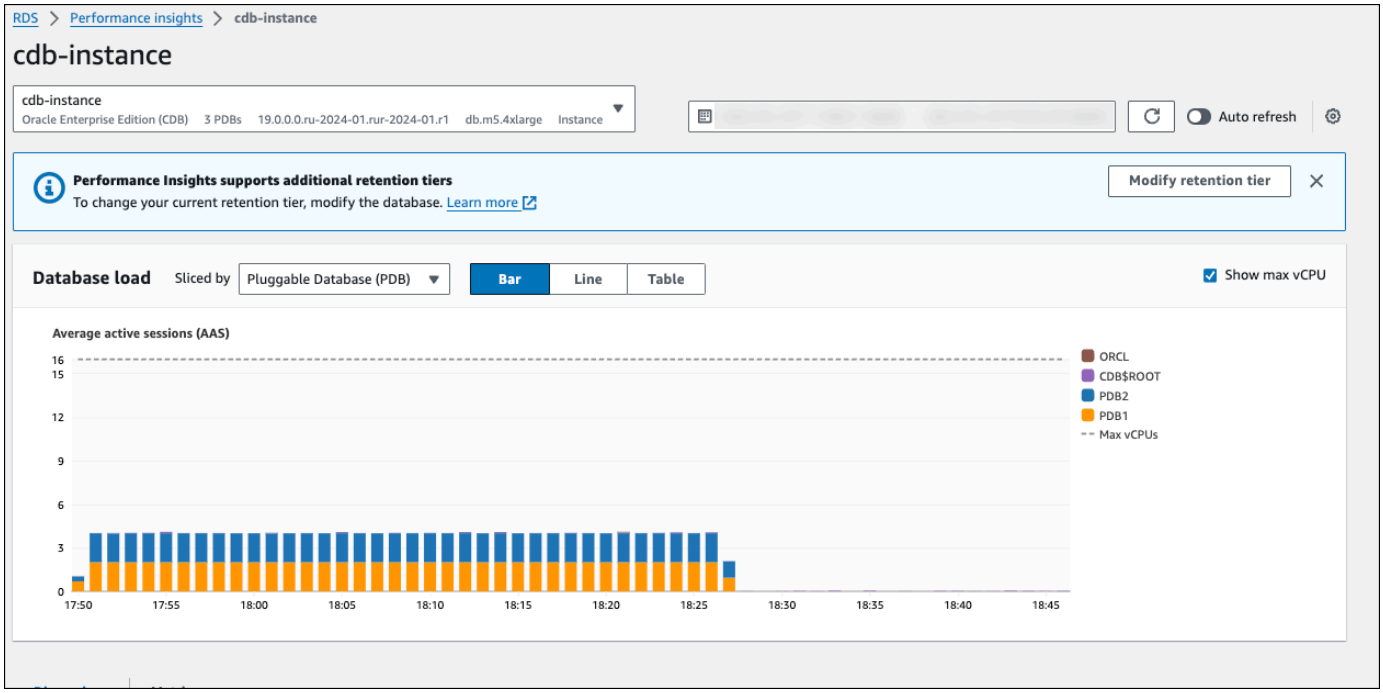
Para obtener información sobre la compatibilidad de esta característica por región, motor de base de datos y clase de instancia, consulte Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento.

Análisis de la carga de PDB principal en una CDB de Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación de la izquierda, seleccione Información sobre rendimiento.
3. Elija una instancia CDB de Oracle.

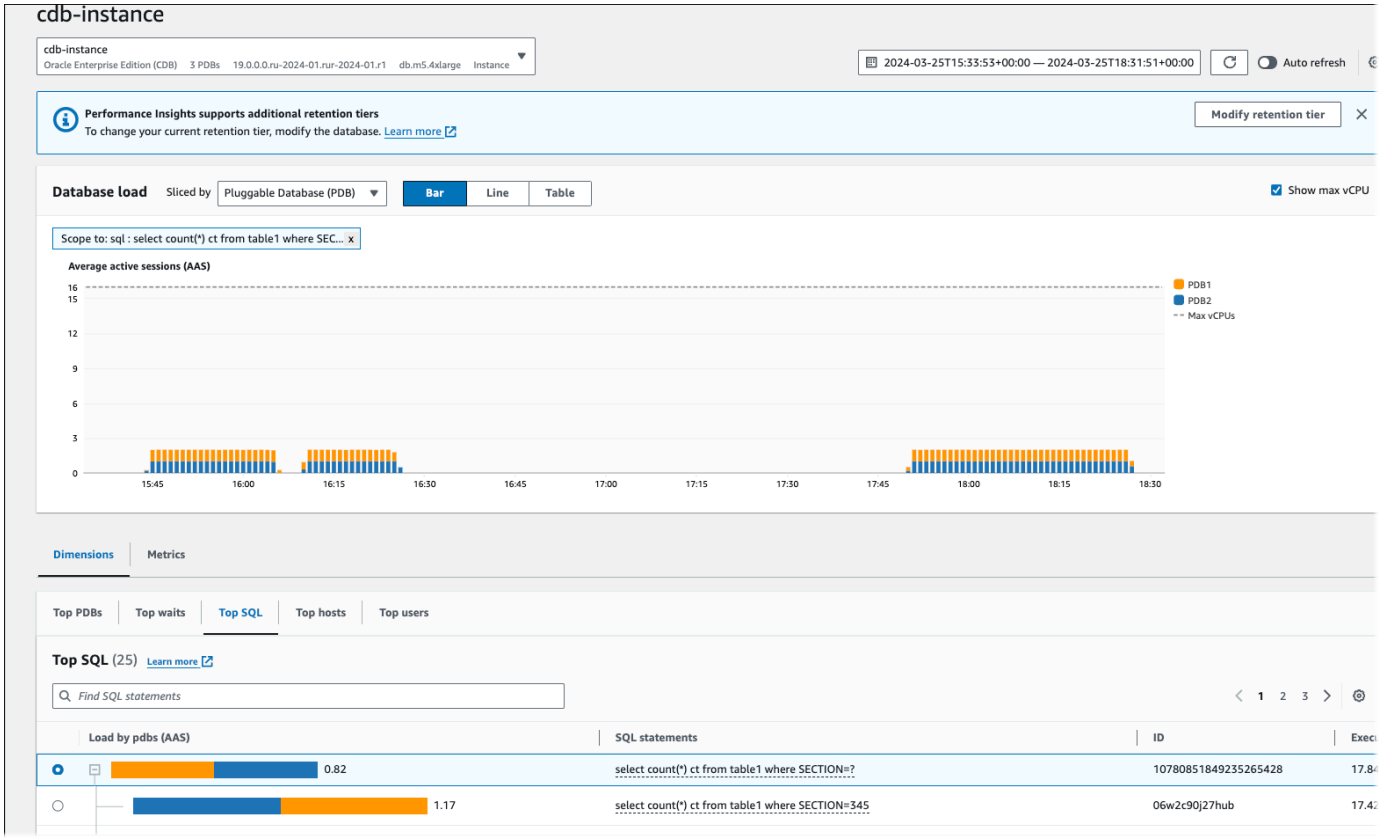
   Se muestra el panel de Información de rendimiento para la instancia de base de datos.
4. En la sección Carga de base de datos, elija Pluggable database (PDB) junto a Segmentar por.

El gráfico de sesiones activas promedio muestra la PDB con la carga más alta. Los identificadores de PDB aparecen a la derecha de los cuadrados codificados por colores. Cada identificador identifica de forma única una PDB.

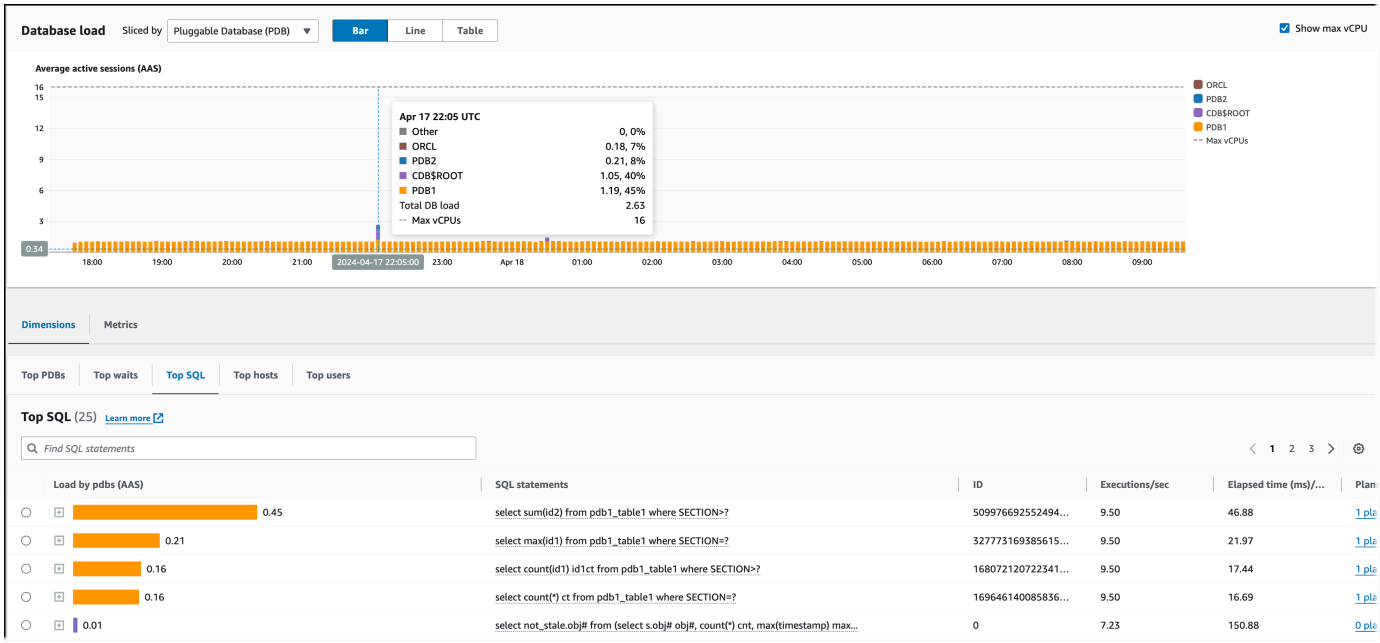


5. Desplácese hasta la pestaña SQL principal.

   En el siguiente ejemplo, puede ver la misma consulta SQL y la carga que genera en varias PDB.



En el siguiente ejemplo, una sola PDB gestiona una carga superior a otras PDB de la CDB.



Para obtener más información acerca de las CDB de Oracle, consulte CDB y PDB.

Análisis de planes de ejecución mediante el panel de Información de rendimiento para Amazon RDS

En el panel de Información de rendimiento de Amazon RDS, puede encontrar información sobre los planes de ejecución para las instancias de base de datos de Oracle y SQL Server. Puede utilizar esta información para saber qué planes contribuyen más a la carga de la base de datos.

Para analizar planes de ejecución de Oracle o SQL Server, consulte los siguientes temas.

Análisis de planes de ejecución

- Análisis de planes de ejecución de Oracle mediante el panel de Información de rendimiento para Amazon RDS
- Análisis de planes de ejecución de SQL Server mediante el panel de Información de rendimiento para Amazon RDS

Descripción general del análisis de los planes de ejecución para Amazon RDS

Puede utilizar el panel de Información de rendimiento de Amazon RDS para saber qué planes contribuyen más a la carga de bases de datos de las instancias de base de datos de Oracle y SQL Server.

Por ejemplo, las principales instrucciones SQL en un momento dado podrían estar utilizando los planes que se muestran en la siguiente tabla.

SQL principal	Plan
SELECT SUM(amount_sold) FROM sales WHERE prod_id = 10	Plan A
SELECT SUM(amount_sold) FROM sales WHERE prod_id = 521	Plan B
SELECT SUM(s_total) FROM sales WHERE region = 10	Plan A
SELECT * FROM emp WHERE emp_id = 1000	Plan C
SELECT SUM(amount_sold) FROM sales WHERE prod_id = 72	Plan A

Con la característica de planificación de Performance Insights, puede hacer lo siguiente:

- Encuentre qué planes utilizan las principales consultas SQL.

  Por ejemplo, podría hallar que la mayor parte de la carga de la base de datos se genera mediante consultas que utilizan el plan A y el plan B, y solo un pequeño porcentaje utiliza el plan C.
- Compare distintos planes para la misma consulta.

  En el ejemplo anterior, tres consultas son idénticas, excepto el ID del producto. Dos consultas utilizan el plan A, pero una consulta utiliza el plan B. Para ver la diferencia en los dos planes, puede utilizar Performance Insights.
- Busque cuándo una consulta cambió a un nuevo plan.

  Es posible que vea que una consulta utiliza el plan A y, luego, cambió al plan B en un momento determinado. ¿Hubo algún cambio en la base de datos en ese momento? Por ejemplo, si una tabla está vacía, el optimizador podría elegir un análisis de tabla completo. Si la tabla se carga con un millón de filas, el optimizador podría cambiar a un análisis de rango de índices.
- Explore a fondo los pasos específicos de un plan con el mayor costo.

  Por ejemplo, para una consulta de larga duración podría mostrar una condición de unión que falta en una combinación de igualdad. Esta condición faltante fuerza una unión cartesiana, que une todas las filas de dos tablas.

Puede hacer las tareas anteriores mediante la característica Captura de planes de Performance Insights. Del mismo modo que puede dividir las consultas de mediante eventos de espera y SQL principal, puede dividirlas por la dimensión del plan.

Análisis de planes de ejecución de Oracle mediante el panel de Información de rendimiento para Amazon RDS

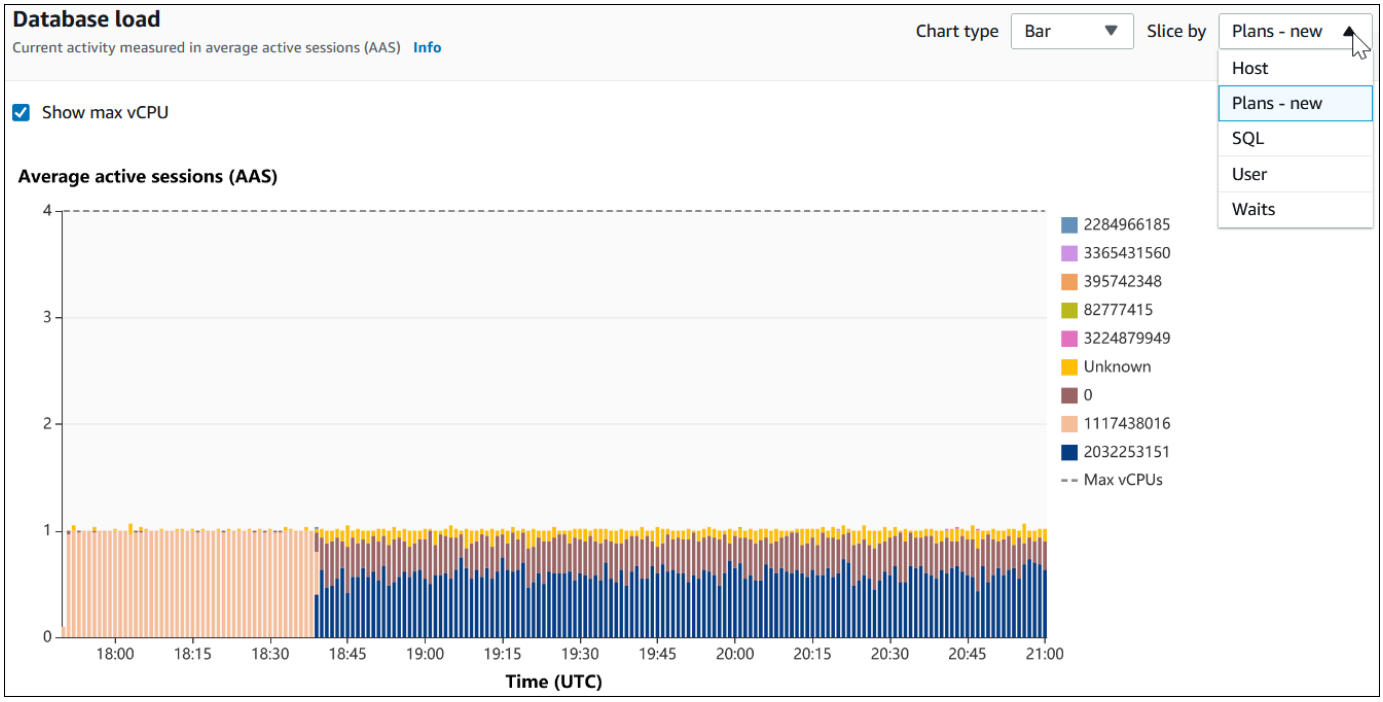
Al analizar la carga de base de datos en una base de datos de Oracle, es posible que quiera saber qué planes contribuyen más a la carga de la base de datos. Puede determinar qué planes contribuyen más a la carga de base de datos mediante la característica de captura de planes de Información de rendimiento.

Para analizar los planes de ejecución de Oracle mediante la consola

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Información de rendimiento.

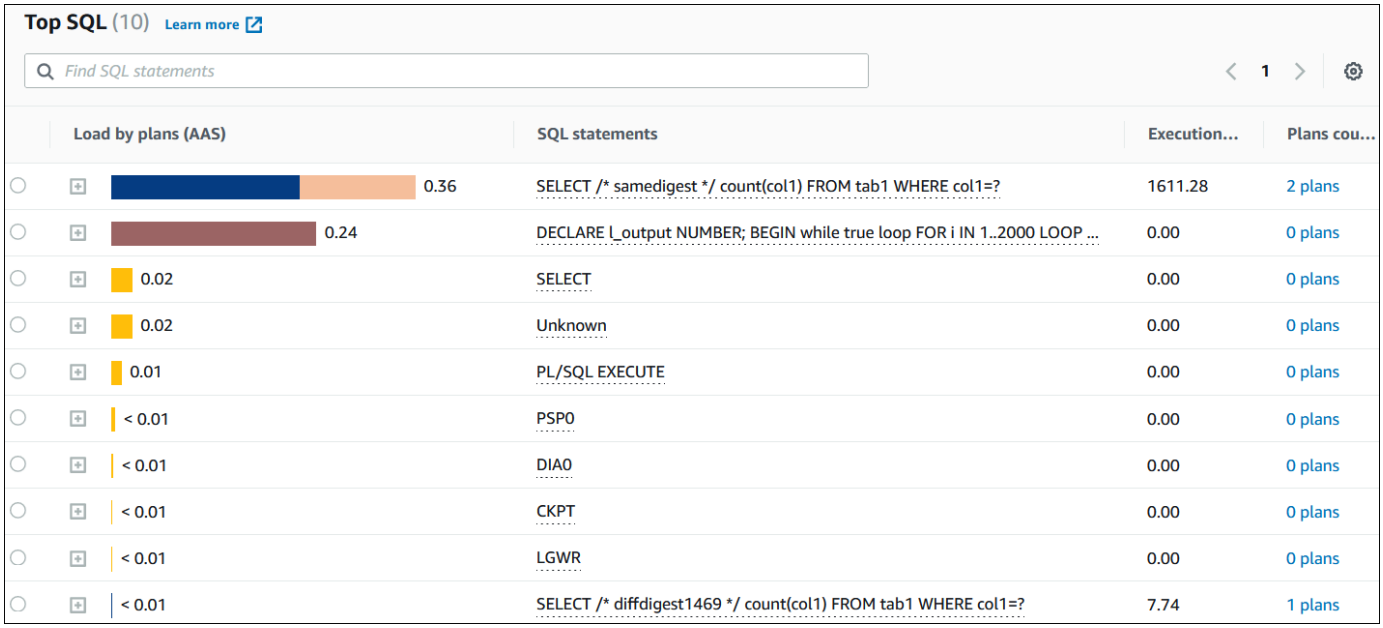
3. Elija una instancia base de datos de Oracle. Se abre el panel de Información sobre rendimiento para esa instancia de base de datos.
4. En la sección Database load (DB load) (Carga de base de datos), elija Plans (Planes) junto a Slice by (Dividir por).

   El gráfico de sesiones activas promedio muestra los planes utilizados por las instrucciones SQL principales. Los valores hash del plan aparecen a la derecha de los cuadrados codificados por colores. Cada valor hash identifica de forma exclusiva un plan.



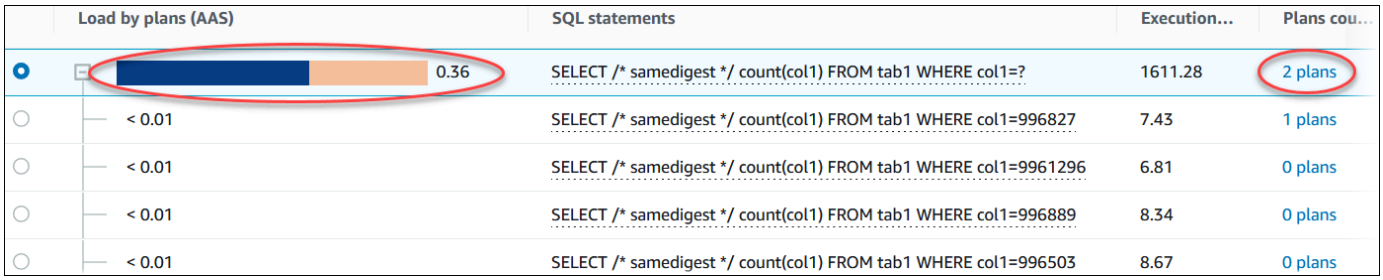
5. Desplácese hasta la pestaña Top SQL (SQL principal).

   En el siguiente ejemplo, el resumen de SQL principal tiene dos planes. Puede notar que es un resumen según el signo de interrogación de la instrucción.



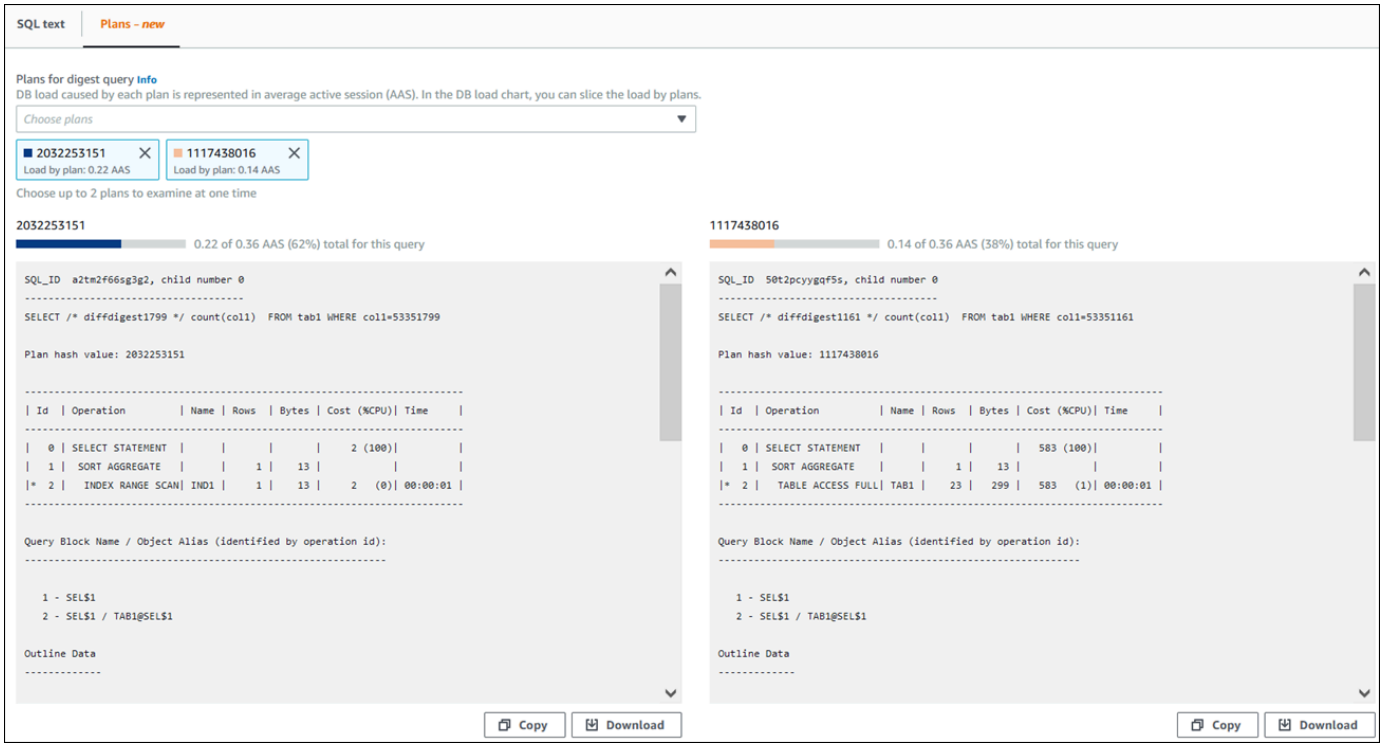
6. Elija el resumen para expandirlo a sus instrucciones de componentes.

   En el siguiente ejemplo, la instrucción SELECT es una consulta de resumen. Las consultas de componentes del resumen utilizan dos plan diferentes. Los colores de los planes corresponden al gráfico de la carga de la base de datos. El número total de planes del resumen se muestra en la segunda columna.

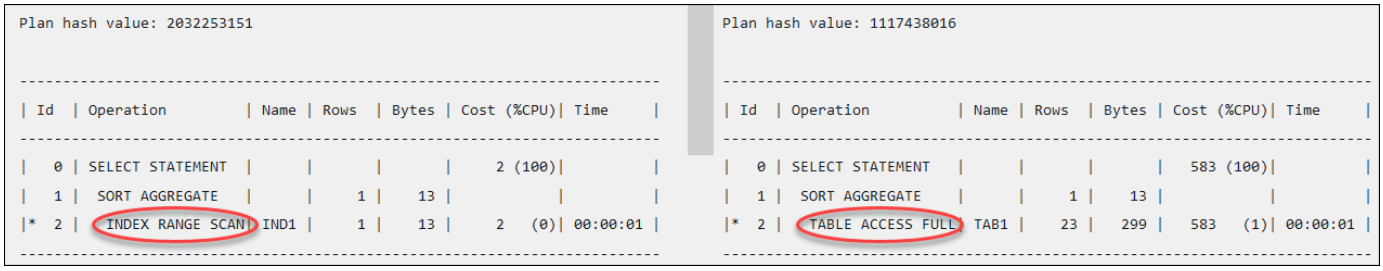


7. Desplácese hacia abajo y elija dos Planes que comparar de la lista Plans for digest query (Planes para consulta de resumen).

   Puede ver uno o dos planes para una consulta a la vez. La siguiente captura de pantalla compara los dos planes del resumen, con el hash 2032253151 y el hash 1117438016. En el siguiente ejemplo, el 62 % de las sesiones activas promedio que ejecutan esta consulta de resumen utilizan el plan de la izquierda, mientras que el 38 % utiliza el plan de la derecha.



En este ejemplo, los planes difieren de una manera importante. El paso 2 del plan 2032253151 utiliza un análisis de índice, mientras que el plan 1117438016 utiliza un análisis de tabla completo. Para una tabla con un gran número de filas, una consulta de una sola fila es casi siempre más rápida con un escaneo de índices.



8. (Opcional) Elija Copy (Copia) para copiar el plan en el portapapeles, o Download (Descargar) para guardar el plan en el disco duro.

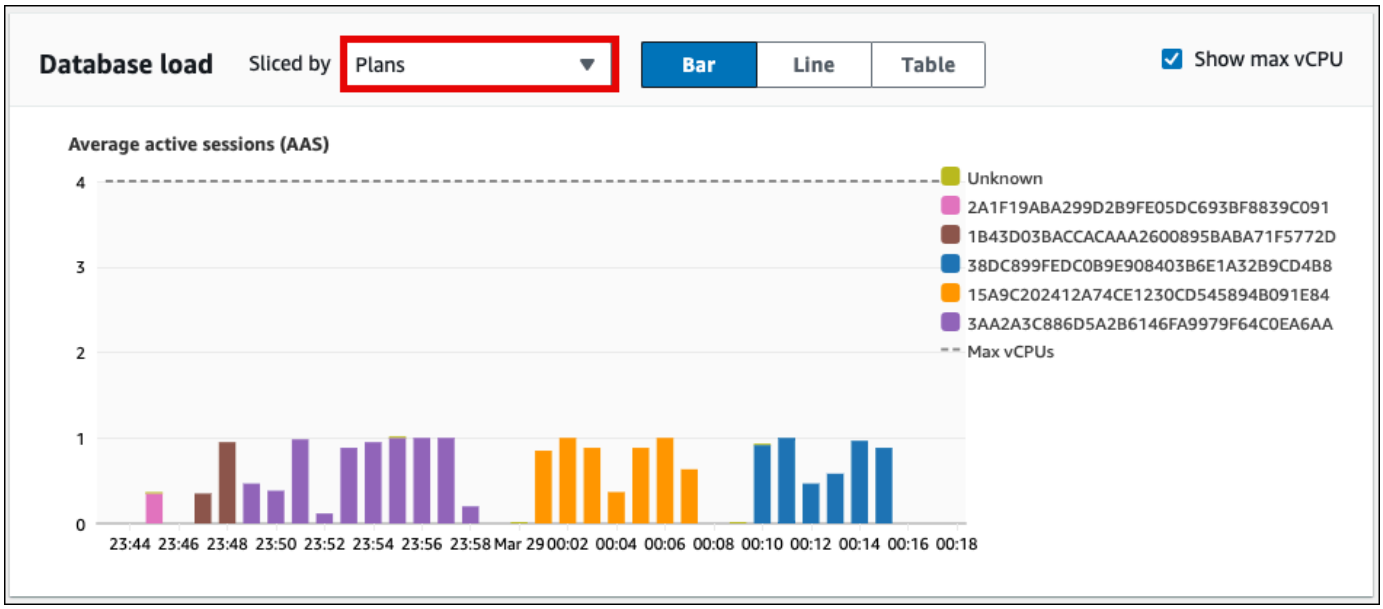
Análisis de planes de ejecución de SQL Server mediante el panel de Información de rendimiento para Amazon RDS

Al analizar la carga de base de datos en una base de datos de SQL Server, es posible que quiera saber qué planes contribuyen más a la carga de la base de datos. Puede determinar qué planes contribuyen más a la carga de base de datos mediante la característica de captura de planes de Información de rendimiento.

Análisis de los planes de ejecución de SQL Server mediante la consola

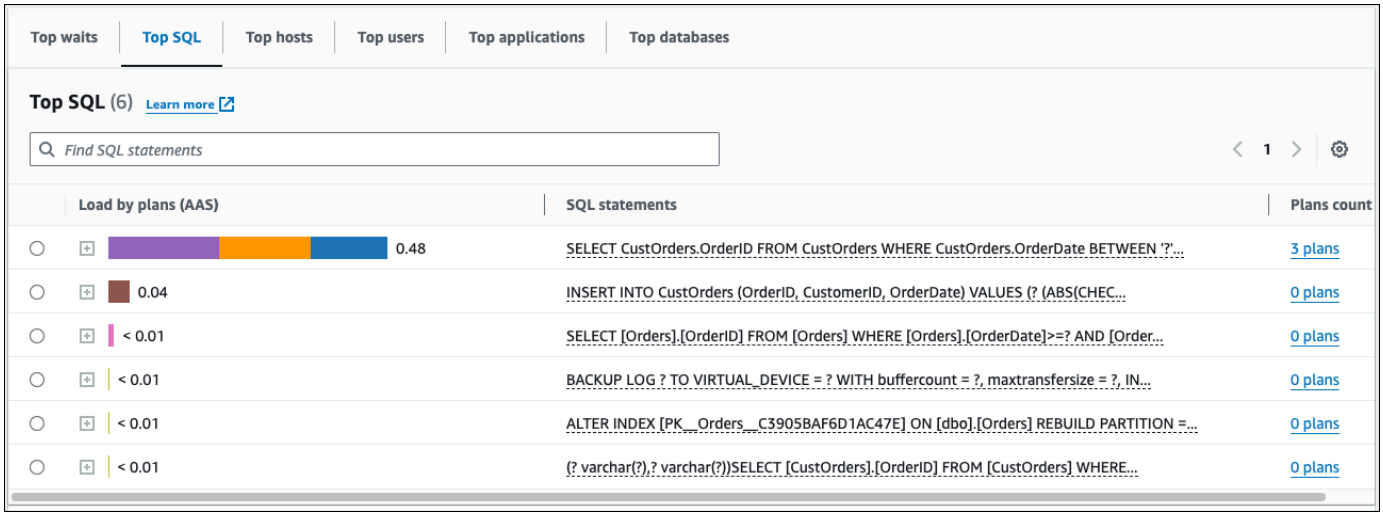
1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Información de rendimiento.
3. Elija una instancia de base de datos SQL Server. Se abre el panel de Información sobre rendimiento para esa instancia de base de datos.
4. En la sección Database load (DB load) (Carga de base de datos), elija Plans (Planes) junto a Slice by (Dividir por).

   El gráfico de sesiones activas promedio muestra los planes utilizados por las instrucciones SQL principales. Los valores hash del plan aparecen a la derecha de los cuadrados codificados por colores. Cada valor hash identifica de forma exclusiva un plan.



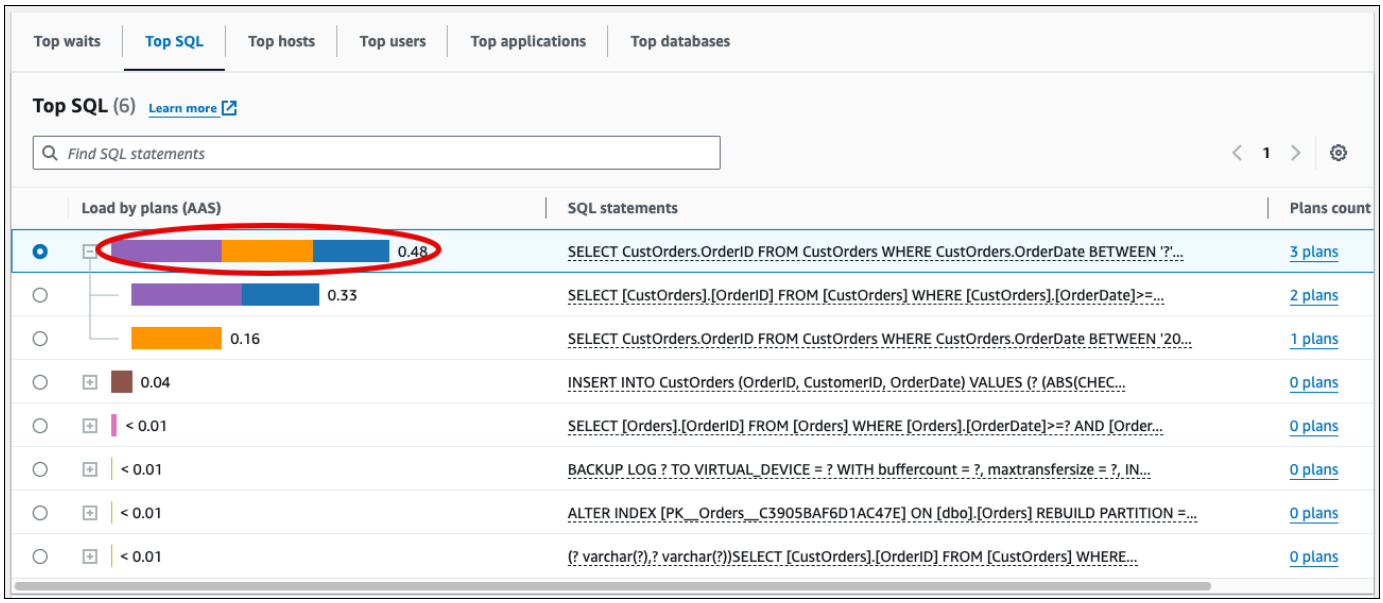
5. Desplácese hasta la pestaña Top SQL (SQL principal).

   En el siguiente ejemplo, el resumen de SQL principal tiene tres planes. La presencia de un signo de interrogación en la instrucción de SQL indica que se trata de un resumen. Para ver la instrucción de SQL completa, elija un valor en la columna Instrucciones de SQL.



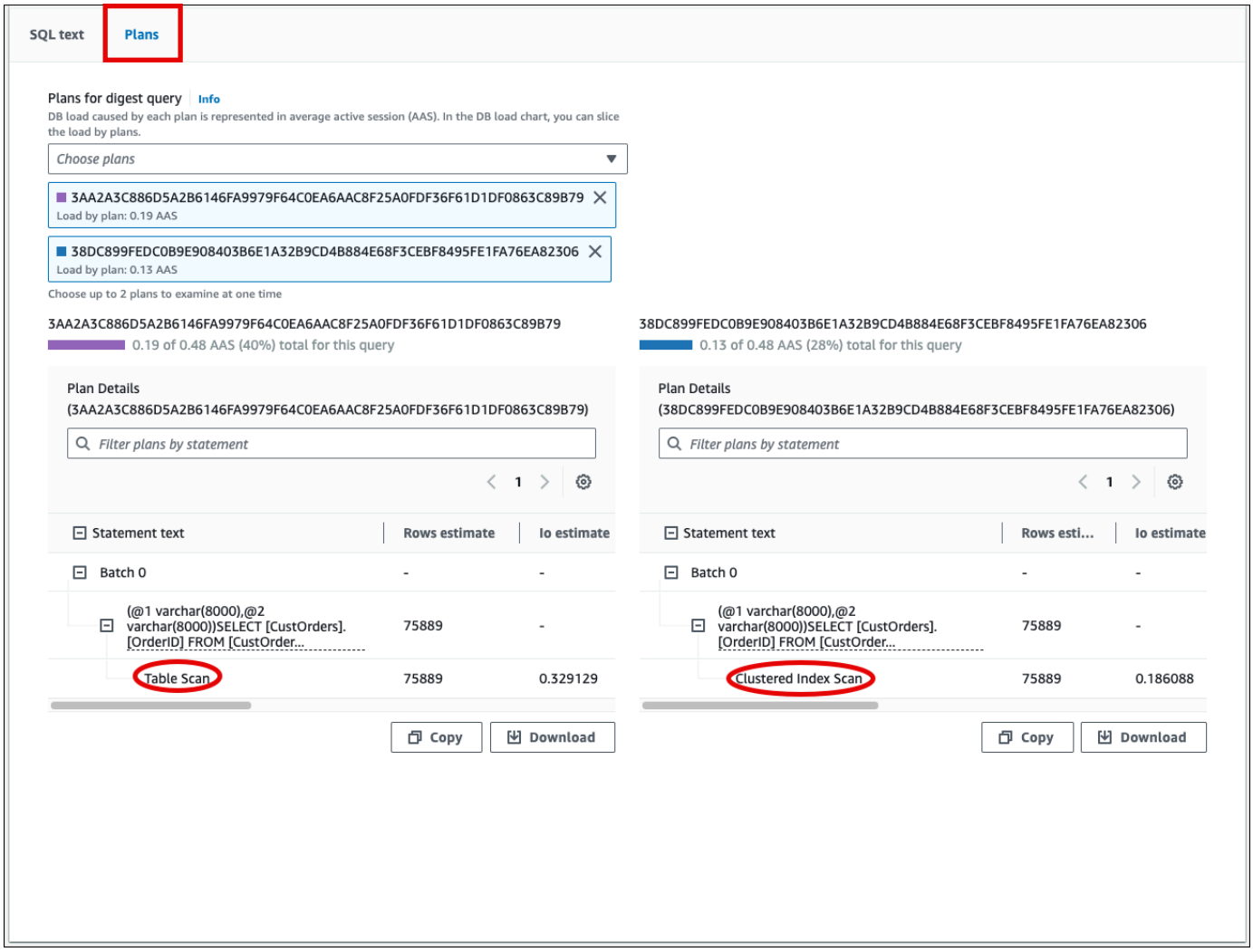
6. Elija el resumen para expandirlo a sus instrucciones de componentes.

   En el siguiente ejemplo, la instrucción SELECT es una consulta de resumen. Las consultas de componentes del resumen utilizan tres planes de ejecución diferentes. Los colores asignados a los planes corresponden al gráfico de la carga de la base de datos.



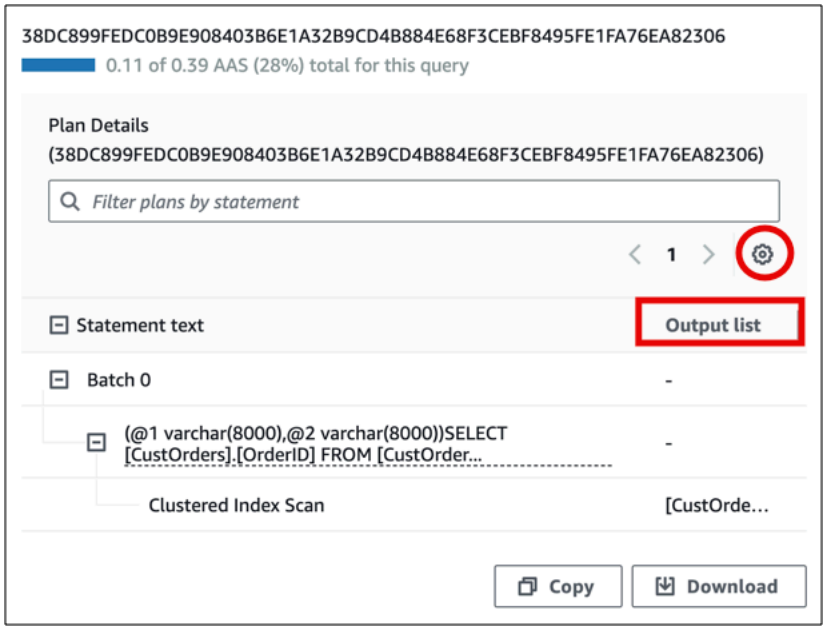
7. Desplácese hacia abajo y elija dos Planes que comparar de la lista Plans for digest query (Planes para consulta de resumen).

   Puede ver uno o dos planes para una consulta a la vez. La siguiente captura de pantalla compara los dos planes del resumen. En el siguiente ejemplo, el 40 % de las sesiones activas promedio que ejecutan esta consulta de resumen utilizan el plan de la izquierda, mientras que el 28 % utiliza el plan de la derecha.



En el ejemplo anterior, los planes difieren de una manera importante. El paso 2 del plan de la izquierda usa un análisis de tablas, mientras que el plan de la derecha usa un análisis de índices agrupados. Para una tabla con un gran número de filas, una consulta que recupera una sola fila es casi siempre más rápida con un análisis de índices agrupados.

8. (Opcional) Seleccione el icono Configuración en la tabla de detalles del plan para personalizar la visibilidad y el orden de las columnas. La siguiente captura de pantalla muestra la tabla de detalles del plan con la columna Lista de resultados como segunda columna.



9. (Opcional) Elija Copy (Copia) para copiar el plan en el portapapeles, o Download (Descargar) para guardar el plan en el disco duro.

> **Note**
>
> Información de rendimiento muestra los planes de ejecución estimados mediante una tabla de árbol jerárquico. La tabla incluye la información de ejecución parcial de cada instrucción. Para obtener más información sobre las columnas de la tabla de detalles del plan, consulte SET SHOWPLAN_ALL en la documentación de SQL Server. Para ver la información de ejecución completa de un plan de ejecución estimado, seleccione Descargar para descargar el plan y, a continuación, cárguelo en SQL Server Management Studio. Para obtener más información sobre cómo mostrar un plan de ejecución estimado con SQL Server Management Studio, consulte Display an Estimated Execution Plan en la documentación de SQL Server.

Visualización de las recomendaciones proactivas de Información de rendimiento

Información de rendimiento de Amazon RDS monitoriza automáticamente métricas específicas y crea umbrales. Para ello, analiza qué niveles podrían ser potencialmente problemáticos para un recurso específico. Cuando los nuevos valores de las métricas cruzan un umbral predefinido durante un

período de tiempo determinado, Información de rendimiento genera una recomendación proactiva. Esta recomendación ayuda a evitar que el rendimiento de la base de datos se vea afectado en el futuro. Para recibir estas recomendaciones proactivas, debe activar Información de rendimiento con un período de retención de nivel de pago.

Para obtener más información acerca de la activación de Información de rendimiento, consulte Activación y desactivación de Información de rendimiento de Amazon RDS. Para obtener información sobre los precios y la retención de datos de Información de rendimiento, consulte Precios y retención de datos de Performance Insights.

Para obtener información sobre las regiones, los motores de bases de datos y las clases de instancias compatibles con las recomendaciones proactivas, consulte Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento.

Puede ver el análisis detallado y las investigaciones recomendadas de las recomendaciones proactivas en la página de detalles de las recomendaciones.

Para obtener más información sobre recomendaciones, consulte Recomendaciones para Amazon RDS.

Para ver el análisis detallado de una recomendación proactiva

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, realice cualquiera de las siguientes acciones:

   - Elija Recomendaciones.

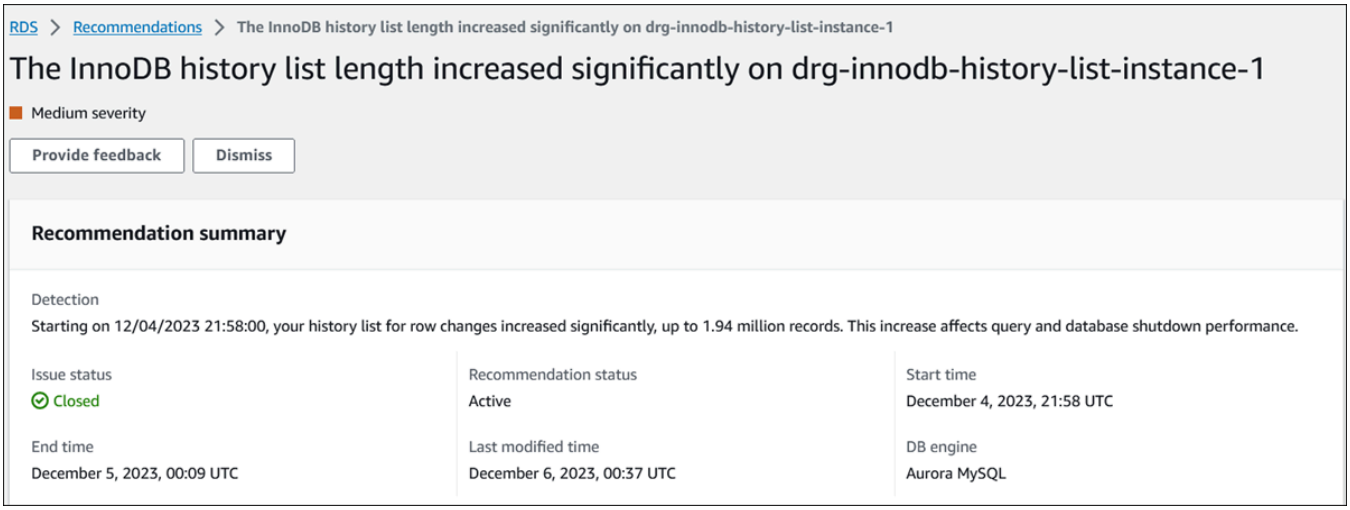
     En la página Recomendaciones, se muestra una lista de recomendaciones ordenadas por su gravedad para todos los recursos de su cuenta.
   - Elija Bases de datos y, a continuación, elija Recomendaciones para un recurso en la página de bases de datos.

     La pestaña Recomendaciones muestra las recomendaciones y sus detalles para el recurso seleccionado.
3. Busque una recomendación proactiva y elija Ver detalles.

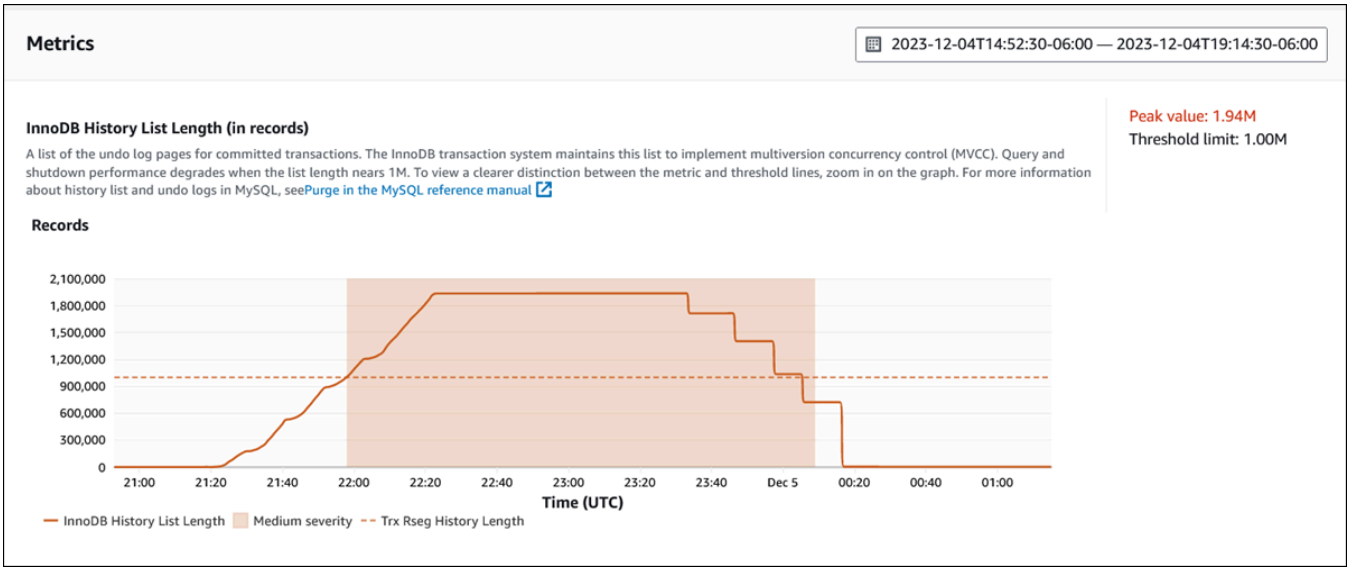
   Aparece la página de detalles de la recomendación. En el título se proporciona el nombre del recurso afectado con el problema detectado y su gravedad.

A continuación figuran los componentes de la página de detalles de la recomendación:

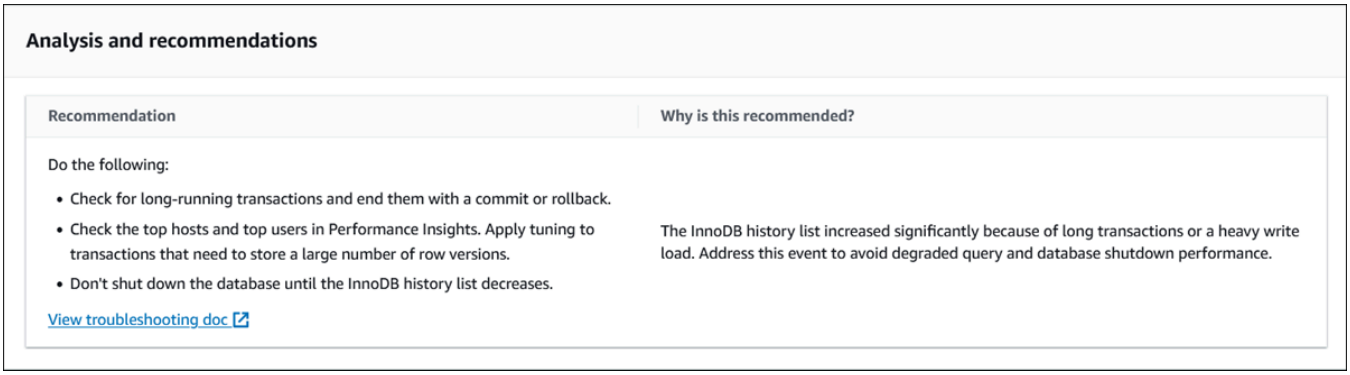
- Resumen de la recomendación: el problema detectado, el estado de la recomendación y el problema, la hora de inicio y finalización del problema, la hora de modificación de la recomendación y el tipo de motor.



- Métricas: los gráficos del problema detectado. Cada gráfico muestra un umbral determinado por el comportamiento de referencia del recurso, así como los datos de la métrica informados desde el momento de inicio de la anomalía.



- Análisis y recomendaciones: la recomendación y el motivo de la recomendación sugerida.



Puede revisar la causa del problema y, a continuación, realizar las acciones recomendadas para solucionarlo o seleccionar Descartar en la esquina superior derecha para descartar la recomendación.

Recuperación de métricas con la API de Información sobre rendimiento para Amazon RDS

Cuando se activa la Información de rendimiento, la API proporciona visibilidad sobre el rendimiento de la instancia. registros de Amazon Cloudwatch proporciona la fuente autorizada de las métricas de monitoreo vendidas para servicios de AWS.

Con Performance Insights se ofrece una vista propia del dominio de la carga de la base de datos entendida como el promedio de sesiones activas (AAS). Esta métrica aparece para los consumidores de API como conjunto de datos de serie temporal bidimensional. La dimensión temporal de los datos ofrece datos de carga de base de datos para cada punto temporal del intervalo de tiempo consultado. Cada punto temporal descompone la carga global en relación con las dimensiones solicitadas, tales como `SQL`, `Wait-event`, `User` o `Host`, medidas en ese punto temporal.

La información sobre rendimiento de Amazon RDS monitorea el clúster de instancia de base de datos de Amazon RDS para poder analizar y solucionar los problemas de desempeño de la base de datos. Una forma de ver los datos de Performance Insights es a través de la AWS Management Console. Performance Insights además ofrece una API pública, para poder consultar en sus propios datos. Puede utilizar la API para hacer lo siguiente:

- Descarga de datos en una base de datos
- Agregación de datos de Performance Insights a los paneles de monitoreo existentes
- Crear herramientas de monitoreo.

Para utilizar la API de Performance Insights, habilite Performance Insights en una de sus instancias de base de datos de Amazon RDS. Para obtener información sobre la habilitación de Performance Insights, consulte Activación y desactivación de Información de rendimiento de Amazon RDS. Para obtener información sobre la API de Performance Insights, consulte la Referencia de la API de Performance Insights de Amazon RDS.

La API de Información sobre rendimiento proporciona las siguientes operaciones.

Acción de Performance Insights	AWS CLI command	Descripción
CreatePerformanceAnalysisReport	aws pi create-performance-analysis-report	Crea un informe de análisis de rendimiento para un período de tiempo específico para la instancia de base de datos. El resultado es AnalysisReportId que es el identificador único del informe.
DeletePerformanceAnalysisReport	aws pi delete-performance-analysis-report	Elimina un informe de análisis de rendimiento.
DescribeDimensionKeys	aws pi describe-dimension-keys	Recupera las principales claves de dimensión N de una métrica para un periodo de tiempo específico.
GetDimensionKeyDetails	aws pi get-dimension-key-details	Recupera los atributos del grupo de dimension es especificado para una instancia de base de datos o un origen de datos. Por ejemplo, si especifica un ID de SQL y si los detalles de la dimensión están disponibles, GetDimensionKeyDetails recupera el texto

Acción de Performance Insights	AWS CLI command	Descripción
		completo de la dimensión `db.sql.statement` asociada a este ID. Esta operación resulta útil porque `GetResourceMetrics` y `DescribeDimensionKeys` no admiten la recuperación de texto de instrucción SQL grande.
`GetPerformanceAnalysisReport`	`aws pi get-performance-analysis-report`	Recupera el informe, incluidos los datos del informe. El resultado incluye el estado del informe, el identificador del informe, los detalles del tiempo del informe, la información y las recomendaciones.
`GetResourceMetadata`	`aws pi get-resource-metadata`	Recupere los metadatos de las distintas características. Por ejemplo, los metadatos podrían indicar que una característica está activada o desactivada en una instancia de base de datos específica.

Acción de Performance Insights	AWS CLI command	Descripción
GetResourceMetrics	aws pi get-resource-metrics	Recupera las métricas de Información sobre rendimiento de un conjunto de orígenes de datos, durante un periodo de tiempo. Puede proporcionar grupos de dimensiones y dimensiones específicas, y proporcionar criterios de agregación y filtrado para cada grupo.
ListAvailableResourceDimensions	aws pi list-available-resource-dimensions	Recupere las dimensiones que se pueden consultar para cada tipo de métrica especificado en una instancia especificada.
ListAvailableResourceMetrics	aws pi list-available-resource-metrics	Recupere todas las métricas disponibles de los tipos de métricas especificados que se pueden consultar de una instancia de base de datos especificada.
ListPerformanceAnalysisReports	aws pi list-performance-analysis-reports	Recupera todos los informes de análisis disponibles para la instancia de base de datos. Los informes se enumeran en función de la hora de inicio de cada informe.

Acción de Performance Insights	AWS CLI command	Descripción
ListTagsForResource	aws pi list-tags-for-resource	Muestra todas las etiquetas de metadatos agregadas al recurso. La lista incluye el nombre y el valor de la etiqueta.
TagResource	aws pi tag-resource	Añade etiquetas de metadatos a un recurso de Amazon RDS. La etiqueta incluye un nombre y un valor.
UntagResource	aws pi untag-resource	Elimina la etiqueta de metadatos del recurso.

Para obtener más información sobre la recuperación de métricas de series temporales y ver ejemplos de la AWS CLI para Información de rendimiento, consulte los siguientes temas.

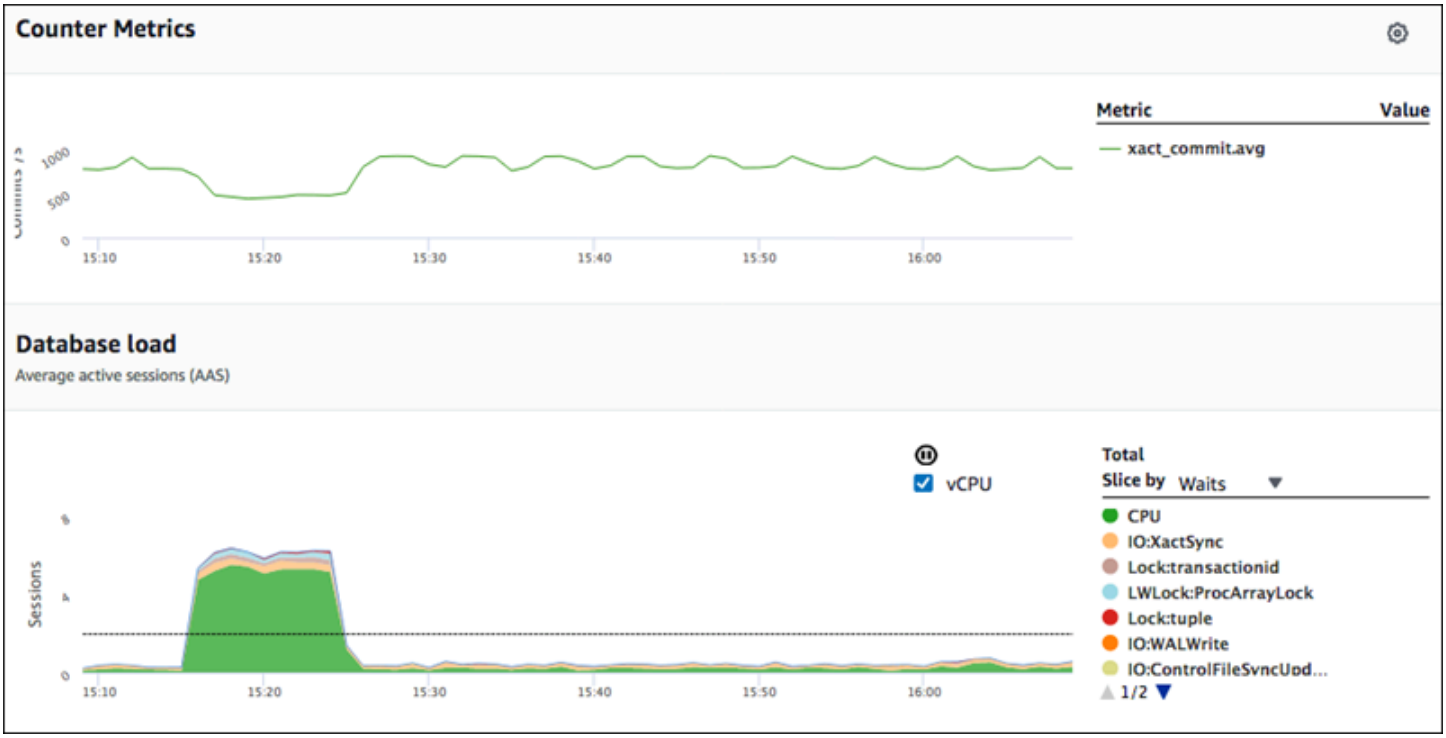
Temas

- Recuperación de métricas de series temporales para Información de rendimiento
- Ejemplos de la AWS CLI para Performance Insights

Recuperación de métricas de series temporales para Información de rendimiento

La operación `GetResourceMetrics` recupera una o más métricas de series temporales a partir de los datos de Performance Insights. `GetResourceMetrics` requiere una métrica y un periodo de tiempo y devuelve una respuesta con una lista de puntos de datos.

Por ejemplo, la AWS Management Console usa `GetResourceMetrics` para completar el gráfico Counter Metrics (Métricas de contador) y el gráfico Database Load (Carga de la base de datos), como se muestra en la siguiente imagen.



Todas las métricas que devuelve `GetResourceMetrics` son métricas de series temporales estándar con la excepción de `db.load`. Esta métrica se muestra en el gráfico Database Load (Carga de base de datos). La métrica `db.load` es distinta de las demás métricas de series temporales porque puede desglosarla en subcomponentes llamados dimensiones. En la imagen anterior, `db.load` está desglosado y agrupado por los estados de espera que forman el `db.load`.

> **Note**
>
> `GetResourceMetrics` también puede devolver la métrica `db.sampleload`, pero la métrica `db.load` es apropiada en la mayoría de los casos.

Para obtener información sobre las métricas de contador devueltas por `GetResourceMetrics`, consulte Métricas de contador de Información de rendimiento.

Para las métricas se admiten los siguientes cálculos:

- Media: el valor medio de la métrica durante un período de tiempo. Añada `.avg` al nombre de la métrica.
- Mínimo: el valor mínimo de la métrica durante un período de tiempo. Añada `.min` al nombre de la métrica.

- Máximo: el valor máximo de la métrica durante un período de tiempo. Añada `.max` al nombre de la métrica.
- Suma: la suma de los valores de la métrica durante un periodo de tiempo. Añada `.sum` al nombre de la métrica.
- Número de muestras: El número de veces que se recopiló la métrica durante un período de tiempo. Añada `.sample_count` al nombre de la métrica.

Supongamos, por ejemplo, que una métrica se recopila durante 300 segundos (5 minutos) y que la métrica se recopila una vez cada minuto. Los valores para cada minuto son 1, 2, 3, 4 y 5. En este caso, se devuelven los siguientes cálculos:

- Media: 3
- Mínimo: 1
- Máximo: 5
- Suma: 15
- Número de muestras: 5

Para obtener información acerca del uso del comando `get-resource-metrics` de la AWS CLI, consulte `get-resource-metrics`.

Para la opción `--metric-queries`, especifique una o más consultas para las que desea obtener resultados. Cada consulta consta de un parámetro `Metric` obligatorio y de parámetros opcionales `GroupBy` y `Filter`. A continuación, se muestra un ejemplo de una especificación de opción `--metric-queries`.

```
{
   "Metric": "string",
   "GroupBy": {
     "Group": "string",
     "Dimensions": ["string", ...],
     "Limit": integer
   },
   "Filter": {"string": "string"
     ...}
```

Ejemplos de la AWS CLI para Performance Insights

En las siguientes secciones, obtendrá más información sobre AWS Command Line Interface (AWS CLI) para Información de rendimiento, así como ejemplos de uso de la AWS CLI.

Temas

- Ayuda integrada en la AWS CLI para Información de rendimiento
- Recuperación de métricas de contador
- Recuperación del promedio de carga de base de datos para los eventos de espera principales
- Recuperación del promedio de carga de base de datos para las instrucciones SQL principales
- Recuperación del promedio de carga de base de datos filtrado por SQL
- Recuperación del texto completo de una instrucción SQL
- Creación de un informe de análisis de rendimiento para un período de tiempo
- Recuperación de un informe de análisis de rendimiento
- Enumeración de todos los informes de análisis de rendimiento de la instancia de base de datos
- Eliminación de un informe de análisis de rendimiento
- Adición de una etiqueta a un informe de análisis de rendimiento
- Enumeración de todas las etiquetas de un informe de análisis de rendimiento
- Eliminación de etiquetas de un informe de análisis de rendimiento

Ayuda integrada en la AWS CLI para Información de rendimiento

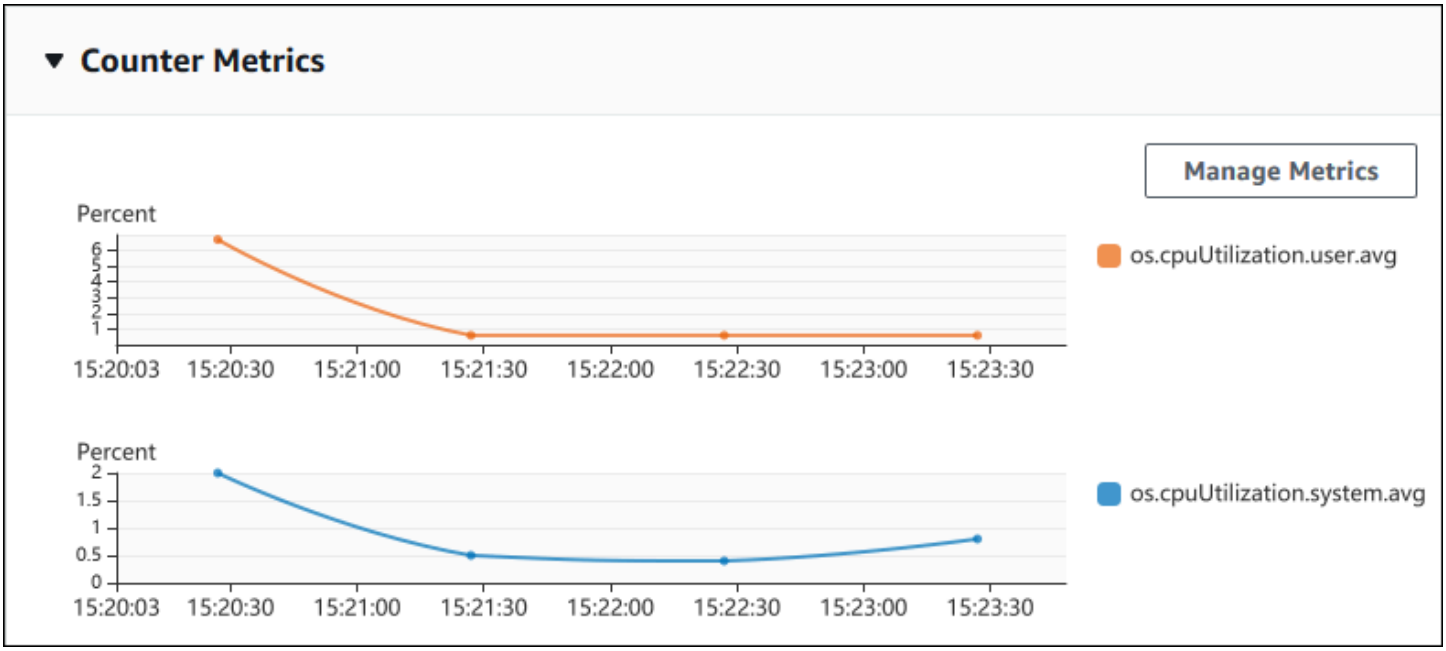
Puede ver los datos de Performance Insights a través de la AWS CLI. Puede obtener ayuda sobre los comandos de la AWS CLI de Performance Insights escribiendo lo siguiente en la línea de comandos.

```
aws pi help
```

Si no tiene instalada la AWS CLI, consulte Instalación de la AWS CLI en la Guía del usuario de la AWS CLI para obtener información sobre cómo instalarla.

Recuperación de métricas de contador

La siguiente captura de pantalla muestra dos gráficos de métricas de contador en la AWS Management Console.



El siguiente ejemplo muestra cómo recopilar los mismos datos que utiliza la AWS Management Console para generar los dos gráficos de métricas de contador.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries '[{"Metric": "os.cpuUtilization.user.avg"  },
                      {"Metric": "os.cpuUtilization.idle.avg"}]'
```

También puede hacer que un comando sea más fácil de leer especificando un archivo para la opción `--metrics-query`. El siguiente ejemplo utiliza un archivo llamado query.json para la opción. El archivo tiene el siguiente contenido.

```
[
    {
        "Metric": "os.cpuUtilization.user.avg"
    },
    {
        "Metric": "os.cpuUtilization.idle.avg"
    }
]
```

Ejecute el siguiente comando para utilizar el archivo.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

El ejemplo anterior especifica los siguientes valores para las opciones:

- `--service-type`: RDS para Amazon RDS
- `--identifier`: el ID de recurso para la instancia de base de datos
- `--start-time` y:`--end-time` los valores ISO 8601 `DateTime` para el periodo de consulta, con varios formatos admitidos

Consulta durante un intervalo de una hora:

- `--period-in-seconds`: `60` para una consulta por minuto
- `--metric-queries`: una matriz de dos consultas, cada una para una métrica.

  El nombre de la métrica utiliza puntos para clasificar la métrica en categorías útiles y el elemento final es una función. En el ejemplo, la función es `avg` para cada consulta. Al igual que con Amazon CloudWatch, las funciones admitidas son `min`, `max`, `total` y `avg`.

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1540857600.0,
    "AlignedEndTime": 1540861200.0,
    "MetricList": [
        { //A list of key/datapoints
            "Key": {
                "Metric": "os.cpuUtilization.user.avg" //Metric1
            },
            "DataPoints": [
                //Each list of datapoints has the same timestamps and same number of
 items
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 4.0
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 4.0
                },
                {
                    "Timestamp": 1540857780.0, //Minute 3
                    "Value": 10.0
                }
                //... 60 datapoints for the os.cpuUtilization.user.avg metric
            ]
        },
        {
            "Key": {
                "Metric": "os.cpuUtilization.idle.avg" //Metric2
            },
```

```
            "DataPoints": [
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 12.0
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 13.5
                },
                //... 60 datapoints for the os.cpuUtilization.idle.avg metric
            ]
        }
    ] //end of MetricList
} //end of response
```

La respuesta tiene `Identifier`, `AlignedStartTime` y `AlignedEndTime`. Como el valor `--period-in-seconds` era `60`, los tiempos de inicio y final se han alineado con el minuto. Si el `--period-in-seconds` fuera `3600`, los tiempos de inicio y final se habrían alineado con la hora.

La `MetricList` en la respuesta tiene una serie de entradas, cada una con una entrada `Key` y una entrada `DataPoints`. Cada `DataPoint` tiene un `Timestamp` y un `Value`. Cada lista de `Datapoints` tiene 60 puntos de datos porque las consultas son datos por minuto sobre una hora, con `Timestamp1/Minute1`, `Timestamp2/Minute2` y así sucesivamente, hasta `Timestamp60/Minute60`.

Como la consulta es para dos métricas de contador distintas, hay dos elementos en la respuesta `MetricList`.

Recuperación del promedio de carga de base de datos para los eventos de espera principales

El siguiente ejemplo es la misma consulta que utiliza la AWS Management Console para generar un gráfico de línea de área apilada. Este ejemplo recupera el `db.load.avg` durante la última hora con la carga dividida según los siete eventos de espera principales. El comando es el mismo que el comando en Recuperación de métricas de contador. Sin embargo, el archivo query.json tiene los elementos indicados a continuación.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 7 }
    }
```

```
]
```

Ejecute el comando siguiente.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

El ejemplo especifica la métrica de `db.load.avg` y un `GroupBy` de los siete eventos de espera principales. Para obtener detalles acerca de los valores válidos para este ejemplo, consulte DimensionGroup en la Referencia de la API de Performance Insights.

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1540857600.0,
    "AlignedEndTime": 1540861200.0,
    "MetricList": [
        { //A list of key/datapoints
            "Key": {
                //A Metric with no dimensions. This is the total db.load.avg
                "Metric": "db.load.avg"
            },
            "DataPoints": [
```

```
                //Each list of datapoints has the same timestamps and same number of
 items
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 0.5166666666666667
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 0.38333333333333336
                },
                {
                    "Timestamp": 1540857780.0, //Minute 3
                    "Value": 0.26666666666666666
                }
                //... 60 datapoints for the total db.load.avg key
            ]
        },
        {
            "Key": {
                //Another key. This is db.load.avg broken down by CPU
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.name": "CPU",
                    "db.wait_event.type": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1540857660.0, //Minute1
                    "Value": 0.35
                },
                {
                    "Timestamp": 1540857720.0, //Minute2
                    "Value": 0.15
                },
                //... 60 datapoints for the CPU key
            ]
        },
        //... In total we have 8 key/datapoints entries, 1) total, 2-8) Top Wait Events
    ] //end of MetricList
} //end of response
```

En esta respuesta, hay ocho entradas en la `MetricList`. Hay una entrada para el `db.load.avg` total y siete entradas para el `db.load.avg` divididas según uno de los siete eventos de espera principales. A diferencia del primer ejemplo, como había una dimensión de agrupación, debe haber una clave para cada agrupación de la métrica. No puede haber solo una clave para cada métrica, como en el caso de uso de métrica de contador básica.

Recuperación del promedio de carga de base de datos para las instrucciones SQL principales

El siguiente ejemplo agrupa `db.wait_events` por las 10 instrucciones SQL principales. Hay dos grupos distintos para instrucciones SQL:

- `db.sql` – la instrucción SQL completa, como `select * from customers where customer_id = 123`
- `db.sql_tokenized` – la instrucción SQL tokenizada, como `select * from customers where customer_id = ?`

Al analizar el desempeño de la base de datos, puede resultar útil tener en cuenta instrucciones SQL que solo se diferencien en sus parámetros como un elemento de lógica. Así pues, puede utilizar `db.sql_tokenized` al consultar. Sin embargo, sobre todo cuando le interese explicar planes, a veces es más útil examinar instrucciones SQL completas con parámetros y consultar agrupando por `db.sql`. Existe una relación principal-secundaria entre instrucciones SQL tokenizadas y completas, con varias instrucciones SQL completas (secundarias) agrupadas bajo la misma instrucción SQL tokenizada (principal).

El comando en este ejemplo es similar al comando en Recuperación del promedio de carga de base de datos para los eventos de espera principales. Sin embargo, el archivo query.json tiene los elementos indicados a continuación.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.sql_tokenized", "Limit": 10 }
    }
]
```

El siguiente ejemplo utiliza `db.sql_tokenized`.

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-29T00:00:00Z \
   --end-time   2018-10-30T00:00:00Z \
   --period-in-seconds 3600 \
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-29T00:00:00Z ^
   --end-time   2018-10-30T00:00:00Z  ^
   --period-in-seconds 3600 ^
   --metric-queries file://query.json
```

Este ejemplo consulta durante 24 horas, con un periodo de una hora en segundos.

El ejemplo especifica la métrica de `db.load.avg` y un `GroupBy` de los siete eventos de espera principales. Para obtener detalles acerca de los valores válidos para este ejemplo, consulte DimensionGroup en la Referencia de la API de Performance Insights.

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "AlignedStartTime": 1540771200.0,
    "AlignedEndTime": 1540857600.0,
    "Identifier": "db-XXX",

    "MetricList": [ //11 entries in the MetricList
        {
            "Key": { //First key is total
                "Metric": "db.load.avg"
            }
            "DataPoints": [ //Each DataPoints list has 24 per-hour Timestamps and a
 value
                {
                    "Value": 1.6964980544747081,
                    "Timestamp": 1540774800.0
```

```
                },
                //... 24 datapoints
            ]
        },
        {
            "Key": { //Next key is the top tokenized SQL
                "Dimensions": {
                    "db.sql_tokenized.statement": "INSERT INTO authors (id,name,email)
 VALUES\n( nextval(?)  ,?,?)",
                    "db.sql_tokenized.db_id": "pi-2372568224",
                    "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE"
                },
                "Metric": "db.load.avg"
            },
            "DataPoints": [ //... 24 datapoints
            ]
        },
        // In total 11 entries, 10 Keys of top tokenized SQL, 1 total key
    ] //End of MetricList
} //End of response
```

Esta respuesta tiene 11 entradas en la `MetricList` (1 total, 10 SQL tokenizadas principales) y cada entrada tiene 24 `DataPoints` por hora.

Para consultas SQL tokenizadas, hay tres entradas en cada lista de dimensiones:

- `db.sql_tokenized.statement`: la instrucción SQL tokenizada.
- `db.sql_tokenized.db_id` : el ID de base de datos nativo utilizado para hacer referencia a SQL, o un ID sintético que genera Performance Insights para usted si no se encuentra disponible el ID de base de datos nativo. Este ejemplo devuelve el ID sintético de `pi-2372568224`.
- `db.sql_tokenized.id`: el ID de la consulta dentro del panel Performance Insights.

  En la AWS Management Console, este ID se denomina ID de soporte. Se denomina así porque el ID es sobre datos que AWS Support puede examinar para ayudarle a solucionar un problema con la base de datos. AWS se toma muy en serio la seguridad y privacidad de sus datos, y casi todos los datos se almacenan encriptados con su clave AWS KMS. Por lo tanto, nadie dentro de AWS puede ver estos datos. En el ejemplo anterior, tanto `tokenized.statement` como `tokenized.db_id` se almacenan cifrados. Si tiene un problema con su base de datos, AWS Support puede ayudarle, ya que hace referencia al ID de Support.

Al realizar consultas, puede ser conveniente especificar un `Group` en `GroupBy`. Sin embargo, para un control de más precisión sobre los datos que se devuelven, especifique la lista de dimensiones. Por ejemplo, si todo lo que se necesita es `db.sql_tokenized.statement`, entonces se puede añadir un atributo `Dimensions` al archivo query.json.

```
[
    {
        "Metric": "db.load.avg",
        "GroupBy": {
            "Group": "db.sql_tokenized",
            "Dimensions":["db.sql_tokenized.statement"],
            "Limit": 10
        }
    }
]
```

Recuperación del promedio de carga de base de datos filtrado por SQL



La imagen anterior muestra que se ha seleccionado una consulta concreta y el gráfico de línea de área apilada de principales sesiones activas promedio se limita a esa consulta. Aunque se siguen consultando los siete eventos de espera generales principales, se filtra el valor de la respuesta. El filtro hace que solo tenga en cuenta las sesiones que coinciden con el filtro concreto.

La consulta de API correspondiente en este ejemplo es similar al comando en Recuperación del promedio de carga de base de datos para las instrucciones SQL principales. Sin embargo, el archivo query.json tiene los elementos indicados a continuación.

```
[
 {
        "Metric": "db.load.avg",
        "GroupBy": { "Group": "db.wait_event", "Limit": 5  },
        "Filter": { "db.sql_tokenized.id": "AKIAIOSFODNN7EXAMPLE" }
    }
]
```

Para Linux, macOS o Unix:

```
aws pi get-resource-metrics \
   --service-type RDS \
   --identifier db-ID \
   --start-time 2018-10-30T00:00:00Z \
   --end-time   2018-10-30T01:00:00Z \
   --period-in-seconds 60 \
   --metric-queries file://query.json
```

Para Windows:

```
aws pi get-resource-metrics ^
   --service-type RDS ^
   --identifier db-ID ^
   --start-time 2018-10-30T00:00:00Z ^
   --end-time   2018-10-30T01:00:00Z ^
   --period-in-seconds 60 ^
   --metric-queries file://query.json
```

La respuesta tiene un aspecto similar a la siguiente.

```
{
    "Identifier": "db-XXX",
    "AlignedStartTime": 1556215200.0,
    "MetricList": [
        {
            "Key": {
                "Metric": "db.load.avg"
            },
```

```
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 1.4878117913832196
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 1.192823803967328
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "io",
                    "db.wait_event.name": "wait/io/aurora_redo_log_flush"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 1.1360544217687074
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 1.058051341890315
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "io",
                    "db.wait_event.name": "wait/io/table/sql/handler"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.16241496598639457
                },
                {
```

```
                    "Timestamp": 1556222400.0,
                    "Value": 0.05163360560093349
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "synch",
                    "db.wait_event.name": "wait/synch/mutex/innodb/
aurora_lock_thread_slot_futex"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.11479591836734694
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.013127187864644107
                }
            ]
        },
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "CPU",
                    "db.wait_event.name": "CPU"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.05215419501133787
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.05805134189031505
                }
            ]
        },
```

```
        {
            "Key": {
                "Metric": "db.load.avg",
                "Dimensions": {
                    "db.wait_event.type": "synch",
                    "db.wait_event.name": "wait/synch/mutex/innodb/lock_wait_mutex"
                }
            },
            "DataPoints": [
                {
                    "Timestamp": 1556218800.0,
                    "Value": 0.017573696145124718
                },
                {
                    "Timestamp": 1556222400.0,
                    "Value": 0.002333722287047841
                }
            ]
        }
    ],
    "AlignedEndTime": 1556222400.0
} //end of response
```

En esta respuesta, todos los valores se filtran según la contribución del SQL tokenizado AKIAIOSFODNN7EXAMPLE especificado en el archivo query.json. Las claves también podrían seguir un orden distinto de una consulta sin un filtro, porque el SQL filtrado afectaba a los cinco eventos de espera principales.

Recuperación del texto completo de una instrucción SQL

En el siguiente ejemplo se recupera el texto completo de una instrucción SQL para una instancia de base de datos `db-10BCD2EFGHIJ3KL4M5NO6PQRS5`. El `--group` es `db.sql` y el `--group-identifier` es `db.sql.id`. En este ejemplo, *`my-sql-id`* representa un ID de SQL recuperado al invocar a `pi get-resource-metrics` o`pi describe-dimension-keys`.

Ejecute el siguiente comando de la .

Para Linux, macOS o Unix:

```
aws pi get-dimension-key-details \
   --service-type RDS \
   --identifier db-10BCD2EFGHIJ3KL4M5NO6PQRS5 \
   --group db.sql \
```

```
   --group-identifier my-sql-id \
   --requested-dimensions statement
```

Para Windows:

```
aws pi get-dimension-key-details ^
   --service-type RDS ^
   --identifier db-10BCD2EFGHIJ3KL4M5NO6PQRS5 ^
   --group db.sql ^
   --group-identifier my-sql-id ^
   --requested-dimensions statement
```

En este ejemplo, los detalles de las dimensiones están disponibles. Por lo tanto, Performance Insights recupera el texto completo de la instrucción SQL, sin truncarlo.

```
{
    "Dimensions":[
    {
        "Value": "SELECT e.last_name, d.department_name FROM employees e, departments d
 WHERE e.department_id=d.department_id",
        "Dimension": "db.sql.statement",
        "Status": "AVAILABLE"
    },
    ...
    ]
}
```

Creación de un informe de análisis de rendimiento para un período de tiempo

En el siguiente ejemplo, se crea un informe de análisis de rendimiento con la hora de inicio `1682969503` y la hora de finalización `1682979503` para la base de datos `db-loadtest-0`.

```
aws pi create-performance-analysis-report \
        --service-type RDS \
        --identifier db-loadtest-0 \
        --start-time 1682969503 \
        --end-time 1682979503 \
        --region us-west-2
```

La respuesta es el identificador único `report-0234d3ed98e28fb17` para el informe.

```
{
```

```
   "AnalysisReportId": "report-0234d3ed98e28fb17"
}
```

Recuperación de un informe de análisis de rendimiento

En el siguiente ejemplo se recuperan los detalles del informe de análisis del informe `report-0d99cc91c4422ee61`.

```
aws pi get-performance-analysis-report \
--service-type RDS \
--identifier db-loadtest-0 \
--analysis-report-id report-0d99cc91c4422ee61 \
--region us-west-2
```

La respuesta proporciona el estado del informe, el identificador, los detalles del tiempo y la información.

```
        {
    "AnalysisReport": {
        "Status": "Succeeded",
        "ServiceType": "RDS",
        "Identifier": "db-loadtest-0",
        "StartTime": 1680583486.584,
        "AnalysisReportId": "report-0d99cc91c4422ee61",
        "EndTime": 1680587086.584,
        "CreateTime": 1680587087.139,
        "Insights": [
           ... (Condensed for space)
        ]
    }
}
```

Enumeración de todos los informes de análisis de rendimiento de la instancia de base de datos

En el siguiente ejemplo se enumeran todos los informes de análisis de rendimiento disponibles para la base de datos `db-loadtest-0`.

```
aws pi list-performance-analysis-reports \
--service-type RDS \
--identifier db-loadtest-0 \
--region us-west-2
```

La respuesta enumera todos los informes con el ID del informe, el estado y los detalles del período de tiempo.


```
{
    "AnalysisReports": [
        {
            "Status": "Succeeded",
            "EndTime": 1680587086.584,
            "CreationTime": 1680587087.139,
            "StartTime": 1680583486.584,
            "AnalysisReportId": "report-0d99cc91c4422ee61"
        },
        {
            "Status": "Succeeded",
            "EndTime": 1681491137.914,
            "CreationTime": 1681491145.973,
            "StartTime": 1681487537.914,
            "AnalysisReportId": "report-002633115cc002233"
        },
        {
            "Status": "Succeeded",
            "EndTime": 1681493499.849,
            "CreationTime": 1681493507.762,
            "StartTime": 1681489899.849,
            "AnalysisReportId": "report-043b1e006b47246f9"
        },
        {
            "Status": "InProgress",
            "EndTime": 1682979503.0,
            "CreationTime": 1682979618.994,
            "StartTime": 1682969503.0,
            "AnalysisReportId": "report-01ad15f9b88bcbd56"
        }
    ]
}
```


Eliminación de un informe de análisis de rendimiento

En el siguiente ejemplo, se elimina el informe de análisis de la base de datos `db-loadtest-0`.

```
aws pi delete-performance-analysis-report \
--service-type RDS \
--identifier db-loadtest-0 \
```

```
--analysis-report-id report-0d99cc91c4422ee61 \
--region us-west-2
```

Adición de una etiqueta a un informe de análisis de rendimiento

En el siguiente ejemplo, se agrega una etiqueta con una clave `name` y valor `test-tag` al informe `report-01ad15f9b88bcbd56`.

```
aws pi tag-resource \
--service-type RDS \
--resource-arn arn:aws:pi:us-west-2:356798100956:perf-reports/RDS/db-loadtest-0/
report-01ad15f9b88bcbd56 \
--tags Key=name,Value=test-tag \
--region us-west-2
```

Enumeración de todas las etiquetas de un informe de análisis de rendimiento

En el ejemplo siguiente se enumeran todas las etiquetas del informe `report-01ad15f9b88bcbd56`.

```
aws pi list-tags-for-resource \
--service-type RDS \
--resource-arn arn:aws:pi:us-west-2:356798100956:perf-reports/RDS/db-loadtest-0/
report-01ad15f9b88bcbd56 \
--region us-west-2
```

La respuesta enumera el valor y la clave de todas las etiquetas agregadas al informe:

```
{
    "Tags": [
        {
            "Value": "test-tag",
            "Key": "name"
        }
    ]
}
```

Eliminación de etiquetas de un informe de análisis de rendimiento

En el siguiente ejemplo se elimina la etiqueta `name` de un informe `report-01ad15f9b88bcbd56`.

```
aws pi untag-resource \
```

```
--service-type RDS \
--resource-arn arn:aws:pi:us-west-2:356798100956:perf-reports/RDS/db-loadtest-0/
report-01ad15f9b88bcbd56 \
--tag-keys name \
--region us-west-2
```

Después de eliminar la etiqueta, llamar a la API `list-tags-for-resource` no muestra esta etiqueta.

Registro de llamadas de Performance Insights mediante el uso de AWS CloudTrail

Performance Insights se ejecuta con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Performance Insights. CloudTrail captura todas las llamadas a las API para Performance Insights como eventos. Esta captura incluye llamadas desde la consola de Amazon RDS y desde llamadas de código a las operaciones de la API de Performance Insights.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos eventos para Performance Insights. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail podrá determinar ciertos detalles. Esta información incluye la solicitud que se envió a Performance Insights, la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud y cuándo se realizó. También incluye detalles adicionales.

Para obtener más información sobre CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Trabajar con datos de Performance Insights en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce actividad en Performance Insights, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en la consola de CloudTrail en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail en la guía del usuario de AWS CloudTrail.

Para mantener un registro continuo de los eventos de su cuenta de AWS, incluidos los eventos de Performance Insights, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a

todas las regiones de AWS. El seguimiento registra los eventos de todas las regiones de AWS en la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas en la guía del usuario de:AWS CloudTrail

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las operaciones de Performance Insights que se documentan en la Referencia de la API de Performance Insights. Por ejemplo, las llamadas a las operaciones `DescribeDimensionKeys` y `GetResourceMetrics` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

Entradas del archivo de registro de Performance Insights

Un seguimiento es una configuración que permite la entrega de eventos como archivos de registro en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail contienen una o varias entradas de registro. Un evento representa una única solicitud desde cualquier origen. Cada evento incluye información acerca de la operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el ejemplo que sigue se muestra una entrada de registro de CloudTrail que ilustra la operación `GetResourceMetrics`.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
         "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "johndoe"
    },
    "eventTime": "2019-12-18T19:28:46Z",
    "eventSource": "pi.amazonaws.com",
    "eventName": "GetResourceMetrics",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "aws-cli/1.16.240 Python/3.7.4 Darwin/18.7.0 botocore/1.12.230",
    "requestParameters": {
        "identifier": "db-YTDU5J5V66X7CXSCVDFD2V3SZM",
        "metricQueries": [
            {
                "metric": "os.cpuUtilization.user.avg"
            },
            {
                "metric": "os.cpuUtilization.idle.avg"
            }
        ],
        "startTime": "Dec 18, 2019 5:28:46 PM",
        "periodInSeconds": 60,
        "endTime": "Dec 18, 2019 7:28:46 PM",
        "serviceType": "RDS"
    },
    "responseElements": null,
    "requestID": "9ffbe15c-96b5-4fe6-bed9-9fccff1a0525",
    "eventID": "08908de0-2431-4e2e-ba7b-f5424f908433",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

API de Información de rendimiento y puntos de conexión de VPC de interfaz (AWS PrivateLink)

Puede usar AWS PrivateLink para crear una conexión privada entre la VPC e Información de rendimiento de Amazon RDS. Puede acceder a Información de rendimiento como si estuviera en su VPC, sin utilizar una puerta de enlace de Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a Información de rendimiento.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a Información de rendimiento.

Para obtener más información, consulte Acceso a los Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink.

Consideraciones sobre Información de rendimiento

Antes de configurar un punto de conexión de interfaz para Información de rendimiento, consulte la sección Considerations en la Guía de AWS PrivateLink.

Información de rendimiento admite la realización de llamadas a todas las acciones de la API a través del punto de conexión de interfaz.

De forma predeterminada, el acceso completo a Información de rendimiento se permite a través del punto de conexión de interfaz. Para controlar el tráfico a Información de rendimiento a través del punto de conexión de interfaz, asocie un grupo de seguridad a las interfaces de red de los puntos de conexión.

Disponibilidad

La API de Información de rendimiento actualmente admite puntos de conexión de VPC en Regiones de AWS que admiten Información de rendimiento. Para obtener más información acerca de la disponibilidad de Información de rendimiento, consulte Regiones y motores de base de datos admitidos para Información sobre rendimiento en Amazon RDS .

Creación de un punto de conexión de interfaz para Información de rendimiento

Puede crear un punto de conexión de interfaz para Información de rendimiento mediante la consola de Amazon VPC o la AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink.

Cree un punto de conexión para Información de rendimiento utilizando el siguiente nombre de servicio:

Si habilita el DNS privado para el punto de conexión de interfaz, puede realizar solicitudes a la API para Información de rendimiento usando su nombre de DNS predeterminado para la región. Por ejemplo, `pi.us-east-1.amazonaws.com`.

Creación de una política de puntos de conexión de VPC para la API de Información de rendimiento

Una política de punto de conexión es un recurso de IAM que puede adjuntar a un punto de conexión de interfaz. La política de puntos de conexión predeterminada permite acceso completo a Información de rendimiento a través del punto de conexión de interfaz. Para controlar el acceso permitido a Información de rendimiento desde la VPC, adjunte una política de puntos de conexión personalizada al punto de conexión de interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink.

Ejemplo: Política de punto de conexión de VPC para acciones de Información de rendimiento

El siguiente es un ejemplo de una política de un punto de conexión personalizado. Cuando se asocia con un punto de conexión, esta política concede acceso a las acciones de Información de rendimiento mostradas para todas las entidades principales en todos los recursos.

```
{
```

```
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "rds:CreatePerformanceAnalysisReport",
            "rds:DeletePerformanceAnalysisReport",
            "rds:GetPerformanceAnalysisReport"
         ],
         "Resource":"*"
      }
   ]
}
```

Ejemplo: política de punto de enlace de la VPC que deniega todo el acceso desde una cuenta de AWS especificada

La siguiente política de punto de enlace de la VPC deniega a la cuenta de AWS `123456789012` todo el acceso a los recursos mediante el punto de enlace. La política permite todas las acciones de otras cuentas.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": { "AWS": [ "123456789012" ] }
     }
   ]
}
```

Direcciones IP de Información de rendimiento

Las direcciones IP permiten que los recursos de la VPC se comuniquen entre sí y con otros recursos a través de Internet. Información de rendimiento admite los protocolos de direcciones IPv4 e

IPv6. De forma predeterminada, Información de rendimiento y Amazon VPC utilizan el protocolo de direccionamiento IPv4. No puedes desactivar este comportamiento. Al crear una VPC, debe especificar un bloque de CIDR IPv4 (un intervalo de direcciones IPv4 privadas).

De manera opcional, puede asociar un bloque de CIDR IPv6 a su VPC y sus subredes y asignar direcciones IPv6 de dicho bloque a recursos de RDS de su subred. La compatibilidad con el protocolo IPv6 amplía el número de direcciones IP admitidas. Al utilizar el protocolo IPv6, se asegura de tener suficientes direcciones disponibles para el futuro crecimiento de Internet. Los recursos de RDS nuevos y existentes pueden utilizar direcciones IPv4 e IPv6 dentro de su VPC. Configurar, proteger y traducir el tráfico de red entre los dos protocolos utilizados en diferentes partes de una aplicación puede provocar sobrecarga operativa. Puede estandarizar el protocolo IPv6 para los recursos de Amazon RDS para simplificar la configuración de la red. Para obtener información sobre los puntos de conexión y las cuotas de servicios, consulte Amazon Relational Database Service endpoints and quotas.

Para obtener más información sobre el direccionamiento IP de Amazon RDS, consulte Direccionamiento IP de Amazon RDS.

Análisis de anomalías de rendimiento con Amazon DevOps Guru para Amazon RDS

Amazon DevOps Guru es un servicio de operaciones totalmente administrado que ayuda a los desarrolladores y operadores a mejorar el rendimiento y la disponibilidad de sus aplicaciones. DevOps Guru descarga las tareas asociadas a la identificación de problemas operativos para que pueda implementar rápidamente recomendaciones para mejorar su aplicación. Para obtener más información, consulte What is Amazon DevOps Guru? (¿Qué es Amazon DevOps Guru?) en la Guía del usuario de Amazon DevOps Guru.

DevOps Guru detecta, analiza y hace recomendaciones sobre problemas operativos existentes para todos los motores de base de datos de Amazon RDS. Para ampliar esta capacidad, DevOps Guru para RDS aplica machine learning a las métricas de Información sobre rendimiento de bases de datos RDS para PostgreSQL. Estas funciones de monitoreo permiten a DevOps Guru for RDS detectar y diagnosticar cuellos de botella en el rendimiento y recomendar acciones correctivas específicas. DevOps Guru para RDS también puede detectar condiciones problemáticas en la base de datos RDS para PostgreSQL antes de que se produzcan.

Ahora puede ver estas recomendaciones en la consola de RDS. Para obtener más información, consulte Recomendaciones para Amazon RDS.

El siguiente vídeo contiene información general de DevOps Guru para RDS.

Para profundizar en el tema, consulte la publicación del blog de Amazon DevOps Guru para RDS entre bastidores.

Temas

- Beneficios de DevOps Guru para RDS
- Cómo funciona DevOps Guru for RDS
- Configuración de DevOps Guru for RDS

Beneficios de DevOps Guru para RDS

Si es responsable de una base de datos RDS para PostgreSQL, es posible que no sepa que se está produciendo un evento o una regresión que está afectando a esa base de datos. Cuando aprenda sobre el problema, es posible que no sepa por qué está ocurriendo o qué hacer al respecto. En lugar

de recurrir a un administrador de base de datos (DBA) para obtener ayuda o confiar en herramientas de terceros, puede seguir las recomendaciones de DevOps Guru para RDS.

Obtiene las siguientes ventajas del análisis detallado de DevOps Guru para RDS:

Diagnóstico rápido

DevOps Guru para RDS monitorea y analiza continuamente la telemetría de bases de datos. Información sobre rendimiento, Monitorización mejorada y Amazon CloudWatch recopilan datos de telemetría de su instancia de base de datos. DevOps Guru para RDS utiliza técnicas estadísticas y de machine learning para extraer estos datos y detectar anomalías. Para obtener más información sobre los datos de telemetría, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS y Supervisión de las métricas del sistema operativo con supervisión mejorada en la Guía del usuario de Amazon RDS.

Resolución rápida

Cada anomalía identifica el problema del rendimiento y sugiere vías de investigación o medidas correctivas. Por ejemplo, DevOps Guru para RDS podría recomendar investigar eventos de espera específicos. O podría recomendarle que ajuste la configuración del grupo de aplicaciones para limitar el número de conexiones de base de datos. Según estas recomendaciones, puede resolver los problemas de rendimiento más rápido que mediante la solución de problemas de forma manual.

Información proactiva

DevOps Guru para RDS utiliza métricas de sus recursos para detectar posibles comportamientos problemáticos antes de que se conviertan en un problema mayor. Por ejemplo, puede detectar si la base de datos utiliza un número cada vez mayor de tablas temporales en el disco, lo que podría empezar a afectar al rendimiento. A continuación, DevOps Guru ofrece recomendaciones para ayudarle a solucionar los problemas antes de que se conviertan en problemas mayores.

Conocimiento profundo de los ingenieros de Amazon y machine learning

Para detectar problemas de rendimiento y ayudarle a resolver los cuellos de botella, DevOps Guru para RDS se basa en machine learning (ML) y fórmulas matemáticas avanzadas. Los ingenieros de bases de datos de Amazon contribuyeron al desarrollo de DevOps Guru para los resultados de RDS, que encapsulan muchos años de administración de cientos de miles de bases de datos. Al aprovechar este conocimiento colectivo, DevOps Guru for RDS puede enseñarle las mejores prácticas.

Cómo funciona DevOps Guru for RDS

DevOps Guru para RDS recopila datos sobre sus bases de datos RDS para PostgreSQL desde Información de rendimiento de Amazon RDS. La métrica más importante es `DBLoad`. DevOps Guru for RDS consume las métricas de Información sobre rendimiento, las analiza con machine learning y publica información en el panel de control.

La información es un conjunto de anomalías relacionadas que detecta DevOps Guru.

En DevOps Guru para RDS, una anomalía es un patrón que se desvía de lo que se considera un rendimiento normal para su base de datos RDS para PostgreSQL.

Información proactiva

La información proactiva le permite conocer el comportamiento problemático antes de que se produzca. Contiene anomalías con recomendaciones y métricas relacionadas para ayudarlo a abordar los problemas en sus bases de datos RDS para PostgreSQL antes de que se conviertan en problemas mayores. Esta información se publica en el panel de DevOps Guru.

Por ejemplo, DevOps Guru podría detectar que su base de datos RDS para PostgreSQL está creando muchas tablas temporales en el disco. Si no se soluciona este problema, esta tendencia podría provocar problemas de rendimiento. Cada información proactiva incluye recomendaciones sobre el comportamiento correctivo y enlaces a temas relevantes en Ajuste de RDS para PostgreSQL con información proactiva de Amazon DevOps Guru. Para obtener más información, consulte Working with insights in DevOps Guru (Trabajo con información en DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.

Información reactiva

La información reactiva identifica el comportamiento anómalo a medida que se produce. Si DevOps Guru para RDS detecta problemas de rendimiento en las instancias de bases de datos de RDS para PostgreSQL, publica información reactiva en el panel de DevOps Guru. Para obtener más información, consulte Working with insights in DevOps Guru (Trabajo con información en DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.

Anomalías causales

Una anomalía causal es una anomalía de nivel superior dentro de la información reactiva. Database load (DB load) (Carga de base de datos) es la anomalía causal de DevOps Guru for RDS.

Para medir el impacto del rendimiento, una anomalía asigna un nivel de gravedad de Alto, Mediano o Bajo. Para obtener más información, consulte Conceptos clave de DevOps Guru for RDS en la Guía del usuario de Amazon DevOps Guru.

Si DevOps Guru detecta una anomalía actual en la instancia de base de datos, se le avisará en la página Databases (Bases de datos) de la consola de RDS. La consola también le avisa de las anomalías que se han producido en las últimas 24 horas. Para ir a la página de anomalías desde la consola de RDS, elija el enlace del mensaje de alerta. La consola de RDS también le avisa en la página de la instancia de base de datos de PostgreSQL.

Anomalías contextuales

Una anomalía contextual es un resultado dentro de la carga de base de datos que está relacionada con una información reactiva. Cada anomalía contextual describe un problema de rendimiento específico de RDS para PostgreSQL que requiere investigación. Por ejemplo, DevOps Guru for RDS podría recomendar que considere aumentar la capacidad de la CPU o investigar los eventos de espera que contribuyen a la carga de la base de datos.

> **Important**
>
> Recomendamos que pruebe cualquier cambio en una instancia de prueba antes de modificar una instancia de producción para que pueda entender completamente el impacto de cada cambio. De esta forma, comprende el impacto del cambio.

Para obtener más información, consulte Analyzing anomalies in Amazon Aurora clusters (Análisis de anomalías en clústeres de Amazon RDS) en la Guía del usuario de Amazon DevOps Guru.

Configuración de DevOps Guru for RDS

Para permitir que DevOps Guru para Amazon RDS publique información para una base de datos de RDS para PostgreSQL, realice las siguientes tareas.

Temas

- Configuración de las políticas de acceso de IAM para DevOps Guru para RDS
- Activación de Información sobre rendimiento para sus instancias de base de datos de RDS para PostgreSQL
- Activación de DevOps Guru y especificación de la cobertura de recursos

Configuración de las políticas de acceso de IAM para DevOps Guru para RDS

Para ver las alertas de DevOps Guru en la consola de RDS, su usuario o rol de AWS Identity and Access Management (IAM) debe contar con alguna de las siguientes políticas:

- La política administrada de AWS `AmazonDevOpsGuruConsoleFullAccess`
- La política administrada de AWS `AmazonDevOpsGuruConsoleReadOnlyAccess` y cualquiera de las siguientes políticas:
  - La política administrada por AWS `AmazonRDSFullAccess`
  - Una política administrada por el cliente que incluya `pi:GetResourceMetrics` y `pi:DescribeDimensionKeys`

Para obtener más información, consulte Configuración de directivas de acceso para información sobre rendimiento.

Activación de Información sobre rendimiento para sus instancias de base de datos de RDS para PostgreSQL

DevOps Guru for RDS confía en Información sobre rendimiento para sus datos. Sin Información sobre rendimiento, DevOps Guru publica anomalías, pero no incluye análisis ni recomendaciones detallados.

Al crear o modificar una instancia de base de datos de RDS para PostgreSQL, puede activar Información sobre rendimiento. Para obtener más información, consulte Activación y desactivación de Información de rendimiento de Amazon RDS.

Activación de DevOps Guru y especificación de la cobertura de recursos

Puede activar DevOps Guru para que supervise sus bases de datos de RDS for PostgreSQL de cualquiera de las siguientes maneras.

Temas

- Activación de DevOps Guru en la consola de RDS
- Adición de recursos de RDS para PostgreSQL en la consola de DevOps Guru
- Adición de recursos de RDS para PostgreSQL mediante AWS CloudFormation

Activación de DevOps Guru en la consola de RDS

Puede seguir varias rutas en la consola de Amazon RDS para activar DevOps Guru.

Temas

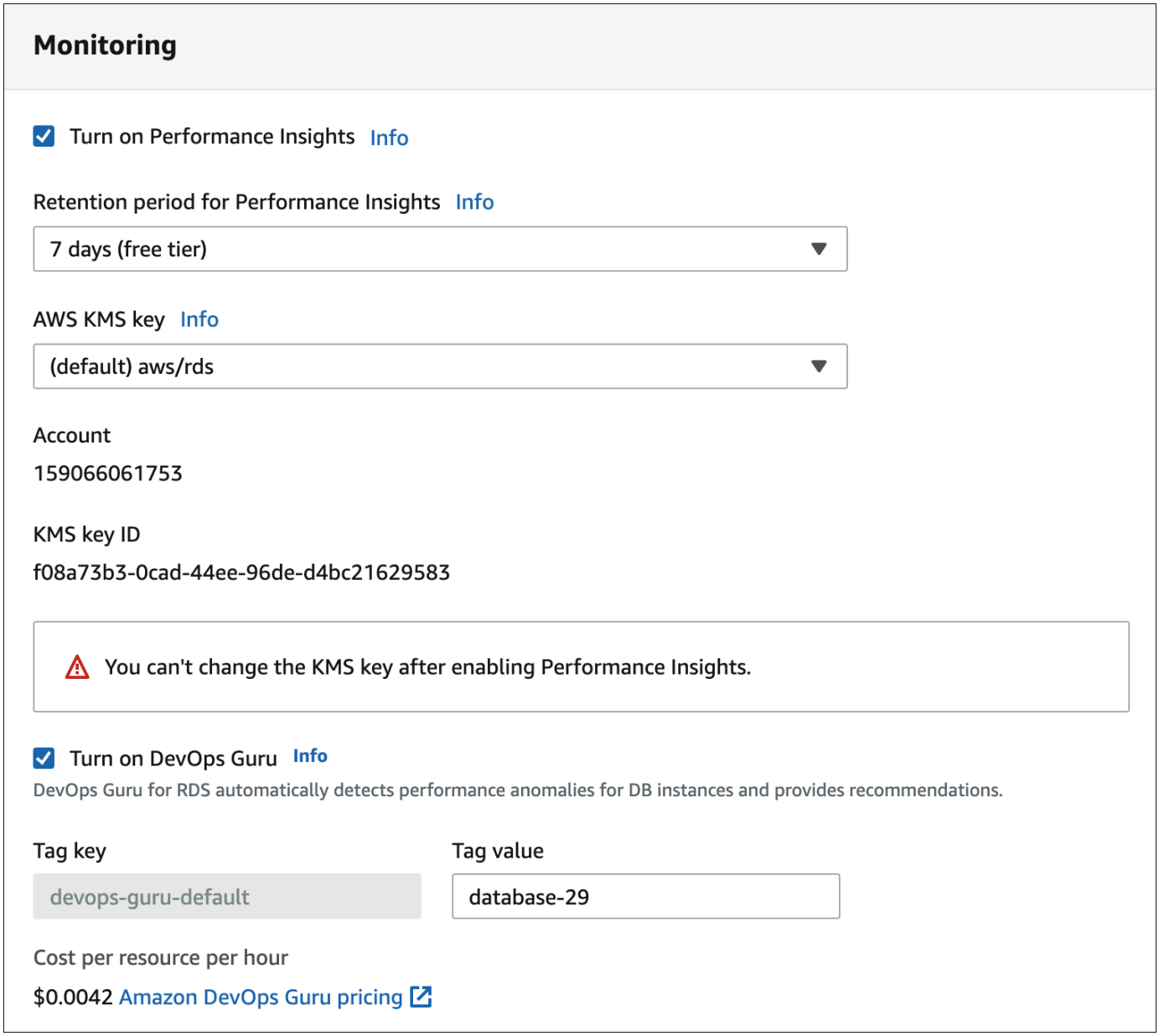
- Activación de DevOps Guru cuando crea una base de datos RDS para PostgreSQL
- Activación de DevOps Guru desde el banner de notificación
- Respuesta a un error de permisos al activar DevOps Guru

Activación de DevOps Guru cuando crea una base de datos RDS para PostgreSQL

El flujo de trabajo de creación incluye una configuración que activa la cobertura de DevOps Guru para su base de datos. Esta configuración se activa de forma predeterminada cuando elige la plantilla Production (Producción).

Para activar DevOps Guru cuando crea una base de datos RDS para PostgreSQL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Siga los pasos de Creación de una instancia de base de datos, hasta el paso en el que elige la configuración de supervisión pero sin incluirlo.
3. En Monitoring (Supervisión), elija Turn on Performance Insights (Activar Performance Insights). Para que DevOps Guru para RDS proporcione un análisis detallado de las anomalías de rendimiento, es necesario activar Performance Insights.
4. Elija Turn on DevOps Guru (Activar DevOps Guru).



5. Cree una etiqueta para la base de datos para que DevOps Guru pueda supervisarla. Haga lo siguiente:

   - En el campo de texto de Tag key (Clave de etiqueta), ingrese un nombre que comience por **`Devops-Guru-`**.
   - En el campo de texto de Tag value (Valor de etiqueta), ingrese cualquier valor. Por ejemplo, si especifica **`rds-database-1`** para el nombre de la base de datos RDS para PostgreSQL, también puede introducir **`rds-database-1`** como el valor de etiqueta.

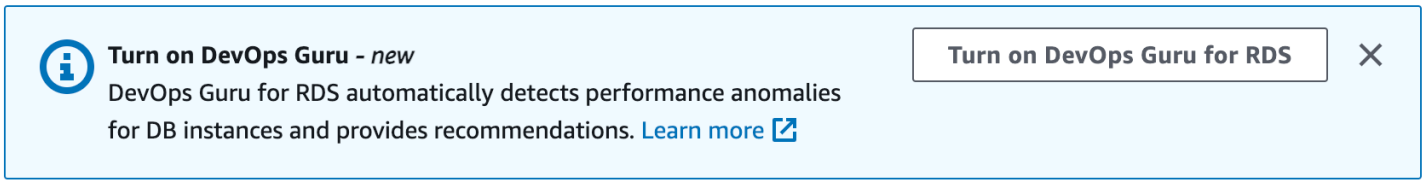
Para obtener más información sobre las etiquetas, consulte "Use tags to identify resources in your DevOps Guru applications" (Usar etiquetas para identificar los recursos en las aplicaciones de DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.

6. Complete los demás pasos proporcionados en Creación de una instancia de base de datos.

Activación de DevOps Guru desde el banner de notificación

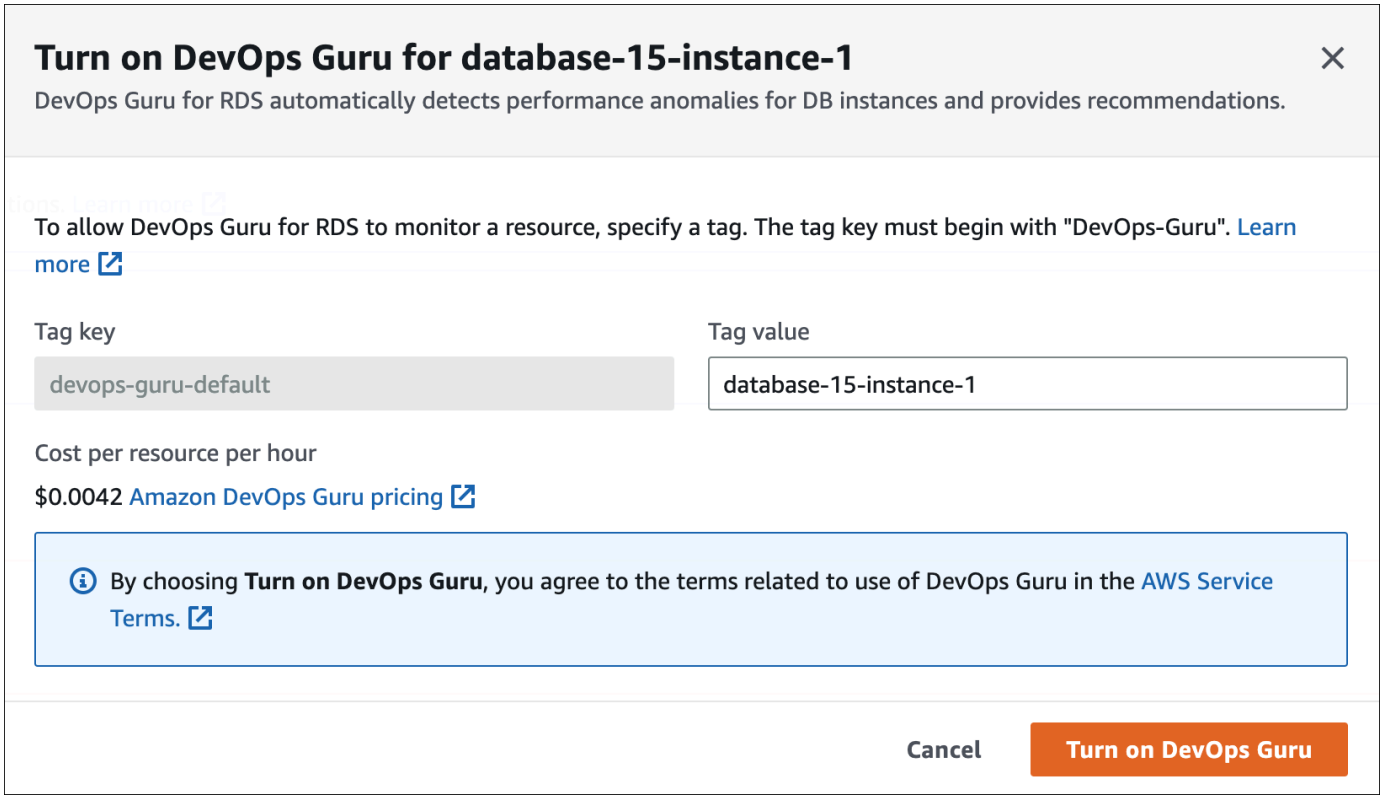
Si sus recursos no están cubiertos por DevOps Guru, Amazon RDS se lo notifica con un banner en las siguientes ubicaciones:

- La pestaña Monitoring (Supervisión) de una instancia de clúster de base de datos
- Panel de Performance Insights



Para activar DevOps Guru para su base de datos RDS para PostgreSQL

1. En el banner, elija Turn on DevOps Guru for RDS (Activar DevOps Guru para RDS).
2. Ingrese un nombre y un valor de la clave de la etiqueta. Para obtener más información sobre las etiquetas, consulte "Use tags to identify resources in your DevOps Guru applications" (Usar etiquetas para identificar los recursos en las aplicaciones de DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.



3. Elija Turn on DevOps Guru (Activar DevOps Guru).

Respuesta a un error de permisos al activar DevOps Guru

Si activa DevOps Guru desde la consola de RDS al crear una base de datos, es posible que RDS muestre el siguiente banner acerca de la ausencia de permisos.

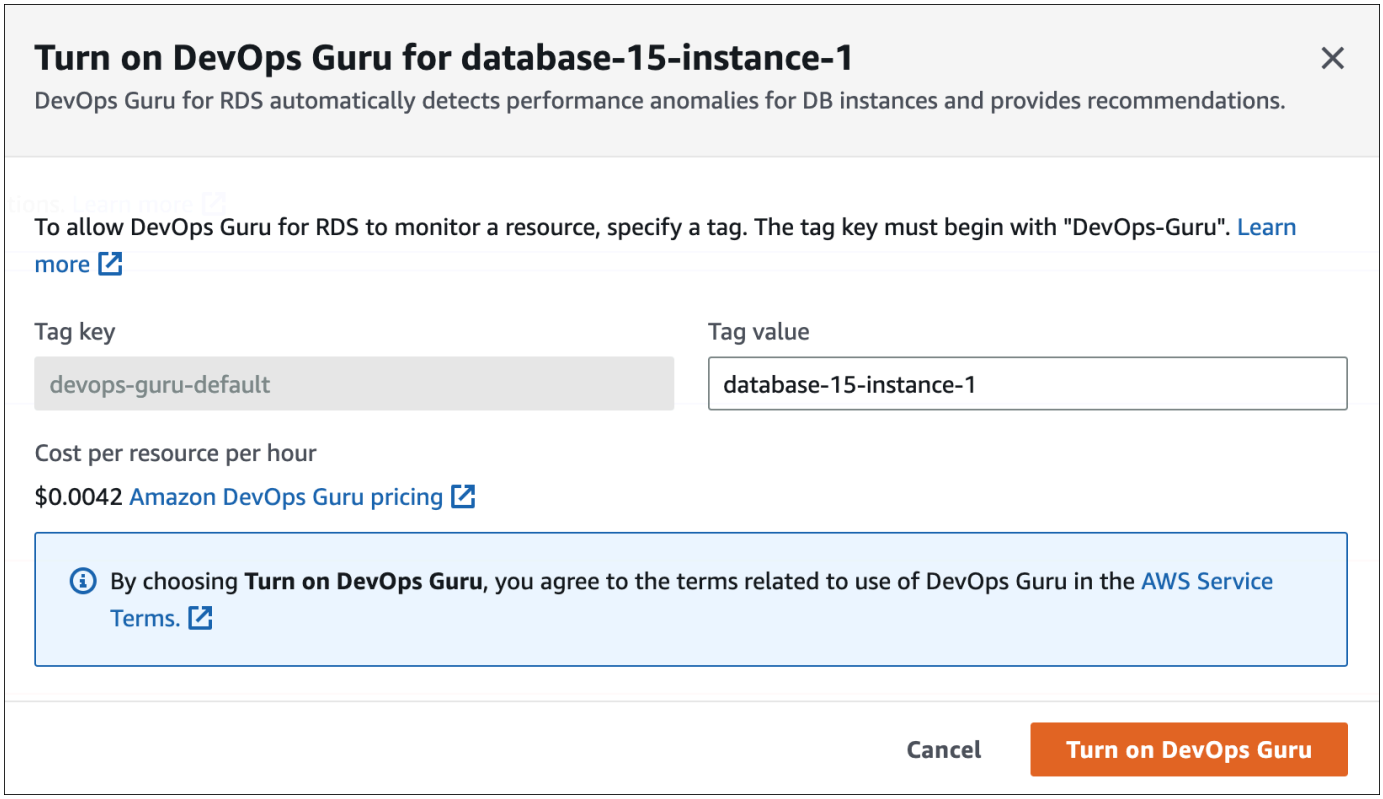


Para responder a un error de permisos

1. Conceda a su usuario o rol de IAM el rol administrado por el usuario `AmazonDevOpsGuruConsoleFullAccess`. Para obtener más información, consulte Configuración de las políticas de acceso de IAM para DevOps Guru para RDS.
2. Abra la consola de RDS.
3. En el panel de navegación, seleccione Información sobre rendimiento.
4. Elija una instancia de base de datos en el clúster que acaba de crear.
5. Elija el conmutador para activar DevOps Guru para RDS.

DevOps Guru for RDS

6. Elija un valor de etiqueta. Para obtener más información, consulte "Use tags to identify resources in your DevOps Guru applications" (Usar etiquetas para identificar los recursos en las aplicaciones de DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.



7. Elija Turn on DevOps Guru (Activar DevOps Guru).

Adición de recursos de RDS para PostgreSQL en la consola de DevOps Guru

Puede especificar su cobertura de recursos de DevOps Guru en la consola de DevOps Guru. Siga el paso descrito en Specify your DevOps Guru resource coverage (Especifique su cobertura de recursos DevOps Guru) en la Guía del usuario de Amazon DevOps Guru. Cuando edite los recursos analizados, elija una de las siguientes opciones:

- Elija Todos los recursos de la cuenta para analizar todos los recursos admitidos, como las bases de datos RDS para PostgreSQL, en su Cuenta de AWS y región.
- Elija Pilas de CloudFormation para analizar las bases de datos RDS para PostgreSQL que se encuentran en las pilas que usted elija. Para obtener más información, consulte el tema sobre usar pilas de AWS CloudFormation para identificar los recursos en sus aplicaciones de DevOps Guru en la Guía del usuario de Amazon DevOps Guru.

- Elija Etiquetas para analizar las bases de datos RDS para PostgreSQL que ha etiquetado. Para obtener más información, consulte Use tags to identify resources in your DevOps Guru applications (Usar etiquetas para identificar los recursos en las aplicaciones de DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.

Para obtener más información, consulte Enable DevOps Guru (Habilitar DevOps Guru) en la Guía del usuario de Amazon DevOps Guru.

Adición de recursos de RDS para PostgreSQL mediante AWS CloudFormation

Puede utilizar etiquetas para añadir cobertura de sus recursos de RDS para PostgreSQL a sus plantillas de CloudFormation. En el siguiente procedimiento, se asume que tiene una plantilla de CloudFormation tanto para la instancia de base de datos de RDS para PostgreSQL como para la pila de DevOps Guru.

Para especificar una instancia de base de datos de RDS para PostgreSQLmediante una etiqueta de CloudFormation

1. En la plantilla de CloudFormation para su instancia de base de datos, defina una etiqueta mediante un par clave/valor.

   En el siguiente ejemplo, se asigna el valor `my-db-instance1` a `Devops-guru-cfn-default` para una instancia de base de datos de RDS para PostgreSQL.

   ```
   MyDBInstance1:
     Type: "AWS::RDS::DBInstance"
     Properties:
       DBInstanceIdentifier: my-db-instance1
       Tags:
         - Key: Devops-guru-cfn-default
           Value: devopsguru-my-db-instance1
   ```

2. En la plantilla de CloudFormation de su pila de DevOps Guru, especifique la misma etiqueta en el filtro de recopilación de recursos.

   En el siguiente ejemplo, se configura DevOps Guru para proporcionar cobertura para el recurso con el valor de etiqueta `my-db-instance1`.

   ```
   DevOpsGuruResourceCollection:
     Type: AWS::DevOpsGuru::ResourceCollection
   ```

```
  Properties:
    ResourceCollectionFilter:
      Tags:
        - AppBoundaryKey: "Devops-guru-cfn-default"
          TagValues:
          - "devopsguru-my-db-instance1"
```

En el siguiente ejemplo, se proporciona cobertura para todos los recursos dentro del límite de la aplicación `Devops-guru-cfn-default`.

```
DevOpsGuruResourceCollection:
  Type: AWS::DevOpsGuru::ResourceCollection
  Properties:
    ResourceCollectionFilter:
      Tags:
        - AppBoundaryKey: "Devops-guru-cfn-default"
          TagValues:
          - "*"
```

Para obtener más información, consulte AWS::DevOpsGuru::ResourceCollection y AWS::RDS::DBInstance en la Guía del usuario de AWS CloudFormation.

Supervisión de las métricas del sistema operativo con Supervisión mejorada

Con la supervisión mejorada, puede monitorear el sistema operativo de su instancia de base de datos en tiempo real. Cuando desea ver cómo diferentes procesos o subprocesos usan la CPU, las métricas de monitorización mejoradas son útiles.

Temas

- Descripción general de la supervisión mejorada
- Configuración y habilitación del monitoreo mejorado
- Visualización de métricas OS en la consola de RDS
- Visualización de métricas del sistema operativo mediante CloudWatch Logs

Descripción general de la supervisión mejorada

Amazon RDS proporciona métricas en tiempo real para el sistema operativo (SO) en el que se ejecuta la instancia de base de datos. Puede ver todas las métricas del sistema y la información de procesos de las instancias de base de datos de RDS en la consola. Puede administrar las métricas que desea monitorear para cada instancia y personalizar el panel de acuerdo con sus requisitos. Para ver descripciones de métricas de la supervisión mejorada, consulte Métricas del sistema operativo en Supervisión mejorada.

RDS entrega las métricas de la monitorización mejorada a su cuenta de registros de Amazon Cloudwatch. Puede crear filtros de métricas en CloudWatch desde CloudWatch Logs y mostrar los gráficos en el panel de CloudWatch. Además, puede consumir la salida JSON de monitorización mejorada desde registros de Amazon Cloudwatch en un sistema de monitoreo de su elección. Para obtener más información, consulte Monitorización mejorada en las preguntas frecuentes de Amazon RDS.

Temas

- Disponibilidad del monitoreo mejorado
- Diferencias entre métricas de monitoreo mejorado y CloudWatch
- Retención de métricas de supervisión mejorada
- Costo de la monitorización mejorada

Disponibilidad del monitoreo mejorado

La monitorización mejorada está disponible para los siguientes motores de base de datos:

- Db2
- MariaDB
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL

El monitoreo mejorado está disponible para todas las clases de instancia de base de datos, excepto la clase db.m1.small.

Diferencias entre métricas de monitoreo mejorado y CloudWatch

Un hipervisor crea y ejecuta máquinas virtuales (VM). Mediante el uso de un hipervisor, una instancia puede admitir varias máquinas virtuales invitadas al compartir virtualmente memoria y CPU. CloudWatch recopila métricas sobre el uso de la CPU del hipervisor para una instancia de base de datos. Por el contrario, la supervisión mejorada recopila sus métricas de un agente en la instancia de base de datos.

Podría encontrar diferencias entre CloudWatch y las medidas de supervisión mejorada, porque la capa del hipervisor realiza una pequeña cantidad de trabajo. Las diferencias pueden ser mayores si sus instancias de base de datos utilizan clases de instancia más pequeñas. En este escenario, es probable que la capa de hipervisor administre más máquinas virtuales (VM) en una única instancia física.

Para ver descripciones de métricas de la supervisión mejorada, consulte Métricas del sistema operativo en Supervisión mejorada. Para obtener más información sobre las métricas de CloudWatch, consulte la Guía del usuario de Amazon CloudWatch.

Retención de métricas de supervisión mejorada

Las métricas de supervisión mejorada se almacenan de forma predeterminada en CloudWatch Logs durante 30 días. Este periodo de retención es diferente de las métricas típicas de CloudWatch.

Para modificar la cantidad de tiempo que se almacenan las métricas en CloudWatch Logs, cambie la retención del grupo de registros `RDSOSMetrics` en la consola de CloudWatch. Para obtener más

información, consulte Cambiar la retención de datos de registro en CloudWatch Logs en la registros de Amazon Cloudwatch User Guide.

Costo de la monitorización mejorada

Las métricas de supervisión mejorada se almacenan en CloudWatch Logs en lugar de en las métricas de Cloudwatch. El costo de la monitorización mejorada depende de los factores siguientes:

- Se le cobrará por la monitorización mejorada solo si supera el nivel gratuito que proporciona registros de Amazon Cloudwatch. Los cargos se basan en las tasas de transferencia de datos y almacenamiento de CloudWatch Logs.
- La cantidad de información transferida para una instancia de RDS es directamente proporcional a la granularidad definida para la función de monitorización mejorada. Un intervalo de monitorización más corto deriva en informes más frecuentes de métricas del SO y aumenta el costo de la monitorización. Para administrar los costos, establezca diferentes granularidades para diferentes instancias en sus cuentas.
- Los costos de uso de la monitorización mejorada se aplican en cada instancia de base de datos para la que está habilitada dicha monitorización. Monitorizar un gran números de instancias de base de datos es más costoso que monitorizar tan solo unas cuantas.
- Las instancias de base de datos que admiten una carga de trabajo con computación más intensiva tienen más actividad de proceso de SO de la que informar y costos más elevados de monitorización mejorada.

Para obtener más información acerca de los precios, consulte Precios de Amazon CloudWatch.

Configuración y habilitación del monitoreo mejorado

Para utilizar el Monitoreo mejorado, debe crear un rol de IAM y, a continuación, habilitar el Monitoreo mejorado.

Temas

- Creación de un rol de IAM para el monitoreo mejorado
- Activación y desactivación de la supervisión mejorada
- Protección contra el problema del suplente confuso

Creación de un rol de IAM para el monitoreo mejorado

La monitorización mejorada necesita permiso para actuar en su nombre y enviar información de métrica del SO a CloudWatch Logs. Puede conceder los permisos necesarios para Enhanced Monitoring mediante un rol de AWS Identity and Access Management (IAM). Puede crear este rol al habilitar la supervisión mejorada o crearla con anticipación.

Temas

- Creación del rol de IAM cuando habilita el monitoreo mejorado
- Creación del rol de IAM antes de habilitar el monitoreo mejorado

Creación del rol de IAM cuando habilita el monitoreo mejorado

Cuando habilita el monitoreo mejorado en la consola de RDS, con Amazon RDS se puede crear el rol de IAM que usted necesite. El rol se denomina `rds-monitoring-role`. RDS utiliza este rol para la instancia de base de datos, la réplica de lectura o el clúster de base de datos Multi-AZ especificados.

Cómo crear el rol de IAM cuando se habilita el monitoreo mejorado

1. Siga los pasos de Activación y desactivación de la supervisión mejorada.
2. Establezca el Monitoring Role (Rol de monitoreo) en Default (Predeterminado) en el paso en el que elija un rol.

Creación del rol de IAM antes de habilitar el monitoreo mejorado

Puede crear el rol necesario antes de habilitar el monitoreo mejorado. Cuando habilite el monitoreo mejorado, especifique el nombre del rol nuevo. Debe crear este rol necesario si habilita la monitorización mejorada mediante la AWS CLI o la API de RDS.

Se debe conceder al usuario que habilite la monitorización mejorada el permiso `PassRole`. A fin de obtener más información, consulte el Ejemplo 2 en Concesión de permisos a un usuario para transferir un rol a un servicio de AWS en la Guía del usuario de IAM.

Para crear un rol de IAM para el monitoreo mejorado de Amazon RDS

1. Abra la consola de IAM en https://console.aws.amazon.com.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.

4. Elija la pestaña Servicio de AWS y, a continuación, elija RDS de la lista de servicios.
5. Elija RDS - Enhanced Monitoring (RDS - Supervisión mejorada) y, a continuación, elija Next (Siguiente).
6. Asegúrese de que en Permissions policies (Políticas de permisos) se muestra AmazonRDSEnhancedMonitoringRole y, a continuación, elija Next (Siguiente).
7. Escriba un nombre para el rol en Nombre de rol. Por ejemplo, escriba **`emaccess`**.

   La entidad de confianza para su rol es el servicio de AWS monitoring.rds.amazonaws.com.
8. Seleccione Crear rol.

Activación y desactivación de la supervisión mejorada

Puede administrar Supervisión mejorada mediante la AWS Management Console, la AWS CLI o la API de RDS. Puede establecer diferentes niveles de detalle para la recopilación de métricas en cada instancia de base de datos.

Consola

Puede activar la Supervisión mejorada cuando crea una instancia de base de datos, un clúster de base de datos Multi-AZ o una réplica de lectura, o cuando modifica una instancia de base de datos o un clúster de base de datos Multi-AZ. Si modifica una instancia de base de datos para activar Supervisión mejorada, no necesita reiniciar la instancia de base de datos para que se efectúe el cambio.

Puede activar la Supervisión mejorada en la consola de RDS cuando realiza una de las siguientes acciones en la página Databases (Bases de datos).

- Crear una instancia de base de datos o un clúster de base de datos Multi-AZ: elija Create database (Crear base de datos).
- Crear una réplica de lectura: elija Actions (Acciones) y, luego, Create read replica (Crear una réplica de lectura).
- Modificación de una instancia de base de datos o clúster de base de datos multi-AZ: elija la opción Modificar.

Para activar o desactivar la supervisión mejorada en la consola de RDS

1. Desplácese a Additional configuration (Configuración adicional).

2. En Supervisión, elija Habilitar la monitorización mejorada para la instancia de base de datos o réplica de lectura. Anule la selección de la opción para deshabilitar Supervisión mejorada.
3. Establezca la propiedad Monitoring Role (Rol de monitorización) en el rol de IAM que ha creado para permitir que Amazon RDS se comunique con registros de Amazon Cloudwatch, o bien elija Default (Predeterminado) para que RDS cree un rol denominado `rds-monitoring-role`.
4. Establezca la propiedad Nivel de detalle en el intervalo (en segundos) entre puntos cuando se recopilan métricas para la instancia de base de datos, o réplica de lectura. La propiedad Granularity puede establecerse en uno de los siguientes valores: `1`, `5`, `10`, `15`, `30` o `60`.

   La velocidad más rápida a la que la consola de RDS se actualiza es cada 5 segundos. Si establece la granularidad en 1 segundo en la consola de RDS, seguirá viendo métricas actualizadas solo cada 5 segundos. Puede recuperar actualizaciones de métricas de 1 segundo mediante CloudWatch Logs.

AWS CLI

Para activar la Supervisión mejorada mediante la AWS CLI, en los siguientes comandos, establezca la opción `--monitoring-interval` en un valor distinto de `0` y establezca la opción `--monitoring-role-arn` en el rol que creó en Creación de un rol de IAM para el monitoreo mejorado.

- create-db-instance
- create-db-instance-read-replica
- modify-db-instance
- create-db-clúster (Clúster de base de datos Multi-AZ)
- modify-db-clúster (Clúster de base de datos Multi-AZ)

La opción `--monitoring-interval` especifica el intervalo (en segundos) entre puntos cuando se recopilan métricas de monitoreo mejorado. Los valores válidos para la opción son `0`, `1`, `5`, `10`, `15`, `30` y `60`.

Para desactivar la supervisión mejorada mediante AWS CLI, establezca la opción `--monitoring-interval` en `0` en los siguientes comandos.

Example

El siguiente ejemplo activa la Supervisión mejorada para una instancia de base de datos:

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --monitoring-interval 30 \
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --monitoring-interval 30 ^
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Example

El siguiente ejemplo activa la Supervisión mejorada para una instancia de base de datos Multi-AZ:

Para Linux, macOS o Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --monitoring-interval 30 \
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

Para Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --monitoring-interval 30 ^
    --monitoring-role-arn arn:aws:iam::123456789012:role/emaccess
```

API de RDS

Para activar la supervisión mejorada mediante la API de RDS, establezca el parámetro `MonitoringInterval` en un valor distinto de `0` y establezca el parámetro `MonitoringRoleArn` en el rol que creó en Creación de un rol de IAM para el monitoreo mejorado. Establezca estos parámetros en las siguientes acciones:

- CreateDBInstance
- CreateDBInstanceReadReplica

- ModifyDBInstance
- CreateDBclúster (Clúster de base de datos Multi-AZ)
- ModifyDBclúster (Clúster de base de datos Multi-AZ)

El parámetro `MonitoringInterval` especifica el intervalo (en segundos) entre puntos cuando se recopilan métricas de monitoreo mejorado. Los valores válidos son `0`, `1`, `5`, `10`, `15`, `30` y `60`.

Para desactivar la supervisión mejorada mediante la API de RDS, establezca `MonitoringInterval` en `0`.

Protección contra el problema del suplente confuso

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puedes manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta. Para obtener más información, consulte El problema del suplente confuso.

Para limitar los permisos al recurso que Amazon RDS puede dar a otro servicio, se recomienda utilizar las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en una política de confianza para el rol de supervisión mejorada. Si utiliza ambas claves de contexto de condición global, deben usar el mismo ID de cuenta.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Para Amazon RDS, establezca `aws:SourceArn` en `arn:aws:rds:`*`Region`*`:`*`my-account-id`*`:db:`*`dbname`*.

En los siguientes ejemplos se utilizan las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en una política de confianza para evitar el problema del suplente confuso.

JSON

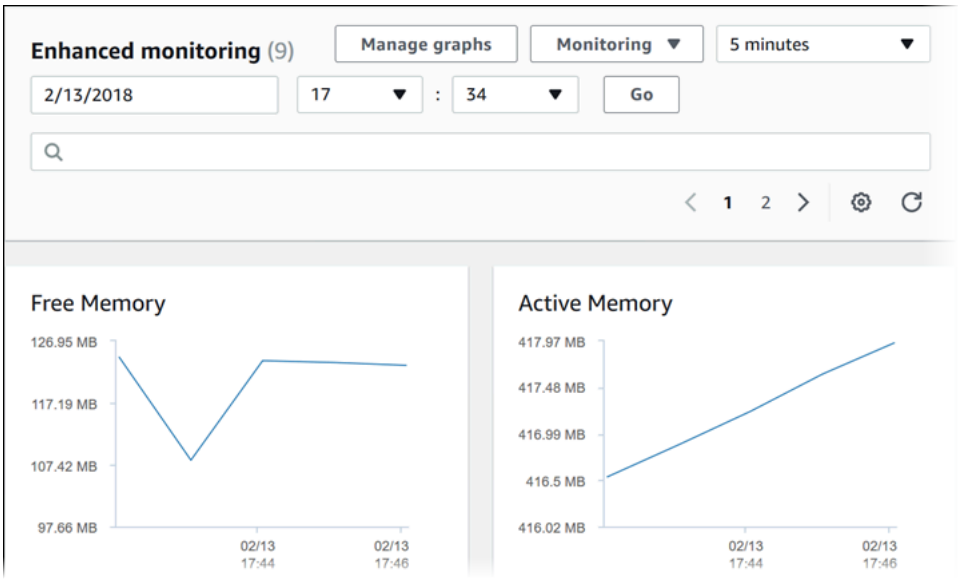
```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "monitoring.rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:rds:Region:my-account-id:db:dbname"
        },
        "StringEquals": {
          "aws:SourceAccount": "my-account-id"
        }
      }
    }
  ]
}
```

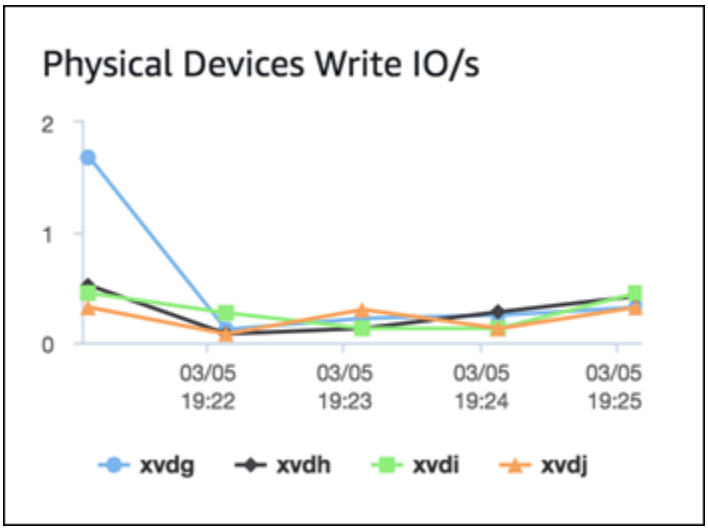
Visualización de métricas OS en la consola de RDS

Puede ver las métricas del SO informadas por la monitorización mejorada en la consola de RDS si elige Enhanced monitoring (Monitorización mejorada) para Monitoring (Monitorización).

El siguiente ejemplo muestra la página Supervisión mejorada. Para ver descripciones de métricas de la supervisión mejorada, consulte Métricas del sistema operativo en Supervisión mejorada.

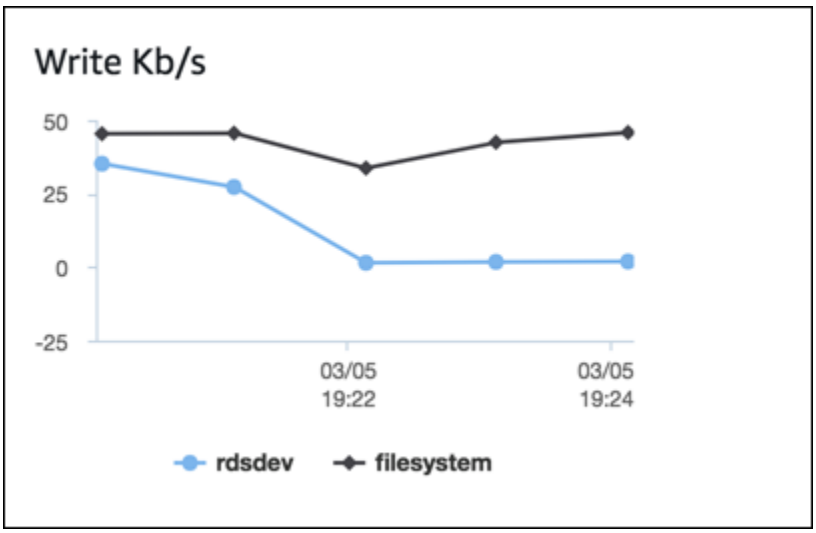


Algunas instancias de base de datos utilizan más de un disco para el volumen de almacenamiento de datos de la instancia de base de datos. En esas instancias de base de datos, los gráficos Physical Devices (Dispositivos físicos) muestran las métricas para cada uno de los discos. Por ejemplo, el siguiente gráfico muestra las métricas para cuatro discos.

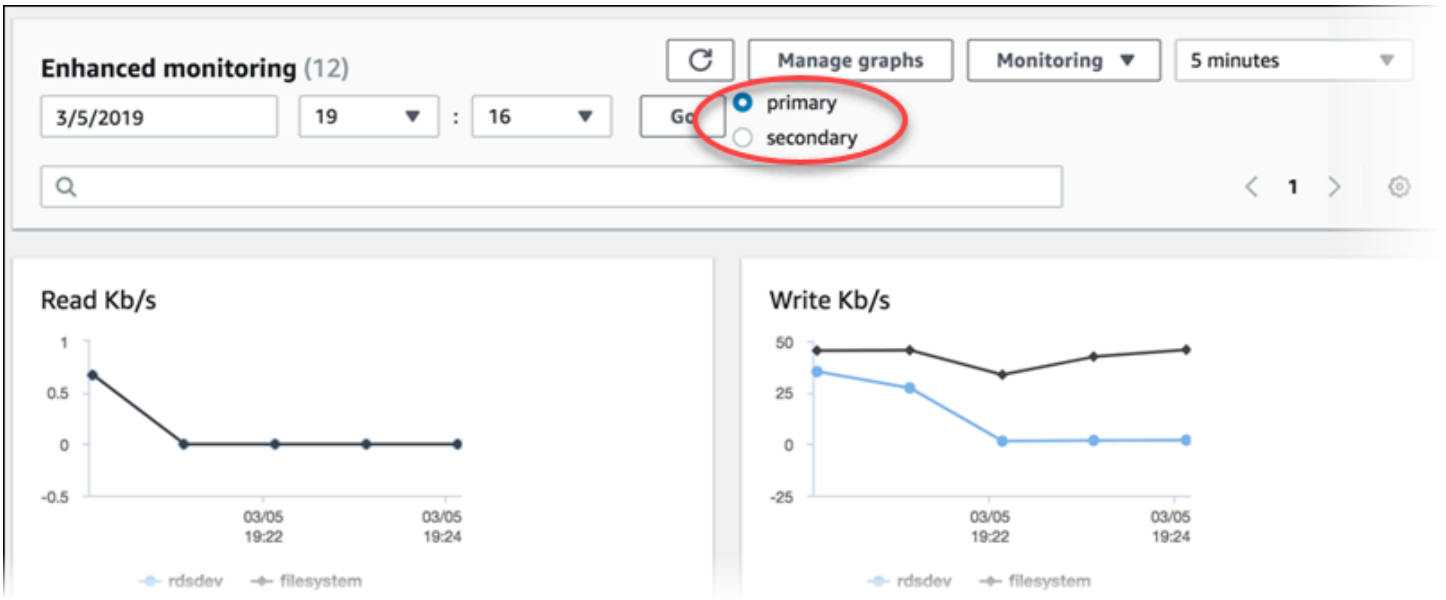


> **Note**
>
> Actualmente, los gráficos Physical Devices (Dispositivos físicos) no están disponibles para instancias de base de datos de Microsoft SQL Server.

Cuando visualiza gráficos de E/S de disco y sistema de archivos agregados, el dispositivo rdsdev se relaciona con el sistema de archivos `/rdsdbdata`, donde se guardan todos los archivos de base de datos y registros. El dispositivo filesystem se relaciona con el sistema de archivos `/` (también conocido como "raíz"), donde se almacenan los archivos relacionados con el sistema operativo.



Si la instancia de base de datos es una implementación Multi-AZ, puede ver las métricas del sistema operativo para la instancia de base de datos principal y su réplica en espera Multi-AZ. En la vista Enhanced monitoring (Monitorización mejorada), elija primary (principal) para ver las métricas del sistema operativo para la instancia de base de datos principal, o elija secondary (secundario) para ver las métricas del sistema operativo para la réplica en espera.

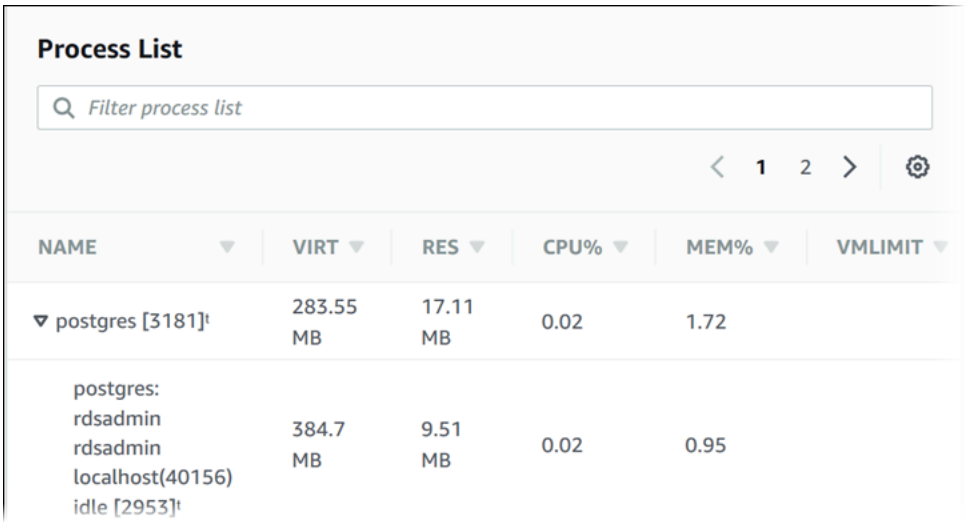


Para obtener más información sobre las implementaciones Multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

> **Note**
>
> Actualmente, no se admite la visualización de métricas del sistema operativo para una réplica en espera Multi-AZ para instancias de base de datos de MariaDB.

Si desea ver detalles para los procesos que se ejecutan en su instancia de base de datos, elija OS process list (Lista de procesos del SO) para Monitoring (Monitorización).

A continuación, se muestra la vista Process List (Lista de procesos).



La métrica de monitorización mejorada que se muestra en la vista Process list (Lista de procesos) se organiza de la siguiente manera:

- RDS child processes (Procesos secundarios de RDS): muestra un resumen de los procesos de RDS que admiten la instancia de base de datos, por ejemplo `mysqld` para instancias de base de datos de MySQL. Los subprocesos aparecen anidados debajo del proceso principal. Los subprocesos solo muestran el uso de la CPU, ya que otras métricas son iguales para todos los subprocesos. La consola muestra un máximo de 100 procesos y subprocesos. Los resultados son una combinación de los principales procesos y subprocesos que consumen memoria y CPU. Si hay más de 50 procesos y más de 50 subprocesos, la consola muestra los 50 consumidores principales de cada categoría. Esta pantalla le ayuda a identificar qué procesos están teniendo mayor impacto en el desempeño.
- Procesos de RDS: muestra un resumen de los recursos utilizados por el agente de administración de RDS, los procesos de monitoreo de diagnóstico y otros procesos de AWS que son necesarios para admitir instancias de base de datos de RDS.

- OS processes (Procesos de SO)–: muestra un resumen del kernel y de los procesos del sistema, que por lo general tienen un impacto mínimo en el rendimiento.

Los elementos enumerados para cada proceso son los siguientes:

- VIRT–: muestra el tamaño virtual del proceso.
- RES–: muestra la memoria física real que utiliza el proceso.
- CPU% (% de CPU): muestra el porcentaje de ancho de banda de CPU total que consume el proceso.
- MEM% (% de memoria): muestra el porcentaje de memoria total que utiliza el proceso.

Los datos de monitorización que se muestran en la consola de RDS se obtienen de registros de Amazon Cloudwatch. También puede obtener la métrica para una instancia de base de datos en forma de flujo de registro de CloudWatch Logs. Para obtener más información, consulte Visualización de métricas del sistema operativo mediante CloudWatch Logs.

La métrica de monitorización mejorada no se devuelve durante las siguientes situaciones:

- Una conmutación por error de la instancia de base de datos.
- Cambio de la clase de una instancia de base de datos (escalado del cómputo).

La métrica de monitorización mejorada se devuelve al reiniciar una instancia de base de datos porque solo se reinicia el motor de la base de datos. Se sigue informando de la métrica correspondiente al sistema operativo.

Visualización de métricas del sistema operativo mediante CloudWatch Logs

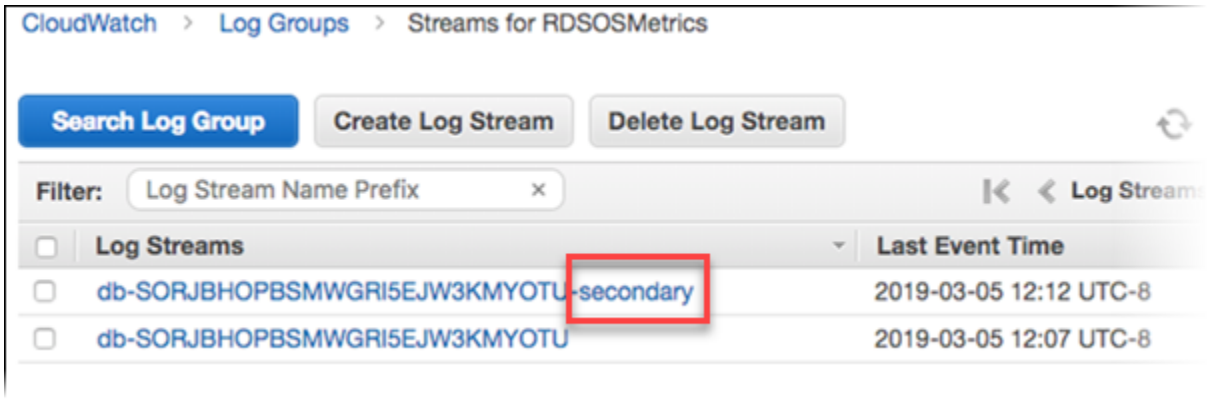
Una vez habilitada la Supervisión mejorada para la instancia de base de datos o el clúster de base de datos Multi-AZ, puede ver las métricas mediante CloudWatch Logs, con cada flujo de registro que representa una sola instancia de base de datos o un clúster de base de datos bajo supervisión. El identificador de flujo de registros es el identificador de recursos (`DbiResourceId`) para la instancia de base de datos o el clúster de base de datos.

Para ver los datos de registro de la Supervisión mejorada

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.

2. Si es necesario, elija la Región de AWS en la que se encuentra su instancia de base de datos o clúster de base de datos Multi-AZ. Para obtener más información, consulte Regiones y puntos de enlace en la Referencia general de Amazon Web Services.
3. En el panel de navegación, elija Logs.
4. Elija RDSOSMetrics en la lista de grupos de registro.

   En una implementación de instancia de base de datos Multi-AZ, los archivos de registro con el nombre adjunto `-secondary` son para la réplica en espera de Multi-AZ.



5. Elija el flujo de registro que desea ver en la lista de flujos de registro.

Referencia de métricas para Amazon RDS

En esta referencia, encontrará descripciones de las métricas de Amazon RDS para Amazon CloudWatch, Información sobre rendimiento y Supervisión mejorada.

Temas

- Métricas de Amazon CloudWatch para Amazon RDS
- Dimensiones de Amazon CloudWatch para Amazon RDS.
- Métricas de Amazon CloudWatch para Información de rendimiento de Amazon RDS
- Métricas de contador de Información de rendimiento
- Estadísticas de SQL para Performance Insights
- Métricas del sistema operativo en Supervisión mejorada

Métricas de Amazon CloudWatch para Amazon RDS

Las métricas de Amazon CloudWatch proporcionan información sobre el rendimiento y el estado de las instancias y los clústeres de Amazon RDS, lo que le permite supervisar el comportamiento del sistema y tomar decisiones basadas en datos. Estas métricas ayudan a realizar un seguimiento de la utilización de los recursos, la actividad de la base de datos y la eficiencia operativa, además de ofrecer visibilidad del rendimiento de las instancias.

En esta referencia se describen las métricas específicas disponibles para Amazon RDS y se explica cómo interpretarlas y utilizarlas para optimizar el rendimiento de la base de datos, solucionar problemas y garantizar una alta disponibilidad.

Amazon RDS publica métricas en Amazon CloudWatch en los espacios de nombres `AWS/RDS` y `AWS/Usage`.

Temas

- Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS
- Métricas de uso de Amazon CloudWatch para Amazon RDS

Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS

El espacio de nombres `AWS/RDS` de Amazon CloudWatch incluye las siguientes métricas de nivel de instancia.

> **Note**
>
> Es posible que la consola de Amazon RDS muestre métricas en unidades distintas de las unidades enviadas a Amazon CloudWatch. Por ejemplo, la consola de Amazon RDS es posible que muestre una métrica en megabytes (MB), mientras que la métrica se envía a Amazon CloudWatch en bytes.

Métrica	Descripción	Se aplica a	Unidades
`BinLogDiskUsage`	La cantidad de espacio en disco ocupado por los registros binarios. Si las copias de seguridad automáticas están habilitadas para las instancias de MySQL y MariaDB, incluidas las réplicas de lectura, se crean registros binarios.	MariaDB MySQL	Bytes
`BurstBalance`	El porcentaje de créditos de E/S del bucket por ráfaga SSD de uso general (gp2) disponibles.	Todos	Porcentaje
`CheckpointLag`	El tiempo transcurrido desde el punto de control más reciente.		Segundos
`ConnectionAttempts`	Número de intentos de conexión a una instancia, tanto si se han realizado correctamente como si no.	MySQL	Recuento
`CPUUtilization`	El porcentaje de utilización de CPU.	Todos	Porcentaje
`CPUCreditUsage`	La cantidad de créditos de CPU gastados por la instancia para la utilización de la CPU. Un crédito de CPU es igual a una vCPU que se ejecuta al 100 % durante un minuto o una combinación equivalente de		Créditos (vCPU/minutos)

Métrica	Descripción	Se aplica a	Unidades
	vCPU, uso y tiempo. Por ejemplo, puede tener una vCPU que se ejecuta al 50 % durante dos minutos o dos vCPU que se ejecutan al 25 % durante dos minutos. Esta métrica solo se aplica a las instancias de `db.t2`, `db.t3` y `db.t4g`. **Note** Recomendamos que las clases de instancia de base de datos T se utilicen solo para los servidores de desarrollo y de pruebas, o para otros servidores que no se utilicen para la producción. Para obtener más detalles sobre las clases de instancia T, consulte Tipos de clase de instancia de base de datos. Las métricas de créditos de CPU solo están disponibles cada cinco minutos. Si especifica un periodo superior a cinco minutos, use la estadística `Sum` en lugar de `Average`.		

Métrica	Descripción	Se aplica a	Unidades
`CPUCredit Balance`	La cantidad de créditos de la CPU obtenidos que una instancia ha acumulado desde que se lanzó o se inició. Para T2 Standard, el `CPUCredit Balance` incluye además el número de créditos de inicialización que se han acumulado. Los créditos se acumulan en el saldo de créditos una vez obtenidos y se eliminan del saldo de créditos cuando se gastan. El saldo de créditos tiene un límite máximo, determinado por el tamaño de la instancia. Una vez que se ha alcanzado el límite, los nuevos créditos obtenidos se descartarán. Para T2 Standard, los créditos de lanzamien to no cuentan para el límite. Los créditos de `CPUCreditBalance` están disponibles para que la instancia los gaste para aumentar la utilización de la CPU por encima de la referencia. Cuando una instancia está en ejecución , los créditos en el `CPUCredit Balance` no caducan. Cuando se detiene la instancia, el `CPUCredit Balance` no persiste y se pierden todos los créditos acumulados. Las métricas de créditos de CPU solo están disponibles cada cinco minutos. Esta métrica solo se aplica a las instancias de `db.t2`, `db.t3` y `db.t4g`.		Créditos (vCPU/ minutos)

Métrica	Descripción	Se aplica a	Unidades
	Note Recomendamos que las clases de instancia de base de datos T se utilicen solo para los servidores de desarrollo y de pruebas, o para otros servidores que no se utilicen para la producción. Para obtener más detalles sobre las clases de instancia T, consulte Tipos de clase de instancia de base de datos. Los créditos de lanzamiento funcionan de la misma manera en Amazon RDS que en Amazon EC2. Para obtener más información, consulte el tema sobre créditos de lanzamiento en la guía del usuario de Amazon Elastic Compute Cloud para instancias de Linux.		

Métrica	Descripción	Se aplica a	Unidades
`CPUSurplusCreditBalance`	La cantidad de créditos sobrantes que ha gastado una instancia ilimitada cuando su valor `CPUCreditBalance` es igual a cero. El valor de `CPUSurplusCreditBalance` se compensa con los créditos de CPU obtenidos. Si el número de créditos sobrantes supera el número máximo de créditos que la instancia puede ganar en un periodo de 24 horas, los créditos sobrantes gastados por encima del máximo implican un cargo adicional. Las métricas de créditos de CPU solo se encuentran disponibles cada 5 minutos.	Todos	Créditos (vCPU/minutos)

Métrica	Descripción	Se aplica a	Unidades
`CPUSurplusCreditsCharged`	La cantidad de créditos sobrantes gastados que no se han compensado con créditos de CPU obtenido y, por lo tanto, implican un cargo adicional. Los créditos sobrantes gastados se cobran cuando se da alguno de los casos siguientes: • Los créditos sobrantes gastados superan el número máximo de créditos que la instancia puede obtener en un periodo de 24 horas. Los créditos sobrantes gastados por encima de la cantidad máxima se cobran al final de la hora. • La instancia se detiene o se termina. • La instancia se cambia de `unlimited` a `standard`. Las métricas de créditos de CPU solo se encuentran disponibles cada 5 minutos.	Todos	Créditos (vCPU/minutos)

Métrica	Descripción	Se aplica a	Unidades
`DatabaseConnections`	El número de conexiones de red de cliente a la instancia de base de datos. El número de sesiones de base de datos puede ser superior al valor de métrica porque el valor de métrica no incluye lo siguiente: • Sesiones que ya no tienen conexión de red, pero que la base de datos no ha limpiado. • Sesiones creadas por el motor de base de datos para sus propios fines. • Sesiones creadas por las capacidades de ejecución paralela del motor de base de datos. • Sesiones creadas por el programador de trabajos del motor de base de datos • Conexiones de Amazon RDS	Todos	Recuento
`DiskQueueDepth`	El número de operaciones de E/S pendientes (solicitudes de lectura/escritura) a la espera de obtener acceso al disco.	Todos	Recuento
`DiskQueueDepthLogVolume`	El número de operaciones de E/S pendientes (solicitudes de lectura/escritura) a la espera de obtener acceso al disco de volumen de registro.	Instancias de bases de datos con volumen de registro específico habilitado	Recuento

Métrica	Descripción	Se aplica a	Unidades
`EBSByteBalance%`	El porcentaje de créditos de rendimiento que quedan en el bucket de ráfaga de la base de datos RDS. Esta métrica solo está disponible para la monitorización básica. El valor de la métrica se basa en el rendimiento de todos los volúmenes, lo que incluye el volumen raíz, y no solo de los volúmenes que contienen archivos de base de datos. Para encontrar los tamaños de instancia que admiten esta métrica, consulte los tamaños de instancia con un asterisco (*) en la tabla EBS optimizado de forma predeterminada en la Guía del usuario de Amazon EC2. La estadística `Sum` no es aplicable a esta métrica.	Todos	Porcentaje

Métrica	Descripción	Se aplica a	Unidades
`EBSIOBalance%`	El porcentaje de créditos de E/S que quedan en el bucket de ráfaga de la base de datos RDS. Esta métrica solo está disponible para la monitorización básica. El valor de la métrica se basa en las IOPS de todos los volúmenes, incluido el volumen raíz, y no solo de los volúmenes que contienen archivos de base de datos. Para encontrar cuáles son los tamaños de instancia que admiten esta métrica, consulte Tipos de instancias optimizadas para Amazon EBS en la Guía del usuario de Amazon EC2. La estadística `Sum` no es aplicable a esta métrica. Esta métrica es diferente de `BurstBalance` . Para obtener información sobre cómo utilizar esta métrica, consulte Improving application performance and reducing costs with Amazon EBS-Optimized Instance burst capability.	Todos	Porcentaje
`FailedSQLServerAgentJobsCount`	El número de trabajos de Microsoft SQL Server Agent que han producido algún error durante el último minuto.	Microsoft SQL Server	Recuento por minuto

Métrica	Descripción	Se aplica a	Unidades
`FreeableMemory`	La cantidad de memoria de acceso aleatorio disponible. Para las instancias de base de datos de MariaDB, MySQL y PostgreSQL, esta métrica informa del valor del campo `MemAvailable` de `/proc/meminfo` .	Todos	Bytes
`FreeLocalStorage`	La cantidad de espacio de almacenamiento local disponible. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Bytes

Métrica	Descripción	Se aplica a	Unidades
`FreeLocalStoragePercent`	El porcentaje de espacio de almacenamiento local disponible. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Porcentaje
`FreeStorageSpace`	La cantidad de espacio de almacenamiento disponible.	Todos	Bytes
`FreeStorageSpaceLogVolume`	La cantidad de espacio de almacenamiento disponible en el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Bytes
`IamDbAuthConnectionRequests`	El número de solicitudes de conexión que utilizan la autenticación de IAM a la instancia de base de datos.	Todos	Recuento

Métrica	Descripción	Se aplica a	Unidades
`MaximumUsedTransactionIDs`	El número máximo de ID de transacción que se han utilizado.	PostgreSQL	Recuento
`NetworkReceiveThroughput`	El tráfico de red de entrada (recepción) en la instancia de base de datos, incluidos el tráfico de base de datos del cliente y el tráfico de Amazon RDS utilizado en monitoreo y replicación.	Todos	Bytes por segundo
`NetworkTransmitThroughput`	El tráfico de red de salida (transmisión) en la instancia de base de datos, incluidos el tráfico de base de datos del cliente y el tráfico de Amazon RDS utilizado en monitoreo y replicación.	Todos	Bytes por segundo
`OldestLogicalReplicationSlotLag`	El volumen de retardo de Amazon RDS confirma una transacción en la base de datos de origen y el momento en que RDS aplica la transacción en la base de datos de réplica.	PostgreSQL	Bytes
`OldestReplicationSlotLag`	El tamaño de retardo de la réplica con mayor retardo en cuanto a los datos de registro de escritura anticipada (WAL) recibidos.	PostgreSQL	Bytes
`ReadIOPS`	Número medio de operaciones de E/S de lectura en disco por segundo.	Todos	Recuento por segundo

Métrica	Descripción	Se aplica a	Unidades
`ReadIOPSLocalStorage`	Número promedio de operaciones de E/S de lectura en disco a almacenamiento local por segundo. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Recuento por segundo
`ReadIOPSLogVolume`	Número medio de operaciones de E/S de lectura en disco por segundo para el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Recuento por segundo
`ReadLatency`	Tiempo medio de cada operación de E/S en el disco.	Todos	Segundos

Métrica	Descripción	Se aplica a	Unidades
`ReadLatencyLocalStorage`	Tiempo promedio que toma cada operación de E/S en disco para el almacenamiento local. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Segundos
`ReadLatencyLogVolume`	Tiempo medio de cada operación de E/S en el disco para el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Segundos
`ReadThroughput`	El número medio de bytes leídos del disco por segundo.	Todos	Bytes por segundo

Métrica	Descripción	Se aplica a	Unidades
`ReadThroughputLocalStorage`	Número promedio de bytes leídos en el disco por segundo para el almacenamiento local. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Bytes por segundo
`ReadThroughputLogVolume`	El número medio de bytes leídos del disco por segundo para el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Bytes por segundo

Métrica	Descripción	Se aplica a	Unidades
`ReplicaLag`	Para configuraciones de réplica de lectura, la cantidad de tiempo que una instancia de base de datos de réplica de lectura se retrasa con respecto a la instancia de base de datos de origen. Se aplica a las réplicas de lectura de MariaDB, Microsoft SQL Server, MySQL, Oracle y PostgreSQL. Para clústeres de base de datos Multi-AZ, la diferencia de tiempo entre la última transacción en la instancia de base de datos del escritor y la última transacción aplicada en una instancia de base de datos del lector.		Segundos
`ReplicationChannelLag`	Para configuraciones de réplica de varios orígenes, la cantidad de tiempo que un canal en particular de la réplica de varios orígenes se retrasa con respecto a la instancia de base de datos de origen. Para obtener más información, consulte the section called “Monitorización de canales de replicación de varios orígenes”.	MySQL	Segundos
`ReplicationSlotDiskUsage`	El espacio de disco utilizado por los archivos de ranura de la replicación.	PostgreSQL	Bytes

Métrica	Descripción	Se aplica a	Unidades
`SwapUsage`	La cantidad de espacio de intercambio utilizado en la instancia de base de datos.	MariaDB MySQL Oracle PostgreSQL	Bytes
`TempDbAvailableDataSpace`	La cantidad de espacio de datos disponible en tempdb y en el volumen en el que se encuentra tempdb. Utilice esta métrica para supervisar la disponibilidad del espacio de datos de tempdb y planificar la capacidad en consecuencia. Los valores bajos pueden indicar la necesidad de aumentar el almacenamiento u optimizar las consultas que utilizan mucho tempdb.	SQL Server	Bytes
`TempDbAvailableLogSpace`	La cantidad de espacio de registro disponible en tempdb y en el volumen en el que se encuentra tempdb. Utilice esta métrica para supervisar la disponibilidad del espacio en el registro de tempdb y evitar que el registro de transacciones se llene. Es fundamental para cargas de trabajo con transacciones grandes o alta concurrencia que generan actividad de registro significativa.	SQL Server	Bytes

Métrica	Descripción	Se aplica a	Unidades
`TempDbDataFileUsage`	El porcentaje de archivos de datos utilizados en tempdb. Esta métrica no tiene en cuenta el posible crecimiento de los archivos. Utilice esta métrica para supervisar la utilización de los archivos de datos de tempdb e identificar posibles cuellos de botella del rendimiento. Los valores altos pueden indicar la necesidad de optimizar las consultas que crean objetos temporales de gran tamaño o aumentar el tamaño de tempdb.	SQL Server	Porcentaje
`TempDbLogFileUsage`	El porcentaje de archivos de registro utilizados en tempdb. Esta métrica no tiene en cuenta el posible crecimiento de los archivos. Utilice esta métrica para supervisar la utilización del archivo de registro tempdb y evitar problemas de rendimiento. Los valores altos pueden indicar transacciones de larga duración o una actividad de registro excesiva que podría afectar al rendimiento general de la base de datos.	SQL Server	Porcentaje
`TransactionLogsDiskUsage`	El espacio de disco utilizado por los registros de transacciones.	PostgreSQL	Bytes
`TransactionLogsGeneration`	El tamaño de los registros de transacciones generados por segundo.	PostgreSQL	Bytes por segundo

Métrica	Descripción	Se aplica a	Unidades
`WriteIOPS`	Número medio de operaciones de E/S de escritura en disco por segundo.	Todos	Recuento por segundo
`WriteIOPSLocalStorage`	El número medio de operaciones de E/S de escritura en disco por segundo en el almacenamiento local. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Recuento por segundo
`WriteIOPSLogVolume`	Número medio de operaciones de E/S de escritura en disco por segundo para el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Recuento por segundo
`WriteLatency`	Tiempo medio de cada operación de E/S en el disco.	Todos	Segundos

Métrica	Descripción	Se aplica a	Unidades
`WriteLatencyLocalStorage`	Tiempo promedio que toma cada operación de E/S en disco para el almacenamiento local. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Segundos
`WriteLatencyLogVolume`	Tiempo medio de cada operación de E/S en el disco para el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Segundos
`WriteThroughput`	Número medio de bytes que se escriben en el disco por segundo.	Todos	Bytes por segundo

Métrica	Descripción	Se aplica a	Unidades
`WriteThroughputLogVolume`	Número medio de bytes que se escriben en el disco por segundo para el volumen del registro.	Instancias de bases de datos con volumen de registro específico habilitado	Bytes por segundo
`WriteThroughputLocalStorage`	Número promedio de bytes escritos en el disco por segundo para el almacenamiento local. Esta métrica solo se aplica a las clases de instancias de base de datos con volúmenes de almacén de instancias SSD NVMe. Para obtener información sobre las instancias de Amazon EC2 con volúmenes de almacén de instancias SSD NVMe, consulte el tema sobre volúmenes de almacén de instancias. Las clases de instancias de base de datos de RDS equivalentes tienen los mismos volúmenes de almacén de instancias. Por ejemplo, las clases de instancias de base de datos db.m6gd y db.r6gd tienen volúmenes de almacén de instancias de SSD NVMe.		Bytes por segundo

Métricas de uso de Amazon CloudWatch para Amazon RDS

El espacio de nombres `AWS/Usage` de Amazon CloudWatch incluye métricas de uso en el nivel de cuenta para sus cuotas de servicio de Amazon RDS. CloudWatch recopila métricas de uso automáticamente para todas las Regiones de AWS.

Para obtener más información, consulte Uso de métricas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch. Para obtener más información acerca de las cuotas, consulte Cuotas y restricciones para Amazon RDS y Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Métrica	Descripción	Unidades*
`AllocatedStorage`	El almacenamiento total para todas las instancias de base de datos La suma excluye las instancias de migración temporales.	Gigabytes
`AuthorizationsPerDBSecurityGroup`	Es el número de reglas de entrada por grupo de seguridad de base de datos de su Cuenta de AWS. El valor utilizado es el número más alto de reglas de entrada en un grupo de seguridad de base de datos de la cuenta. Es posible que otros grupos de seguridad de base de datos de la cuenta tengan un número menor de reglas de entrada.	Recuento
`CustomEndpointsPerDBCluster`	Es el número de puntos de conexión personalizados por clúster de base de datos de su Cuenta de AWS. El valor utilizado es el número más alto de puntos de conexión personalizados en un clúster de base de datos de la cuenta. Es posible que otros clústeres de bases de datos de la cuenta tengan un número inferior de puntos de conexión personalizados.	Recuento
`CustomEngineVersions`	Es el número de versiones de motor personalizado (CEV) para Amazon RDS Custom en su Cuenta de AWS.	Recuento
`DBClusterParameterGroups`	El número de grupos de parámetros del clúster de base de datos en la Cuenta de AWS. El recuento excluye los grupos de parámetros predeterminados.	Recuento
`DBClusterRoles`	Es el número de roles de AWS Identity and Access Management (IAM) asociados por clúster de base de datos en su Cuenta de AWS. El valor utilizado es el número máximo de roles de IAM asociados a un clúster de base de datos de la cuenta. Es posible que otros clústeres de	Recuento

Métrica	Descripción	Unidades*
	bases de datos de la cuenta tengan un número inferior de roles de IAM asociados.	
DBClusters	El número de clústeres de base de datos de Amazon Aurora en la Cuenta de AWS.	Recuento
DBInstanceRoles	Es el número de roles de AWS Identity and Access Management (IAM) asociados por instancia de base de datos en su Cuenta de AWS. El valor utilizado es el número máximo de roles de IAM asociados a una instancia de base de datos de la cuenta. Es posible que otras instancias de bases de datos de la cuenta tengan un número inferior de roles de IAM asociados.	Recuento
DBInstances	El número de instancias de base de datos de la Cuenta de AWS.	Recuento
DBParameterGroups	El número de grupos de parámetros de base de datos de la Cuenta de AWS. El recuento excluye los grupos de parámetros de base de datos predeterminados.	Recuento
DBSecurityGroups	El número de grupos de seguridad de la Cuenta de AWS. El recuento excluye el grupo de seguridad predeterminado y el grupo de seguridad de VPC predeterminado.	Recuento
DBSubnetGroups	El número de grupos de subredes de base de datos de la Cuenta de AWS. El recuento excluye el grupo de subred predeterminado.	Recuento
EventSubscriptions	El número de suscripciones de notificación de eventos en la Cuenta de AWS.	Recuento
Integrations	El número de integraciones sin ETL con Amazon Redshift en la Cuenta de AWS.	Recuento

Métrica	Descripción	Unidades*
`ManualClusterSnapshots`	El número de instantáneas de clúster de base de datos creadas manualmente en la Cuenta de AWS. El recuento excluye las instantáneas no válidas.	Recuento
`ManualSnapshots`	El número de instantáneas de base de datos creadas manualmente en la Cuenta de AWS. El recuento excluye las instantáneas no válidas.	Recuento
`OptionGroups`	El número de grupos de opciones de la Cuenta de AWS. El recuento excluye los grupos de opciones predeterminados.	Recuento
`Proxies`	Es el número de proxies de RDS en su cuenta de AWS.	Recuento
`ReadReplicasPerMaster`	Es el número de réplicas de lectura por instancia de base de datos en la cuenta. El valor utilizado es el número máximo de réplicas de lectura para una instancia de base de datos de la cuenta. Es posible que otras instancias de bases de datos de la cuenta tengan un número inferior de réplicas de lectura.	Recuento
`ReservedDBInstances`	El número de instancias de base de datos reservadas en la Cuenta de AWS. El recuento excluye las instancias retiradas o rechazadas.	Recuento
`SubnetsPerDBSubnetGroup`	Número de subredes por grupo de subredes de base de datos en su Cuenta de AWS. Es el número más alto de subredes de un grupo de subredes de base de datos de la cuenta. Es posible que otros grupos de subredes de base de datos de la cuenta tengan un número menor de subredes.	Recuento

> **Note**
>
> Amazon RDS no publica unidades para métricas de uso en CloudWatch. Las unidades solo aparecen en la documentación.

Dimensiones de Amazon CloudWatch para Amazon RDS.

Los datos de las métricas de Amazon RDS se pueden filtrar usando cualesquiera de las dimensiones de la tabla siguiente:

Dimensión	Filtrar los datos solicitados por…
`DBInstanceIdentifier`	Una instancia de base de datos específica.
`DatabaseClass`	Todas las instancias de una clase de base de datos. Por ejemplo, puede agregar métricas para todas las instancias que pertenezcan a la clase de base de datos `db.r5.large` .
`EngineName`	Sólo el nombre del motor identificado. Por ejemplo, puede agregar métricas para todas las instancias que tengan el nombre de motor `postgres`.
`SourceRegion`	Use la región especificada. Por ejemplo, puede agregar métricas para todas las instancias de bases de datos de la `us-east-1` región.

Métricas de Amazon CloudWatch para Información de rendimiento de Amazon RDS

Performance Insights publica automáticamente algunas métricas en Amazon CloudWatch. Se pueden consultar los mismos datos en Performance Insights, pero al contar con las métricas en CloudWatch es sencillo añadir alarmas de CloudWatch. También resulta fácil añadir las métricas a paneles de CloudWatch existentes.

Métrica	Descripción
DBLoad	El número de sesiones activas de la base de datos. Normalmente, necesita los datos del número promedio de sesiones activas. En Performance Insights, estos datos se consultan como `db.load.avg` .

Métrica	Descripción
DBLoadCPU	El número de sesiones activas cuyo tipo de evento de espera es CPU. En Performance Insights, estos datos se consultan como `db.load.avg` , filtrados por el tipo de evento de espera `CPU`.
DBLoadNonCPU	Promedio de sesiones activas cuyo tipo de evento de espera no es CPU.
DBLoadRelativeToNumVCPUs	La relación entre la carga de base de datos y el número de CPU virtuales para la base de datos.

> **Note**
>
> Estas métricas se publican en CloudWatch solo si hay una carga en la instancia de base de datos.

Puede examinar estas métricas mediante la consola de CloudWatch, la AWS CLI o la API de CloudWatch. También puede examinar otras métricas de contador de Performance Insights mediante una función matemática métrica especial. Para obtener más información, consulte Consulta de otras métricas de contador de Performance Insights en CloudWatch.

Por ejemplo, puede obtener las estadísticas para la métrica `DBLoad` ejecutando el comando get-metric-statistics.

```
aws cloudwatch get-metric-statistics \
    --region us-west-2 \
    --namespace AWS/RDS \
    --metric-name DBLoad  \
    --period 60 \
    --statistics Average \
    --start-time 1532035185 \
    --end-time 1532036185 \
    --dimensions Name=DBInstanceIdentifier,Value=db-loadtest-0
```

Este ejemplo genera un resultado similar al siguiente.


```
{
  "Datapoints": [
  {
  "Timestamp": "2021-07-19T21:30:00Z",
  "Unit": "None",
  "Average": 2.1
  },
  {
  "Timestamp": "2021-07-19T21:34:00Z",
  "Unit": "None",
  "Average": 1.7
  },
  {
  "Timestamp": "2021-07-19T21:35:00Z",
  "Unit": "None",
  "Average": 2.8
  },
  {
  "Timestamp": "2021-07-19T21:31:00Z",
  "Unit": "None",
  "Average": 1.5
  },
  {
  "Timestamp": "2021-07-19T21:32:00Z",
  "Unit": "None",
  "Average": 1.8
  },
  {
  "Timestamp": "2021-07-19T21:29:00Z",
  "Unit": "None",
  "Average": 3.0
  },
  {
  "Timestamp": "2021-07-19T21:33:00Z",
  "Unit": "None",
  "Average": 2.4
  }
  ],
  "Label": "DBLoad"
  }
```

Para obtener más información acerca de CloudWatch, consulte ¿Qué es Amazon CloudWatch? en la Guía del usuario de Amazon CloudWatch.

Consulta de otras métricas de contador de Performance Insights en CloudWatch

> **Note**
>
> Si habilita el modo avanzado de Información sobre las bases de datos, Amazon RDS publica las métricas del contador de Información de rendimiento en Amazon CloudWatch. Con Información sobre las bases de datos, no necesita utilizar la función matemática de métrica `DB_PERF_INSIGHTS`. Puede utilizar el panel de Información sobre las bases de datos de CloudWatch para buscar, consultar y configurar alarmas para las métricas de los contadores de Información de rendimiento.

Puede realizar consultas, generar alarmas y crear gráficos en las métricas de Performance Insights de RDS desde CloudWatch. Puede acceder a la información sobre su instancia de base de datos mediante la función matemática de la métrica `DB_PERF_INSIGHTS` para CloudWatch. Esta función le permite utilizar las métricas de Performance Insights que no se notifican directamente a CloudWatch para crear una nueva serie temporal.

Para utilizar la nueva función Metric Math, haga clic en el menú desplegable Agregar matemática, en la pantalla Seleccionar una métrica de la consola de CloudWatch. Puede usarla para crear alarmas y gráficos en métricas de Performance Insights o en combinaciones de métricas de CloudWatch y Performance Insights, lo que incluye alarmas de alta resolución para métricas de menos de un minuto. También puede utilizar la función mediante programación al incluir la expresión de Metric Math en una solicitud `get-metric-data`. Para obtener más información, consulte Sintaxis de matemáticas en las métricas y funciones y Crear una alarma en las métricas del contador de Performance Insights desde una base de datos AWS.

Métricas de contador de Información de rendimiento

Las métricas de contador son métricas de rendimiento de sistemas operativos y bases de datos en el panel de control de Información de rendimiento. Para ayudar a identificar y analizar los problemas de rendimiento, puede correlacionar las métricas de contador con la carga de base de datos. Debe anexar una función estadística a la métrica para obtener los valores de la métrica. Por ejemplo, las funciones compatibles con `os.memory.active`, las métricas son `.avg`, `.min`, `.max`, `.sum` y `.sample_count`.

Las métricas del contador se recopilan una vez por minuto. La recopilación de métricas del sistema operativo depende de si la monitorización mejorada está activada o desactivada. Si la monitorización mejorada está desactivada, las métricas del sistema operativo se recopilan una vez por minuto. Si la monitorización mejorada está activada, las métricas del sistema operativo se recopilan durante el período de tiempo seleccionado. Para obtener más información acerca de si activar o desactivar la monitorización mejorada, consulte Activación y desactivación de la supervisión mejorada.

Temas

- Contadores de sistemas operativos de Información de rendimiento
- Contadores de Información sobre rendimiento para Amazon RDS para MariaDB y MySQL
- Contadores de información sobre rendimiento para Amazon RDS for Microsoft SQL Server
- Contadores de Performance Insights para Amazon RDS para Oracle
- Contadores de Información sobre rendimiento para Amazon RDS para PostgreSQL

Contadores de sistemas operativos de Información de rendimiento

Los siguientes contadores de sistemas operativos, que llevan el prefijo `os`, están disponibles con Información sobre rendimiento para todos los motores de RDS excepto RDS para SQL Server .

Puede utilizar la API `ListAvailableResourceMetrics` para obtener la lista de métricas de contador disponibles para su instancia de base de datos. Para obtener más información, consulte ListAvailableResourceMetrics en la guía de referencia de la API Información de rendimiento de Amazon RDS.

Contador	Tipo	Unidad	Métrica	Descripción
Activa	Memoria	Kilobytes	os.memory .active	La cantidad de memoria asignada, en kilobytes.
Búferes	Memoria	Kilobytes	os.memory .buffers	La cantidad de memoria utilizada para almacenar en búfer solicitud

Contador	Tipo	Unidad	Métrica	Descripción
				es de E/S antes de escribir en el dispositivo de almacenamiento, en kilobytes.
Cached	Memoria	Kilobytes	os.memory .cached	La cantidad de memoria utilizada para almacenar en la caché las E/S basadas en el sistema de archivos, en kilobytes.
DB Cache	Memoria	Bytes	os.memory .db.cache	La cantidad de memoria utilizada para la caché de páginas por proceso de base de datos, incluido tmpfs (shmem), en bytes.

Contador	Tipo	Unidad	Métrica	Descripción
DB Resident Set Size	Memoria	Bytes	os.memory.db.residentSetSize	La cantidad de memoria utilizada para la caché anónima y de intercambio por proceso de base de datos, sin incluir tmpfs (shmem), en bytes.
DB Swap	Memoria	Bytes	os.memory.db.swap	La cantidad de memoria utilizada para el intercambio por proceso de base de datos, en bytes.
Dirty	Memoria	Kilobytes	os.memory.dirty	La cantidad de páginas de memoria en la RAM que se han modificado, pero no escrito, en su bloque de datos relacionado en el almacenamiento, en kilobytes.
Free	Memoria	Kilobytes	os.memory.free	La cantidad de memoria no asignada, en kilobytes.

Contador	Tipo	Unidad	Métrica	Descripción
Huge Pages Free	Memoria	Páginas	os.memory .hugePagesFree	El número de páginas de gran tamaño libres. Las páginas de gran tamaño son una caracterí stica del kernel de Linux.
Huge Pages Rsvd	Memoria	Páginas	os.memory .hugePagesRsvd	El número de páginas de gran tamaño confirmadas.
Huge Pages Size	Memoria	Kilobytes	os.memory .hugePagesSize	El tamaño de cada unidad de páginas de gran tamaño, en kilobytes.
Huge Pages Surp	Memoria	Páginas	os.memory .hugePagesSurp	El número de páginas de gran tamaño sobrantes disponibles con respecto al total.
Huge Pages Total	Memoria	Páginas	os.memory .hugePagesTotal	El número total de páginas enormes.

Contador	Tipo	Unidad	Métrica	Descripción
Inactive	Memoria	Kilobytes	os.memory .inactive	La cantidad de páginas de memoria utilizadas con menor frecuenci a, en kilobytes.
Mapped	Memoria	Kilobytes	os.memory .mapped	La cantidad total de contenido del sistema de archivos mapeado a la memoria dentro de un espacio de direcciones de proceso, en kilobytes.
Out of Memory Kill Count	Memoria	Eliminaciones	os.memory .outOfMem oryKillCount	El número de terminaciones de OOM que se produjeron durante el último intervalo de recopilación.
Page Tables	Memoria	Kilobytes	os.memory .pageTables	La cantidad de memoria utilizada por tablas de página, en kilobytes.

Contador	Tipo	Unidad	Métrica	Descripción
Slab	Memoria	Kilobytes	os.memory.slab	La cantidad de estructuras de datos de kernel reutilizables, en kilobytes.
Total	Memoria	Kilobytes	os.memory.total	La cantidad total de memoria, en kilobytes.
Writeback	Memoria	Kilobytes	os.memory .writeback	La cantidad de páginas desfasadas s en la RAM que se siguen escribiendo en el almacenamiento de respaldo, en kilobytes.
Guest	Utilización de la CPU	Porcentaje	os.cpuUtilization. guest	El porcentaje de CPU utilizado por programas invitados.
Idle	Utilización de la CPU	Porcentaje	os.cpuUtilization. idle	El porcentaje inactivo de CPU.
Irq	Utilización de la CPU	Porcentaje	os.cpuUtilization. irq	El porcentaj e de CPU utilizado por interrupciones de software.

Contador	Tipo	Unidad	Métrica	Descripción
Nice	Utilización de la CPU	Porcentaje	os.cpuUtilization.nice	El porcentaje de CPU utilizado por programas que se ejecutan con la prioridad más baja.
Steal	Utilización de la CPU	Porcentaje	os.cpuUtilization.steal	El porcentaje de CPU utilizado por otras máquinas virtuales.
System	Utilización de la CPU	Porcentaje	os.cpuUtilization.system	El porcentaje de CPU utilizado por el kernel.
Total	Utilización de la CPU	Porcentaje	os.cpuUtilization.total	El porcentaje total de CPU utilizado. Este valor incluye el valor nice.
User	Utilización de la CPU	Porcentaje	os.cpuUtilization.user	El porcentaje de CPU utilizado por programas de usuario.
Wait	Utilización de la CPU	Porcentaje	os.cpuUtilization.wait	El porcentaje de CPU sin utilizar mientras se espera el acceso de E/S.

Contador	Tipo	Unidad	Métrica	Descripción
Read IOs PS	E/S de disco	Solicitudes por segundo	os.diskIO.<nombre del dispositivo>.readIOsPS	El número de operaciones de lectura por segundo.
Write IOs PS	E/S de disco	Solicitudes por segundo	os.diskIO.<nombre del dispositivo>.writeIOsPS	El número de operaciones de escritura por segundo.
Avg Queue Len	E/S de disco	Solicitudes	os.diskIO.<nombre del dispositivo>.avgQueueLen	El número de solicitudes que espera en la cola del dispositivo de E/S.
Avg Req Sz	E/S de disco	Solicitudes	os.diskIO.<nombre del dispositivo>.avgReqSz	El número de solicitudes que espera en la cola del dispositivo de E/S.
Await	E/S de disco	Milisegundos	os.diskIO.<nombre del dispositivo>.await	El número de milisegundos necesarios para responder a las solicitudes, incluido el tiempo de cola y el tiempo de servicio.

Contador	Tipo	Unidad	Métrica	Descripción
Read IOs PS	E/S de disco	Solicitudes	os.diskIO .<nombre del dispositivo>.readIOsPS	El número de operaciones de lectura por segundo.
Read KB	E/S de disco	Kilobytes	os.diskIO .<nombre del dispositivo>.readKb	El número total de kilobytes leídos.
Read KB PS	E/S de disco	Kilobytes por segundo	os.diskIO .<nombre del dispositivo>.readKbPS	El número de kilobytes leídos por segundo.
Rrqm PS	E/S de disco	Solicitudes por segundo	os.diskIO .<nombre del dispositivo>.rrqmPS	El número de solicitudes leídas fusionadas en cola por segundo.
TPS	E/S de disco	Transacciones por segundo	os.diskIO .<nombre del dispositivo>.tps	El número de transacciones de E/S por segundo.
Util	E/S de disco	Porcentaje	os.diskIO .<nombre del dispositivo>.util	El porcentaje de tiempo de CPU durante el cual se emitieron las solicitudes.

Contador	Tipo	Unidad	Métrica	Descripción
Write KB	E/S de disco	Kilobytes	os.diskIO .<nombre del dispositivo>.writeKb	El número total de kilobytes escritos.
Write KB PS	E/S de disco	Kilobytes por segundo	os.diskIO .<nombre del dispositivo>.writeKbPS	El número de kilobytes escritos por segundo.
Wrqm PS	E/S de disco	Solicitudes por segundo	os.diskIO .<nombre del dispositivo>.wrqmPS	El número de solicitudes de escritura fusionadas en cola por segundo.
Blocked	Tareas	Tareas	os.tasks.blocked	El número de tareas que están bloqueadas.
Running	Tareas	Tareas	os.tasks.running	El número de tareas que están en ejecución.
Sleeping	Tareas	Tareas	os.tasks.sleeping	El número de tareas que están inactivas.
Stopped	Tareas	Tareas	os.tasks.stopped	El número de tareas que se han detenido.
Total	Tareas	Tareas	os.tasks.total	El número total de tareas.

Contador	Tipo	Unidad	Métrica	Descripción
Zombie	Tareas	Tareas	os.tasks.zombie	El número de tareas secundarias inactivas con una tarea principal activa.
One	Promedio de carga por minuto	Processes	os.loadAverageMinute.one	El número de procesos que solicitan tiempo de la CPU en el último minuto.
Fifteen	Promedio de carga por minuto	Processes	os.loadAverageMinute.fifteen	El número de procesos que solicitan tiempo de la CPU en los últimos 15 minutos.
Five	Promedio de carga por minuto	Processes	os.loadAverageMinute.five	El número de procesos que solicitan tiempo de la CPU en los últimos 5 minutos.
Cached	Intercambio	Kilobytes	os.swap.cached	La cantidad de memoria de intercambio, en kilobytes, utilizada como memoria caché.

Contador	Tipo	Unidad	Métrica	Descripción
Free	Intercambio	Kilobytes	os.swap.free	La cantidad de memoria de intercambio no asignada, en kilobytes.
In	Intercambio	Kilobytes	os.swap.in	La cantidad de memoria, en kilobytes, intercambiada desde disco.
Out	Intercambio	Kilobytes	os.swap.out	La cantidad de memoria, en kilobytes, intercambiada del disco.
Total	Intercambio	Kilobytes	os.swap.total	La cantidad de memoria de intercambio disponible, en kilobytes.
Max Files	Sistema de archivos	Archivos	os.fileSys.maxFiles	El número máximo de archivos que se pueden crear para el sistema de archivos.
Used Files	Sistema de archivos	Archivos	os.fileSys.usedFiles	El número de archivos en el sistema de archivos.

Contador	Tipo	Unidad	Métrica	Descripción
Used File Percent	Sistema de archivos	Archivos	os.fileSys.usedFilePercent	El porcentaje de archivos disponibles en uso.
Used Percent	Sistema de archivos	Porcentaje	os.fileSys.usedPercent	El porcentaje de espacio en disco del sistema de archivos que está en uso.
Used	Sistema de archivos	Kilobytes	os.fileSys.used	La cantidad de espacio en disco utilizado por los archivos en el sistema de archivos, en kilobytes.
Total	File Sys	Kilobytes	os.fileSys.total	La cantidad total de espacio en disco disponible para el sistema de archivos, en kilobytes.
Rx	Network	Bytes por segundo	os.network.rx	El número de bytes recibidos por segundo.
Tx	Network	Bytes por segundo	os.network.tx	El número de bytes cargados por segundo.

Contador	Tipo	Unidad	Métrica	Descripción
Acu Utilization	General	Porcentaje	os.general.acuUtilization	El porcentaje de la capacidad actual fuera de la capacidad máxima configurada.
Max Configured Acu	General	ACU	os.general.maxConfiguredAcu	La capacidad máxima configurada por el usuario, en unidades de capacidad de Aurora (ACU).
Min Configured Acu	General	ACU	os.general.minConfiguredAcu	La capacidad mínima configurada por el usuario, en ACU.
Num VCPUs	General	vCPU	os.general.numVCPUs	El número de CPU virtuales (vCPU) para la instancia de base de datos.
Serverless Database Capacity	General	ACU	os.general.serverlessDatabaseCapacity	La capacidad actual de la instancia, en ACU.

Contadores de Información sobre rendimiento para Amazon RDS para MariaDB y MySQL

Los siguientes contadores de base de datos están disponibles con Performance Insights para Amazon RDS para MariaDB y MySQL.

Temas

- Contadores nativos para RDS para MariaDB y RDS para MySQL
- Contadores no nativos para Amazon RDS para MariaDB y MySQL

Contadores nativos para RDS para MariaDB y RDS para MySQL

Las métricas nativas las define el motor de base de datos y no Amazon RDS. Para ver las definiciones de estas métricas nativas, consulte Server Status Variables (para 8.0) y Server Status Variables (para 8.4) en la documentación de MySQL.

Contador	Tipo	Unidad	Métrica
Com_analyze	SQL	Consultas por segundo	db.SQL.Com_analyze
Com_optimize	SQL	Consultas por segundo	db.SQL.Com_optimize
Com_select	SQL	Consultas por segundo	db.SQL.Com_select
Conexiones	SQL	El número de intentos de conexión por minuto (logrados o no) al servidor MySC	db.Users.Connections
Innodb_rows_deleted	SQL	Filas por segundo	db.SQL.Innodb_rows_deleted

Contador	Tipo	Unidad	Métrica
Innodb_rows_inserted	SQL	Filas por segundo	db.SQL.Innodb_rows_inserted
Innodb_rows_read	SQL	Filas por segundo	db.SQL.Innodb_rows_read
Innodb_rows_updated	SQL	Filas por segundo	db.SQL.Innodb_rows_updated
Select_full_join	SQL	Consultas por segundo	db.SQL.Select_full_join
Select_full_range_join	SQL	Consultas por segundo	db.SQL.Select_full_range_join
Select_range	SQL	Consultas por segundo	db.SQL.Select_range
Select_range_check	SQL	Consultas por segundo	db.SQL.Select_range_check
Select_scan	SQL	Consultas por segundo	db.SQL.Select_scan
Slow_queries	SQL	Consultas por segundo	db.SQL.Slow_queries
Sort_merge_passes	SQL	Consultas por segundo	db.SQL.Sort_merge_passes
Sort_range	SQL	Consultas por segundo	db.SQL.Sort_range
Sort_rows	SQL	Consultas por segundo	db.SQL.Sort_rows
Sort_scan	SQL	Consultas por segundo	db.SQL.Sort_scan

Contador	Tipo	Unidad	Métrica
Preguntas	SQL	Consultas por segundo	db.SQL.Questions
Innodb_row_lock_time	Bloqueos	Milisegundos (promedio)	db.Locks.Innodb_row_lock_time
Table_locks_immediate	Bloqueos	Solicitudes por segundo	db.Locks.Table_locks_immediate
Table_locks_waited	Bloqueos	Solicitudes por segundo	db.Locks.Table_locks_waited
Aborted_clients	Usuarios	Conexiones	db.Users.Aborted_clients
Aborted_connects	Usuarios	Conexiones	db.Users.Aborted_connects
max_connections	Usuarios	Connections	db.User.max_connections
Threads_created	Usuarios	Conexiones	db.Users.Threads_created
Threads_running	Usuarios	Conexiones	db.Users.Threads_running
Innodb_data_writes	I/O	Operaciones por segundo	db.IO.Innodb_data_writes
Innodb_dblwr_writes	I/O	Operaciones por segundo	db.IO.Innodb_dblwr_writes
Innodb_log_write_requests	I/O	Operaciones por segundo	db.IO.Innodb_log_write_requests
Innodb_log_writes	I/O	Operaciones por segundo	db.IO.Innodb_log_writes
Innodb_pages_written	I/O	Páginas por segundo	db.IO.Innodb_pages_written

Contador	Tipo	Unidad	Métrica
Created_tmp_disk_tables	Temp	Tablas por segundo	db.Temp.Created_tmp_disk_tables
Created_tmp_tables	Temp	Tablas por segundo	db.Temp.Created_tmp_tables
Innodb_buffer_pool_pages_data	Caché	Páginas	db.Cache.Innodb_buffer_pool_pages_data
Innodb_buffer_pool_pages_total	Caché	Páginas	db.Cache.Innodb_buffer_pool_pages_total
Innodb_buffer_pool_read_requests	Caché	Páginas por segundo	db.Cache.Innodb_buffer_pool_read_requests
Innodb_buffer_pool_reads	Caché	Páginas por segundo	db.Cache.Innodb_buffer_pool_reads
Opened_tables	Caché	Tablas	db.Cache.Opened_tables
Opened_table_definitions	Caché	Tablas	db.Cache.Opened_table_definitions
Qcache_hits	Caché	Consultas	db.Cache.Qcache_hits

Contadores no nativos para Amazon RDS para MariaDB y MySQL

Las métricas de contadores no nativos se definen mediante Amazon RDS. Una métrica no nativa puede ser una métrica que obtiene con una consulta concreta. Una métrica no nativa también puede ser una métrica derivada, en la que se utilicen dos o más contadores nativos en cálculos para proporciones, aciertos o latencias.

Contador	Tipo	Unidad	Métrica	Descripción	Definición
innodb_buffer_pool_hits	Caché	Lecturas	db.Cache.innoDB_buffer_pool_hits	El número de lecturas que InnoDB podría cumplir del grupo de búferes.	`innodb_buffer_pool_read_requests - innodb_buffer_pool_reads`
innodb_buffer_pool_hit_rate	Caché	Porcentaje	db.Cache.innoDB_buffer_pool_hit_rate	El porcentaje de lecturas que InnoDB podría cumplir del grupo de búferes.	`100 * innodb_buffer_pool_read_requests / (innodb_buffer_pool_read_requests + innodb_buffer_pool_reads)`
innodb_buffer_pool_usage	Caché	Porcentaje	db.Cache.innoDB_buffer_pool_usage	El porcentaje del grupo de búferes de InnoDB que contiene datos (páginas).	`Innodb_buffer_pool_pages_data / Innodb_buffer_pool_pages_total * 100.0`

Contador	Tipo	Unidad	Métrica	Descripción	Definición
				Note Al usar tablas compri as, este valor puede variar. Para obtene más inform ón, consul la inform ón acerca de `Innod ffer_ _page ta` y `Innod ffer_ _page tal` en Server Status	

Contador	Tipo	Unidad	Métrica	Descripción	Definición
				Variab (para E y Server Status Variab (para E en la docum ción de MySQ	
query_cache_hit_rate	Caché	Porcenta e	db.Cache. query_cac he_hit_rate	Proporció n de aciertos de caché de conjunto de resultado s MySQL (caché de consultas).	`Qcache_hits / (QCache_hits + Com_select) * 100`

Contador	Tipo	Unidad	Métrica	Descripción	Definición
innodb_datafile_writes_to_disk	E/S	Escrituras	db.IO.innoDB_datafile_writes_to_disk	El número de escrituras en disco de archivos de datos InnoDB, sin incluir operaciones de escritura doble y de registro de rehacer.	`Innodb_data_writes - Innodb_log_writes - Innodb_dblwr_writes`
innodb_rows_changed	SQL	Filas	db.SQL.innodb_rows_changed	Las operaciones de filas de InnoDB totales.	`db.SQL.Innodb_rows_inserted + db.SQL.Innodb_rows_deleted + db.SQL.Innodb_rows_updated`
active_transactions	Transacciones	Transacciones	db.Transactions.active_transactions	Las transacciones activas totales.	`SELECT COUNT(1) AS active_transactions FROM INFORMATION_SCHEMA.INNODB_TRX`

Contador	Tipo	Unidad	Métrica	Descripción	Definición
trx_rseg_history_len	Transacciones	Ninguno	db.Transactions.trx_rseg_history_len	Una lista de las páginas de registro de deshacer de las transacciones confirmadas que mantiene el sistema de transacciones InnoDB para implementar el control de concurrencia de varias versiones. Para obtener más información sobre cómo deshacer los	`SELECT COUNT AS trx_rseg_history_len FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='trx_rseg_history_len'`

Contador	Tipo	Unidad	Métrica	Descripción	Definición
				detalles de registros, consulte InnoDB Multi-Versioning (para 8.0) e InnoDB Multi-Versioning (para 8.4) en la documentación de MySQL.	
innodb_deadlocks	Interbloqueos	Interbloqueos	db.Locks.innodb_deadlocks	El número total de interbloqueos.	`SELECT COUNT AS innodb_deadlocks FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_deadlocks'`

Contador	Tipo	Unidad	Métrica	Descripción	Definición
innodb_lock_timeouts	Interbloqueos	Interbloqueos	db.Locks.innodb_lock_timeouts	El número total de bloqueos que agotaron el tiempo de espera.	`SELECT COUNT AS innodb_lock_timeouts FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_timeouts'`
innodb_row_lock_waits	Interbloqueos	Interbloqueos	db.Locks.innodb_row_lock_waits	El número total de bloqueos que resultaron en una espera.	`SELECT COUNT AS innodb_row_lock_waits FROM INFORMATION_SCHEMA.INNODB_METRICS WHERE NAME='lock_row_lock_waits'`

Contadores de información sobre rendimiento para Amazon RDS for Microsoft SQL Server

Los siguientes contadores de base de datos están disponibles con Performance Insights para RDS Microsoft SQL Server.

Contadores nativos para RDS para Microsoft SQL Server

Las métricas nativas las define el motor de base de datos y no Amazon RDS. Puede encontrar las definiciones de estas métricas nativas en Utilizar objetos de SQL Server en la documentación de Microsoft SQL Server.

Contador	Tipo	Unidad	Métrica
Registros reenviados	Métodos de acceso	Registros por segundo	db.Access Methods.Forwarded Records
División de páginas	Métodos de acceso	Divisiones por segundo	db.Access Methods.Page Splits
Proporción de aciertos de la caché del búfer	Administración del búfer	Proporción	db.Buffer Manager.Buffer cache hit ratio
Duración prevista de la página	Administración del búfer	Previsión en segundos	db.Buffer Manager.Page life expectancy
Búsquedas en la página	Administración del búfer	Búsquedas por segundo	db.Buffer Manager.Page lookups
Lecturas de la página	Administración del búfer	Lecturas por segundo	db.Buffer Manager.Page reads
Escrituras de la página	Administración del búfer	Escrituras por segundo	db.Buffer Manager.Page writes
Transacciones activas	Bases de datos	Transacciones	db.Databases.Active Transactions (_Total)
Bytes de registro vacíos	Bases de datos	Bytes vaciados por segundo	db.Databases.Log Bytes Flushed (_Total)
Esperas del vaciado de registro	Bases de datos	Esperas por segundo	db.Databases.Log Flush Waits (_Total)
Vaciados de registro	Bases de datos	Vaciados por segundo	db.Databases.Log Flushes (_Total)
Transacciones de escritura	Bases de datos	Transacciones por segundo	db.Databases.Write Transactions (_Total)

Contador	Tipo	Unidad	Métrica
Procesos bloqueados	Estadísticas generales	Procesos bloqueados	db.General Statistics.Processes blocked
Conexiones de usuario	Estadísticas generales	Conexiones	db.General Statistics.User Connections
Esperas de bloqueo	Bloqueos	Esperas por segundo	db.Latches.Latch Waits
Número de interbloqueos	Interbloqueos	Interbloqueos por segundo	db.Locks.Number of Deadlocks (_Total)
Concesiones de memoria pendientes	Gestor de memoria	Concesiones de memoria	db.Memory Manager.Memory Grants Pending
Solicitudes de lotes	Estadísticas de SQL	Solicitudes por segundo	db.SQL Statistics.Batch Requests
Compilaciones de SQL	Estadísticas de SQL	Compilaciones por segundo	db.SQL Statistics.SQL Compilations
Recopilaciones de SLQ	Estadísticas de SQL	Recopilaciones por segundo	db.SQL Statistics.SQL Re-Compilations

Contadores de Performance Insights para Amazon RDS para Oracle

Los siguientes contadores de base de datos están disponibles con Performance Insights para RDS para Oracle.

Contadores nativos para RDS para Oracle

Las métricas nativas las define el motor de base de datos y no Amazon RDS. Puede encontrar las definiciones de estas métricas nativas en Statistics Descriptions en la documentación de Oracle.

> **Note**
>
> Para la métrica de contador `CPU used by this session`, la unidad se ha transformado desde las centésimas de segundo nativas a las sesiones activas para que el valor sea más sencillo de usar. Por ejemplo, el envío de CPU en el gráfico de carga de base de datos representa la demanda de CPU. La métrica de contador `CPU used by this session` representa la cantidad de CPU utilizada por las sesiones de Oracle. Puede comparar el envío de CPU con la métrica de contador `CPU used by this session`. Cuando la demanda de CPU es superior a la CPU utilizada, las sesiones esperan tiempo de CPU.

Contador	Tipo	Unidad	Métrica
CPU used by this session	Usuario	Sesiones activas	db.User.CPU used by this session
SQL*Net roundtrips to/from client	Usuario	Viajes de ida y vuelta por segundo	db.User.SQL*Net roundtrips to/from client
Bytes received via SQL*Net from client	Usuario	Bytes por segundo	db.User.bytes received via SQL*Net from client
User commits	Usuario	Confirmaciones por segundo	db.User.user commits
Logons cumulative	Usuario	Inicios de sesión por segundo	db.User.logons cumulative
User calls	Usuario	Llamadas por segundo	db.User.user calls
Bytes sent via SQL*Net to client	Usuario	Bytes por segundo	db.User.bytes sent via SQL*Net to client
User rollbacks	Usuario	Restauraciones por segundo	db.User.user rollbacks

Contador	Tipo	Unidad	Métrica
Redo size	Rehacer	Bytes por segundo	db.Redo.redo size
Parse count (total)	SQL	Análisis por segundo	db.SQL.parse count (total)
Parse count (hard)	SQL	Análisis por segundo	db.SQL.parse count (hard)
Table scan rows gotten	SQL	Filas por segundo	db.SQL.table scan rows gotten
Sorts (memory)	SQL	Ordenaciones por segundo	db.SQL.sorts (memory)
Sorts (disk)	SQL	Ordenaciones por segundo	db.SQL.sorts (disk)
Sorts (rows)	SQL	Ordenaciones por segundo	db.SQL.sorts (rows)
Physical read bytes	Caché	Bytes por segundo	db.Cache.physical read bytes
DB block gets	Caché	Bloques por segundo	db.Cache.db block gets
DBWR checkpoints	Caché	Puntos de comprobación por minuto	db.Cache.DBWR checkpoints
Physical reads	Caché	Lecturas por segundo	db.Cache.physical reads
Consistent gets from cache	Caché	Obtenciones por segundo	db.Cache.consistent gets from cache
DB block gets from cache	Caché	Obtenciones por segundo	db.Cache.db block gets from cache

Contador	Tipo	Unidad	Métrica
Consistent gets	Caché	Obtenciones por segundo	db.Cache.consistent gets

Contadores de Información sobre rendimiento para Amazon RDS para PostgreSQL

Los siguientes contadores de base de datos están disponibles con Información sobre rendimiento para Amazon RDS para PostgreSQL.

Temas

- Contadores para Amazon RDS para PostgreSQL
- Contadores no nativos para Amazon RDS para PostgreSQL

Contadores para Amazon RDS para PostgreSQL

Las métricas nativas las define el motor de base de datos y no Amazon RDS. Puede encontrar definiciones para estas métricas en Ver estadísticas en la documentación de PostgreSQL.

Contador	Tipo	Unidad	Métrica
blks_hit	Caché	Bloques por segundo	db.Cache.blks_hit
buffers_alloc	Caché	Bloques por segundo	db.Cache.buffers_alloc
buffers_checkpoint	Punto de comprobación	Bloques por segundo	db.Checkpoint.buffers_checkpoint
checkpoint_sync_time	Punto de comprobación	Milisegundos por punto de comprobación	db.Checkpoint.checkpoint_sync_time

Contador	Tipo	Unidad	Métrica
checkpoint_write_time	Punto de comprobación	Milisegundos por punto de comprobación	db.Checkpoint.checkpoint_write_time
checkpoints_req	Punto de comprobación	Puntos de comprobación por minuto	db.Checkpoint.checkpoints_req
checkpoints_timed	Punto de comprobación	Puntos de comprobación por minuto	db.Checkpoint.checkpoints_timed
maxwritten_clean	Punto de comprobación	Paradas de eliminación de Bgwriter por minuto	db.Checkpoint.maxwritten_clean
deadlocks	Simultaneidad	Interbloqueos por minuto	db.Concurrency.deadlocks
blk_read_time	I/O	Milisegundos	db.IO.blk_read_time
blks_read	I/O	Bloques por segundo	db.IO.blks_read
buffers_backend	I/O	Bloques por segundo	db.IO.buffers_backend
buffers_backend_fsync	I/O	Bloques por segundo	db.IO.buffers_backend_fsync
buffers_clean	I/O	Bloques por segundo	db.IO.buffers_clean
tup_deleted	SQL	Tuplas por segundo	db.SQL.tup_deleted

Contador	Tipo	Unidad	Métrica
tup_fetched	SQL	Tuplas por segundo	db.SQL.tup_fetched
tup_inserted	SQL	Tuplas por segundo	db.SQL.tup_inserted
tup_returned	SQL	Tuplas por segundo	db.SQL.tup_returned
tup_updated	SQL	Tuplas por segundo	db.SQL.tup_updated
temp_bytes	Temp	Bytes por segundo	db.Temp.temp_bytes
temp_files	Temp	Archivos por minuto	db.Temp.temp_files
xact_commit	Transacciones	Confirmaciones por segundo	db.Transactions.xact_commit
xact_rollback	Transacciones	Restauraciones por segundo	db.Transactions.xact_rollback
numbackends	Usuario	Conexiones	db.User.numbackends
archived_count	Registro antes de la escritura (WAL)	Archivos por minuto	db.WAL.archived_count

Contadores no nativos para Amazon RDS para PostgreSQL

Las métricas de contadores no nativos se definen mediante Amazon RDS. Una métrica no nativa puede ser una métrica que obtiene con una consulta concreta. Una métrica no nativa también puede ser una métrica derivada, en la que se utilicen dos o más contadores nativos en cálculos para proporciones, aciertos o latencias.

Contador	Tipo	Unidad	Métrica	Descripción	Definición
checkpoint_sync_latency	Punto de compr ión	db.Che oint.ch kpoint_ nc_late y		La cantidad de tiempo invertido en la parte del procesamiento del punto de comprobación en la que los archivos se han sincroniz ado en el disco.	`checkpoint_sync_time / (checkpoints_timed + checkpoints_req)`
checkpoint_write_latency	Punto de compr ión	db.Che oint.ch kpoint_ ite_late cy	La cantidad de tiempo invertido en la parte del procesami ento del punto de comprobación en la que los archivos se han escrito en el disco.	`checkpoint_write_time / (checkpoints_timed + checkpoints_req)`	
read_latency	E/S	db.IO.r d_later	El tiempo invertido leyendo bloques de archivos de datos por backends en esta instancia.	`blk_read_time / blks_read`	
idle_in_transaction_aborted_count	Estado	Sesior	db.state.idle_in_transaction_aborted_count	El número de sesiones en el estado `idle in transaction (aborted)` .	No aplicable
idle_in_transaction_count	Estado	Sesior	db.state.idle_in_transaction_count	El número de sesiones en el estado `idle in transaction` .	No aplicable

Contador	Tipo	Unidad	Métrica	Descripción	Definición
idle_in_transaction_max_time	Estado	Segun	db.state.idle_in_transaction_max_time	La duración de la transacción de mayor duración en el estado `idle in transaction` , en segundos.	No aplicable
active_transactions	Transa ones	Transa ones	db.Transactions.active_transactions	El número de transacciones activas.	No aplicable
blocked_transactions	Transa ones	Transa ones	db.Transactions.blocked_transactions	El número de transacciones bloqueadas.	No aplicable
oldest_active_logical_replication_slot_xid_age	Transa ones	db.Transactions.dest_ave_logl_replic tion_sl_xid_a	La antigüedad de la transacción más antigua en una ranura de replicación lógica activa. Para obtener más información, consulte Ranura de replicación lógica.	–	

Contador	Tipo	Unidad	Métrica	Descripción	Definición
oldest_inactive_logical_replication_slot_xid_age	Transa ones	db.Transactions.dest_inactive_logical_replication_ot_xid_e	La antigüedad de la transacción más antigua en una ranura de replicación lógica inactiva. Para obtener más información, consulte Ranura de replicación lógica.	–	
oldest_prepared_transaction_xid_age	Transa ones	db.Transactions.dest_prepared_transaction_id_age	La antigüedad de la transacción preparada más antigua. Para obtener más información, consulte Transacción preparada.	–	

Contador	Tipo	Unidad	Métrica	Descripción	Definición
oldest_running_transaction_xid_age	Transa ones	db.Transactions.oldest_running_transaction_xid_age	La antigüedad de la transacción en ejecución más antigua. Para obtener más información, consulte Instrucción activa sobre la transacción activa en ejecución más antigua y Inactividad en la transacción sobre la transacción inactiva en ejecución más antigua.	–	
oldest_hot_standby_feedback_xid_age	Transa ones	db.Transactions.oldest_hot_standby_feedback_xid_age	La antigüedad de la transacción en ejecución más antigua en una réplica de lectura con `hot_standby_feedback` habilitado. Para obtener más información, consulte Réplicas de lectura.	–	
max_used_xact_ids	Transa ones	Transa ones	db.Transactions.max_used_xact_ids	El número de transacciones que no se han vaciado.	No aplicable

Contador	Tipo	Unidad	Métrica	Descripción	Definición
max_connections	Usuari	Conne ns	db.User.max_connections	El número máximo de conexiones permitidas para una instancia de base de datos, según lo configurado en el parámetro `max_connections` .	No aplicable
archive_failed_count	WAL	Archiv por minuto	db.WAL.archive_failed_count	El número de intentos fallidos de archivado de archivos WAL, en archivos por minuto.	No aplicable

Estadísticas de SQL para Performance Insights

Las estadísticas de SQL son métricas relacionadas con el rendimiento de las consultas SQL que recopila Performance Insights. Performance Insights recopila estadísticas de cada segundo que se ejecuta una consulta y para cada llamada SQL. Las estadísticas de SQL son un promedio del intervalo de tiempo seleccionado.

Un resumen de SQL es un conjunto de todas las consultas que tienen un patrón dado, pero no necesariamente tienen los mismos valores literales. El resumen reemplaza los valores literales por un signo de interrogación. Por ejemplo, `SELECT * FROM emp WHERE lname= ?`. Este resumen podría incluir las siguientes consultas secundarias:

```
SELECT * FROM emp WHERE lname = 'Sanchez'
SELECT * FROM emp WHERE lname = 'Olagappan'
SELECT * FROM emp WHERE lname = 'Wu'
```

Todos los motores admiten estadísticas de SQL para las consultas de resumen.

Para obtener información sobre la compatibilidad de esta característica por región, motor de base de datos y clase de instancia, consulte Compatibilidad del motor de la base de datos, la región y la clase de instancia de Amazon RDS con características de Información de rendimiento.

Temas

- Estadísticas de SQL de MariaDB y MySQL
- Estadísticas de SQL de Amazon RDS para Oracle
- Estadísticas de SQL de Amazon RDS para SQL Server
- Estadísticas de SQL de RDS PostgreSQL

Estadísticas de SQL de MariaDB y MySQL

MariaDB y MySQL recopilan estadísticas de SQL solo en el nivel de resumen. No se muestran estadísticas en el nivel de instrucción.

Temas

- Estadísticas de resumen para MariaDB y MySQL
- Estadísticas por segundo de MariaDB y MySQL
- Estadísticas por llamada de MariaDB y MySQL
- Estadísticas principales para MariaDB y MySQL

Estadísticas de resumen para MariaDB y MySQL

Información sobre rendimiento recopila estadísticas de resumen SQL de la tabla `events_statements_summary_by_digest`. La base de datos administra la tabla `events_statements_summary_by_digest`.

Esta tabla no tiene una política de expulsión. Cuando la tabla está llena, se muestra el siguiente mensaje en la:AWS Management Console

```
Performance Insights is unable to collect SQL Digest statistics on new queries because
 the table events_statements_summary_by_digest is full.
Please truncate events_statements_summary_by_digest table to clear the issue. Check the
 User Guide for more details.
```

En esta situación, MariaDB y MySQL no llevan a cabo un seguimiento de las consultas SQL. Para solucionar este problema, la Información sobre rendimiento trunca automáticamente la tabla de resumen cuando se cumplen estas dos condiciones:

- La tabla está llena.
- La Información sobre rendimiento administra automáticamente el Esquema de rendimiento.

  Para la administración automática, el parámetro `performance_schema` se debe establecer en `0` y la Fuente no se debe establecer en `user`. Si Información sobre rendimiento no administra el esquema de rendimiento automáticamente, consulte Descripción general de Performance Schema para Información de rendimiento en Amazon RDS para MariaDB o MySQL.

En la AWS CLI, compruebe el fuente de un valor de parámetro ejecutando el comando describe-db-parameters.

Estadísticas por segundo de MariaDB y MySQL

Las siguientes estadísticas de SQL están disponibles para las instancias de base de datos de MariaDB y MySQL.

Métrica	Unidad
db.sql_tokenized.stats.count_star_per_sec	Llamadas por segundo
db.sql_tokenized.stats.sum_timer_wait_per_sec	Latencia media por segundo (en milisegundos)
db.sql_tokenized.stats.sum_select_full_join_per_sec	Unión completa de seleccionar por segundo
db.sql_tokenized.stats.sum_select_range_check_per_sec	Control de rango de seleccionar por segundo
db.sql_tokenized.stats.sum_select_scan_per_sec	Escaneo de seleccionar por segundo
db.sql_tokenized.stats.sum_sort_merge_passes_per_sec	Pases de fusión de clasificación por segundo
db.sql_tokenized.stats.sum_sort_scan_per_sec	Escaneos de clasificación por segundo

Métrica	Unidad
db.sql_tokenized.stats.sum_sort_rang e_per_sec	Rangos de clasificación por segundo
db.sql_tokenized.stats.sum_sort_rows_per_sec	Filas de clasificación por segundo
db.sql_tokenized.stats.sum_rows_affected_per_ sec	Filas afectadas por segundo
db.sql_tokenized.stats.sum_rows_exam ined_per_sec	Filas examinadas por segundo
db.sql_tokenized.stats.sum_rows_sent_per_sec	Filas enviadas por segundo
db.sql_tokenized.stats.sum_created_tmp_disk_t ables_per_sec	Tablas de disco temporales creadas por segundo
db.sql_tokenized.stats.sum_created_tmp_tables _per_sec	Tablas temporales creadas por segundo
db.sql_tokenized.stats.sum_lock_time_per_sec	Tiempo de bloqueo por segundo (en milisegun dos)

Estadísticas por llamada de MariaDB y MySQL

Las siguientes métricas ofrecen estadísticas por llamada para una instrucción SQL.

Métrica	Unidad
db.sql_tokenized.stats.sum_timer_wait_per_call	Latencia media por llamada (en milisegundos)
db.sql_tokenized.stats.sum_select_full_join_p er_call	Uniones completas de seleccionar por llamada
db.sql_tokenized.stats.sum_select_ra nge_check_per_call	Control de rango de s por llamada

Métrica	Unidad
db.sql_tokenized.stats.sum_select_scan_per_call	Escaneos de seleccionar por llamada
db.sql_tokenized.stats.sum_sort_merge_passes_per_call	Pases de fusión de clasificación por llamada
db.sql_tokenized.stats.sum_sort_scan_per_call	Escaneos de clasificación por llamada
db.sql_tokenized.stats.sum_sort_range_per_call	Rangos de clasificación por llamada
db.sql_tokenized.stats.sum_sort_rows_per_call	Filas de clasificación por llamada
db.sql_tokenized.stats.sum_rows_affected_per_call	Filas afectadas por llamada
db.sql_tokenized.stats.sum_rows_examined_per_call	Filas examinadas por llamada
db.sql_tokenized.stats.sum_rows_sent_per_call	Filas enviadas por llamada
db.sql_tokenized.stats.sum_created_tmp_disk_tables_per_call	Tablas de disco temporales creadas por llamada
db.sql_tokenized.stats.sum_created_tmp_tables_per_call	Tablas temporales creadas por llamada
db.sql_tokenized.stats.sum_lock_time_per_call	Tiempo de bloqueo por llamada (en milisegundos)

Estadísticas principales para MariaDB y MySQL

Las siguientes estadísticas de SQL están disponibles para las instancias de base de datos de MariaDB y MySQL.

Métrica	Unidad
db.sql_tokenized.stats.count_star	Calls

Métrica	Unidad
db.sql_tokenized.stats.sum_timer_wait	Tiempo de espera (en ms)
db.sql_tokenized.stats.sum_select_full_join	Seleccionar unión completa
db.sql_tokenized.stats.sum_select_range_check	Seleccionar comprobaciones de intervalos
db.sql_tokenized.stats.sum_select_scan	Seleccionar análisis
db.sql_tokenized.stats.sum_sort_merge_passes	Ordenar pasadas de combinación
db.sql_tokenized.stats.sum_sort_scan	Ordenar análisis
db.sql_tokenized.stats.sum_sort_range	Ordenar intervalos
db.sql_tokenized.stats.sum_sort_rows	Ordenar filas
db.sql_tokenized.stats.sum_rows_affected	Filas afectadas
db.sql_tokenized.stats.sum_rows_examined	Filas examinadas
db.sql_tokenized.stats.sum_rows_sent	Filas enviadas
db.sql_tokenized.stats.sum_created_tmp_disk_tables	Tablas de disco temporales creadas
db.sql_tokenized.stats.sum_created_tmp_tables	Tablas temporales creadas
db.sql_tokenized.stats.sum_lock_time	Tiempo de bloqueo (en ms)

Estadísticas de SQL de Amazon RDS para Oracle

Amazon RDS for Oracle recopila estadísticas de SQL tanto a nivel de instrucción como en el de resumen. En el nivel de instrucción, la columna ID representa el valor de `V$SQL.SQL_ID`. En el nivel de resumen, la columna ID muestra el valor de `V$SQL.FORCE_MATCHING_SIGNATURE`.

Si el ID es `0` en el nivel de resumen, la base de datos de Oracle ha determinado que esta instrucción no es adecuada para su reutilización. En este caso, las instrucciones SQL secundarias podrían

pertenecer a resúmenes diferentes. Sin embargo, las instrucciones se agrupan en `digest_text` para la primera instrucción SQL recopilada.

Temas

- Estadísticas por segundo de Oracle
- Estadísticas por llamada de Oracle
- Estadísticas principales para Oracle

Estadísticas por segundo de Oracle

Las siguientes métricas proporcionan estadísticas por segundo de una consulta SQL de Oracle.

Métrica	Unidad
db.sql.stats.executions_per_sec	Número de ejecuciones por segundo
db.sql.stats.elapsed_time_per_sec	Media de ejecuciones activas (AAE)
db.sql.stats.rows_processed_per_sec	Filas procesadas por segundo
db.sql.stats.buffer_gets_per_sec	Obtenciones del búfer por segundo
db.sql.stats.physical_read_requests_per_sec	Lecturas físicas por segundo
db.sql.stats.physical_write_requests_per_sec	Escrituras físicas por segundo
db.sql.stats.total_sharable_mem_per_sec	Memoria compartida total por segundo (en bytes)
db.sql.stats.cpu_time_per_sec	Tiempo de CPU por segundo (en milisegundos)

Las siguientes métricas proporcionan estadísticas por segundo de una consulta de resumen SQL de Oracle.

Métrica	Unidad
db.sql_tokenized.stats.executions_per_sec	Número de ejecuciones por segundo

Métrica	Unidad
db.sql_tokenized.stats.elapsed_time_per_sec	Media de ejecuciones activas (AAE)
db.sql_tokenized.stats.rows_processed_per_sec	Filas procesadas por segundo
db.sql_tokenized.stats.buffer_gets_per_sec	Obtenciones del búfer por segundo
db.sql_tokenized.stats.physical_read_requests_per_sec	Lecturas físicas por segundo
db.sql_tokenized.stats.physical_write_requests_per_sec	Escrituras físicas por segundo
db.sql_tokenized.stats.total_sharable_mem_per_sec	Memoria compartida total por segundo (en bytes)
db.sql_tokenized.stats.cpu_time_per_sec	Tiempo de CPU por segundo (en milisegundos)

Estadísticas por llamada de Oracle

Las siguientes métricas ofrecen estadísticas por llamada de una instrucción SQL.

Métrica	Unidad
db.sql.stats.elapsed_time_per_exec	Tiempo trascurrido por ejecuciones (en milisegundos)
db.sql.stats.rows_processed_per_exec	Filas procesadas por ejecución
db.sql.stats.buffer_gets_per_exec	Obtenciones del búfer por ejecución
db.sql.stats.physical_read_requests_per_exec	Lecturas físicas por ejecución
db.sql.stats.physical_write_requests_per_exec	Escrituras físicas por ejecución
db.sql.stats.total_sharable_mem_per_exec	Memoria compartida total por ejecución (en bytes)

Métrica	Unidad
db.sql.stats.cpu_time_per_exec	Tiempo de CPU por ejecución (en milisegundos)

Las siguientes métricas ofrecen estadísticas por llamada de una consulta de resumen SQL de Oracle.

Métrica	Unidad
db.sql_tokenized.stats.elapsed_time_per_exec	Tiempo trascurrido por ejecuciones (en milisegundos)
db.sql_tokenized.stats.rows_processed_per_exec	Filas procesadas por ejecución
db.sql_tokenized.stats.buffer_gets_per_exec	Obtenciones del búfer por ejecución
db.sql_tokenized.stats.physical_read_requests_per_exec	Lecturas físicas por ejecución
db.sql_tokenized.stats.physical_write_requests_per_exec	Escrituras físicas por ejecución
db.sql_tokenized.stats.total_sharable_mem_per_exec	Memoria compartida total por ejecución (en bytes)
db.sql_tokenized.stats.cpu_time_per_exec	Tiempo de CPU por ejecución (en milisegundos)

Estadísticas principales para Oracle

Las siguientes métricas proporcionan las estadísticas principales para una consulta SQL de Oracle.

Métrica	Unidad
db.sql.stats.executions	Número de ejecuciones

Métrica	Unidad
db.sql.stats.elapsed_time	Tiempo transcurrido (en ms)
db.sql.stats.rows_processed	Filas procesadas
db.sql.stats.buffer_gets	Obtenciones del búfer
db.sql.stats.physical_read_requests	Physical reads
db.sql.stats.physical_write_requests	Escrituras físicas
db.sql.stats.total_sharable_mem	Memoria compartida total (en bytes)
db.sql.stats.cpu_time	Tiempo de CPU (en ms)

Las siguientes métricas proporcionan las estadísticas principales para una consulta de resumen SQL de Oracle.

Métrica	Unidad
db.sql_tokenized.stats.executions	Número de ejecuciones
db.sql_tokenized.stats.elapsed_time	Tiempo transcurrido (en ms)
db.sql_tokenized.stats.rows_processed	Filas procesadas
db.sql_tokenized.stats.buffer_gets	Obtenciones del búfer
db.sql_tokenized.stats.physical_read_requests	Physical reads
db.sql_tokenized.stats.physical_write_requests	Escrituras físicas
db.sql_tokenized.stats.total_sharable_mem	Memoria compartida total (en bytes)
db.sql_tokenized.stats.cpu_time	Tiempo de CPU (en ms)

Estadísticas de SQL de Amazon RDS para SQL Server

Amazon RDS para SQL Server recopila estadísticas de SQL tanto en el nivel de instrucción como en el de resumen. En el nivel de instrucción, la columna ID representa el valor de `sql_handle`. En el nivel de resumen, la columna ID muestra el valor de `query_hash`.

SQL Server devuelve valores NULL para `query_hash` en algunas instruccioens. Por ejemplo, ALTER INDEX, CHECKPOINT, UPDATE STATISTICS, COMMIT TRANSACTION, FETCH NEXT FROM Cursor y algunas instrucciones INSERT, SELECT @<variable>, instrucciones condicionales y procedimientos almacenados ejecutables. En este caso, el valor de `sql_handle` se muestra como el ID en el nivel de resumen de esa instrucción.

Temas

- Estadísticas por segundo de SQL Server
- Estadísticas por llamada de SQL Server
- Estadísticas principales de SQL Server

Estadísticas por segundo de SQL Server

Las siguientes métricas proporcionan estadísticas por segundo de una consulta SQL de SQL Server.

Métrica	Unidad
db.sql.stats.execution_count_per_sec	Número de ejecuciones por segundo
db.sql.stats.total_elapsed_time_per_sec	Tiempo total transcurrido por segundo
db.sql.stats.total_rows_per_sec	Filas procesadas por segundo
db.sql.stats.total_logical_reads_per_sec	Total de lecturas lógicas por segundo
db.sql.stats.total_logical_writes_per_sec	Número total de escrituras lógicas por segundo
db.sql.stats.total_physical_reads_per_sec	Lecturas físicas totales por segundo
db.sql.stats.total_worker_time_per_sec	Tiempo total de CPU (en ms)

Las siguientes métricas proporcionan estadísticas por segundo de una consulta de resumen SQL de SQL Server.

Métrica	Unidad
db.sql_tokenized.stats.execution_count_per_sec	Número de ejecuciones por segundo
db.sql_tokenized.stats.total_elapsed_time_per_sec	Tiempo total transcurrido por segundo
db.sql_tokenized.stats.total_rows_per_sec	Filas procesadas por segundo
db.sql_tokenized.stats.total_logical_reads_per_sec	Total de lecturas lógicas por segundo
db.sql_tokenized.stats.total_logical_writes_per_sec	Número total de escrituras lógicas por segundo
db.sql_tokenized.stats.total_physical_reads_per_sec	Lecturas físicas totales por segundo
db.sql_tokenized.stats.total_worker_time_per_sec	Tiempo total de CPU (en ms)

Estadísticas por llamada de SQL Server

Las siguientes métricas ofrecen estadísticas por llamada para una instrucción SQL de SQL Server.

Métrica	Unidad
db.sql.stats.total_elapsed_time_per_call	Tiempo total transcurrido por ejecución (en milisegundos)
db.sql.stats.total_rows_per_call	Filas totales procesadas por ejecución
db.sql.stats.total_logical_reads_per_call	Total de lecturas lógicas por segundo
db.sql.stats.total_logical_writes_per_call	Total de escrituras lógicas por ejecución

Métrica	Unidad
db.sql.stats.total_physical_reads_per_call	Total de lecturas físicas por ejecución
db.sql.stats.total_worker_time_per_call	Tiempo total de CPU por ejecución (en ms)

Las siguientes métricas proporcionan estadísticas por llamada de una consulta de resumen SQL de SQL Server.

Métrica	Unidad
db.sql_tokenized.stats.total_elapsed_time_per_call	Tiempo total transcurrido por ejecución
db.sql_tokenized.stats.total_rows_per_call	Filas totales procesadas por ejecución
db.sql_tokenized.stats.total_logical_reads_per_call	Total de lecturas lógicas por segundo
db.sql_tokenized.stats.total_logical_writes_per_call	Total de escrituras lógicas por ejecución
db.sql_tokenized.stats.total_physical_reads_per_call	Total de lecturas físicas por ejecución
db.sql_tokenized.stats.total_worker_time_per_call	Tiempo total de CPU por ejecución (en ms)

Estadísticas principales de SQL Server

Las siguientes métricas proporcionan las estadísticas principales para una consulta SQL de SQL Server.

Métrica	Unidad
db.sql.stats.execution_count	Número de ejecuciones
db.sql.stats.total_elapsed_time	Tiempo total transcurrido (en ms)

Métrica	Unidad
db.sql.stats.total_rows	Total de filas procesadas
db.sql.stats.total_logical_reads	Total de lecturas lógicas
db.sql.stats.total_logical_writes	Total de escrituras lógicas
db.sql.stats.total_physical_reads	Total de lecturas físicas
db.sql.stats.total_worker_time	Tiempo total de CPU (en ms)

Las siguientes métricas proporcionan las estadísticas principales para una consulta de resumen SQL de SQL Server.

Métrica	Unidad
db.sql_tokenized.stats.execution_count	Número de ejecuciones
db.sql_tokenized.stats.total_elapsed_time	Tiempo total transcurrido (en ms)
db.sql_tokenized.stats.total_rows	Total de filas procesadas
db.sql_tokenized.stats.total_logical_reads	Total de lecturas lógicas
db.sql_tokenized.stats.total_logical_writes	Total de escrituras lógicas
db.sql_tokenized.stats.total_physical_reads	Total de lecturas físicas
db.sql_tokenized.stats.total_worker_time	Tiempo total de CPU (en ms)

Estadísticas de SQL de RDS PostgreSQL

Para cada llamada SQL y para cada segundo que se ejecuta una consulta, Performance Insights recopila estadísticas SQL. RDS para PostgreSQL recopila estadísticas de SQL solo en el nivel de resumen. No se muestran estadísticas en el nivel de instrucción.

A continuación, encontrará información sobre las estadísticas de resumen de RDS para PostgreSQL.

Temas

- Estadísticas de resumen de RDS PostgreSQL:
- Estadísticas de resumen por segundo de RDS PostgreSQL
- Estadísticas de resumen por llamada de RDS PostgreSQL
- Estadísticas principales para RDS PostgreSQL

Estadísticas de resumen de RDS PostgreSQL:

Para ver las estadísticas de resumen de SQL, RDS PostgreSQL debe cargar la biblioteca de `pg_stat_statements`. La base de datos carga esta biblioteca de forma predeterminada para las instancias de bases de datos de PostgreSQL compatibles con PostgreSQL 11 o una versión posterior. Esta biblioteca se habilita manualmente para las instancias de base de datos de PostgreSQL compatibles con PostgreSQL 10 o una versión anterior. Para habilitarlo de forma manual, añada `pg_stat_statements` a `shared_preload_libraries` en el grupo de parámetros de base de datos asociado a la instancia de base de datos. Después, reinicie la instancia de base de datos. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

> **Note**
>
> Con Información sobre rendimiento solo se pueden recopilar estadísticas para consultas en `pg_stat_activity` que no estén truncadas. De forma predeterminada, las bases de datos de PostgreSQL truncan consultas de más de 1024 bytes. Para aumentar el volumen de la consulta, cambie el parámetro `track_activity_query_size` en el grupo de parámetros de base de datos asociado con la instancia de base de datos. Cuando se cambia este parámetro, se requiere un reinicio de la instancia de base de datos.

Estadísticas de resumen por segundo de RDS PostgreSQL

Las siguientes estadísticas de resumen de SQL se encuentran disponibles para las instancias de base de datos de PostgreSLQ.

Métrica	Unidad
db.sql_tokenized.stats.calls_per_sec	Llamadas por segundo

Métrica	Unidad
db.sql_tokenized.stats.rows_per_sec	Filas por segundo
db.sql_tokenized.stats.total_time_per_sec	Media de ejecuciones activas (AAE) por segundo
db.sql_tokenized.stats.shared_blks_hit_per_sec	Aciertos en bloque por segundo
db.sql_tokenized.stats.shared_blks_read_per_sec	Lecturas en bloque por segundo
db.sql_tokenized.stats.shared_blks_dirtied_per_sec	Bloques ensuciados por segundo
db.sql_tokenized.stats.shared_blks_written_per_sec	Escrituras en bloque por segundo
db.sql_tokenized.stats.local_blks_hit_per_sec	Aciertos en bloque locales por segundo
db.sql_tokenized.stats.local_blks_read_per_sec	Lecturas en bloque locales por segundo
db.sql_tokenized.stats.local_blks_dirtied_per_sec	Suciedades en bloque locales por segundo
db.sql_tokenized.stats.local_blks_written_per_sec	Escrituras en bloque locales por segundo
db.sql_tokenized.stats.temp_blks_written_per_sec	Escrituras en temporales por segundo
db.sql_tokenized.stats.temp_blks_read_per_sec	Lecturas temporales por segundo
db.sql_tokenized.stats.blk_read_time_per_sec	Media de lecturas actuales por segundo
db.sql_tokenized.stats.blk_write_time_per_sec	Media de escrituras actuales por segundo

Estadísticas de resumen por llamada de RDS PostgreSQL

Las siguientes métricas ofrecen estadísticas por llamada para una instrucción SQL.

Métrica	Unidad
db.sql_tokenized.stats.rows_per_call	Filas por llamada
db.sql_tokenized.stats.avg_latency_per_call	Latencia media por llamada (en milisegundos)
db.sql_tokenized.stats.shared_blks_hit_per_call	Aciertos en bloque por llamada
db.sql_tokenized.stats.shared_blks_read_per_call	Lecturas en bloque por llamada
db.sql_tokenized.stats.shared_blks_written_per_call	Escrituras en bloque por llamada
db.sql_tokenized.stats.shared_blks_dirtied_per_call	Bloques ensuciados por llamada
db.sql_tokenized.stats.local_blks_hit_per_call	Aciertos en bloque locales por llamada
db.sql_tokenized.stats.local_blks_read_per_call	Lecturas en bloques locales por llamada
db.sql_tokenized.stats.local_blks_dirtied_per_call	Suciedades en bloque local por llamada
db.sql_tokenized.stats.local_blks_written_per_call	Escrituras en bloque local por llamada
db.sql_tokenized.stats.temp_blks_written_per_call	Escrituras en bloque temporal por llamada
db.sql_tokenized.stats.temp_blks_read_per_call	Lecturas en bloque temporal por llamada
db.sql_tokenized.stats.blk_read_time_per_call	Tiempo de lectura por llamada (en milisegundos)
db.sql_tokenized.stats.blk_write_time_per_call	Tiempo de escritura por llamada (en milisegundos)

Estadísticas principales para RDS PostgreSQL

Las siguientes estadísticas de SQL se encuentran disponibles para las instancias de base de datos de PostgreSQL.

Métrica	Unidad
db.sql_tokenized.stats.calls	Calls
db.sql_tokenized.stats.rows	Filas
db.sql_tokenized.stats.total_time	Tiempo total (en ms)
db.sql_tokenized.stats.shared_blks_hit	Aciertos en bloque
db.sql_tokenized.stats.shared_blks_read	Lecturas en bloque
db.sql_tokenized.stats.shared_blks_dirtied	Bloques ensuciados
db.sql_tokenized.stats.shared_blks_written	Escrituras en bloque
db.sql_tokenized.stats.local_blks_hit	Aciertos en bloque locales
db.sql_tokenized.stats.local_blks_read	Lecturas en bloque locales
db.sql_tokenized.stats.local_blks_dirtied	Bloques locales ensuciados
db.sql_tokenized.stats.local_blks_written	Escrituras en bloque locales
db.sql_tokenized.stats.temp_blks_written	Escrituras temporales
db.sql_tokenized.stats.temp_blks_read	Lecturas temporales
db.sql_tokenized.stats.blk_read_time	Promedio de lecturas simultáneas (en ms)
db.sql_tokenized.stats.blk_write_time	Promedio de escrituras simultáneas (en ms)

Para obtener más información acerca de estas métricas, consulte pg_stat_statements en la documentación de PostgreSQL.

Métricas del sistema operativo en Supervisión mejorada

Amazon RDS proporciona métricas en tiempo real para el sistema operativo (SO) en el que se ejecuta la instancia. RDS entrega las métricas de la Supervisión mejorada a su cuenta de registros de Amazon Cloudwatch. Las tablas siguientes incluyen las métricas de SO disponibles al usar registros de Amazon Cloudwatch.

Temas

- Métricas del sistema operativo para Db2, MariaDB, MySQL, Oracle y PostgreSQL
- Métricas del sistema operativo para Microsoft SQL Server

Métricas del sistema operativo para Db2, MariaDB, MySQL, Oracle y PostgreSQL

Grupo	Métrica	Nombre de la consola	Descripción
`General`	`engine`	No aplicable	El motor de base de datos para la instancia de base de datos.
	`instanceID`	No aplicable	El identificador de instancias de base de datos.
	`instanceResourceID`	No aplicable	Un identificador inmutable para la instancia de base de datos que es exclusivo de una región de AWS, también utilizado como identificador de secuencia de registro.
	`numVCPUs`	No aplicable	El número de CPU virtuales para la instancia de base de datos.
	`timestamp`	No aplicable	La hora a la que se tomó la métrica.
	`uptime`	No aplicable	La cantidad de tiempo que ha estado activa la instancia de base de datos.

Grupo	Métrica	Nombre de la consola	Descripción
	`version`	No aplicable	La versión del formato JSON del flujo de la métrica del SO.
`cpuUtilization`	`guest`	CPU Guest	El porcentaje de CPU utilizado por programas invitados.
	`idle`	CPU Idle	El porcentaje inactivo de CPU.
	`irq`	CPU IRQ	El porcentaje de CPU utilizado por interrupciones de software.
	`nice`	CPU Nice	El porcentaje de CPU utilizado por programas que se ejecutan con la prioridad más baja.
	`steal`	CPU Steal	El porcentaje de CPU utilizado por otras máquinas virtuales.
	`system`	CPU System	El porcentaje de CPU utilizado por el kernel.
	`total`	CPU Total	El porcentaje total de CPU utilizado. Este valor incluye el valor `nice`.
	`user`	CPU User	El porcentaje de CPU utilizado por programas de usuario.
	`wait`	CPU Wait	El porcentaje de CPU sin utilizar mientras se espera el acceso de E/S.
`diskIO`	`avgQueueLen`	Avg Queue Size	El número de solicitudes que espera en la cola del dispositivo de E/S.
	`avgReqSz`	Ave Request Size	El tamaño promedio de la solicitudes, en kilobytes.

Grupo	Métrica	Nombre de la consola	Descripción
	`await`	Disk I/O Await	El número de milisegundos necesarios para responder a las solicitudes, incluido el tiempo de cola y el tiempo de servicio.
	`device`	No aplicable	El identificador del dispositivo de disco en uso.
	`readIOsPS`	Read IO/s	El número de operaciones de lectura por segundo.
	`readKb`	Read Total	El número total de kilobytes leídos.
	`readKbPS`	Read Kb/s	El número de kilobytes leídos por segundo.
	`readLatency`	Read Latency	El tiempo transcurrido entre el envío de una solicitud de E/S de lectura y su finalización, en milisegundos. Esta métrica solo está disponible para Amazon Aurora.
	`readThroughput`	Read Throughput	La cantidad de rendimiento de red utilizada por las solicitudes al clúster de bases de datos, en bytes por segundo. Esta métrica solo está disponible para Amazon Aurora.
	`rrqmPS`	Rrqms	El número de solicitudes leídas fusionadas en cola por segundo.
	`tps`	TPS	El número de transacciones de E/S por segundo.
	`util`	Disk I/O Util	El porcentaje de tiempo de CPU durante el cual se emitieron las solicitudes.
	`writeIOsPS`	Write IO/s	El número de operaciones de escritura por segundo.
	`writeKb`	Write Total	El número total de kilobytes escritos.

Grupo	Métrica	Nombre de la consola	Descripción
	`writeKbPS`	Write Kb/s	El número de kilobytes escritos por segundo.
	`writeLatency`	Write Latency	Tiempo medio transcurrido entre el envío de una solicitud de E/S de escritura y su finalización, en milisegundos. Esta métrica solo está disponible para Amazon Aurora.
	`writeThroughput`	Write Throughput	La cantidad de rendimiento de red utilizada por las respuestas del clúster de bases de datos, en bytes por segundo. Esta métrica solo está disponible para Amazon Aurora.
	`wrqmPS`	Wrqms	El número de solicitudes de escritura fusionadas en cola por segundo.
`physicalDeviceIO`	`avgQueueLen`	Tamaño medio de la cola de dispositivos físicos	El número de solicitudes que espera en la cola del dispositivo de E/S.
	`avgReqSz`	Tamaño de solicitud medio de dispositivos físicos	El tamaño promedio de la solicitudes, en kilobytes.
	`await`	Espera de E/S de disco de dispositivos físicos	El número de milisegundos necesarios para responder a las solicitudes, incluido el tiempo de cola y el tiempo de servicio.

Grupo	Métrica	Nombre de la consola	Descripción
	`device`	No aplicable	El identificador del dispositivo de disco en uso.
	`readIOsPS`	ES/s de lectura de dispositivos físicos	El número de operaciones de lectura por segundo.
	`readKb`	Total de lectura de dispositivos físicos	El número total de kilobytes leídos.
	`readKbPS`	Kb/s de lectura de dispositivos físicos	El número de kilobytes leídos por segundo.
	`rrqmPS`	Rrqms de dispositivos físicos	El número de solicitudes leídas fusionadas en cola por segundo.
	`tps`	TPS de dispositivos físicos	El número de transacciones de E/S por segundo.
	`util`	Util de E/S de disco de dispositivos físicos	El porcentaje de tiempo de CPU durante el cual se emitieron las solicitudes.
	`writeIOsPS`	ES/s de escritura de dispositivos físicos	El número de operaciones de escritura por segundo.

Grupo	Métrica	Nombre de la consola	Descripción
	`writeKb`	Total de escritura de dispositivos físicos	El número total de kilobytes escritos.
	`writeKbPS`	Kb/s de escritura de dispositivos físicos	El número de kilobytes escritos por segundo.
	`wrqmPS`	Wrqms de dispositivos físicos	El número de solicitudes de escritura fusionadas en cola por segundo.
`fileSys`	`maxFiles`	Max Inodes	El número máximo de archivos que se pueden crear para el sistema de archivos.
	`mountPoint`	No aplicable	La ruta al sistema de archivos.
	`name`	No aplicable	El nombre del sistema de archivos.
	`total`	Total Filesystem	La cantidad total de espacio en disco disponible para el sistema de archivos, en kilobytes.
	`used`	Used Filesystem	La cantidad de espacio en disco utilizado por los archivos en el sistema de archivos, en kilobytes.
	`usedFilePercent`	Used Inodes	El porcentaje de archivos disponibles en uso.
	`usedFiles`	Used%	El número de archivos en el sistema de archivos.

Grupo	Métrica	Nombre de la consola	Descripción
	`usedPercent`	Used Filesystem	El porcentaje de espacio en disco del sistema de archivos que está en uso.
`loadAverageMinute`	`fifteen`	Load Avg 15 min	El número de procesos que solicitan tiempo de la CPU en los últimos 15 minutos.
	`five`	Load Avg 5 min	El número de procesos que solicitan tiempo de la CPU en los últimos 5 minutos.
	`one`	Load Avg 1 min	El número de procesos que solicitan tiempo de la CPU en el último minuto.
`memory`	`active`	Active Memory	La cantidad de memoria asignada, en kilobytes.
	`buffers`	Buffered Memory	La cantidad de memoria utilizada para almacenar en búfer solicitudes de E/S antes de escribir en el dispositivo de almacenamiento, en kilobytes.
	`cached`	Cached Memory	La cantidad de memoria utilizada para almacenar en la caché las E/S basadas en el sistema de archivos.
	`dirty`	Dirty Memory	La cantidad de páginas de memoria en la RAM que se han modificado, pero no escrito, en su bloque de datos relacionado en el almacenamiento, en kilobytes.
	`free`	Free Memory	La cantidad de memoria no asignada, en kilobytes.
	`hugePagesFree`	Huge Pages Free	El número de páginas de gran tamaño libres. Las páginas de gran tamaño son una característica del kernel de Linux.
	`hugePagesRsvd`	Huge Pages Rsvd	El número de páginas de gran tamaño confirmadas.

Grupo	Métrica	Nombre de la consola	Descripción
	`hugePagesSize`	Huge Pages Size	El tamaño de cada unidad de páginas de gran tamaño, en kilobytes.
	`hugePagesSurp`	Huge Pages Surp	El número de páginas de gran tamaño sobrantes disponibles con respecto al total.
	`hugePagesTotal`	Huge Pages Total	El número total de páginas enormes.
	`inactive`	Inactive Memory	La cantidad de páginas de memoria utilizadas con menor frecuencia, en kilobytes.
	`mapped`	Mapped Memory	La cantidad total de contenido del sistema de archivos mapeado a la memoria dentro de un espacio de direcciones de proceso, en kilobytes.
	`pageTables`	Page Tables	La cantidad de memoria utilizada por tablas de página, en kilobytes.
	`slab`	Slab Memory	La cantidad de estructuras de datos de kernel reutilizables, en kilobytes.
	`total`	Memoria total	La cantidad total de memoria, en kilobytes.
	`writeback`	Writeback Memory	La cantidad de páginas desfasadas en la RAM que se siguen escribiendo en el almacenamiento de respaldo, en kilobytes.
`network`	`interface`	No aplicable	El identificador para la interfaz de red que se utiliza para la instancia de base de datos.
	`rx`	RX	El número de bytes recibidos por segundo.

Grupo	Métrica	Nombre de la consola	Descripción
	`tx`	TX	El número de bytes cargados por segundo.
`processList`	`cpuUsedPc`	CPU %	El porcentaje de CPU utilizado por el proceso.
	`id`	No aplicable	El identificador del proceso.
	`memoryUsedPc`	MEM%	El porcentaje de memoria que utiliza el proceso.
	`name`	No aplicable	El nombre del proceso.
	`parentID`	No aplicable	El identificador correspondiente al proceso principal.
	`rss`	RES	La cantidad de RAM asignada al proceso, en kilobytes.
	`tgid`	No aplicable	El identificador del grupo de subprocesos, que es un número que representa el ID del proceso al que pertenece un subproceso. Este identificador se utiliza para agrupar subprocesos del mismo proceso.
	`vss`	VIRT	La cantidad de memoria virtual asignada al proceso, en kilobytes.
`swap`	`total`	Swap	La cantidad de memoria de intercambio disponible, en kilobytes.
	`in`	Swaps in	La cantidad de memoria, en kilobytes, intercambiada desde disco.
	`out`	Swaps out	La cantidad de memoria, en kilobytes, intercambiada del disco.

Grupo	Métrica	Nombre de la consola	Descripción
	`free`	Free Swap	La cantidad de memoria de intercambio no asignada, en kilobytes.
	`cached`	Committed Swap	La cantidad de memoria de intercambio, en kilobytes, utilizada como memoria caché.
`tasks`	`blocked`	Tasks Blocked	El número de tareas que están bloqueadas.
	`running`	Tasks Running	El número de tareas que están en ejecución.
	`sleeping`	Tasks Sleeping	El número de tareas que están inactivas.
	`stopped`	Tasks Stopped	El número de tareas que se han detenido.
	`total`	Tasks Total	El número total de tareas.
	`zombie`	Tasks Zombie	El número de tareas secundarias inactivas con una tarea principal activa.

Métricas del sistema operativo para Microsoft SQL Server

Grupo	Métrica	Nombre de la consola	Descripción
`General`	`engine`	No aplicable	El motor de base de datos para la instancia de base de datos.
	`instanceID`	No aplicable	El identificador de instancias de base de datos.

Grupo	Métrica	Nombre de la consola	Descripción
	instanceResourceID	No aplicable	Un identificador inmutable para la instancia de base de datos que es exclusivo de una región de AWS, también utilizado como identificador de secuencia de registro.
	numVCPUs	No aplicable	El número de CPU virtuales para la instancia de base de datos.
	timestamp	No aplicable	La hora a la que se tomó la métrica.
	uptime	No aplicable	La cantidad de tiempo que ha estado activa la instancia de base de datos.
	version	No aplicable	La versión del formato JSON del flujo de la métrica del SO.
cpuUtilization	idle	CPU Idle	El porcentaje inactivo de CPU.
	kern	CPU Kernel	El porcentaje de CPU utilizado por el kernel.
	user	CPU User	El porcentaje de CPU utilizado por programas de usuario.
disks	name	No aplicable	El identificador para el disco.
	totalKb	Total Disk Space	El espacio total del disco, en kilobytes.
	usedKb	Used Disk Space	La cantidad de espacio utilizado en el disco, en kilobytes.
	usedPc	Used Disk Space %	El porcentaje de espacio utilizado en el disco.
	availKb	Available Disk Space	El espacio disponible en el disco, en kilobytes.

Grupo	Métrica	Nombre de la consola	Descripción
	availPc	Available Disk Space %	El porcentaje de espacio disponible en el disco.
	rdCountPS	Reads/s	El número de operaciones de lectura por segundo.
	rdBytesPS	Read Kb/s	El número de bytes leídos por segundo.
	wrCountPS	Write IO/s	El número de operaciones de escritura por segundo.
	wrBytesPS	Write Kb/s	La cantidad de bytes escritos por segundo.
memory	commitTotKb	Commit Total	La cantidad de espacio de direcciones virtual respaldado por archivo de paginación en uso, es decir, la carga de confirmación actual. Este valor está compuesto por la memoria principal (RAM) y el disco (archivos de paginación).
	commitLimitKb	Maximum Commit	El valor máximo posible para la métrica commitTotKb . Este valor es la suma del tamaño de archivo de paginación actual más la memoria física disponible para contenido paginable, se excluye la RAM asignada a áreas no paginables.
	commitPeakKb	Commit Peak	El valor máximo de la métrica commitTotKb desde la última vez que se inició el sistema operativo.
	kernTotKb	Total Kernel Memory	La suma de la memoria en los grupos de kernel paginados y no paginados, en kilobytes.
	kernPagedKb	Paged Kernel Memory	La cantidad de memoria en el grupo de kernel paginado, en kilobytes.

Grupo	Métrica	Nombre de la consola	Descripción
	kernNonpagedKb	Nonpaged Kernel Memory	La cantidad de memoria en el grupo de kernel no paginado, en kilobytes.
	pageSize	Page Size	El tamaño de una página, en bytes.
	physTotKb	Memoria total	La cantidad de memoria física, en kilobytes.
	physAvailKb	Memoria disponible	La cantidad de memoria física disponible, en kilobytes.
	sqlServerTotKb	SQL Server Total Memory	La cantidad de memoria confirmada a SQL Server, en kilobytes.
	sysCacheKb	System Cache	La cantidad de memoria caché del sistema, en kilobytes.
network	interface	No aplicable	El identificador para la interfaz de red que se utiliza para la instancia de base de datos.
	rdBytesPS	Network Read Kb/s	El número de bytes recibidos por segundo.
	wrBytesPS	Network Write Kb/s	El número de bytes enviados por segundo.
processList	cpuUsedPc	Used%	El porcentaje de CPU utilizado por el proceso.
	memUsedPc	MEM%	El porcentaje de memoria total utilizada por el proceso.
	name	No aplicable	El nombre del proceso.
	pid	No aplicable	El identificador del proceso. Este valor no está presente para procesos propiedad de Amazon RDS.

Grupo	Métrica	Nombre de la consola	Descripción
	ppid	No aplicable	El identificador correspondiente al proceso principal. Este valor solo está presente para procesos secundarios.
	tid	No aplicable	El identificador del subproceso. Este valor solo está presente para subprocesos. El proceso de propiedad puede identificarse mediante el valor pid.
	workingSetKb	No aplicable	La cantidad de memoria en el conjunto de trabajo privado más la cantidad de memoria en uso por parte del proceso y que puede compartirse con otros procesos, en kilobytes.
	workingSetPrivKb	No aplicable	La cantidad de memoria en uso por parte de un proceso, pero que no puede compartirse con otros procesos, en kilobytes.
	workingSetShareableKb	No aplicable	La cantidad de memoria en uso por parte de un proceso y que puede compartirse con otros procesos, en kilobytes.
	virtKb	No aplicable	La cantidad de espacio de direcciones virtual que está utilizando el proceso, en kilobytes . El uso del espacio de direcciones virtual no implica necesariamente que corresponda al uso de las páginas de memoria principal o del disco.
system	handles	Handles	El número de controladores que está usando el sistema.
	processes	Processes	El número de procesos que se están ejecutando en el sistema.

Grupo	Métrica	Nombre de la consola	Descripción
	`threads`	Threads	El número de subprocesos que se están ejecutando en el sistema.

Supervisión de eventos, registros y flujos en una instancia de Amazon RDS

Cuando supervisa sus bases de datos de Amazon RDS y sus otras soluciones de AWS, su objetivo es mantener lo siguiente:

- Fiabilidad
- Disponibilidad
- Rendimiento
- Seguridad

Supervisión de métricas en una instancia de Amazon RDS explica cómo supervisar su instancia mediante las métricas. Una solución completa también debe supervisar los eventos, los archivos de registro y los flujos de actividad de la base de datos. AWS le proporciona las siguientes herramientas de supervisión:

- Amazon EventBridge es un bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de varios orígenes. EventBridge proporciona un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y servicios de AWS. EventBridge dirige esos datos a los objetivos, como AWS Lambda. De esta forma, puede supervisar los eventos que ocurren en los servicios y crear arquitecturas basadas en eventos. Para más información, consulte la Guía del usuario de Amazon EventBridge.
- Registros de Amazon CloudWatch le permite supervisar, almacenar y acceder a los archivos de registro desde instancias de Amazon RDS, AWS CloudTrail y otros orígenes. registros de Amazon Cloudwatch puede supervisar información en los archivos de registro y enviar una notificación cuando se llega a determinados umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulte la Guía del usuario de Registros de Amazon CloudWatch.
- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su cuenta de Cuenta de AWS o en su nombre. CloudTrail entrega los archivos de registros a un bucket de Amazon S3 que especifique. También puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para más información, consulte la Guía del usuario de AWS CloudTrail.

- Los flujos de actividad de la base de datos son una característica de Amazon RDS que proporciona un flujo casi en tiempo real de la actividad en su clúster de base de datos. Amazon RDS envía actividades a un flujo de datos de Amazon Kinesis. El flujo de Kinesis se crea automáticamente. Desde Kinesis, puede configurar servicios de AWS como Amazon Data Firehose y AWS Lambda para utilizar el flujo y almacenar los datos.

Temas

- Visualización de los registros, los eventos y los flujos en la consola de Amazon RDS
- Supervisión de eventos de Amazon RDS
- Supervisión de archivos de registro de Amazon RDS
- Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail
- Supervisión de Amazon RDS con flujos de actividad de la base de datos
- Supervisión de amenazas con Amazon GuardDuty para protección de RDS

Visualización de los registros, los eventos y los flujos en la consola de Amazon RDS

Amazon RDS se integra con Servicios de AWS para mostrar información sobre registros, eventos y flujos de actividad de bases de datos en la consola de RDS.

La pestaña Logs & events (Registros y eventos) para la instancia de base de datos de Aurora muestra la siguiente información:

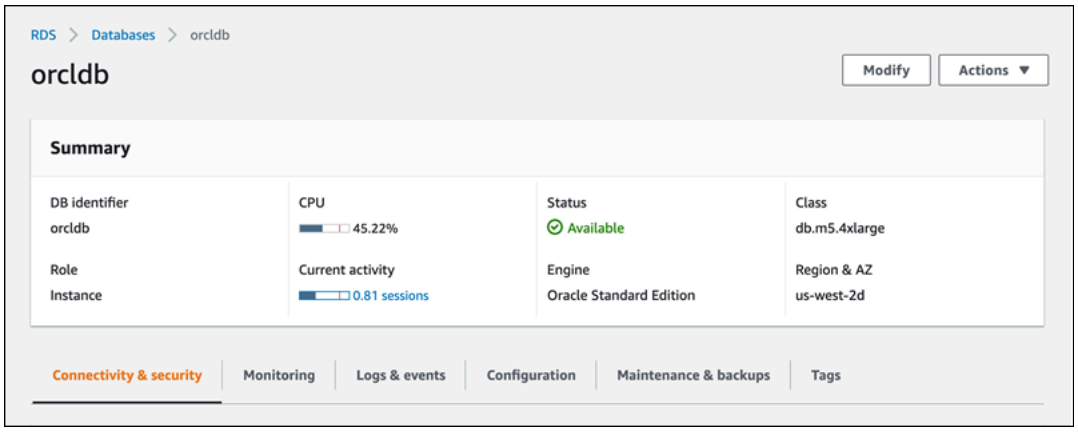
- Amazon CloudWatch alarms (Alarmas de Amazon CloudWatch): muestra las alarmas de métricas que ha configurado para la instancia de base de datos. Si no ha configurado las alarmas, puede crearlas en la consola de RDS. Para obtener más información, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch.
- Recent events (Eventos recientes): muestra un resumen de los eventos (cambios de entorno) para la instancia de base de datos o Aurora. Para obtener más información, consulte Consulta de eventos de Amazon RDS.
- Logs (Registros): muestra los archivos de registro de base de datos generados por una instancia de base de datos. Para obtener más información, consulte Supervisión de archivos de registro de Amazon RDS.

La pestaña Configuration (Configuración) muestra información sobre flujos de actividad de la base de datos.

Para ver los registros, eventos y flujos de su clúster de bases de datos de en la consola de RDS

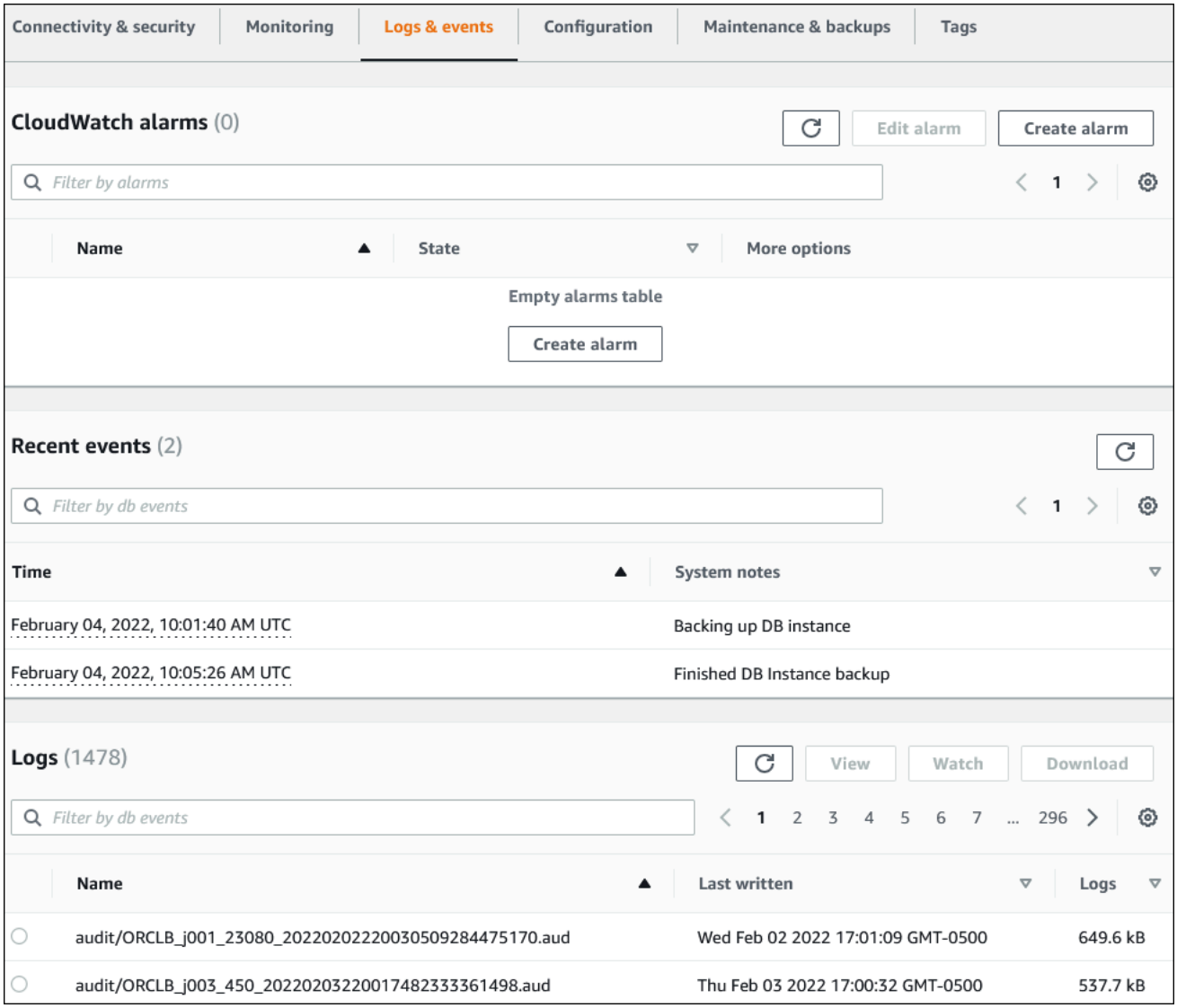
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el nombre de su clúster de bases de datos de que desea supervisar.

   Aparece la página de la base de datos. En el siguiente ejemplo, se muestra una base de datos Oracle denominada `orclb`.



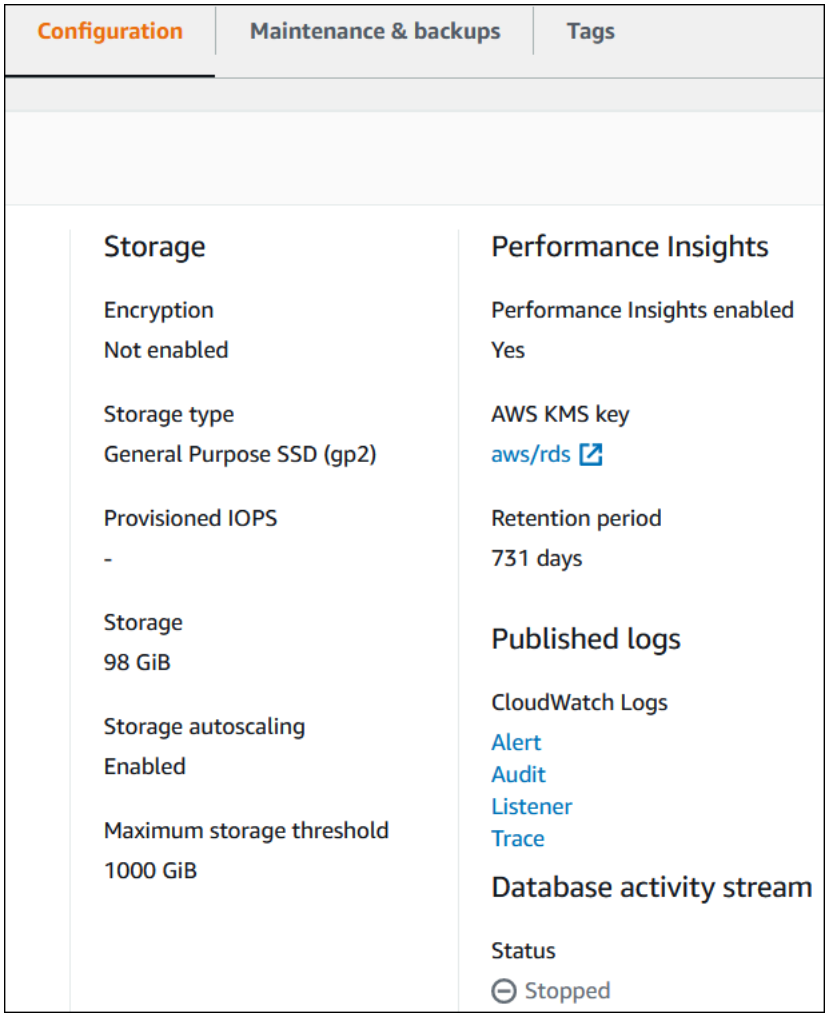
4. Seleccione Logs & events (Registros y eventos).

   Aparece la sección Logs & events (Registros y eventos).



5. Elija Configuration (Configuración).

   En el siguiente ejemplo, se muestra el estado de los flujos de actividad de la base de datos para la instancia de base de datos.


Configuration
Maintenance & backups
Tags
Storage
Encryption
Not enabled
Storage type
General Purpose SSD (gp2)
Provisioned IOPS
-
Storage
98 GiB
Storage autoscaling
Enabled
Maximum storage threshold
1000 GiB
Performance Insights
Performance Insights enabled
Yes
AWS KMS key
aws/rds
Retention period
731 days
Published logs
CloudWatch Logs
Alert
Audit
Listener
Trace
Database activity stream
Status
Stopped

Supervisión de eventos de Amazon RDS

Un evento indica un cambio en el entorno. Puede ser un entorno de AWS, un servicio o aplicación de socios SaaS o una aplicación o servicio personalizados. Para obtener descripciones de los eventos de RDS, consulte Categorías y mensajes de eventos de Amazon RDS.

Temas

- Información general de los eventos para Amazon RDS
- Consulta de eventos de Amazon RDS
- Uso de notificaciones de eventos de Amazon RDS
- Creación de una regla que se desencadena en función de un evento Amazon RDS
- Categorías y mensajes de eventos de Amazon RDS

Información general de los eventos para Amazon RDS

Un evento de RDS indica un cambio en el entorno de Amazon RDS. Por ejemplo, Amazon RDS genera un evento cuando el estado de una instancia de base de datos cambia de pendiente a en ejecución. Amazon RDS envía eventos a EventBridge casi en tiempo real.

> **Note**
>
> Amazon RDS emite eventos de la mejor forma posible. Recomendamos que evite escribir programas que dependan del orden o de la existencia de eventos de notificación, ya que pueden faltar o no estar ordenados.

Amazon RDS registra eventos relacionados con los siguientes recursos:

- Instancias de base de datos

  Para obtener una lista de los eventos de instancia de base de datos, consulte Eventos de instancia de base de datos.
- Grupos de parámetros de base de datos

  Para obtener una lista de eventos de grupos de parámetros de base de datos, consulte Eventos de grupo de parámetros de base de datos.
- Grupos de seguridad de base de datos

Para obtener una lista de eventos de grupo de seguridad de base de datos, consulte Eventos de grupo de seguridad de base de datos.

- Instantáneas de base de datos

  Para obtener una lista de los eventos de instantánea de base de datos, consulte Eventos de instantánea de base de datos.

- Eventos de RDS Proxy

  Para obtener una lista de los eventos de RDS Proxy, consulte Eventos de RDS Proxy.

- Eventos de implementación azul/verde

  Para obtener una lista de los eventos de implementación azul/verde, consulte Eventos de implementación azul/verde.

La información incluye lo siguiente:

- La fecha y la hora del evento
- El nombre de origen y el tipo de origen del evento
- Un mensaje asociado al evento
- Las notificaciones de eventos incluyen etiquetas de cuando se envió el mensaje y es posible que no reflejen las etiquetas del momento en que se produjo el evento.

Consulta de eventos de Amazon RDS

Puede recuperar la siguiente información del evento para sus recursos de Amazon RDS:

- Nombre del recurso
- Tipo de recurso
- Hora del evento
- Resumen del mensaje del evento

Puede acceder a los eventos en las siguientes partes de la:AWS Management Console

- La pestaña Eventos, que muestra los eventos de las últimas 24 horas.
- La tabla Eventos recientes de la sección Registros y eventos de la pestaña Bases de datos, que puede mostrar los eventos de las últimas 2 semanas.

También puede recuperar eventos utilizando el comando describe-events de la AWS CLI o la operación DescribeEvents de la API de RDS. Si utiliza la AWS CLI o la API de RDS para ver eventos, puede recuperar eventos de los últimos 14 días como máximo.

> **Note**
>
> Si necesita almacenar eventos durante periodos de tiempo más largos, puede enviar eventos de Amazon RDS a EventBridge. Para obtener más información, consulte Creación de una regla que se desencadena en función de un evento Amazon RDS.

Para obtener descripciones de los eventos de Amazon RDS, consulte Categorías y mensajes de eventos de Amazon RDS.

Para acceder a información detallada sobre los eventos mediante AWS CloudTrail, incluidos los parámetros de la solicitud, consulte Eventos de CloudTrail.

Consola

Para ver todos los eventos de Amazon RDS de las últimas 24 horas

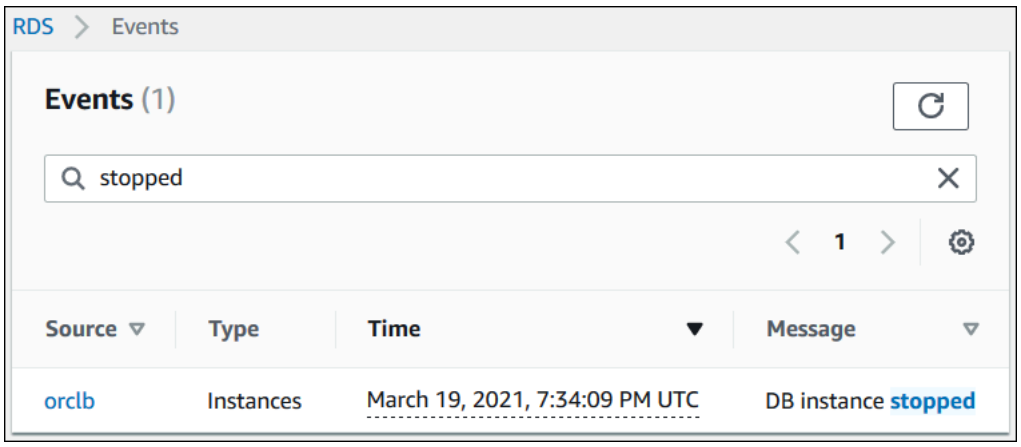
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Events.

   Los eventos disponibles aparecen en una lista.

3. (Opcional) Ingrese una palabra de búsqueda para filtrar los resultados.

   En el siguiente ejemplo se muestra una lista de eventos filtrados por los caracteres **`stopped`**.



AWS CLI

Para ver todos los eventos generados en la última hora, llame a describe-events sin parámetros.

```
aws rds describe-events
```

El siguiente ejemplo muestra que se ha detenido una instancia de base de datos.

```
{
    "Events": [
        {
            "EventCategories": [
                "notification"
            ],
            "SourceType": "db-instance",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:testinst",
            "Date": "2022-04-22T21:31:00.681Z",
            "Message": "DB instance stopped",
            "SourceIdentifier": "testinst"
        }
    ]
}
```

Para ver todos los eventos de Amazon RDS de los últimos 10 080 minutos (7 días), llame al comando describe-events de la AWS CLI y establezca el parámetro `--duration` en `10080`.

```
aws rds describe-events --duration 10080
```

El siguiente ejemplo muestra los eventos del intervalo de tiempo especificado para la instancia de base de datos *test-instance*.

```
aws rds describe-events \
    --source-identifier test-instance \
    --source-type db-instance \
    --start-time 2022-03-13T22:00Z \
    --end-time 2022-03-13T23:59Z
```

El siguiente ejemplo muestra el estado de una copia de seguridad.

```
{
    "Events": [
        {
            "SourceType": "db-instance",
            "SourceIdentifier": "test-instance",
            "EventCategories": [
                "backup"
            ],
            "Message": "Backing up DB instance",
            "Date": "2022-03-13T23:09:23.983Z",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"
        },
        {
            "SourceType": "db-instance",
            "SourceIdentifier": "test-instance",
            "EventCategories": [
                "backup"
            ],
            "Message": "Finished DB Instance backup",
            "Date": "2022-03-13T23:15:13.049Z",
            "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance"
        }
    ]
}
```

API

Puede ver todos los eventos de las instancias de Amazon RDS de los últimos 14 días llamando a la operación DescribeEvents de la API de RDS y estableciendo el parámetro `Duration` en `20160`.

Uso de notificaciones de eventos de Amazon RDS

Amazon RDS utiliza Amazon Simple Notification Service (Amazon SNS) para proporcionar una notificación cuando se produce un evento de Amazon RDS. Estas notificaciones pueden realizarse con cualquier método que admita Amazon SNS para una región de AWS, como un email, un mensaje de texto o una llamada a un punto de enlace HTTP.

Temas

- Información general de las notificaciones de eventos de Amazon RDS
- Concesión de permisos para publicar notificaciones en un tema de Amazon SNS
- Suscripción a notificaciones de eventos de Amazon RDS
- Atributos y etiquetas de notificación de eventos de Amazon RDS
- Descripción de suscripciones a notificaciones de eventos de Amazon RDS
- Modificación de una suscripción a notificaciones de eventos de Amazon RDS
- Agregar un identificador de origen a una suscripción de notificación de eventos de Amazon RDS
- Quitar un identificador de origen de una suscripción de notificación de eventos de Amazon RDS
- Descripción de la lista de categorías de notificaciones de eventos de Amazon RDS
- Eliminar una suscripción de notificación de eventos de Amazon RDS

Información general de las notificaciones de eventos de Amazon RDS

Amazon RDS agrupa los eventos en categorías a las que puede suscribirse para recibir una notificación cada vez que se produzca un evento en esa categoría.

Temas

- Recursos de RDS aptos para la suscripción a eventos
- Proceso básico para suscribirse a las notificaciones de eventos de Amazon RDS
- Entrega de notificaciones de eventos de RDS
- Facturación de notificaciones de eventos de Amazon RDS
- Ejemplos de eventos de Amazon RDS con Amazon EventBridge

Recursos de RDS aptos para la suscripción a eventos

Puede suscribirse a una categoría de evento para los recursos siguientes:

- Instancia de base de datos
- instantánea de base de datos
- Grupo de parámetros de base de datos
- Grupo de seguridad de base de datos
- RDS Proxy
- Versión del motor personalizada

Por ejemplo, si se suscribe a la categoría de copia de seguridad de una instancia de base de datos determinada, recibirá una notificación cada vez que se produzca un evento relacionado con las copias de seguridad que afecte a la instancia de base de datos. Si se suscribe a una categoría de cambio de configuración para una instancia de base de datos, recibirá una notificación cuando la instancia de base de datos se modifique. También recibirá una notificación cuando cambie una suscripción de notificación de eventos.

Es posible que desee crear varias suscripciones diferentes. Por ejemplo, puede crear una suscripción que reciba todas las notificaciones de eventos de todas las instancias de base de datos y otra que incluya solo los eventos fundamentales de un subconjunto de instancias de base de datos. Para la segunda suscripción, especifique una o más instancias de base de datos en el filtro.

Proceso básico para suscribirse a las notificaciones de eventos de Amazon RDS

El proceso para suscribirse a las notificaciones de eventos de Amazon RDS es el siguiente:

1. Cree una suscripción de notificación de eventos de Amazon RDS mediante la consola de Amazon RDS, la AWS CLI o la API.

   Amazon RDS utiliza el ARN de un tema de Amazon SNS para identificar cada suscripción. La consola de Amazon RDS crea el ARN automáticamente cuando se crea la suscripción. Cree el ARN a través de la consola de Amazon SNS, la AWS CLI o la API de Amazon SNS.
2. Amazon RDS envía un mensaje de correo electrónico o SMS de aprobación a las direcciones que envió con la suscripción.
3. Para confirmar la suscripción, elija el enlace de la notificación que ha recibido.
4. La consola de Amazon RDS actualiza la sección My Event Subscriptions (Mis suscripciones a eventos) con el estado de la suscripción.
5. Amazon RDS empieza a enviar notificaciones a las direcciones que se proporcionan al crear la suscripción.

Para obtener información acerca de Identity and access management cuando se utilice Amazon SNS, consulte Identity and access management en Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Puede utilizar AWS Lambda para procesar notificaciones de eventos desde una instancia de base de datos. Para obtener más información, consulte Uso de AWS Lambda con Amazon RDS en la Guía para desarrolladores de AWS Lambda.

Entrega de notificaciones de eventos de RDS

Amazon RDS envía notificaciones a las direcciones que se proporcionan al crear la suscripción. La notificación puede incluir atributos de mensaje que proporcionan metadatos estructurados sobre el mensaje. Para obtener más información acerca de los atributos de los mensajes, consulte Categorías y mensajes de eventos de Amazon RDS.

Las notificaciones de eventos pueden tardar hasta cinco minutos en entregarse.

> **Important**
>
> Amazon RDS no garantiza el orden de los eventos enviados en una secuencia de eventos. El orden de los eventos está sujeto a cambio.

Cuando Amazon SNS envía una notificación a un punto de enlace HTTP o HTTPS suscrito, el cuerpo del mensaje POST enviado al punto de enlace contiene un documento JSON. Para obtener más información, consulte Formatos de mensaje y JSON de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Puede configurar SNS para que le notifique con mensajes de texto. Para obtener más información, consulte Mensajería de texto móvil (SMS) en la Guía para desarrolladores de Simple Notification Service.

Para desactivar las notificaciones sin eliminar una suscripción, elija No en Enabled (Habilitado) en la consola de Amazon RDS. O bien, puede establecer el parámetro `Enabled` en `false` mediante la AWS CLI o la API de Amazon RDS.

Facturación de notificaciones de eventos de Amazon RDS

La facturación de notificaciones de eventos de Amazon RDS se efectúa a través de Amazon SNS. Se aplican las tarifas de Amazon SNS cuando se utiliza la notificación de eventos. Para obtener más

información sobre la facturación de Amazon SNS, consulte Precios de Amazon Simple Notification Service.

Ejemplos de eventos de Amazon RDS con Amazon EventBridge

Los siguientes ejemplos muestran los diferentes tipos de eventos de Amazon RDS en formato JSON. Para ver un tutorial que muestra cómo capturar y ver eventos en formato JSON, consulte Tutorial: Registrar el estado de una instancia de base de datos con Amazon EventBridge.

Temas

- Ejemplo de evento de instancia de base de datos
- Ejemplo de evento de grupo de parámetros de base de datos
- Ejemplo de evento de instantánea de base de datos

Ejemplo de evento de instancia de base de datos

A continuación, se muestra un ejemplo de un evento de instancia de base de datos en formato JSON. El evento muestra que RDS realizó una conmutación por error Multi-AZ para la instancia denominada `my-db-instance`. El ID de evento es RDS-EVENT-0049.

```
{
  "version": "0",
  "id": "68f6e973-1a0c-d37b-f2f2-94a7f62ffd4e",
  "detail-type": "RDS DB Instance Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-09-27T22:36:43Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:rds:us-east-1:123456789012:db:my-db-instance"
  ],
  "detail": {
    "EventCategories": [
      "failover"
    ],
    "SourceType": "DB_INSTANCE",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:db:my-db-instance",
    "Date": "2018-09-27T22:36:43.292Z",
    "Message": "A Multi-AZ failover has completed.",
    "SourceIdentifier": "my-db-instance",
    "EventID": "RDS-EVENT-0049"
```

```
  }
}
```

Ejemplo de evento de grupo de parámetros de base de datos

A continuación, se muestra un ejemplo de un evento de grupo de parámetros de base de datos en formato JSON. El evento muestra que el parámetro `time_zone` se actualizó en el grupo de parámetros `my-db-param-group`. El ID de evento es RDS-EVENT-0037.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
  "detail-type": "RDS DB Parameter Group Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-10-06T12:26:13Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:rds:us-east-1:123456789012:pg:my-db-param-group"
  ],
  "detail": {
    "EventCategories": [
      "configuration change"
    ],
    "SourceType": "DB_PARAM",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:pg:my-db-param-group",
    "Date": "2018-10-06T12:26:13.882Z",
    "Message": "Updated parameter time_zone to UTC with apply method immediate",
    "SourceIdentifier": "my-db-param-group",
    "EventID": "RDS-EVENT-0037"
  }
}
```

Ejemplo de evento de instantánea de base de datos

A continuación, se muestra un ejemplo de un evento de instantánea de base de datos en formato JSON. El evento muestra la eliminación de la instantánea denominada `my-db-snapshot`. El ID de evento es RDS-EVENT-0041.

```
{
  "version": "0",
  "id": "844e2571-85d4-695f-b930-0153b71dcb42",
```

```
  "detail-type": "RDS DB Snapshot Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-10-06T12:26:13Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:rds:us-east-1:123456789012:snapshot:rds:my-db-snapshot"
  ],
  "detail": {
    "EventCategories": [
      "deletion"
    ],
    "SourceType": "SNAPSHOT",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:snapshot:rds:my-db-snapshot",
    "Date": "2018-10-06T12:26:13.882Z",
    "Message": "Deleted manual snapshot",
    "SourceIdentifier": "my-db-snapshot",
    "EventID": "RDS-EVENT-0041"
  }
}
```

Concesión de permisos para publicar notificaciones en un tema de Amazon SNS

Para conceder a Amazon RDS permisos para publicar notificaciones en un tema de Amazon Simple Notification Service (Amazon SNS), adjunte una política de AWS Identity and Access Management (IAM) al tema de destino. Para obtener más información sobre los permisos, consulte Ejemplos de casos de control de acceso con Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

De forma predeterminada, un tema de Amazon SNS tiene una política que permite a todos los recursos de Amazon RDS de la misma cuenta publicar notificaciones en él. Puede adjuntar una política personalizada para permitir las notificaciones entre cuentas o para restringir el acceso a determinados recursos.

A continuación se muestra un ejemplo de una política de IAM que se asocia al tema de Amazon SNS de destino. Restringe el tema a instancias de base de datos con nombres que coinciden con el prefijo especificado. Para utilizar esta política, especifique los siguientes valores:

- `Resource`: el nombre de recurso de Amazon (ARN) para el tema de Amazon SNS
- `SourceARN`: su ARN de recursos de RDS
- `SourceAccount`: su ID de Cuenta de AWS

Para ver una lista de tipos de recursos y sus ARN, consulte Tipos de recurso definidos por Amazon RDS en la Referencia de autorizaciones de servicio.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.rds.amazonaws.com"
      },
      "Action": [
        "sns:Publish"
      ],
      "Resource": "arn:aws:sns:us-east-1:123456789012:topic_name",
      "Condition": {
```

```
        "ArnLike": {
          "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:prefix-*"
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

Suscripción a notificaciones de eventos de Amazon RDS

La forma más sencilla de crear una suscripción es con la consola de RDS. Si decide crear las suscripciones de notificaciones de eventos a través de la CLI o la API, debe crear un tema de Amazon Simple Notification Service y suscribirse a dicho tema con la consola de Amazon SNS o la API de Amazon SNS. También deberá conservar el Nombre de recurso de Amazon (ARN) del tema, ya que este se utiliza al enviar los comandos de la CLI o las operaciones de la API. Para obtener información acerca de cómo crear un tema de SNS y suscribirse a él, consulte Introducción a Amazon SNS en la Guía del desarrollador de Amazon Simple Notification Service.

Puede especificar el tipo de origen sobre el que desea recibir notificaciones y el origen de Amazon RDS que inicia el evento:

Source type (Tipo de origen)

Tipo de origen. Por ejemplo, Source Type (Tipo de origen) podría ser Instances (Instancias). Debe elegir un tipo de origen.

Resources to include (Recursos a incluir)

Los recursos de Amazon RDS que están generando los eventos. Por ejemplo, es posible que tenga que elegir Select specific instances (Seleccionar instancias específicas) y luego myDBInstance1.

En la siguiente tabla se explica lo que ocurre si se especifica o no ***Resources*** to include (Recursos a incluir).

Recursos a incluir	Descripción	Ejemplo
Especificado	RDS le notifica todos los eventos relacionados únicamente con el recurso especificado.	Si Source type (Tipo de origen) es Instances (Instancias) y tu recurso es myDBInstance1, RDS le notifica sobre todos los eventos de MyDBInstance1 únicamente.

Recursos a incluir	Descripción	Ejemplo
No especificada	RDS le notifica los eventos del tipo de origen especificado para todos los recursos de Amazon RDS.	Si Source type (Tipo de origen) es Instances (Instancias), RDS le notifica sobre todos los eventos relacionados con las instancias en su cuenta.

Un suscriptor de temas de Amazon SNS recibe de forma predeterminada todos los mensajes publicados en el tema. Para recibir solo un subconjunto de los mensajes, el suscriptor debe asignar una política de filtrado a la suscripción del tema. Para obtener más información sobre el filtrado de mensajes SNS, consulte Filtrado de mensajes en Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Consola

Para suscribirse a las notificaciones de eventos de RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación seleccione Event Subscriptions (Suscripciones de eventos).
3. En la página Event Subscriptions (Suscripciones de eventos) seleccione Create Event Subscription (Crear suscripción de eventos).
4. Introduzca los detalles de su suscripción de la siguiente manera:
   a. En Name (Nombre) escriba un nombre para la suscripción de notificación de evento.
   b. En Send notification to (Enviar notificaciones a), realice una de las siguientes acciones:
      - Elija New email topic (Nuevo tema de correo electrónico). Introduzca un nombre para su tema de correo electrónico y una lista de destinatarios. Le recomendamos que configure las suscripciones a los eventos con la misma dirección de correo electrónico que tiene el contacto principal de su cuenta. Las recomendaciones, los eventos de servicio y los mensajes sanitarios personales se envían a través de diferentes canales. Las suscripciones a la misma dirección de correo electrónico garantizan que todos los mensajes se consoliden en una sola ubicación.

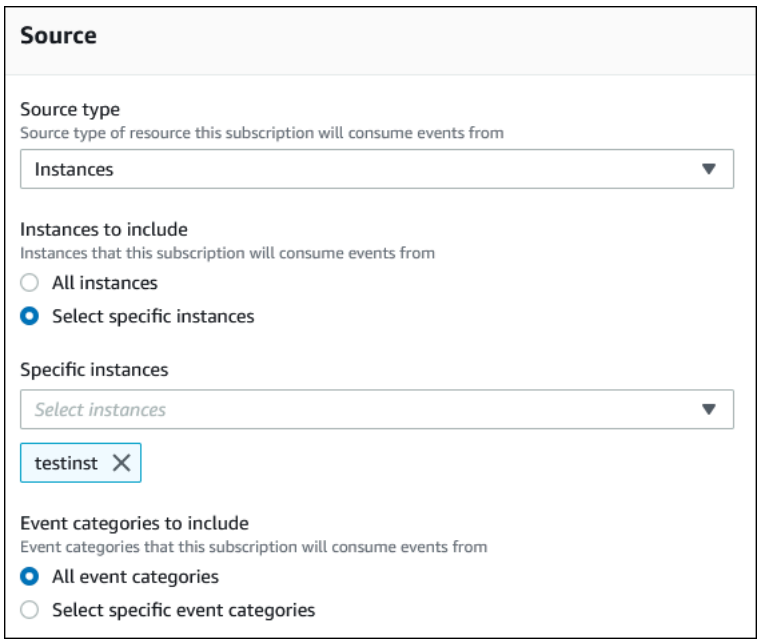
- Elija Amazon Resource Name (ARN) [Nombre de recurso de Amazon (ARN)]. A continuación, seleccione el ARN de Amazon SNS existente para un tema de Amazon SNS.

  Si desea utilizar un tema que se haya habilitado para el cifrado del servidor (SSE), conceda a Amazon RDS los permisos necesarios para acceder a la AWS KMS key. Para obtener más información, consulte Habilitar la compatibilidad entre los orígenes de eventos de los servicios de AWS y los temas cifrados en la Guía para desarrolladores de Amazon Simple Notification Service.

c. En Source type (Tipo de origen) elija un tipo de origen. Por ejemplo, elija Instances (Instancias) o Parameter groups(Grupos de parámetros).

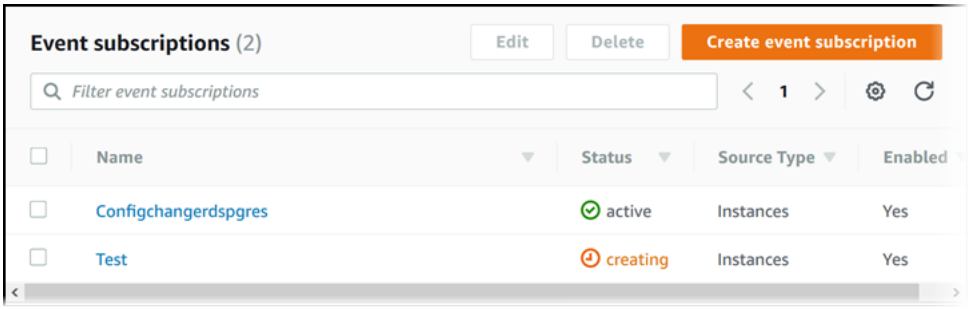
d. Elija las categorías y recursos del evento de las que desea recibir notificaciones.

   En el ejemplo siguiente se configuran las notificaciones de eventos de la instancia de base de datos denominada `testinst`.



e. Seleccione Crear.

La consola de Amazon RDS indica que se está creando la suscripción.



AWS CLI

Para suscribirse a notificaciones de eventos de RDS, utilice el comando AWS CLI de la `create-event-subscription`. Incluya los siguientes parámetros obligatorios:

- `--subscription-name`
- `--sns-topic-arn`

Example

Para Linux, macOS o:Unix

```
aws rds create-event-subscription \
    --subscription-name myeventsubscription \
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:myawsuser-RDS \
    --enabled
```

En:Windows

```
aws rds create-event-subscription ^
    --subscription-name myeventsubscription ^
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:myawsuser-RDS ^
    --enabled
```

API

Para suscribirse a notificaciones de eventos de Amazon RDS, llame a la función `CreateEventSubscription` de la API de Amazon RDS. Incluya los siguientes parámetros obligatorios:

- `SubscriptionName`

- `SnsTopicArn`

Atributos y etiquetas de notificación de eventos de Amazon RDS

Cuando Amazon RDS envía una notificación de evento a Amazon Simple Notification Service (SNS) o Amazon EventBridge, esa notificación contiene los atributos del mensaje y las etiquetas del evento. RDS envía los atributos del mensaje por separado junto con el mensaje, mientras que las etiquetas de eventos se encuentran en el cuerpo del mensaje. Utilice los atributos de los mensajes y las etiquetas de Amazon RDS para añadir metadatos a sus recursos. Puede modificar estas etiquetas con sus propias anotaciones sobre las instancias de base de datos. Para obtener más información acerca del etiquetado de recursos de Amazon RDS, consulte Etiquetado de los recursos de y Amazon RDS.

De forma predeterminada, Amazon SNS y Amazon EventBridge reciben todos los mensajes que se les envían. SNS y EventBridge pueden filtrar el mensaje y enviar las notificaciones a través del método de comunicación que se prefiera, como un correo electrónico, un mensaje de texto o una llamada a un punto de conexión HTTP.

> **Note**
>
> La notificación que se envía por correo electrónico o en mensaje de texto no tiene etiquetas de evento.

En la tabla siguiente, se muestran los atributos de mensaje para los eventos de RDS que se han enviado al suscriptor de temas.

Atributo de evento de Amazon RDS	Descripción
EventID	Identificador de mensajes de eventos de RDS, por ejemplo, RDS-EVENT-0006.
Recurso	Identificador ARN del recurso que emite el evento como, por ejemplo, `arn:aws:rds:ap-southeast-2:123456789012:db:database-1` .

Las etiquetas RDS proporcionan datos sobre el recurso afectado por el evento de servicio. RDS añade el estado actual de las etiquetas en el cuerpo del mensaje cuando la notificación se envía a SNS o EventBridge.

Para obtener más información sobre el filtrado de atributos de mensajes SNS, consulte Filtrado de mensajes en Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Para obtener más información sobre etiquetas de eventos de EventBridge, consulte Operadores de comparación para su uso en patrones de eventos en Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Para obtener más información sobre el filtrado etiquetas basadas en cargas útiles para SNS, consulte Introducing payload-based message filtering for Amazon SNS.

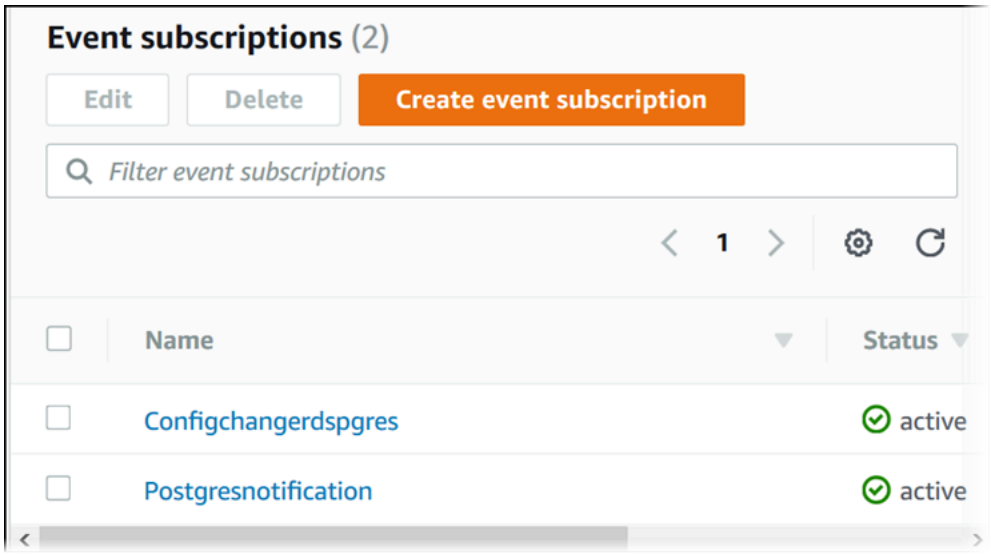
Descripción de suscripciones a notificaciones de eventos de Amazon RDS

Puede mostrar las suscripciones actuales de notificación de eventos de Amazon RDS.

Consola

Pasos mostrar las sus suscripciones actuales de notificación de eventos de Amazon RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación seleccione Event Subscriptions (Suscripciones de eventos). El panel Event subscriptions (Suscripciones de eventos) muestra todas sus suscripciones a notificaciones de eventos.



AWS CLI

Para obtener una lista de sus suscripciones a notificaciones de eventos de Amazon RDS, utilice el comando `describe-event-subscriptions` de la AWS CLI.

Example

En el siguiente ejemplo se obtienen todas las suscripciones a eventos.

```
aws rds describe-event-subscriptions
```

En el siguiente ejemplo se obtiene la descripción de `myfirsteventsubscription`.

```
aws rds describe-event-subscriptions --subscription-name myfirsteventsubscription
```

API

Para obtener una lista de sus suscripciones actuales a notificaciones de eventos de Amazon RDS, llame a la acción `DescribeEventSubscriptions` de la API de Amazon RDS.

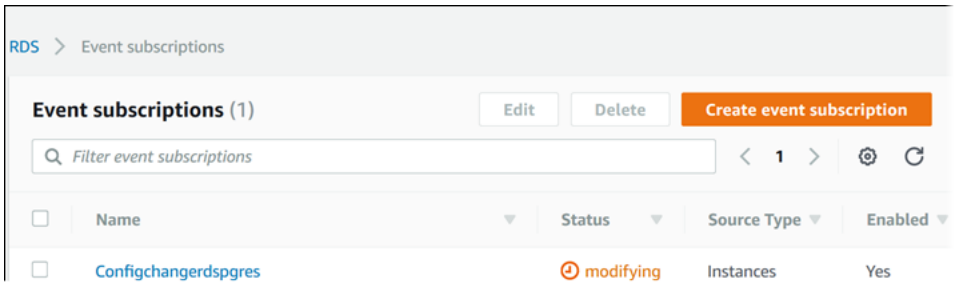
Modificación de una suscripción a notificaciones de eventos de Amazon RDS

Después de crear una suscripción, puede cambiar el nombre de la suscripción, el identificador del origen, las categorías o el ARN del tema.

Consola

Para modificar una suscripción de notificación de eventos de Amazon RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación seleccione Event Subscriptions (Suscripciones de eventos).
3. En el panel Event subscriptions (Suscripciones de eventos), elija la suscripción que desea modificar y elija Edit (Editar).
4. Realice los cambios que desee en la suscripción en las secciones Target (Objetivo) o Source (Fuente).
5. Elija Edit (Editar). La consola de Amazon RDS indica que se está modificando la suscripción.



AWS CLI

Para modificar una suscripción a notificaciones de eventos de Amazon RDS, utilice el comando `modify-event-subscription` de la AWS CLI. Incluya el siguiente parámetro obligatorio:

- `--subscription-name`

Example

El siguiente código activa `myeventsubscription`.

Para Linux, macOS o:Unix

```
aws rds modify-event-subscription \
    --subscription-name myeventsubscription \
    --enabled
```

En:Windows

```
aws rds modify-event-subscription ^
    --subscription-name myeventsubscription ^
    --enabled
```

API

Para modificar un evento de Amazon RDS, llame a la operación de la API de Amazon RDS `ModifyEventSubscription`. Incluya el siguiente parámetro obligatorio:

- `SubscriptionName`

Agregar un identificador de origen a una suscripción de notificación de eventos de Amazon RDS

Puede añadir un identificador de origen (el origen de Amazon RDS que genera el evento) a una suscripción existente.

Consola

Puede añadir o eliminar fácilmente identificadores de origen mediante la consola de Amazon RDS activándolos o desactivándolos al modificar una suscripción. Para obtener más información, consulte Modificación de una suscripción a notificaciones de eventos de Amazon RDS.

AWS CLI

Para agregar un identificador de origen a una suscripción a notificaciones de eventos de Amazon RDS, utilice el comando `add-source-identifier-to-subscription` de la AWS CLI. Incluya los siguientes parámetros obligatorios:

- `--subscription-name`
- `--source-identifier`

Example

En el siguiente ejemplo se añade el identificador de origen `mysqldb` a la suscripción `myrdseventsubscription`

Para Linux, macOS o:Unix

```
aws rds add-source-identifier-to-subscription \
    --subscription-name myrdseventsubscription \
    --source-identifier mysqldb
```

En:Windows

```
aws rds add-source-identifier-to-subscription ^
    --subscription-name myrdseventsubscription ^
    --source-identifier mysqldb
```

API

Para añadir un identificador de origen a una suscripción a notificaciones de eventos de Amazon RDS, llame a la acción de la API de Amazon RDS `AddSourceIdentifierToSubscription`. Incluya los siguientes parámetros obligatorios:

- `SubscriptionName`
- `SourceIdentifier`

Quitar un identificador de origen de una suscripción de notificación de eventos de Amazon RDS

Puede eliminar un identificador de origen (el origen de Amazon RDS que genera el evento) de una suscripción si ya no desea recibir notificaciones de los eventos de ese origen.

Consola

Puede añadir o eliminar fácilmente identificadores de origen mediante la consola de Amazon RDS activándolos o desactivándolos al modificar una suscripción. Para obtener más información, consulte Modificación de una suscripción a notificaciones de eventos de Amazon RDS.

AWS CLI

Para eliminar un identificador de origen de una suscripción a notificaciones de eventos de Amazon RDS, utilice el comando `remove-source-identifier-from-subscription` de la AWS CLI. Incluya los siguientes parámetros obligatorios:

- `--subscription-name`
- `--source-identifier`

Example

En el siguiente ejemplo, se elimina el identificador de origen `mysqldb` de la suscripción `myrdseventsubscription`.

Para Linux, macOS o:Unix

```
aws rds remove-source-identifier-from-subscription \
    --subscription-name myrdseventsubscription \
    --source-identifier mysqldb
```

En:Windows

```
aws rds remove-source-identifier-from-subscription ^
    --subscription-name myrdseventsubscription ^
    --source-identifier mysqldb
```

API

Para eliminar un identificador de origen de una suscripción a notificaciones de eventos de Amazon RDS, utilice el comando `RemoveSourceIdentifierFromSubscription` de la API de Amazon RDS. Incluya los siguientes parámetros obligatorios:

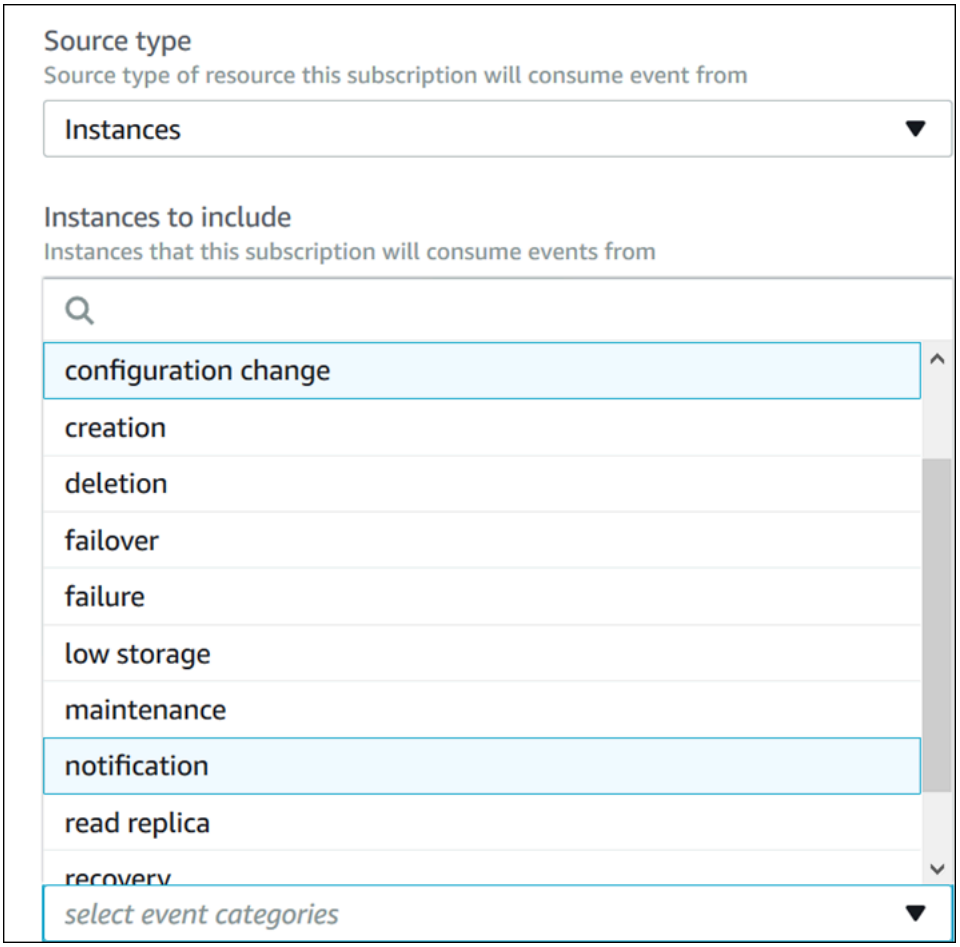
- `SubscriptionName`
- `SourceIdentifier`

Descripción de la lista de categorías de notificaciones de eventos de Amazon RDS

Todos los eventos de un tipo de recurso se agrupan en categorías. Para ver la lista de categorías disponibles, utilice los siguientes procedimientos.

Consola

Cuando se crea o modifica una suscripción a notificaciones de eventos, las categorías de eventos se muestran en la consola de Amazon RDS. Para obtener más información, consulte Modificación de una suscripción a notificaciones de eventos de Amazon RDS.



AWS CLI

Para obtener la lista de categorías de notificaciones de eventos de Amazon RDS, utilice el comando `describe-event-categories` de la AWS CLI. Este comando no tiene parámetros obligatorios.

Example

```
aws rds describe-event-categories
```

API

Para obtener la lista de categorías de notificaciones de eventos de Amazon RDS, utilice el comando `DescribeEventCategories` de la API de Amazon RDS. Este comando no tiene parámetros obligatorios.

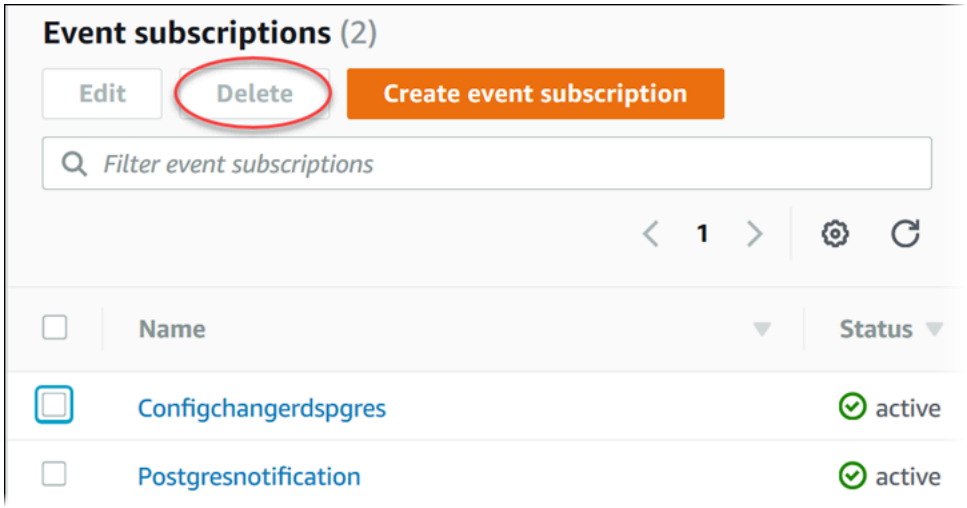
Eliminar una suscripción de notificación de eventos de Amazon RDS

Puede eliminar una suscripción cuando ya no la necesite. Los suscriptores del tema dejarán de recibir notificaciones de los eventos especificados en la suscripción.

Consola

Para eliminar una suscripción de notificación de eventos de Amazon RDS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación seleccione DB Event Subscriptions (Suscripciones a eventos de base de datos).
3. En el panel My DB Event Subscriptions (Mis suscripciones a eventos de base de datos), elija la suscripción que desea eliminar.
4. Elija Eliminar.
5. La consola de Amazon RDS indica que se está eliminando la suscripción.



AWS CLI

Para eliminar una suscripción a notificaciones de eventos de Amazon RDS, utilice el comando `delete-event-subscription` de la AWS CLI. Incluya el siguiente parámetro obligatorio:

- `--subscription-name`

Example

En el siguiente ejemplo se elimina la suscripción `myrdssubscription`.

```
aws rds delete-event-subscription --subscription-name myrdssubscription
```

API

Para eliminar una suscripción a notificaciones de eventos de Amazon RDS, utilice el comando `DeleteEventSubscription` de la API de RDS. Incluya el siguiente parámetro obligatorio:

- `SubscriptionName`

Creación de una regla que se desencadena en función de un evento Amazon RDS

Al utilizar Amazon EventBridge, puede automatizar los servicios de AWS y responder a eventos del sistema, como problemas de disponibilidad de aplicaciones o cambios de recursos.

Temas

- Creación de reglas para enviar eventos de Amazon RDS a Amazon EventBridge
- Tutorial: Registrar el estado de una instancia de base de datos con Amazon EventBridge

Creación de reglas para enviar eventos de Amazon RDS a Amazon EventBridge

Puede escribir reglas sencillas para indicar qué eventos de Amazon RDS le resultan de interés, así como qué acciones automatizadas se van a llevar a cabo cuando un evento cumple una de las reglas. Puede configurar varios destinos, como una función de AWS Lambda o un tema de Amazon SNS, que reciban eventos en formato JSON. Por ejemplo, puede configurar Amazon RDS para enviar eventos a Amazon EventBridge cada vez que se cree o elimine una instancia de base de datos. Para obtener más información, consulte la guía del usuario de Amazon CloudWatch Events y la guía del usuario de Amazon EventBridge.

Para crear una regla que se active en función de un evento RDS:

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, en Events (Eventos), elija Rules (Reglas).
3. Elija Create rule.
4. En Event Source, haga lo siguiente:
    a. Seleccione Event Pattern.
    b. En Service Name (Nombre de servicio), elija Relational Database Service (RDS).
    c. En Event Type (Tipo de evento), elija el tipo de recurso de Amazon RDS que desencadena el evento. Por ejemplo, si una instancia de base de datos desencadena el evento, elija RDS DB Instance Event (Evento de instancia de base de datos de RDS).
5. En Targets (Destinos), seleccione Add Target (Agregar destino) y elija el servicio de AWS que va a actuar cuando se detecte un evento del tipo seleccionado.
6. En el resto de los campos de esta sección, especifique los datos concretos de este tipo de destino, si es necesario.

7. Si hay muchos tipos de destinos, EventBridge necesita permisos para enviar eventos al destino. En estos casos, EventBridge puede crear el rol de IAM necesario para que se ejecute el evento:
   - Para crear un rol de IAM automáticamente, elija Crear un nuevo rol para este recurso específico.
   - Para utilizar una función de IAM que haya creado antes, elija Use existing role (Usar función existente).
8. Si lo desea, puede repetir los pasos 5 a 7 para agregar otro destino en esta regla.
9. Seleccione Configure details. En Rule definition, escriba un nombre y la descripción de la regla.

   El nombre de la regla debe ser exclusivo dentro de esta región.
10. Elija Create rule.

Para obtener más información, consulte Creating an EventBridge Rule That Triggers on an Event en la Guía del usuario de Amazon CloudWatch.

Tutorial: Registrar el estado de una instancia de base de datos con Amazon EventBridge

En este tutorial puede crear una función de AWS Lambda que registre los cambios de estado de una instancia de Amazon RDS. A continuación, puede crea una regla que ejecute la función cuando se produzca un cambio de estado de una instancia de base de datos de RDS existente. En el tutorial se asume que tiene una pequeña instancia de prueba en ejecución que puede apagar temporalmente.

> **Important**
>
> No realice este tutorial en una instancia de base de datos de producción en ejecución.

Temas

- Paso 1: Crear una función de AWS Lambda
- Paso 2: Crear una regla
- Paso 3: Probar la regla

Paso 1: Crear una función de AWS Lambda

Cree una función Lambda para registrar los eventos de cambio de estado. Especifique esta función cuando cree la regla.

Para crear una función Lambda

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Si es la primera vez que utiliza Lambda, aparecerá una página de bienvenida. Seleccione Get Started Now. De lo contrario, seleccione Create function (Crear función).
3. Elija Author from scratch.
4. En la página Create function (Crear función), proceda del modo siguiente:
   a. Introduzca un nombre y la descripción de la función Lambda. Por ejemplo, asigne un nombre a la función **`RDSInstanceStateChange`**.
   b. En Runtime (Tiempo de ejecución), seleccione Node.js 14x.
   c. En Architecture (Arquitectura), elija x86_64.
   d. En Execution role (Rol de ejecución), haga una de estas dos operaciones:
      - Elija Create a new role with basic Lambda permissions (Crear un nuevo rol con permisos básicos de Lambda).
      - En Existing role (Rol existente), elija Use an existing role (Usar un rol existente). Elija el rol que desee usar.
   e. Elija Create function (Crear función).
5. En la página RDSInstanceStateChange, haga lo siguiente:
   a. En Code source (Fuente del código), seleccione index.js.
   b. En el panel deindex.js, elimine el código existente.
   c. Escriba el código siguiente:

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('Received event:', JSON.stringify(event));
};
```

   d. Elija Deploy (Implementar).

Paso 2: Crear una regla

Cree una regla para ejecutar su función Lambda siempre que lance una instancia Amazon RDS.

Para crear la regla de EventBridge

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Reglas.
3. Elija Crear regla.
4. Escriba un nombre y una descripción de la regla. Por ejemplo, escriba **`RDSInstanceStateChangeRule`**.
5. Elija Rule with an event pattern (Regla con un patrón de evento) y, a continuación, elija Next (Siguiente).
6. En Origen del evento, elija Eventos de AWS o eventos de socios de EventBridge.
7. Desplácese hacia abajo en la sección Event pattern (Patrón de eventos).
8. En Origen del evento, elija Servicios de AWS.
9. En AWS service (Servicio de), elija Relational Database Service (RDS).
10. Para Event type (Tipo de evento), elija RDS DB Instance Event (Evento de instancia de base de datos RDS).
11. Deje el patrón de eventos predeterminado. A continuación, elija Next.
12. En Tipos de destino, seleccione Servicio de AWS.
13. En Select a target (Seleccione destino), elija Lambda function (Función de Lambda).
14. En Function (Función), seleccione la función Lambda que ha creado. A continuación, elija Next.
15. En Configure tags (Configurar etiquetas), elija Next (Siguiente).
16. Revise los pasos de la regla. A continuación, elija Create rule (Crear regla).

Paso 3: Probar la regla

Para probar su regla, cierre una instancia de base de datos de RDS. Después de esperar unos minutos a que la instancia se detenga, compruebe que se haya invocado la función Lambda.

Para probar la regla mediante la detención de una instancia de base de datos

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. Detenga una instancia de base de datos de RDS.
3. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.
4. En el panel de navegación, elija Rules (Reglas) y elija el nombre de la regla que ha creado.
5. En Detalles de la regla, seleccione Monitoreo.

   Se lo redirigirá a la consola de Amazon CloudWatch. Si no se le redirige, haga clic en Ver métricas en CloudWatch.
6. En All metrics (Todas las métricas), elija el nombre de la regla que creó.

   El gráfico debe indicar que se ha invocado la regla.
7. En el panel de navegación, seleccione Log groups (Grupos de registro).
8. Seleccione el nombre del grupo de registro de su función de Lambda (/aws/lambda/***function-name***).
9. Elija el nombre del flujo de registro para ver los datos proporcionados por la función para la instancia que ha lanzado. Debería recibir un resultado similar al siguiente:

```
{
    "version": "0",
    "id": "12a345b6-78c9-01d2-34e5-123f4ghi5j6k",
    "detail-type": "RDS DB Instance Event",
    "source": "aws.rds",
    "account": "111111111111",
    "time": "2021-03-19T19:34:09Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:rds:us-east-1:111111111111:db:testdb"
    ],
    "detail": {
        "EventCategories": [
            "notification"
        ],
        "SourceType": "DB_INSTANCE",
        "SourceArn": "arn:aws:rds:us-east-1:111111111111:db:testdb",
        "Date": "2021-03-19T19:34:09.293Z",
        "Message": "DB instance stopped",
        "SourceIdentifier": "testdb",
        "EventID": "RDS-EVENT-0087"
    }
}
```

Para ver más ejemplos de eventos de RDS en formato JSON, consulte Información general de los eventos para Amazon RDS.

10. (Opcional) Cuando haya terminado, puede abrir la consola de Amazon RDS y comenzar la instancia que ha lanzado.

Categorías y mensajes de eventos de Amazon RDS

Amazon RDS genera un número significativo de eventos en categorías a las que puede suscribirse a través de la consola de Amazon RDS, la AWS CLI o la API.

Temas

- Eventos de clúster de bases de datos
- Eventos de instancia de base de datos
- Eventos de grupo de parámetros de base de datos
- Eventos de grupo de seguridad de base de datos
- Eventos de instantánea de base de datos
- Eventos de instantánea de clúster de bases de datos
- Eventos de RDS Proxy
- Eventos de implementación azul/verde
- Eventos de versiones del motor personalizadas

Eventos de clúster de bases de datos

En la siguiente tabla se muestran las categorías de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es un clúster de base de datos.

Para obtener más información sobre implementaciones de clústeres de base de datos Multi-AZ, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0016	Restablecer las credencia les maestras.	
creation	RDS-EVENT-0170	Se ha creado un clúster de bases de datos.	
conmutación por error	RDS-EVENT-0069	Ha fallado la conmutaci ón por error del clúster. Compruebe el estado de	

Categoría	ID de evento de RDS	Mensaje	Notas
		las instancias del clúster e inténtelo de nuevo.	
conmutación por error	RDS-EVENT-0070	Volver a promocionar el principal anterior: *nombre*.	
conmutación por error	RDS-EVENT-0071	Se ha completado la conmutación por error en la instancia de base de datos: *nombre*.	
failover	RDS-EVENT-0072	Se ha iniciado la misma conmutación por error de AZ en la instancia de base de datos: *nombre*.	
conmutación por error	RDS-EVENT-0073	Se ha iniciado la conmutación por error entre AZ en la instancia de base de datos: *nombre*.	
failure	RDS-EVENT-0354	No puede crear el clúster de base de datos porque los recursos son incompatibles. *mensaje*.	El *message* incluye detalles sobre el error.
failure	RDS-EVENT-0240	El clúster de base de datos no se puede crear porque los límites de recursos son insuficientes. *mensaje*.	El *message* incluye detalles sobre el error.

Categoría	ID de evento de RDS	Mensaje	Notas
Conmutación por error global	RDS-EVENT-0181	Se ha iniciado la transición al clúster de base de datos *nombre* de la región *nombre*.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”). El proceso se puede retrasar porque están en ejecución otras operaciones en el clúster de bases de datos.
Conmutación por error global	RDS-EVENT-0182	El clúster de base de datos principal *nombre* anterior en la región *nombre* se ha cerrado correctamente.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”). La antigua instancia principal de la base de datos global no acepta escrituras. Todos los volúmenes están sincronizados.

Categoría	ID de evento de RDS	Mensaje	Notas
Conmutación por error global	RDS-EVENT-0183	Esperando a que se sincronicen los datos entre los miembros del clúster global. Retrasos actuales debidos al clúster de base de datos principal: *`motivo`*.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”). Se produce un retraso de replicación durante la fase de sincronización de la conmutación por error de la base de datos global.
Conmutación por error global	RDS-EVENT-0184	El clúster de base de datos principal *`nombre`* anterior en la región *`nombre`* se ha promovido correctamente.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”). La topología de volúmenes de la base de datos global se restablece con el nuevo volumen principal.

Categoría	ID de evento de RDS	Mensaje	Notas
Conmutación por error global	RDS-EVENT-0185	Ha finalizado la transición al clúster de base de datos *nombre* de la región *nombre*.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”). Se ha finalizado la transición de la base de datos global en el clúster de la base de datos principal. Las réplicas pueden tardar mucho en ponerse en línea una vez completada la conmutación por error.
Conmutación por error global	RDS-EVENT-0186	Se ha cancelado la transición al clúster de base de datos *nombre* de la región *nombre*.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”).
Conmutación por error global	RDS-EVENT-0187	Se ha producido un error en la transición al clúster de base de datos *nombre* de la región *nombre*.	Este evento es para una operación de transición (antes denominada “conmutación por error planificada administrada”).
Conmutación por error global	RDS-EVENT-0238	Se ha completado la conmutación por error global en el clúster de base de datos *nombre* de la región *nombre*.	

Categoría	ID de evento de RDS	Mensaje	Notas
Conmutación por error global	RDS-EVENT-0239	Ha fallado la conmutación por error global en el clúster de base de datos *nombre* de la región *nombre*.	
Conmutación por error global	RDS-EVENT-0240	Se ha iniciado la resincronización de los miembros del clúster de base de datos *nombre* de la región *nombre* después de una conmutación por error global.	
Conmutación por error global	RDS-EVENT-0241	Ha finalizado la resincronización de los miembros del clúster de base de datos *nombre* de la región *nombre* después de una conmutación por error global.	
maintenance	RDS-EVENT-0156	El clúster de bases de datos tiene disponible una actualización de versiones secundarias de motor de base de datos.	
maintenance	RDS-EVENT-0176	Se ha actualizado la versión principal del motor de clústeres de bases de datos.	

Categoría	ID de evento de RDS	Mensaje	Notas
maintenance	RDS-EVENT-0177	La actualización del clúster de base de datos está en curso.	
maintenance	RDS-EVENT-0286	Se ha iniciado la actualización de la versión del motor de clústeres de bases de datos.	
maintenance	RDS-EVENT-0287	Se ha detectado el requisito de actualización del sistema operativo.	
maintenance	RDS-EVENT-0288	Se ha iniciado la actualización del sistema operativo del clúster.	
maintenance	RDS-EVENT-0289	Se ha completado la actualización del sistema operativo del clúster.	
notification	RDS-EVENT-0172	Se ha cambiado el nombre del clúster de *nombre* a *nombre*.	

Eventos de instancia de base de datos

En la siguiente tabla se muestran las categorías de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es una instancia de base de datos.

Categoría	ID de evento de RDS	Mensaje	Notas
disponibilidad	RDS-EVENT-0004	Instancia de base de datos cerrada.	
availability	RDS-EVENT-0006	Se ha reiniciado la instancia de base de datos.	
disponibilidad	RDS-EVENT-0022	Error al reiniciar mysql: *mensaje*.	Se ha producido un error al reiniciar MySQL.
disponibilidad	RDS-EVENT-0221	La instancia de base de datos ha alcanzado el umbral de almacenamiento completo y se ha cerrado la base de datos. Puede aumentar el almacenamiento asignado para solucionar este problema.	
disponibilidad	RDS-EVENT-0222	La capacidad de almacenamiento libre de la instancia de base de datos *nombre* es baja en un *porcentaje* del almacenamiento asignado [Almacenamiento asignado: *cantidad*, Almacenamiento gratuito: *cantidad*]. La base de datos se cerrará para evitar daños si el almacenamiento gratuito es inferior a *cantidad*. Puede aumentar el almacenam	Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Categoría	ID de evento de RDS	Mensaje	Notas
		iento asignado para solucionar este problema.	
disponibilidad	RDS-EVENT-0330	La capacidad de almacenamiento libre del volumen de registro de transacciones específico es demasiado baja para la instancia de base de datos *nombre*. El almacenam iento libre del volumen de registro es un *porcentaj e* del almacenamiento asignado. [Almacenamiento asignado: *cantidad*, almacenamiento libre: *cantidad*] La base de datos se cerrará para evitar daños si el almacenam iento libre es inferior a *cantidad*. Puede deshabilitar el volumen de registro de transacciones específico para resolver este problema.	Para obtener más informaci ón, consulte Volumen de registro específico (DLV).

Categoría	ID de evento de RDS	Mensaje	Notas
disponibilidad	RDS-EVENT-0331	La capacidad de almacenamiento libre del volumen de registro de transacciones específico es demasiado baja para la instancia de base de datos *nombre*. El almacenamiento libre del volumen de registro es un *porcentaje* del almacenamiento aprovisionado. [Almacenamiento aprovisionado: *cantidad*, almacenamiento libre: *cantidad*] Puede deshabilitar el volumen de registro de transacciones específico para resolver este problema.	Para obtener más información, consulte Volumen de registro específico (DLV).
disponibilidad	RDS-EVENT-0396	Amazon RDS ha programado el reinicio de esta réplica de lectura en el siguiente periodo de mantenimiento de la instancia tras la rotación de la contraseña del usuario interno.	No aplicable
backup	RDS-EVENT-0001	Se está realizando una copia de seguridad de la instancia de base de datos.	

Categoría	ID de evento de RDS	Mensaje	Notas
backup	RDS-EVENT-0002	Ha finalizado la copia de seguridad de la instancia de base de datos.	
backup	RDS-EVENT-0086	No hemos podido asociar el grupo de opciones *nombre* con la instancia de base de datos *nombre*. Confirme que el grupo de opciones *nombre* sea compatible con la clase de instancia de base de datos y la configuración. Si es así, compruebe todos los ajustes del grupo de opciones y vuelva a intentarlo.	Para obtener más informaci ón, consulte Trabajo con grupos de opciones.
configuration change	RDS-EVENT-0011	Actualizado para usar dbParameterGroup *nombre*.	
configuration change	RDS-EVENT-0012	Se está aplicando la modificación a la clase de instancia de base de datos.	
configuration change	RDS-EVENT-0014	Ha finalizado la aplicació n de la modificación a la clase de instancia de base de datos.	
configuration change	RDS-EVENT-0016	Restablecer las credencia les maestras.	

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0017	Ha finalizado la aplicación de la modificación al almacenamiento asignado.	
configuration change	RDS-EVENT-0018	Aplicación de la modificación al almacenamiento asignado.	
configuration change	RDS-EVENT-0024	Aplicación de la modificación para convertirla en una instancia de base de datos multi-AZ.	
configuration change	RDS-EVENT-0025	Ha finalizado la aplicación de la modificación para convertirla en una instancia de base de datos multi-AZ.	
configuration change	RDS-EVENT-0028	Se han deshabilitado las copias de seguridad automatizadas.	
configuration change	RDS-EVENT-0029	Ha finalizado la aplicación de la modificación para convertirla en una instancia de base de datos (single-AZ) estándar.	
configuration change	RDS-EVENT-0030	Aplicación de la modificación para convertirla en una instancia de base de datos (single-AZ) estándar.	

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0032	Se han habilitado las copias de seguridad automatizadas.	
configuration change	RDS-EVENT-0033	Hay *número* usuarios que coinciden con el nombre de usuario maestro; solo se restablece el que no esté vinculado a un host específico.	
configuration change	RDS-EVENT-0067	No se ha podido restablecer la contraseña. Información de error: *mensaje*.	
configuration change	RDS-EVENT-0078	El intervalo de monitorización ha cambiado a *número*.	Se ha cambiado la configuración de monitorización mejorada.
configuration change	RDS-EVENT-0092	Se ha terminado de actualizar el grupo de parámetros de base de datos.	
configuration change	RDS-EVENT-0217	Aplicación de la modificación iniciada por el escalado automático al almacenamiento asignado.	
configuration change	RDS-EVENT-0218	Se ha terminado de aplicar la modificación iniciada por el escalado automático al almacenamiento asignado.	

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0295	Se inició la actualización de la configuración del almacenamiento.	
configuration change	RDS-EVENT-0296	Se completó la actualización de la configuración del almacenamiento.	
configuration change	RDS-EVENT-0332	El volumen de registro específico está deshabilitado.	Para obtener más información, consulte Volumen de registro específico (DLV).
configuration change	RDS-EVENT-0333	Se ha iniciado la deshabilitación del volumen de registro específico.	Para obtener más información, consulte Volumen de registro específico (DLV).
configuration change	RDS-EVENT-0334	Se ha iniciado la habilitación del volumen de registro específico.	Para obtener más información, consulte Volumen de registro específico (DLV).
configuration change	RDS-EVENT-0335	El volumen de registro específico está habilitado.	Para obtener más información, consulte Volumen de registro específico (DLV).
configuration change	RDS-EVENT-0383	La *`versión del motor`* no es compatible con el complemento memcached. RDS seguirá actualizando su instancia de base de datos y eliminará este complemento.	A partir de MySQL 8.3.0, el complemento memcached no es compatible. Para obtener más información, consulte Changes in MySQL 8.3.0 (2024-01-16, Innovation Release).
creación	RDS-EVENT-0005	Instancia de base de datos creada.	

Categoría	ID de evento de RDS	Mensaje	Notas
deletion	RDS-EVENT-0003	Se ha eliminado la instancia de base de datos.	
conmutación por error	RDS-EVENT-0013	Se ha iniciado la conmutación por error de la instancia multi-AZ.	Se ha iniciado una conmutación por error multi-AZ que ha dado como resultado la promoción de una instancia de base de datos en espera.
conmutación por error	RDS-EVENT-0015	Se ha completado la conmutación por error multi-AZ al modo de espera: la propagación del DNS puede tardar unos minutos.	Ha finalizado una conmutación por error multi-AZ que ha dado como resultado la promoción de una instancia de base de datos en espera. El DNS puede tardar varios minutos en realizar la transferencia a la nueva instancia de base de datos principal.
conmutación por error	RDS-EVENT-0034	Abandonar la conmutación por error solicitada por el usuario debido a que recientemente se ha producido una conmutación por error en la instancia de base de datos.	Amazon RDS no está intentando realizar la conmutación por error solicitada porque recientemente se ha producido una conmutación por error en la instancia de base de datos.
conmutación por error	RDS-EVENT-0049	Se ha completado la conmutación por error de instancias multi-AZ.	

Categoría	ID de evento de RDS	Mensaje	Notas
conmutación por error	RDS-EVENT-0050	Se ha iniciado la activación de instancias multi-AZ.	Se ha iniciado una activación multi-AZ después de una recuperación correcta de la instancia de base de datos.
conmutación por error	RDS-EVENT-0051	Se ha completado la activación de instancias multi-AZ.	Ha finalizado una activación Multi-AZ. La base de datos ya debería estar accessible.
conmutación por error	RDS-EVENT-0065	Se ha recuperado de una conmutación por error parcial.	
failure	RDS-EVENT-0031	Instancia de base de datos que pasa al estado *nombre*. RDS recomienda iniciar una restauración a un momento dado.	Se ha producido un error en la instancia de base de datos debido a una configuración incompatible o a un problema de almacenamiento subyacente. Comience una restauración a un momento dado para la instancia de base de datos.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0035	Instancia de base de datos que pasa a *estado*. *mensaje*.	La instancia de base de datos tiene parámetros no válidos. Por ejemplo, no se ha podido iniciar la instancia de base de datos porque un parámetro relacionado con la memoria tiene un valor demasiado alto para esta clase de instancia, por lo que debería modificar el parámetro de memoria y reiniciar la instancia de base de datos.
failure	RDS-EVENT-0036	Instancia de base de datos *estado*. *mensaje*.	La instancia de base de datos está en una red incompatible. Algunos de los ID de subred especific ados no son válidos o no existen.
failure	RDS-EVENT-0058	Ha fallado la instalación de Statspack. *mensaje*.	Error al crear la cuenta de usuario de Oracle Statspack PERFSTAT. Elimine la cuenta antes de agregar la opción STATSPACK .

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0079	Amazon RDS no ha podido crear credenciales para mejorar la monitorización y se ha deshabilitado la característica. Es probable que esto se deba a que rds-monitoring-role no está presente pero está configurado correctamente en su cuenta. Consulte la sección de solución de problemas de la documentación de Amazon RDS para obtener más información.	La monitorización mejorada no se puede activar sin el rol de IAM de monitorización mejorada. Para obtener información acerca de la creación del rol de IAM, consulte Para crear un rol de IAM para el monitoreo mejorado de Amazon RDS.
failure	RDS-EVENT-0080	Amazon RDS no ha podido configurar la monitorización mejorada en su instancia: *nombre* y se ha deshabilitado esta característica. Es probable que esto se deba a que rds-monitoring-role no está presente pero está configurado correctamente en su cuenta. Consulte la sección de solución de problemas de la documentación de Amazon RDS para obtener más información.	La monitorización mejorada se ha desactivado porque ha surgido un error al realizar el cambio de configuración. Es probable que el rol de IAM de monitorización mejorada se haya configurado incorrectamente. Para obtener información acerca de la creación del rol de IAM de monitorización mejorada, consulte Para crear un rol de IAM para el monitoreo mejorado de Amazon RDS.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0081	Amazon RDS no ha podido crear credenciales para la opción *nombre*. Esto se debe a que el rol de IAM *nombre* no está configura do correctamente en su cuenta. Consulte la sección de solución de problemas de la documentación de Amazon RDS para obtener más información.	El rol de IAM que se utiliza para obtener acceso al bucket de Amazon S3 para las operaciones nativas de copia de seguridad y restauración de SQL Server se ha configura do incorrectamente. Para obtener más información, consulte Configuración de la copia de seguridad y la restauración nativas.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0165	La instancia de base de datos de RDS Custom se encuentra fuera del perímetro de soporte.	Es su responsabilidad corregir los problemas de configuración que colocan la instancia de base de datos de RDS Custom en el estado `unsupported-configuration` . Si el problema está relaciona do con la infraestructura de AWS, puede utilizar la consola o la AWS CLI para solucionarlo. Si el problema está relacionado con el sistema operativo o la configuración de la base de datos, puede iniciar sesión en el host para soluciona rlo. Para obtener más informaci ón, consulte Perímetro de soporte de RDS Custom.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0188	La instancia de base de datos tiene un estado que no se puede actualizar. *mensaje*	Amazon RDS no pudo actualizar una instancia de base de datos MySQL de la versión 5.7 a la versión 8.0 debido a incompatibilidades relacionadas con el diccionario de datos. La instancia de base de datos volvió a la versión 5.7 de MySQL. Para obtener más información, consulte Reversión tras un fallo en la actualización.
failure	RDS-EVENT-0219	La instancia de base de datos tiene un estado no válido. No es necesaria ninguna acción. El escalado automático se volverá a intentar más tarde.	

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0220	La instancia de base de datos se encuentra en el periodo de reflexión de una operación de escala de almacenamiento anterior. Estamos optimizando su instancia de base de datos. Puede tardar unas seis horas. No es necesaria ninguna acción. El escalado automático se volverá a intentar después del periodo de reflexión.	
failure	RDS-EVENT-0223	El escalado automático del almacenamiento no puede escalar el almacenamiento por el siguiente motivo: *motivo*.	
failure	RDS-EVENT-0224	El escalado automático del almacenamiento ha desencadenado una tarea de escala de almacenam iento pendiente que alcanzará o superará el umbral máximo de almacenamiento. Aumente el umbral máximo de almacenamiento.	

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0237	La instancia de base de datos tiene un tipo de almacenamiento que no está disponible actualmente en la zona de disponibilidad. El escalado automático se volverá a intentar más tarde.	
failure	RDS-EVENT-0254	La cuota de almacenamiento subyacente de esta cuenta de cliente ha superado el límite. Aumente la cuota de almacenamiento permitida para admitir el escalado en la instancia.	
failure	RDS-EVENT-0278	No se ha podido crear la instancia de base de datos. *message*	El *message* incluye detalles sobre el error.
failure	RDS-EVENT-0279	Ha fallado la promoción de la réplica de lectura de RDS Custom. *message*	El *message* incluye detalles sobre el error.
failure	RDS-EVENT-0280	RDS Custom no ha podido actualizar la instancia de base de datos porque se ha producido un error en la comprobación previa. *message*	El *message* incluye detalles sobre el error.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0281	RDS Custom no ha podido modificar la instancia de base de datos porque se ha producido un error en la comprobación previa. *message*	El *message* incluye detalles sobre el error.
failure	RDS-EVENT-0282	RDS Custom no ha podido modificar la instancia de base de datos porque los permisos de IP elásticas no son correctos. Confirme que la dirección IP elástica esté etiquetada con `AWSRDSCustom` .	
failure	RDS-EVENT-0283	RDS Custom no ha podido modificar la instancia de base de datos porque se ha alcanzado el límite de IP elástica de su cuenta. Libere las IP elásticas no utilizadas o solicite un aumento de cuota para su límite de direcciones IP elásticas.	
failure	RDS-EVENT-0284	RDS Custom no ha podido modificar la instancia a alta disponibilidad porque se ha producido un error en la comprobación previa. *message*	El *message* incluye detalles sobre el error.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0285	RDS Custom no ha podido crear una instantánea final para la instancia de base de datos debido a *message*.	El *message* incluye detalles sobre el error.
failure	RDS-EVENT-0306	Error en la actualización de la configuración del almacenamiento. Intente actualizar de nuevo.	
failure	RDS-EVENT-0315	No se puede mover la base de datos de red incompatible, *nombre*, al estado disponible: *mensaje*	La configuración de red de la base de datos no es válida. No se pudo mover la base de datos de red incompatible a disponible.
failure	RDS-EVENT-0328	No se pudo unir un host a un dominio. El estado de pertenencia al dominio (por ejemplo, *instancename*) se ha establecido en Con error.	

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0329	No se pudo unir un host a su dominio. Durante el proceso de unión al dominio, Microsoft Windows devolvió el *mensaje* de código de error. Compruebe las configuraciones de red y permisos y emita una solicitud `modify-db-instance` para volver a intentar unirse al dominio.	Al usar un Active Directory autoadministrado, consulte Solución de problemas de Active Directory autoadministrado.
failure	RDS-EVENT-0240	La instancia de base de datos no se puede crear porque los límites de recursos son insuficientes. *mensaje*.	El *message* incluye detalles sobre el error.
failure	RDS-EVENT-0356	RDS no ha podido configurar el punto de conexión Kerberos en su dominio. Esto podría impedir la autenticación de Kerberos en su instancia de base de datos. Compruebe la configuración de red entre la instancia de base de datos y los controladores de dominio.	

Categoría	ID de evento de RDS	Mensaje	Notas
low storage	RDS-EVENT-0007	Se ha agotado el almacenamiento asignado. Asigne almacenamiento adicional para resolver el problema.	Se ha agotado el almacenamiento asignado a la instancia de base de datos. Para solucionar este problema, asigne almacenamiento adicional a la instancia de base de datos. Para obtener más información, consulte las Preguntas frecuentes de RDS. El espacio de almacenamiento de una instancia de base de datos se puede monitorizar con la métrica Free Storage Space.
low storage	RDS-EVENT-0089	La capacidad de almacenamiento libre de la instancia de base de datos: *nombre* es baja un *porcentaje* del almacenamiento aprovisionado [Almacenamiento aprovisionado: *tamaño*, Almacenamiento gratuito: *tamaño*]. Puede que desee aumentar el almacenamiento aprovisionado para solucionar este problema.	La instancia de base de datos ha consumido más del 90 % del almacenamiento asignado. El espacio de almacenamiento de una instancia de base de datos se puede monitorizar con la métrica Free Storage Space.

Categoría	ID de evento de RDS	Mensaje	Notas
low storage	RDS-EVENT-0227	El almacenamiento de su clúster de Aurora es peligrosamente bajo y solo quedan *cantidad* terabytes. Tome medidas para reducir la carga de almacenamiento en el clúster.	El subsistema de almacenamiento de Aurora se está quedando sin espacio.
maintenance	RDS-EVENT-0026	Se aplican parches fuera de línea a la instancia de base de datos.	Se está realizando el mantenimiento sin conexión de la instancia de base de datos. La instancia de base de datos no está disponible en este momento.
maintenance	RDS-EVENT-0027	Ha finalizado la aplicación de parches fuera de línea a la instancia de base de datos.	Ha finalizado el mantenimi ento sin conexión de la instancia de base de datos. La instancia de base de datos ya está disponible.
maintenance	RDS-EVENT-0047	Se han aplicado parches a la instancia de base de datos.	
maintenance	RDS-EVENT-0155	La instancia de base de datos tiene disponible una actualización de versiones secundarias de motor de base de datos.	

Categoría	ID de evento de RDS	Mensaje	Notas
maintenance	RDS-EVENT-0178	La actualización de la instancia de base de datos está en curso.	
maintenance	RDS-EVENT-0264	Se inició la comprobación previa para la actualización de la versión del motor de base de datos.	
maintenance	RDS-EVENT-0265	Finalizó la comprobación previa para la actualización de la versión del motor de base de datos.	
maintenance	RDS-EVENT-0266	Comenzó el tiempo de inactividad de la instancia de base de datos.	
maintenance	RDS-EVENT-0267	Se inició la actualización de la versión del motor.	
maintenance	RDS-EVENT-0268	La actualización de la versión del motor ha finalizado.	
maintenance	RDS-EVENT-0269	Las tareas posteriores a la actualización están en curso.	
maintenance	RDS-EVENT-0270	Falló la actualización de la versión del motor de base de datos. La reversión de la actualización de la versión del motor se realizó correctamente.	

Categoría	ID de evento de RDS	Mensaje	Notas
mantenimiento, error	RDS-EVENT-0195	*message*	Error al actualizar el archivo de zona horaria de Oracle. Para obtener más información, consulte Actualización automática del archivo de zona horaria de Oracle.
mantenimiento, notificación	RDS-EVENT-0191	Hay disponible una nueva versión del archivo de zona horaria para su actualización.	Si actualiza el motor de base de datos de RDS para Oracle, Amazon RDS genera este evento si no ha elegido una actualización de archivo de zona horaria y la base de datos no utiliza el archivo de zona horaria DST más reciente disponible en la instancia. Para obtener más información, consulte Actualización automática del archivo de zona horaria de Oracle.
mantenimiento, notificación	RDS-EVENT-0192	Ha comenzado la actualización del archivo de zona horaria.	Ha comenzado la actualización del archivo de zona horaria de Oracle. Para obtener más información, consulte Actualización automática del archivo de zona horaria de Oracle.

Categoría	ID de evento de RDS	Mensaje	Notas
mantenimiento, notificación	RDS-EVENT-0193	No hay disponible ninguna actualización para la versión del archivo de zona horaria actual.	La instancia de base de datos de Oracle utiliza la última versión del archivo de zona horaria y se cumple cualquiera de las siguientes instrucciones: • Recientemente ha agregado la opción `TIMEZONE_FILE_AUTOUPGRADE` . • Se está actualizando el motor de base de datos de Oracle. Para obtener más información, consulte Actualización automática del archivo de zona horaria de Oracle.
mantenimiento, notificación	RDS-EVENT-0194	Ha finalizado la actualización del archivo de zona horaria.	Se ha completado la actualización del archivo de zona horaria de Oracle. Para obtener más información, consulte Actualización automática del archivo de zona horaria de Oracle.
notification	RDS-EVENT-0044	*message*	Se trata de una notificación emitida por el operador. Para obtener más información, consulte el mensaje del evento.

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0048	Se debe retrasar la actualización del motor de base de datos, ya que esta instancia tiene réplicas de lectura que deben actualizarse primero.	Se ha retrasado la aplicación de parches a la instancia de base de datos.
notification	RDS-EVENT-0054	*message*	El motor de almacenamiento de MySQL que está utilizando no es InnoDB, que es el motor de almacenamiento de MySQL recomendado para Amazon RDS. Para obtener más información sobre los motores de almacenamiento de MySQL, consulte Motores de almacenamiento admitidos por RDS for MySQL.
notification	RDS-EVENT-0055	*message*	La instancia de base de datos tiene un número de tablas que supera las prácticas recomendadas para Amazon RDS. Reduzca el número de tablas de la instancia de base de datos. Para obtener más información acerca de las prácticas recomendadas, consulte Directrices operativas básicas de Amazon RDS.

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0056	*message*	La instancia de base de datos tiene un número de bases de datos que supera las prácticas recomendadas para Amazon RDS. Reduzca el número de bases de datos de la instancia de base de datos. Para obtener más información acerca de las prácticas recomendadas, consulte Directrices operativas básicas de Amazon RDS.
notification	RDS-EVENT-0064	La clave de cifrado TDE ha rotado correctamente.	Para obtener más información acerca de las prácticas recomendadas, consulte Directrices operativas básicas de Amazon RDS.
notification	RDS-EVENT-0084	La instancia de base de datos no se puede convertir en multi-AZ: *mensaje*.	Ha intentado convertir una instancia de base de datos en Multi-AZ, pero contiene grupos de archivos en memoria que no son compatibles con Multi-AZ. Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.
notification	RDS-EVENT-0087	Se ha detenido la instancia de base de datos.	

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0088	Se ha iniciado la instancia de base de datos.	
notification	RDS-EVENT-0154	La instancia de base de datos se está iniciando debido a que se supera el tiempo máximo permitido para estar detenida.	
notification	RDS-EVENT-0157	No se puede modificar la clase de instancia de base de datos. *mensaje*.	RDS no puede modificar la clase de instancia de base de datos porque la clase de instancia de destino no puede admitir el número de bases de datos que hay en la instancia de base de datos de origen. El mensaje de error aparece como: "The instance has N databases, but after conversion it would only support N" (La instancia dispone de N bases de datos, pero después de la conversión solo admitirá N). Para obtener más información, consulte Limitaciones para instancias de base de datos de Microsoft SQL Server.

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0158	La instancia de base de datos tiene un estado que no se puede actualizar: *mensaje*.	
notification	RDS-EVENT-0167	*message*	Cambió la configuración del perímetro de soporte de RDS Custom.
notification	RDS-EVENT-0189	Se agotan los créditos de saldo de ráfaga gp2 para la instancia de base de datos de RDS. Para resolver este problema, reduzca el uso de IOPS o modifique la configura ción de almacenamiento para permitir un mayor rendimiento.	Se agotan los créditos de saldo de ráfaga gp2 para la instancia de base de datos de RDS. Para resolver este problema, reduzca el uso de IOPS o modifique la configura ción de almacenam iento para permitir un mayor rendimiento. Para obtener más información, consulte Créditos de E/S y rendimiento por ráfagas en la guía del usuario de Amazon Elastic Compute Cloud.
notification	RDS-EVENT-0225	El *tamaño* (GB) de almacenamiento designado se acerca a la *cantidad* (GB) máxima de almacenamiento. Aumente el umbral máximo de almacenamiento.	Este evento se invoca cuando el almacenam iento designado alcanza el 80 % del umbral máximo de almacenamiento. Para evitar el evento, aumente el umbral máximo de almacenamiento.

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0231	La modificación del almacenamiento de la instancia de base de datos ha detectado un error interno. La solicitud de modificación está pendiente y se volverá a intentar más tarde.	Se ha producido un error en el proceso de replicación de una réplica de lectura. Para obtener más información, consulte el mensaje del evento. Además, consulte la sección de solución de problemas para obtener réplicas de lectura para su motor de base de datos. • Solución de problemas de una réplica de lectura de MariaDB • Solución de problemas de réplicas de lectura de SQL Server • Solución de problemas de réplicas de lectura de MySQL • Solución de problemas de réplicas de RDS para Oracle

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0253	La base de datos utiliza el búfer de doble escritura . *mensaje*. Para obtener más información, consulte la documentación de *nombre* sobre Escrituras optimizadas para RDS.	RDS Optimized Writes no es compatible con la configuración de almacenamiento de instancias. Para obtener más información, consulte Mejora del rendimiento de escritura con escrituras optimizadas para RDS para MySQL y Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB. Puede actualizar la configuración del almacenamiento para habilitar las escrituras optimizadas mediante la creación de una implementación azul/verde.

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0297	La configuración de almacenamiento para el *nombre* de la instancia de base de datos admite un tamaño máximo de 16 384 GiB. Actualice la configuración de almacenamiento para admitir tamaños de almacenamiento superiores a 16 384 GiB.	No puede aumentar el tamaño de almacenamiento asignado a la instancia de base de datos por encima de 16 384 GiB. Para superar esta limitación, actualice la configuración de almacenamiento. Para obtener más información, consulte Actualización del sistema de archivos de almacenamiento para una instancia de base de datos.
notification	RDS-EVENT-0298	La configuración de almacenamiento para el *nombre* de la instancia de base de datos admite un tamaño máximo de 2048 GiB. Actualice la configuración de almacenamiento para admitir tamaños de tabla superiores a 2048 GiB.	Las instancias de RDS MySQL y MariaDB con esta limitación no pueden tener un tamaño de tabla superior a 2048 GiB. Para superar esta limitación, actualice la configuración de almacenamiento. Para obtener más información, consulte Actualización del sistema de archivos de almacenamiento para una instancia de base de datos.
notification	RDS-EVENT-0327	Amazon RDS no pudo encontrar el *mensaje SECRET ARN* secreto.	

Categoría	ID de evento de RDS	Mensaje	Notas
read replica	RDS-EVENT-0045	Se ha detenido la replicación.	Se ha detenido la replicación en la instancia de base de datos debido a la falta de almacenamiento suficiente. Escale el almacenamiento o reduzca el tamaño máximo de los registros REDO para permitir que la replicación continúe. Para guardar registros REDO de tamaño *amount* MiB, necesita al menos *amount* MiB de almacenamiento libre.
read replica	RDS-EVENT-0046	Se ha reanudado la replicación de la réplica de lectura.	Este mensaje aparece cuando se crea por primera vez una réplica de lectura o como mensaje de monitoreo que confirma que la replicación funciona correctamente. Si este mensaje es posterior a una notificación `RDS-EVENT-0045` , significa que la replicación se ha reanudado después de detenerla o tras producirse un error.
read replica	RDS-EVENT-0057	Se ha interrumpido la transmisión de la replicación.	

Categoría	ID de evento de RDS	Mensaje	Notas
read replica	RDS-EVENT-0062	La replicación de la réplica de lectura se ha detenido manualmente.	
read replica	RDS-EVENT-0063	Se ha restablecido la replicación desde una instancia que no es de RDS.	
read replica	RDS-EVENT-0202	Error al crear réplica de lectura.	
read replica	RDS-EVENT-0240	Se inició el canal de replicación *`nombre`*.	Para obtener información acerca de los canales de replicación, consulte the section called “Configuración de la replicación de varios orígenes”.
read replica	RDS-EVENT-0240	Se detuvo el canal de replicación *`nombre`*.	Para obtener información acerca de los canales de replicación, consulte the section called “Configuración de la replicación de varios orígenes”.
read replica	RDS-EVENT-0240	Se detuvo manualmente el canal de replicación *`nombre`*.	Para obtener información acerca de los canales de replicación, consulte the section called “Configuración de la replicación de varios orígenes”.

Categoría	ID de evento de RDS	Mensaje	Notas
read replica	RDS-EVENT-0240	Se restableció el canal de replicación *nombre*.	Para obtener información acerca de los canales de replicación, consulte the section called “Configuración de la replicación de varios orígenes”.
recovery	RDS-EVENT-0020	Se ha iniciado la recuperación de la instancia de base de datos. El tiempo de recuperación dependerá de la cantidad de datos que deban recuperarse.	
recovery	RDS-EVENT-0021	Ha finalizado la recuperación de la instancia de base de datos.	
recovery	RDS-EVENT-0023	Solicitud de instantánea emergente: *mensaje*.	Se ha solicitado una copia de seguridad manual, pero Amazon RDS está creando una instantánea de base de datos. Envíe de nuevo la solicitud cuando Amazon RDS haya terminado la instantánea de base de datos.
recovery	RDS-EVENT-0052	Se ha iniciado la recuperación de instancias multi-AZ.	El tiempo de recuperación dependerá de la cantidad de datos que deban recuperarse.

Categoría	ID de evento de RDS	Mensaje	Notas
recovery	RDS-EVENT-0053	Se ha completado la recuperación de instancias de multi-AZ. Conmutación por error o activación pendientes.	
recovery	RDS-EVENT-0066	La instancia se degradará mientras se restablezca la duplicación: *mensaje*.	La instancia de base de datos de SQL Server está restableciendo su imagen reflejada. El desempeño se degradará hasta que se restablezca la imagen reflejada. Se ha encontrado una base de datos con un modelo de recuperación no completa (non-FULL). El modelo de recuperación se ha cambiado de nuevo a FULL y se ha iniciado la recuperación de la imagen reflejada. (<dbname>: <recovery model found>[,…])”
recovery	RDS-EVENT-0166	*message*	La instancia de base de datos de RDS Custom se encuentra dentro del perímetro de soporte.

Categoría	ID de evento de RDS	Mensaje	Notas
recovery	RDS-EVENT-0361	Se ha iniciado la recuperación de la instancia de base de datos en espera.	La instancia de base de datos en espera se reconstruye durante el proceso de recuperación. El rendimiento de la base de datos se ve afectado durante el proceso de recuperación.
recovery	RDS-EVENT-0362	Se ha completado la recuperación de la instancia de base de datos en espera.	La instancia de base de datos en espera se reconstruye durante el proceso de recuperación. El rendimiento de la base de datos se ve afectado durante el proceso de recuperación.
restoration	RDS-EVENT-0019	Se ha restaurado de la instancia de base de datos *`nombre`* a *`nombre`*.	La instancia de base de datos se ha restaurado a partir de una copia de seguridad de un momento dado.

Categoría	ID de evento de RDS	Mensaje	Notas
security	RDS-EVENT-0068	Descifrar la contraseña de la partición hsm para actualizar la instancia.	RDS está descifrando la contraseña de partición AWS CloudHSM para realizar actualizaciones en la instancia de base de datos. Para obtener más información, consulte Transparent Data Encryption (TDE) de la base de datos de Oracle con AWS CloudHSM en la Guía del usuario de AWS CloudHSM.
Creación de parches de seguridad	RDS-EVENT-0230	Hay disponible una actualización del sistema operativo para su instancia de base de datos. Para obtener información acerca de la aplicación de actualizaciones, consulte «Mantenimiento de una instancia de base de datos» en la Guía del usuario de RDS.	Hay disponible una nueva actualización del sistema operativo. Hay disponible una nueva versión secundaria de actualización del sistema operativo para su instancia de base de datos. Para obtener más información acerca de cómo se aplican las actualizaciones, consulte Actualizaciones del sistema operativo de instancias de base de datos de RDS.

Eventos de grupo de parámetros de base de datos

En la siguiente tabla se muestra la categoría de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es un grupo de parámetros de base de datos.

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0037	Se actualizó el parámetro *`nombre`* por *`valor`* con el método de aplicación *`método`*.	

Eventos de grupo de seguridad de base de datos

En la siguiente tabla se muestran las categorías de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es un grupo de seguridad de base de datos.

> **Note**
>
> Los grupos de seguridad de base de datos son recursos de EC2-Classic. EC2-Classic se retirará el 15 de agosto de 2022. Si todavía no ha migrado de EC2-Classic a una VPC, le recomendamos que migre lo antes posible. Para obtener más información, consulte el tema Migrar de EC2-Classic a una VPC en la guía del usuario de Amazon EC2 y la publicación del blog EC2-Classic Networking is Retiring – Here's How to Prepare.

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0038	Se ha aplicado el cambio al grupo de seguridad.	
failure	RDS-EVENT-0039	Revocar la autorización como *`usuario`*.	El grupo de seguridad propiedad de *`usuario`* no existe. Se ha revocado la

Categoría	ID de evento de RDS	Mensaje	Notas
			autorización para el grupo de seguridad porque no es válida.

Eventos de instantánea de base de datos

En la siguiente tabla se muestran las categorías de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es una instantánea de base de datos.

Categoría	ID de evento de RDS	Mensaje	Notas
creación	RDS-EVENT-0040	Crear una instantánea manual.	
creación	RDS-EVENT-0042	Se ha creado una instantán ea manual.	
creación	RDS-EVENT-0090	Crear instantáneas automáticas.	
creación	RDS-EVENT-0091	Se han creado instantán eas automáticas.	
deletion	RDS-EVENT-0041	Se ha eliminado la instantánea de usuario.	
notification	RDS-EVENT-0059	Se ha iniciado la copia de la instantánea *`nombre`* desde la región *`nombre`*.	Esta es una copia de instantánea entre regiones.
notification	RDS-EVENT-0060	Ha finalizado la copia de la instantánea *`nombre`* desde la región *`nombre`* en *`número`* minutos.	Esta es una copia de instantánea entre regiones.

Categoría	ID de evento de RDS	Mensaje	Notas
notification	RDS-EVENT-0061	Se ha cancelado la solicitud de copia de la instantánea *nombre* desde la región *nombre*.	Esta es una copia de instantánea entre regiones.
notification	RDS-EVENT-0159	Error en la tarea de exportación de instantán eas.	
notification	RDS-EVENT-0160	Se ha cancelado la tarea de exportación de instantán eas.	
notification	RDS-EVENT-0161	Se ha completado la tarea de exportación de instantán eas.	
notification	RDS-EVENT-0196	Se ha iniciado la copia de la instantánea *nombre* a la región *nombre*.	Se trata de una copia instantánea local.
notification	RDS-EVENT-0197	Ha finalizado la copia de la instantánea *nombre* a la región *nombre*.	Se trata de una copia instantánea local.
notification	RDS-EVENT-0190	Se ha cancelado la solicitud de copia de la instantánea *nombre* a la región *nombre*.	Se trata de una copia instantánea local.
restoration	RDS-EVENT-0043	Se ha restaurado a partir de la instantánea *nombre*.	Se está restaurando una instancia de base de datos a partir de una instantánea de base de datos.

Eventos de instantánea de clúster de bases de datos

En la siguiente tabla se muestra la categoría de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es una instantánea de clúster de base de datos.

Categoría	ID de evento de RDS	Mensaje	Notas
backup	RDS-EVENT-0074	Crear una instantánea manual del clúster.	
backup	RDS-EVENT-0075	Se ha creado una instantán ea manual del clúster.	
backup	RDS-EVENT-0168	Creación de instantáneas de clúster automatizadas.	
backup	RDS-EVENT-0169	Se ha creado una instantán ea de clúster automatizada.	

Eventos de RDS Proxy

En la siguiente tabla se muestran las categorías de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es una instancia de RDS Proxy.

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0204	RDS ha modificado el proxy de la base de datos *nombre*.	
configuration change	RDS-EVENT-0207	RDS ha modificado el punto de conexión del proxy de la base de datos *nombre*.	

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0213	RDS ha detectado la adición de la instancia de base de datos y la ha agregado automáticamente al grupo de destino del proxy de la base de datos *nombre*.	
configuration change	RDS-EVENT-0213	RDS ha detectado la creación de la instancia de base de datos *nombre* y la ha añadido automátic amente en el grupo de destino *nombre* del proxy de la base de datos *nombre*.	
configuration change	RDS-EVENT-0214	RDS ha detectado la eliminación de la instancia de base de datos *nombre* y la ha borrado automátic amente del grupo de destino *nombre* del proxy de la base de datos *nombre*.	
configuration change	RDS-EVENT-0215	RDS ha detectado la eliminación del clúster de base de datos *nombre* y la ha borrado automátic amente del grupo de destino *nombre* del proxy de la base de datos *nombre*.	

Categoría	ID de evento de RDS	Mensaje	Notas
creación	RDS-EVENT-0203	RDS ha creado el proxy de la base de datos *nombre*.	
creación	RDS-EVENT-0206	RDS ha creado el punto de conexión *nombre* del para el proxy de la base de datos *nombre*.	
deletion	RDS-EVENT-0205	RDS ha eliminado el proxy de la base de datos *nombre*.	
deletion	RDS-EVENT-0208	RDS ha eliminado el punto de conexión *nombre* del proxy de la base de datos *nombre*.	
failure	RDS-EVENT-0243	RDS no ha podido aprovisionar capacidad para el proxy *nombre* porque no hay suficientes direcciones IP disponibles en las subredes: *nombre*. Para resolver el problema, asegúrese de que sus subredes tengan el número mínimo de direcciones IP sin usar, tal como se recomienda en la documentación de RDS Proxy.	Para determinar el número recomendado para la clase de instancia, consulte Planificación de la capacidad de direcciones IP.

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0275	RDS ha limitado algunas conexiones al proxy de base de datos *nombre*. El número de solicitudes de conexión simultáne as del cliente al proxy ha superado el límite.	

Eventos de implementación azul/verde

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos cuando el tipo de origen es una implementación azul/verde.

Para obtener más información acerca de las implementaciones blue/green, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Categoría	ID de evento de Amazon RDS	Mensaje	Notas
creación	RDS-EVENT-0244	Se han completado las tareas de implementación azul/verde. Puede realizar más modificaciones en las bases de datos del entorno verde o cambiar la implementación.	
failure	RDS-EVENT-0245	No se ha podido crear la implementación azul/verde porque no se ha encontrado (la instancia/el clúster) de la base de datos (de origen/de stino).	

Categoría	ID de evento de Amazon RDS	Mensaje	Notas
deletion	RDS-EVENT-0246	Se ha eliminado la implementación azul/verde.	
notification	RDS-EVENT-0247	Se ha iniciado la transición de *azul* a *verde*.	
notification	RDS-EVENT-0248	Se ha completado el cambio en la implement ación azul/verde.	
failure	RDS-EVENT-0249	Se ha cancelado el cambio en la implementación azul/ verde.	
notification	RDS-EVENT-0250	La transición de la réplica de lectura principal *azul* a *verde* ha comenzado.	
notification	RDS-EVENT-0251	La transición de la réplica de lectura principal *azul* a *verde* ha finalizado. Se ha cambiado el nombre *azul* por *azul-antiguo* y *verde* por *azul*.	
failure	RDS-EVENT-0252	La transición de la réplica de lectura principal *azul* a *verde* se ha cancelado por *motivo*.	

Categoría	ID de evento de Amazon RDS	Mensaje	Notas
notification	RDS-EVENT-0307	La sincronización de la secuencia para la transición del *azul* a *verde* ha comenzado. La transición al usar secuencias puede provocar un tiempo de inactividad prolongado.	
notification	RDS-EVENT-0308	La sincronización de la secuencia para la transición del *azul* a *verde* ha finalizado.	
failure	RDS-EVENT-0310	La sincronización de la secuencia para la transición del *azul* a *verde* se ha cancelado porque las secuencias no se han sincronizado.	

Eventos de versiones del motor personalizadas

En la siguiente tabla se muestra la categoría de eventos y una lista de eventos cuando el tipo de origen es una versión de motor personalizada.

Categoría	ID de evento de Amazon RDS	Mensaje	Notas
creación	RDS-EVENT-0316	Preparación para crear un *nombre* de versión de motor personalizado. Todo el proceso de creación	

Categoría	ID de evento de Amazon RDS	Mensaje	Notas
		puede tardar hasta cuatro horas en completarse.	
creación	RDS-EVENT-0317	Creación de un *nombre* de versión de motor personalizado.	
creación	RDS-EVENT-0318	Validación de un *nombre* de versión de motor personalizado.	
creación	RDS-EVENT-0319	El *nombre* de la versión de motor personalizado se ha creado correctamente.	
creación	RDS-EVENT-0320	RDS no puede crear un *nombre* de versión de motor personalizado debido a un problema interno. Estamos resolviendo el problema y nos pondremos en contacto con usted si es necesario. Para obtener más ayuda, póngase en contacto con AWS Premium Support/.	
failure	RDS-EVENT-0198	Error al crear la versión de motor personalizada *nombre*. *mensaje*.	El *message* incluye detalles sobre el error, como los archivos que faltan.

Categoría	ID de evento de Amazon RDS	Mensaje	Notas
failure	RDS-EVENT-0277	Se ha producido un error al eliminar el *name* de la versión personalizada del motor. *message*	El *message* incluye detalles sobre el error.
restauración	RDS-EVENT-0240	El número máximo de bases de datos que se admite para la restauración en un momento dado ha cambiado.	El *message* incluye detalles sobre el evento.

Supervisión de archivos de registro de Amazon RDS

Cada motor de base de datos de RDS genera registros a los que puede acceder para realizar auditorías y solucionar problemas. El tipo de registros depende del motor de base de datos.

Puede acceder a los registros de base de datos de instancias de base de datos mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de Amazon RDS. No puede visualizar, ver ni descargar registros de transacciones.

Temas

- Visualización y descripción de archivos de registro de base de datos
- Descarga de un archivo de registro de base de datos
- Ver un archivo de registro de base de datos
- Publicación de registros de base de datos en registros de Amazon Cloudwatch
- Lectura del contenido del archivo de registro mediante REST
- Archivos de registro de base de datos de Amazon RDS para Db2
- Archivos de registro de base de datos de MariaDB
- Archivos de registro de base de datos de Amazon RDS para Microsoft SQL Server
- Archivos de registro de base de datos de MySQL
- Archivos de registro de base de datos de Amazon RDS para Oracle
- Archivos de registro de bases de datos de RDS para PostgreSQL

Visualización y descripción de archivos de registro de base de datos

Puede ver los archivos de registro de base de datos de su motor de base de datos de Amazon RDS con la AWS Management Console. Puede ver los archivos de registro que están disponibles para descargar o monitorear mediante la AWS CLI o la API de Amazon RDS.

> **Note**
>
> Si no puede ver la lista de archivos de registro de una instancia de base de datos de RDS para Oracle, reinicie la instancia para ver la lista.

Consola

Para ver un archivo de registro de base de datos

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione el nombre de la instancia de base de datos que tiene el archivo de registro que desea visualizar.
4. Seleccione la pestaña Logs & events (Registros y eventos).
5. Desplácese hacia abajo hasta la sección Logs (Registros).
6. (Opcional) Ingrese un término de búsqueda para filtrar los resultados.
7. Elija el registro que quiera visualizar y, a continuación, elija View (Ver).

AWS CLI

Para ver los archivos de registro de base de datos disponibles para una instancia de base de datos, use el comando AWS CLI de la `describe-db-log-files`.

El siguiente ejemplo devuelve una lista de los archivos de registro de una instancia de base de datos denominada `my-db-instance`.

Example

```
aws rds describe-db-log-files --db-instance-identifier my-db-instance
```

API de RDS

Para ver los archivos de registro de base de datos de una instancia de base de datos, use la acción `DescribeDBLogFiles` de la API de Amazon RDS.

Descarga de un archivo de registro de base de datos

Puede usar la AWS Management Console, la AWS CLI o la API para descargar un archivo de registro de base de datos.

Consola

Para descargar un archivo de registro de base de datos

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione el nombre de la instancia de base de datos que tiene el archivo de registro que desea visualizar.
4. Seleccione la pestaña Logs & events (Registros y eventos).
5. Desplácese hacia abajo hasta la sección Logs (Registros).
6. En la sección Logs (Registros), elija el botón junto al registro que desee descargar y, a continuación, elija Download (Descargar).
7. Abra el menú contextual (haga clic con el botón derecho) del enlace que se proporciona y elija Save Link As (Guardar enlace como). Escriba la ubicación en la que desee guardar el archivo de registro y elija Save (Guardar).



AWS CLI

Para descargar un archivo de registro de base de datos, use el comando AWS CLI de la `download-db-log-file-portion`. De forma predeterminada, este comando solo descarga la última porción de un archivo de registro. Sin embargo, puede descargar un archivo entero especificando el parámetro `--starting-token 0`.

En el siguiente ejemplo se muestra cómo descargar todo el contenido de un archivo de registro llamado log/ERROR.4 y almacenarlo en un archivo local denominado errorlog.txt.

Example

Para Linux, macOS o:Unix

```
aws rds download-db-log-file-portion \
    --db-instance-identifier myexampledb \
    --starting-token 0 --output text \
    --log-file-name log/ERROR.4 > errorlog.txt
```

En:Windows

```
aws rds download-db-log-file-portion ^
    --db-instance-identifier myexampledb ^
    --starting-token 0 --output text ^
    --log-file-name log/ERROR.4 > errorlog.txt
```

API de RDS

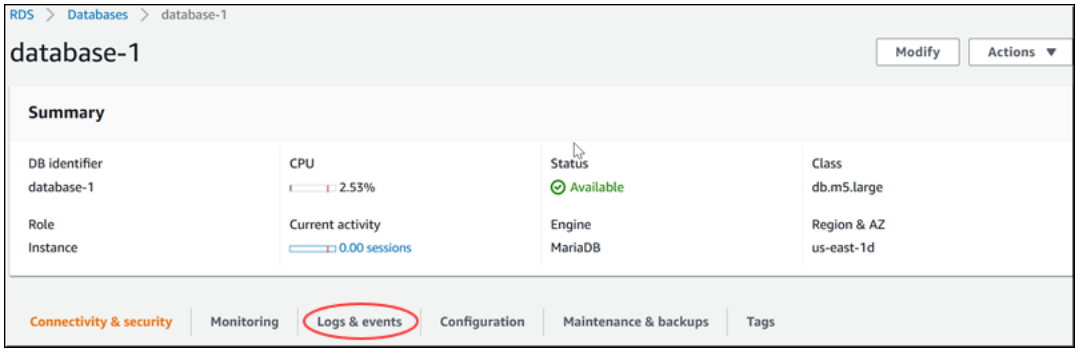
Para descargar un archivo de registro de base de datos, use la acción `DownloadDBLogFilePortion` de la API de Amazon RDS.

Ver un archivo de registro de base de datos

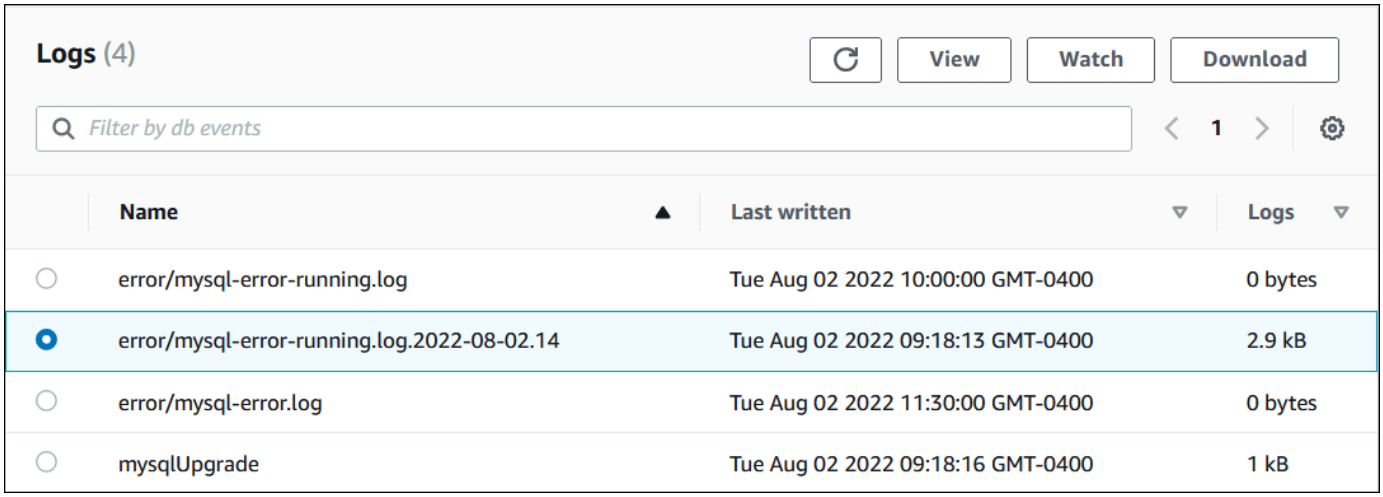
Ver un archivo de registro de base de datos equivale a detallar el archivo en un sistema UNIX o Linux. Puede ver un archivo de registro usando la AWS Management Console. RDS actualiza el detalle del registro cada 5 segundos.

Para monitorizar un archivo de registro de base de datos

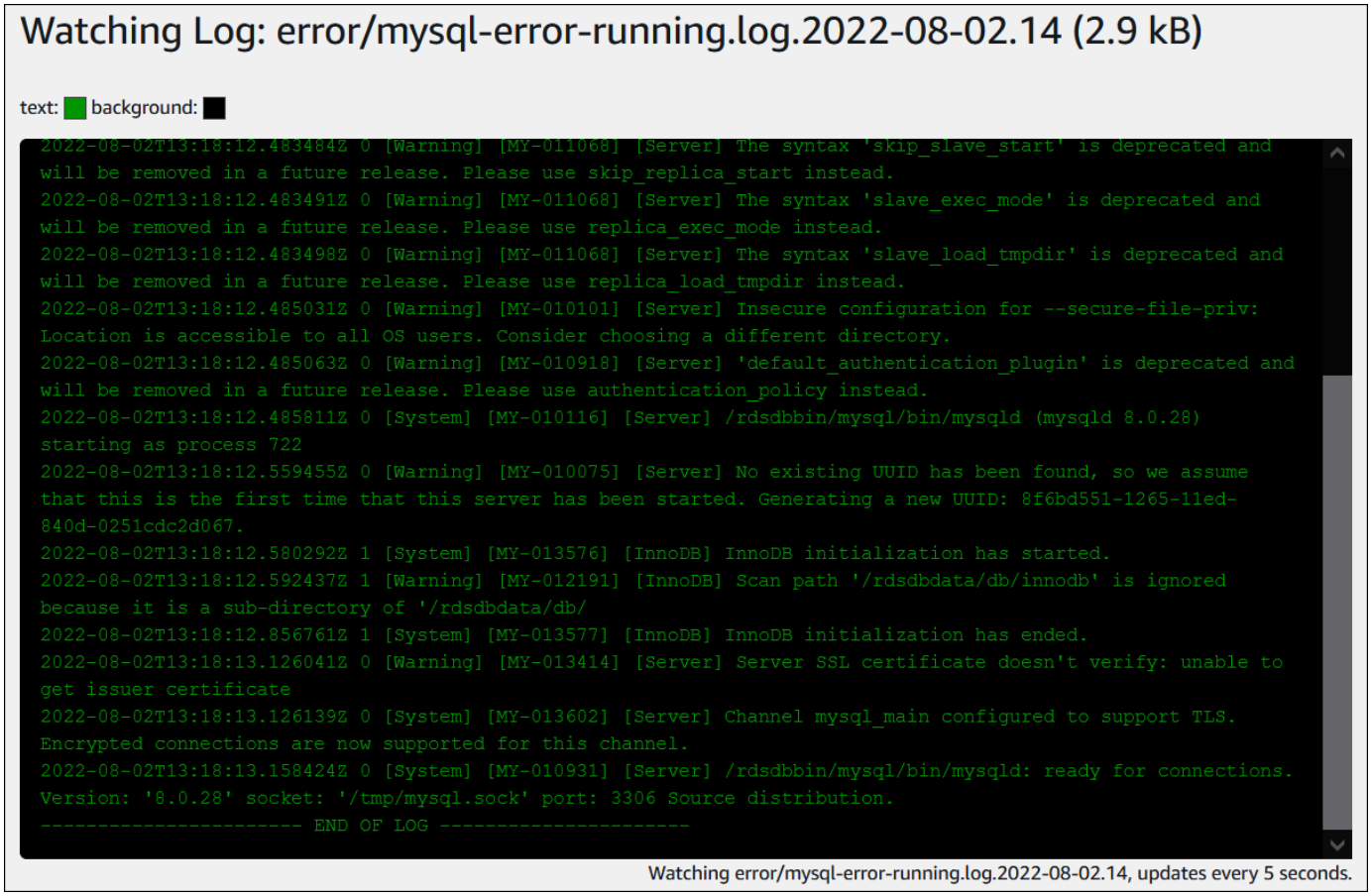
1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione el nombre de la instancia de base de datos que tiene el archivo de registro que desea visualizar.
4. Seleccione la pestaña Logs & events (Registros y eventos).



5. En la sección Logs (Registros), elija un archivo de registro y, a continuación, elija Watch (Ver).



RDS muestra el detalle del registro, como en el siguiente ejemplo de MySQL.



Publicación de registros de base de datos en registros de Amazon Cloudwatch

En una base de datos en las instalaciones, los registros de la base de datos residen en el sistema de archivos. Amazon RDS no proporciona acceso de host a los registros de base de datos del sistema de archivos de la instancia de base de datos. Por este motivo, Amazon RDS le permite exportar registros de base de datos a registros de Amazon CloudWatch. Con CloudWatch Logs, puede realizar análisis en tiempo real de los datos de registro. También puede guardarlos en un almacenamiento de larga duración y gestionarlos con el agente de CloudWatch Logs.

Temas

- Descripción general de la integración de RDS con CloudWatch Logs
- Decisión sobre los registros que desea publicar en CloudWatch Logs
- Especificación de registros que desea publicar en CloudWatch Logs
- Búsqueda y filtrado de los registros en CloudWatch Logs

Descripción general de la integración de RDS con CloudWatch Logs

En CloudWatch Logs, un flujo de registro es una secuencia de eventos de registro que comparten el mismo origen. Cada fuente independiente de registros en Registros de CloudWatch constituye un flujo de registros independiente. Un grupo de registro es un grupo de flujos de registro que comparten la misma configuración de retención, monitorización y control de acceso.

Amazon RDS transmite continuamente sus registros de instancia de base de datos en un grupo de registro. Por ejemplo, hay un grupo de registros `/aws/rds/instance/`*`instance_name`*`/`*`log_type`* para cada tipo de registro que se publica. Este grupo de registros se encuentra en la misma región de AWS que la instancia de base de datos que genera el registro.

AWS conserva los datos de registro publicados en CloudWatch Logs durante un periodo de tiempo indefinido a menos que se especifique un periodo de retención. Para obtener más información, consulte Cambiar la retención de datos de registro en CloudWatch Logs.

Decisión sobre los registros que desea publicar en CloudWatch Logs

Cada motor de base de datos RDS admite su propio conjunto de registros. Para obtener más información sobre las opciones del motor de base de datos, revise los siguientes temas:

- the section called “Publicación de registros de Db2 en Registros de Amazon CloudWatch”
- the section called “Publicación de registros de MariaDB en Amazon CloudWatch Logs”
- the section called “Publicación de registros de MySQL en Amazon CloudWatch Logs”
- the section called “Publicación de registros de Oracle en Amazon CloudWatch Logs”
- the section called “Publicación de registros de PostgreSQL en Amazon CloudWatch Logs”
- the section called “Publicación de registros de SQL Server en Amazon CloudWatch Logs”

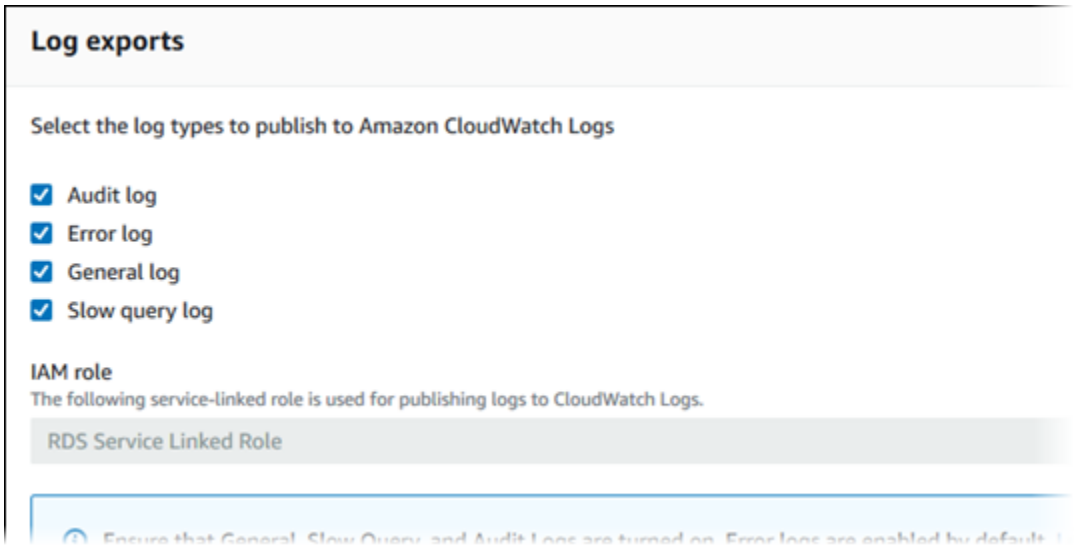
Especificación de registros que desea publicar en CloudWatch Logs

Puede especificar qué registros se van a publicar en la consola. Asegúrese de que tiene un rol vinculado a un servicio en AWS Identity and Access Management (IAM). Para obtener más información acerca de los roles vinculados a servicios, consulte Uso de roles vinculados a servicios de Amazon RDS.

Para especificar los registros que se van a publicar

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Haga una de estas dos operaciones:
   - Elija Creación de base de datos.
   - Elija una base de datos de la lista y luego seleccione Modify (Modificar).
4. En Logs exports (Exportaciones de registros), elija los registros que desea publicar.

   En el siguiente ejemplo se especifican el registro de auditoría, los registros de errores, el registro general y el registro de consultas lentas para una instancia de bases de datos de RDS para MySQL.



Búsqueda y filtrado de los registros en CloudWatch Logs

Puede buscar las entradas de registro que cumplan los criterios especificados mediante la consola de CloudWatch Logs. Puede acceder a los registros a través de la consola de RDS, que lo lleva a la consola de CloudWatch Logs, o directamente desde la consola de CloudWatch Logs.

Para buscar los registros de RDS mediante la consola de RDS

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija un instancia de base de datos.

4. Elija Configuración.
5. En Published logs (Registros publicados), elija el registro de base de datos que desea ver.

Para buscar registros de RDS mediante la consola de CloudWatch Logs

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Grupos de registro.
3. En el cuadro de filtro, escriba **`/aws/rds`**.
4. En Log Groups (Grupos de registro), elija el nombre del grupo de registro que contiene el flujo de registros que desea buscar.
5. En Log Streams (Flujos de registros), elija el nombre del flujo de registros que desea buscar.
6. En Log events (Eventos de registros), escriba la sintaxis del filtro que se va a utilizar.

Para obtener más información, consulte el temas sobre cómo buscar y filtrar datos de registros en la guía del usuario de Amazon CloudWatch. Para ver un tutorial en el blog que explique cómo monitorear los registros de RDS, consulte la publicación del blog sobre cómo crear un monitoreo proactivo de bases de datos para Amazon RDS con registros de Amazon Cloudwatch, AWS Lambda y Amazon SNS.

Lectura del contenido del archivo de registro mediante REST

Amazon RDS proporciona un punto de enlace REST que permite el acceso a los archivos de registro de instancia de base de datos. Esto resulta útil si necesita escribir una aplicación para transmitir el contenido del archivo de registro de Amazon RDS.

La sintaxis es la siguiente:

```
GET /v13/downloadCompleteLogFile/DBInstanceIdentifier/LogFileName HTTP/1.1
Content-type: application/json
host: rds.region.amazonaws.com
```

Se requieren los siguientes parámetros:

- *`DBInstanceIdentifier`*: el nombre asignado de la instancia de base de datos que contiene el archivo de registro que se desea descargar.
- *`LogFileName`*: el nombre del archivo de registro que se va a descargar.

La respuesta incluye el contenido del archivo de registro solicitado como una secuencia.

En el siguiente ejemplo se descarga el archivo de registro denominado log/ERROR.6 para la instancia de base de datos denominada sample-sql en la región us-west-2.

```
GET /v13/downloadCompleteLogFile/sample-sql/log/ERROR.6 HTTP/1.1
host: rds.us-west-2.amazonaws.com
X-Amz-Security-Token: AQoDYXdzEIH//////////
wEa0AIXLhngC5zp9CyB1R6abwKrXHVR5efnAVN3XvR7IwqKYalFSn6UyJuEFTft9nObglx4QJ+GXV9cpACkETq=
X-Amz-Date: 20140903T233749Z
X-Amz-Algorithm: AWS4-HMAC-SHA256
X-Amz-Credential: AKIADQKE4SARGYLE/20140903/us-west-2/rds/aws4_request
X-Amz-SignedHeaders: host
X-Amz-Content-SHA256: e3b0c44298fc1c229afbf4c8996fb92427ae41e4649b934de495991b7852b855
X-Amz-Expires: 86400
X-Amz-Signature: 353a4f14b3f250142d9afc34f9f9948154d46ce7d4ec091d0cdabbcf8b40c558
```

Si especifica una instancia de base de datos no existente, la respuesta consta del error siguiente:

- `DBInstanceNotFound: DBInstanceIdentifier` no hace referencia a una instancia de base de datos existente. (Código de estado HTTP: 404)

Archivos de registro de base de datos de Amazon RDS para Db2

Puede acceder a los registros de diagnóstico y notificación de RDS para Db2 desde la consola de Amazon RDS, la AWS CLI o la API de RDS. Para obtener más información acerca de la visualización, descarga y vigilancia de los registros de bases de datos basados en archivos, consulte Supervisión de archivos de registro de Amazon RDS.

Temas

- Calendario de retención
- Publicación de registros de Db2 en Registros de Amazon CloudWatch

Calendario de retención

Los archivos de registro rotan cada día y cuando se reinicia la instancia de base de datos. A continuación, se muestra el calendario de retención para los registros de RDS para Db2 en Amazon RDS.

Tipo de registro	Calendario de retención
Registros de diagnóstico	Db2 elimina los registros de la configuración de retención de la instancia. Amazon RDS establece el parámetro `diagsize` en 1000.
Registros de notificación	Db2 elimina los registros de la configuración de retención de la instancia. Amazon RDS establece el parámetro `diagsize` en 1000.

Publicación de registros de Db2 en Registros de Amazon CloudWatch

Con RDS para Db2, puede publicar eventos de registro de diagnóstico y notificación directamente en Registros de Amazon CloudWatch. Analice los datos de registro con CloudWatch Logs y utilice CloudWatch para crear alarmas y ver métricas.

En CloudWatch Logs, tiene las siguientes opciones:

- Almacenar registros en un espacio de almacenamiento de larga duración con un periodo de retención que defina.
- Buscar y filtrar los datos de registro.

- Compartir datos de registro entre cuentas.
- Exportar registros a Amazon S3.
- Transmitir datos por streaming a Amazon OpenSearch Service.
- Procesar los datos de registros en tiempo real con Amazon Kinesis Data Streams. Para obtener más información, consulte Uso de Registros de Amazon CloudWatch en la Guía para desarrolladores de aplicaciones SQL de Amazon Managed Service para Apache Flink.

Amazon RDS publica cada registro de base de datos de RDS para Db2 como un flujo de base de datos independiente en el grupo de registros. Por ejemplo, si publica registros de diagnóstico y notificación, se almacenan datos de diagnóstico en un flujo de registro de diagnóstico en el grupo de registro `/aws/rds/instance/my_instance/diagnostic` y los datos de registro de notificación se almacenan en el grupo de registro `/aws/rds/instance/my_instance/notify`.

> **Note**
>
> La publicación de registros de RDS para Db2 en los Registros de CloudWatch no está habilitada de manera predeterminada. No se admite la publicación de registros estadísticos del optimizador y del administrador de memoria autoajustable (STMM). La publicación de registros de RDS para Db2 en Registros de CloudWatch es compatible en todas las regiones, excepto en Asia Pacífico (Hong Kong).

Consola

Publicación de registros de base de datos de RDS para Db2 en Registros de CloudWatch desde AWS Management Console

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify.
4. En la sección Exportaciones de registros, elija los registros que desea comenzar a publicar en Registros de CloudWatch.

   Puede elegir diag.log, notify.log o ambos.
5. Elija Continuar, seguido de Modificar la instancia de base de datos en la página de resumen.

AWS CLI

Para publicar registros de RDS para Db2, puede utilizar el comando `modify-db-instance` con los siguientes parámetros:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Los cambios en la opción `--cloudwatch-logs-export-configuration` siempre se aplican a la instancia de base de datos inmediatamente. Por lo tanto, las opciones `--apply-immediately` y `--no-apply-immediately` no tienen ningún efecto.

También puede publicar registros de RDS para Db2 utilizando los siguientes comandos:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Example

En el siguiente ejemplo se crea una instancia de base de datos de RDS para Db2 con la publicación de Registros de CloudWatch habilitada. El valor `--enable-cloudwatch-logs-exports` es una matriz de cadenas JSON que puede incluir `diag.log`, `notify.log` o ambos.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["diag.log","notify.log"]' \
    --db-instance-class db.m4.large \
    --engine db2-se
```

Para Windows:

```
aws rds create-db-instance ^
```

```
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports "[\"diag.log\",\"notify.log\"]" ^
    --db-instance-class db.m4.large ^
    --engine db2-se
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Example

En el siguiente ejemplo se modifica una instancia de base de datos de RDS para Db2 existente para publicar archivos de registro en Registros de CloudWatch. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `EnableLogTypes` y su valor es una matriz de cadenas que puede incluir `diag.log`, `notify.log` o ambos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["diag.log","notify.log"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"EnableLogTypes\":[\"diag.log\",
\"notify.log\"]}"
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Example

En el siguiente ejemplo se modifica una instancia de base de datos de RDS para Db2 existente para deshabilitar la publicación de archivos de registro de diagnóstico en Registros de CloudWatch. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `DisableLogTypes` y su valor es una matriz de cadenas que puede incluir `diag.log`, `notify.log` o ambos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"DisableLogTypes":["diag.log"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"DisableLogTypes\":[\"diag.log\"]}"
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Archivos de registro de base de datos de MariaDB

Puede supervisar el registro de errores de MariaDB, el registro de consultas lentas, el registro de errores de autenticación de base de datos de IAM y el registro general. El registro de error de MariaDB se genera de forma predeterminada. Para generar la consulta lenta y los registros generales, establezca parámetros en su grupo de parámetros de base de datos. Amazon RDS rota todos los archivos de registro de MariaDB; los intervalos para cada tipo se indican a continuación.

Puede monitorear los registros de MariaDB directamente desde la consola de Amazon RDS, la API de Amazon RDS, la CLI de Amazon RDS o los SDK de AWS. También puede obtener acceso a los registros de MariaDB dirigiéndolos a una tabla de la base de datos principal y consultando esa tabla. Puede usar la utilidad mysqlbinlog para descargar un registro binario.

Para obtener más información acerca de la visualización, descarga y vigilancia de los registros de bases de datos basados en archivos, consulte Supervisión de archivos de registro de Amazon RDS.

Temas

- Acceso a los registros de errores de MariaDB
- Acceso al registro de consultas lentas y al registro general de MariaDB
- Publicación de registros de MariaDB en Amazon CloudWatch Logs
- Rotación y retención de registros para MariaDB
- Administración de registros de MariaDB basados en tablas
- Configuración de registros binarios de MariaDB
- Acceso a los registros binarios de MariaDB
- Habilitación de la anotación de registros binarios de MariaDB

Acceso a los registros de errores de MariaDB

El registro de errores de MariaDB se escribe en el archivo `<host-name>.err`. Puede ver este archivo mediante la consola de Amazon RDS, También puede recuperar el registro mediante la API de Amazon RDS, la CLI de Amazon RDS o los SDK de AWS. El archivo `<host-name>.err` se vacía cada 5 minutos y su contenido se agrega a `mysql-error-running.log`. El archivo `mysql-error-running.log` rota cada hora, y se conservan los archivos generados cada hora durante las últimas 24 horas. Cada archivo de registro tiene la hora a la que se generó (en UTC) agregada a su nombre. Los archivos de registro también tienen una marca temporal que ayuda a determinar cuándo se escribieron las entradas del registro.

MariaDB solo escribe en el registro de errores durante el inicio, el cierre y cuando encuentra errores. Una instancia de base de datos puede pasar horas o días sin que se escriban nuevas entradas en el registro de errores. Si no hay entradas recientes, se debe a que el servidor no ha encontrado ningún error que haya generado una entrada en el registro.

Acceso al registro de consultas lentas y al registro general de MariaDB

Puede escribir el registro de consultas lentas y el registro general de MariaDB en un archivo o en una tabla de la base de datos configurando parámetros en su grupo de parámetros de la base de datos. Para obtener información acerca de cómo crear y modificar un grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS. Debe definir estos parámetros para poder ver el registro de consultas lentas o el registro general en la consola de Amazon RDS o a través de la API de Amazon RDS, la AWS CLI o los SDK de AWS.

Puede controlar lo que registra MariaDB con los parámetros de esta lista:

- `slow_query_log` o `log_slow_query`: para crear el registro de consultas lentas, use el valor 1. El valor predeterminado es 0.
- `general_log`: para crear el registro general, use el valor 1. El valor predeterminado es 0.
- `long_query_time` o `log_slow_query_time`: para evitar que se registren consultas rápidas en el registro de consultas lentas, especifique el valor del tiempo de ejecución mínimo de una consulta, en segundos, para que se registre. El valor predeterminado es 10 segundos y el mínimo es 0. Si log_output = FILE, puede especificar un valor de punto flotante que llega a una resolución de microsegundos. Si log_output = TABLE, debe especificar un valor entero con resolución de segundos. Solo se registran las consultas cuyo tiempo de ejecución supere el valor de `long_query_time` o `log_slow_query_time`. Por ejemplo, si configura `long_query_time` o `log_slow_query_time` como 0,1, evitará que se registren las consultas que tarden menos de 100 milisegundos en ejecutarse.
- `log_queries_not_using_indexes`: para incluir en el registro de consultas lentas todas las consultas que no usen un índice, defina este parámetro como 1. El valor predeterminado es 0. Las consultas que no usen un índice se registran incluso si su tiempo de ejecución es inferior al valor del parámetro `long_query_time`.
- `log_output` *`option`*: puede especificar una de las opciones siguientes para el parámetro `log_output`:
  - TABLE (predeterminada): las consultas generales se escriben en la tabla `mysql.general_log` y las consultas lentas en la tabla `mysql.slow_log`.

- FILE: tanto los registros de las consultas generales como los de las consultas lentas se escriben en el sistema de archivos. Los archivos de registro se rotan cada hora.
- NONE: deshabilitar registro.

Cuando el registro está habilitado, Amazon RDS rota los registros de las tablas o elimina los archivos de registro a intervalos regulares. Esta medida es una precaución para reducir el riesgo de que un archivo de registro grande bloquee el uso de la base de datos o afecte al rendimiento. El registro con las opciones `FILE` y `TABLE` emplea la rotación y eliminación del modo siguiente:

- Cuando está activado el registro `FILE`, los archivos de registro se examinan cada hora, y los que tienen una antigüedad superior a 24 horas se eliminan. En algunos casos, el tamaño restante del archivo de registro combinado después de la eliminación puede superar el umbral del 2 por ciento del espacio asignado a una instancia de base de datos. En estos casos, los archivos de registro más grandes se eliminan hasta que el tamaño del archivo de registro no sobrepase el umbral.
- Cuando el registro de tipo `TABLE` está habilitado, en algunos casos, las tablas de registro se rotan cada 24 horas. Esta rotación de produce cuando el espacio ocupado por los registros de tabla es superior al 20% del espacio de almacenamiento asignado. También ocurre si el tamaño de todos los registros combinados es superior a 10 GB. Si la cantidad de espacio utilizada para una instancia de base de datos es superior al 90% del espacio de almacenamiento asignado a la instancia de base de datos, se reducen los umbrales de la rotación de registros. Las tablas de registro se rotan si el espacio ocupado por los registros de tabla es superior al 10 % del espacio de almacenamiento asignado. También rotan si el tamaño de todos los registros combinados es superior a 5 GB.

  Cuando se rotan las tablas de registro, la tabla de registro actual se copia en una tabla de registro de copia de seguridad y las entradas de la tabla de registro actual se eliminan. Si la tabla de registro de copia de seguridad ya existe, se elimina antes de copiar la tabla del registro actual en la copia de seguridad. Puede consultar la tabla de registro de copia de seguridad si es necesaria. La tabla de registro de copia de seguridad para la tabla `mysql.general_log` se llama `mysql.general_log_backup`. La tabla de registro de copia de seguridad para la tabla `mysql.slow_log` se llama `mysql.slow_log_backup`.

  Para rotar la tabla `mysql.general_log` puede ejecutar el procedimiento `mysql.rds_rotate_general_log`. Para rotar la tabla `mysql.slow_log` puede ejecutar el procedimiento `mysql.rds_rotate_slow_log`.

  Los registros de tabla se rotan durante una actualización de la versión de la base de datos.

Amazon RDS registra la rotación de registros de `TABLE` y de `FILE` en un evento de Amazon RDS y envía una notificación.

Para trabajar con los registros desde la consola de Amazon RDS, la API de Amazon RDS, la CLI de Amazon RDS o los SDK de AWS, configure el parámetro `log_output` en FILE. Al igual que el registro de errores de MariaDB, estos archivos de registro rotan cada hora. Se conservan los archivos de registro que se generaron durante las 24 horas anteriores.

Para obtener más información acerca de los registros de consultas lentas y general, vaya a los siguientes temas de la documentación de MariaDB:

- Registro de consultas lentas
- Registro de consultas generales

Publicación de registros de MariaDB en Amazon CloudWatch Logs

Se puede configurar una instancia de base de datos MariaDB para publicar datos de registro en un grupo de registros en Amazon CloudWatch Logs. Con CloudWatch Logs, puede realizar análisis en tiempo real de los datos de registro y utilizar CloudWatch para crear alarmas y ver métricas. Puede utilizar CloudWatch Logs para almacenar los registros de registros en almacenamiento de larga duración.

Amazon RDS publica cada registro de base de datos de MariaDB como un flujo de base de datos independiente en el grupo de registros. Por ejemplo, supongamos que configura la función de exportación para que incluya el registro de consulta lento. Los datos de las consultas lentas se almacenan en el flujo de registro en el grupo de registro de `/aws/rds/instance/`*`my_instance`*`/slowquery`.

El registro de errores están habilitados de forma predeterminada. La tabla siguiente resume los requisitos para los otros registros de MariaDB.

Registro	Requisito
Registro de auditoría	La instancia de base de datos debe usar un grupo de opciones personalizado con la opción `MARIADB_AUDIT_PLUGIN` .
Registro general	La instancia de base de datos debe usar un grupo de parámetros personalizado con la

Registro	Requisito
	configuración del parámetro `general_log = 1` para habilitar el registro general.
Registro de consultas lentas	La instancia de base de datos debe usar un grupo de parámetros personalizado con la configuración del parámetro `slow_query_log = 1` o `log_slow_query = 1` para habilitar el registro de consultas lentas.
Registro de errores de autenticación de base de datos de IAM	Debe habilitar el tipo de registro `iam-db-auth-error` para una instancia de base de datos mediante la creación o modificación de una instancia de base de datos.
Resultado de registro	La instancia de base de datos debe usar un grupo de parámetros personalizado con la configuración del parámetro `log_output = FILE` para escribir registros en el sistema de archivos y publicarlos en CloudWatch Logs.

Consola

Para publicar registros de MariaDB en CloudWatch Logs desde la consola

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify.
4. En la sección Logs exports (Exportaciones de registros), elija los registros que desea comenzar a publicar en CloudWatch Logs.
5. Elija Continue, seguido de Modify DB Instance en la página de resumen.

AWS CLI

Puede publicar registros de base de datos MariaDB con la AWS CLI. Puede llamar al comando `modify-db-instance` con los parámetros siguientes:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Los cambios en la opción `--cloudwatch-logs-export-configuration` siempre se aplican a la instancia de base de datos inmediatamente. Por lo tanto, las opciones `--apply-immediately` y `--no-apply-immediately` no tienen ningún efecto.

También puede publicar registros de MariaDB si llama a los siguientes comandos de la AWS CLI:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Ejecute uno de estos comandos de la AWS CLI con las siguientes opciones:

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

Podrían ser necesarias otras opciones en función del comando de la AWS CLI que ejecute.

Example

En el siguiente ejemplo se modifica una instancia de base de datos MariaDB existente para publicar archivos de registro en CloudWatch Logs. El valor `--cloudwatch-logs-export-`

`configuration` es un objeto JSON. La clave de este objeto es `EnableLogTypes` y su valor es una matriz de cadenas con cualquier combinación de `audit`, `error`, `general` y `slowquery`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Example

El siguiente comando crea una instancia de base de datos MariaDB y publica archivos de registro en CloudWatch Logs. El valor `--enable-cloudwatch-logs-exports` es una matriz de cadenas JSON. Las cadenas pueden ser cualquier combinación de `audit`, `error`, `general` y `slowquery`.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["audit","error","general","slowquery"]' \
    --db-instance-class db.m4.large \
    --engine mariadb
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports '["audit","error","general","slowquery"]' ^
    --db-instance-class db.m4.large ^
    --engine mariadb
```

API de RDS

Puede publicar registros de MariaDB con la API de RDS. Puede realizar una llamada a la operación `ModifyDBInstance` con los parámetros siguientes:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Los cambios en el parámetro `CloudwatchLogsExportConfiguration` siempre se aplican a la instancia de base de datos inmediatamente. Por tanto, el parámetro `ApplyImmediately` no tiene efecto.

También puede publicar registros de MariaDB llamando a las siguientes operaciones de la API de RDS:

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`

Ejecute una de estas operaciones de la API de RDS con los siguientes parámetros:

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

Podrían ser necesarios otros parámetros en función del comando de la AWS CLI que ejecute.

Rotación y retención de registros para MariaDB

Cuando el registro está habilitado, Amazon RDS rota los registros de las tablas o elimina los archivos de registro a intervalos regulares. Esta medida es una precaución para reducir el riesgo de que un archivo de registro grande bloquee el uso de la base de datos o afecte al desempeño.

El tamaño de los archivos de registro de consultas lentas, registro de errores y registro general de MariaDB está limitado al 2 por ciento del espacio de almacenamiento asignado a una instancia de base de datos. Para mantener este umbral, los registros se rotan automáticamente cada hora y los que tienen una antigüedad superior a 24 horas se eliminan. Si el tamaño combinado de los archivos de registro sobrepasa el umbral después de eliminar los archivos de registro antiguos, los archivos de registro más grandes se eliminan hasta que el tamaño del archivo de registro deje de sobrepasar el umbral.

Amazon RDS rota los archivos de registro de errores de autenticación de la base de datos de IAM de más de 10 MB. Amazon RDS elimina los archivos de registro de errores de autenticación de la base de datos de IAM que tengan más de cinco días o más de 100 MB.

Administración de registros de MariaDB basados en tablas

Puede dirigir los registros de las consultas lentas a tablas de la instancia de base de datos. Para ello, cree un grupo de parámetros de base de datos y defina el parámetro del servidor `log_output` en `TABLE`. Las consultas generales se registrarán entonces en la tabla `mysql.general_log` y las consultas lentas en la tabla `mysql.slow_log`. Puede consultar las tablas para obtener acceso a la información del registro. Al habilitar este registro, se incrementa la cantidad de datos que se escribe en la base de datos, lo que puede degradar el desempeño.

Tanto el registro general como los registros de consultas lentas están deshabilitados de manera predeterminada. Para habilitar el registro en tablas, también debe establecer los siguientes parámetros del servidor en `1`:

- `general_log`
- `slow_query_log` o `log_slow_query`

Las tablas de registro seguirán creciendo hasta que las actividades de registro respectivas se desactiven cambiando el valor del parámetro a `0`. A menudo, se acumula una gran cantidad de datos, lo que puede consumir un porcentaje elevado del espacio de almacenamiento asignado. Amazon RDS no le permite truncar las tablas de registro, pero sí mover su contenido. Al rotar una tabla, su contenido se guarda en una tabla de copia de seguridad y se crea una nueva

tabla de registro vacía. Puede aplicar manualmente la rotación de las tablas de registro con los procedimientos de línea de comandos siguientes, en los que el símbolo del sistema se representa por:PROMPT>

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

Para eliminar por completo los datos antiguos y recuperar el espacio del disco, llame al procedimiento correspondiente dos veces consecutivas.

Configuración de registros binarios de MariaDB

El registro binario es un conjunto de archivos de registro que contienen información acerca de las modificaciones de datos hechas en una instancia de servidor de MariaDB. El registro binario contiene información como la siguiente:

- Eventos que describen cambios en la base de datos, como la creación de tablas o las modificaciones de filas.
- Información sobre la duración de cada instrucción que actualizó los datos.
- Eventos para instrucciones que podrían haber actualizado datos, pero que no lo hicieron.

El registro binario registra las instrucciones que se envían durante la replicación. También es necesario para algunas operaciones de recuperación. Para obtener más información, consulte Binary Log en la documentación de MariaDB.

La característica de copias de seguridad automatizadas determina si el registro binario se activa o desactiva para MariaDB. Dispone de las opciones siguientes:

Activar el registro binario.

Establecer el periodo de retención de copia de seguridad en un valor positivo distinto de cero.

Desactivar el registro binario.

Establecer el periodo de retención de copia de seguridad en cero.

Para obtener más información, consulte Habilitar las copias de seguridad automatizadas.

MariaDB en Amazon RDS admite los formatos de registro binario basado en filas, basado en instrucciones y mixto. El formato de registro binario predeterminado es el mixto. Para obtener

información detallada acerca de los formatos de registro binarios de MariaDB, consulte Binary Log Formats en la documentación de MariaDB.

Si tiene pensado usar la replicación, el formato de registro binario es importante. Esto es importante porque determina el registro de los cambios de datos que se registra en la fuente y se envía a los objetivos de replicación. Para obtener más información acerca de las ventajas y desventajas de distintos tipos de formatos de registro binarios para la replicación, consulte Advantages and Disadvantages of Statement-Based and Row-Based Replication en la documentación de MySQL.

> **Important**
>
> La configuración del formato de registro binario como basado en filas puede generar archivos de registro binario muy grandes. Los archivos de registro binario grandes reducen la cantidad de almacenamiento disponible para una instancia de base de datos. También pueden incrementar la cantidad de tiempo necesaria para llevar a cabo la operación de restauración de una instancia de base de datos.
>
> La replicación basada en instrucciones puede causar incoherencias entre la instancia de base de datos de origen y la réplica de lectura. Para obtener más información, consulte Unsafe Statements for Statement-based Replication en la documentación de MariaDB.
>
> Habilitar el registro binario aumenta el número de operaciones de E/S de escritura en el disco en la instancia de base de datos. Puede supervisar el uso de IOPS con la métrica de CloudWatch `WriteIOPS`.

Para configurar el formato de registro binario de MariaDB

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija el grupo de parámetros utilizados por la instancia de base de datos que quiera modificar.

   No puede modificar un grupo de parámetros predeterminado. Si la instancia de base de datos emplea un grupo de parámetros predeterminado, cree un nuevo grupo de parámetros y asócielo con la instancia de base de datos.

   Para obtener más información acerca de los grupos de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.
4. En Parameter group actions (Acciones de grupos de parámetros), seleccione Edit (Editar).

5. Establezca el parámetro `binlog_format` en el formato de registro binario de su elección (ROW, STATEMENT o MIXED).

   Para desactivar el registro binario establezca el período de retención de copias de seguridad de una instancia de base de datos en cero. Tenga en cuenta que esto deshabilita las copias de seguridad automatizadas diarias. Al deshabilitar las copias de seguridad automatizadas, se desactiva o deshabilita la variable de sesión `log_bin`. Esto deshabilita el registro binario en la instancia de base de datos de RDS para MariaDB, lo que a su vez restablece la variable de sesión `binlog_format` al valor predeterminado de `ROW` en la base de datos. Se recomienda no deshabilitar las copias de seguridad. Para obtener más información acerca de la configuración del Período de retención de copia de seguridad, consulte Configuración de instancias de base de datos.
6. Elija Guardar cambios para guardar los cambios realizados en el grupo de parámetros de base de datos.

Dado que el parámetro `binlog_format` es dinámico en RDS para MariaDB, no es necesario reiniciar la instancia de base de datos para que se apliquen los cambios.

> **Important**
>
> El cambio de un grupo de parámetros de base de datos afecta a todas las instancias de base de datos que utilizan ese grupo de parámetros. Si desea especificar diferentes formatos de registro binario para diferentes instancias de base de datos de MariaDB en una región de AWS, las instancias de base de datos deben utilizar diferentes grupos de parámetros de bases de datos. Estos grupos de parámetros identifican diferentes formatos de registro. Asigne el grupo de parámetros de base de datos apropiado a cada instancia de base de datos.

Acceso a los registros binarios de MariaDB

Puede usar la utilidad mysqlbinlog para descargar los registros binarios en formato de texto desde las instancias de base de datos de MariaDB. El registro binario se descarga en su equipo local. Para obtener más información acerca del uso de la utilidad mysqlbinlog, vaya a Using mysqlbinlog en la documentación de MariaDB.

Para ejecutar la utilidad mysqlbinlog en una instancia de Amazon RDS, use las siguientes opciones:

- Especifique la opción `--read-from-remote-server`.
- `--host`: especifique el nombre de DNS del punto de conexión de la instancia.
- `--port`: especifique el puerto que utiliza la instancia.
- `--user`: especifique un usuario de MariaDB al que se haya asignado el permiso de esclavo de replicación.
- `--password`: especifique la contraseña del usuario o no indique ninguna para que la utilidad pida una contraseña.
- `--result-file`: especifique el archivo local que recibirá la salida.
- Especifique los nombres de uno o varios de los archivos de registro binarios. Para obtener una lista de los registros disponibles, use el comando SHOW BINARY LOGS de SQL.

Para obtener más información acerca de las opciones de mysqlbinlog, vaya a mysqlbinlog Options en la documentación de MariaDB.

A continuación se muestra un ejemplo:

Para Linux, macOS o:Unix

```
mysqlbinlog \
    --read-from-remote-server \
    --host=mariadbinstance1.1234abcd.region.rds.amazonaws.com \
    --port=3306  \
    --user ReplUser \
    --password <password> \
    --result-file=/tmp/binlog.txt
```

En:Windows

```
mysqlbinlog ^
    --read-from-remote-server ^
    --host=mariadbinstance1.1234abcd.region.rds.amazonaws.com ^
    --port=3306  ^
    --user ReplUser ^
    --password <password> ^
    --result-file=/tmp/binlog.txt
```

Normalmente, Amazon RDS limpia un registro binario lo antes posible. Sin embargo, el registro binario debe seguir estando disponible en la instancia para que mysqlbinlog pueda obtener acceso a

él. Para especificar el número de horas que RDS retiene los registros binarios, use el procedimiento almacenado `mysql.rds_set_configuration`. Especifique un período con tiempo suficiente para descargar los registros. Una vez que haya definido el periodo de retención, monitorice el uso del almacenamiento para la instancia de base de datos con el fin de asegurarse de que los registros binarios conservados no consuman demasiado almacenamiento.

En el siguiente ejemplo se define el periodo de retención en 1 día.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Para mostrar el valor actual, utilice el procedimiento almacenado `mysql.rds_show_configuration`.

```
call mysql.rds_show_configuration;
```

Habilitación de la anotación de registros binarios de MariaDB

En una instancia de base de datos de MariaDB, puede usar el evento `Annotate_rows` para incluir en un evento de fila una copia de la consulta de SQL que causó el evento de fila. Este enfoque proporciona una funcionalidad similar a la habilitación del parámetro `binlog_rows_query_log_events` en una instancia de base de datos de RDS para MySQL.

Puede habilitar globalmente las anotaciones de registros binarios creando un grupo de parámetros personalizado y definiendo el parámetro `binlog_annotate_row_events` como **1**. También puede habilitar las anotaciones en el nivel de sesión llamando a `SET SESSION binlog_annotate_row_events = 1`. Use `replicate_annotate_row_events` para reproducir las anotaciones de registros binarios en la instancia réplica si el registro binario está habilitado en ella. No se requieren privilegios especiales para usar estos ajustes.

A continuación se muestra un ejemplo de una transacción basada en filas de MariaDB. El uso del registro basado en filas se dispara definiendo el nivel de aislamiento de transacciones como de lectura confirmada.

```
CREATE DATABASE IF NOT EXISTS test;
USE test;
CREATE TABLE square(x INT PRIMARY KEY, y INT NOT NULL) ENGINE = InnoDB;
SET SESSION TRANSACTION ISOLATION LEVEL READ COMMITTED;
BEGIN
INSERT INTO square(x, y) VALUES(5, 5 * 5);
```

```
COMMIT;
```

Sin anotaciones, las entradas de los registros binarios de la transacción tendrán un aspecto similar al siguiente:

```
BEGIN
/*!*/;
# at 1163
# at 1209
#150922  7:55:57 server id 1855786460  end_log_pos 1209         Table_map:
 `test`.`square` mapped to number 76
#150922  7:55:57 server id 1855786460  end_log_pos 1247         Write_rows: table id 76
 flags: STMT_END_F
### INSERT INTO `test`.`square`
### SET
###   @1=5
###   @2=25
# at 1247
#150922  7:56:01 server id 1855786460  end_log_pos 1274         Xid = 62
COMMIT/*!*/;
```

La siguiente instrucción habilita las anotaciones de nivel de sesión para esta misma transacción y las deshabilita después de confirmar la transacción:

```
CREATE DATABASE IF NOT EXISTS test;
USE test;
CREATE TABLE square(x INT PRIMARY KEY, y INT NOT NULL) ENGINE = InnoDB;
SET SESSION TRANSACTION ISOLATION LEVEL READ COMMITTED;
SET SESSION binlog_annotate_row_events = 1;
BEGIN;
INSERT INTO square(x, y) VALUES(5, 5 * 5);
COMMIT;
SET SESSION binlog_annotate_row_events = 0;
```

Con anotaciones, las entradas de los registros binarios de la transacción tendrán un aspecto similar al siguiente:

```
BEGIN
/*!*/;
# at 423
# at 483
```

```
# at 529
#150922  8:04:24 server id 1855786460  end_log_pos 483  Annotate_rows:
#Q> INSERT INTO square(x, y) VALUES(5, 5 * 5)
#150922  8:04:24 server id 1855786460  end_log_pos 529  Table_map: `test`.`square`
 mapped to number 76
#150922  8:04:24 server id 1855786460  end_log_pos 567  Write_rows: table id 76 flags:
 STMT_END_F
### INSERT INTO `test`.`square`
### SET
###   @1=5
###   @2=25
# at 567
#150922  8:04:26 server id 1855786460  end_log_pos 594  Xid = 88
COMMIT/*!*/;
```

Archivos de registro de base de datos de Amazon RDS para Microsoft SQL Server

Puede acceder a registros de errores, registros de agentes, archivos de seguimiento y archivos de volcado de Microsoft SQL Server mediante la consola de Amazon RDS, la AWS CLI o la API de RDS. Para obtener más información acerca de la visualización, descarga y vigilancia de los registros de bases de datos basados en archivos, consulte Supervisión de archivos de registro de Amazon RDS.

Calendario de retención

Los archivos de registro rotan cada día y cuando se reinicia la instancia de base de datos. A continuación, se muestra el calendario de retención para los registros de Microsoft SQL Server en Amazon RDS.

Log type (Tipo de registro)	Calendario de retención
Registros de errores	Se retiene un máximo de 30 registros de errores. Amazon RDS podría eliminar los registros de errores que tienen más de 7 días.
Registros de agentes	Se retiene un máximo de 10 registros de agente. Amazon RDS podría eliminar los registros de agente que tienen más de 7 días.
Archivos de seguimiento	Los archivos de seguimiento se conservan según el periodo de retención de archivos de seguimiento de la instancia de base de datos. El periodo de retención de archivos de seguimiento predeterminado es de 7 días. Para modificar el periodo de retención de archivos de seguimiento de la instancia de base de datos, consulte Definición del periodo de retención para los archivos de seguimiento y volcado.
Archivos de volcado	Los archivos de volcado se conservan según el periodo de retención de archivos de volcado de la instancia de base de datos. El periodo de retención predeterminado para los archivos de volcado es de 7 días. Para modificar el periodo de retención de los archivos de volcado de la instancia de base de datos, consulte Definición del periodo de retención para los archivos de seguimiento y volcado.

Visualización del registro de errores de SQL Server mediante el procedimiento rds_read_error_log

Puede utilizar el procedimiento almacenado `rds_read_error_log` de Amazon RDS para ver registros de errores y registros de agentes. Para obtener más información, consulte Visualización de registros de agentes y errores.

Publicación de registros de SQL Server en Amazon CloudWatch Logs

Con Amazon RDS for SQL Server, puede publicar eventos de errores y registros de agente directamente en Amazon CloudWatch Logs. Analice los datos de registro con CloudWatch Logs y utilice CloudWatch para crear alarmas y ver métricas.

En CloudWatch Logs, tiene las siguientes opciones:

- Almacenar registros en un espacio de almacenamiento de larga duración con un periodo de retención que defina.
- Buscar y filtrar los datos de registro.
- Compartir datos de registro entre cuentas.
- Exportar registros a Amazon S3.
- Transmitir datos por streaming a Amazon OpenSearch Service.
- Procesar los datos de registros en tiempo real con Amazon Kinesis Data Streams. Para obtener más información, consulte Uso de Registros de Amazon CloudWatch en la Guía para desarrolladores de aplicaciones SQL de Amazon Managed Service para Apache Flink.

Amazon RDS publica cada registro de base de datos de SQL Server como un flujo de base de datos independiente en el grupo de registros. Por ejemplo, si publica registros de agentes y registros de errores, se almacenan datos de errores en un flujo de registro de errores en el grupo de registro `/aws/rds/instance/`*`my_instance.node1`*`/error` y se almacenan los datos de registros de agentes en el grupo de registro `/aws/rds/instance/`*`my_instance.node1`*`/agent`.

Para las instancias de base de datos Multi-AZ, Amazon RDS publica el registro de la base de datos como dos flujos independientes en el grupo de registro. Por ejemplo, si publica registros de errores, los datos de errores se almacenan en los flujos de registro de errores `/aws/rds/instance/`*`my_instance.node1`*`/error` y `/aws/rds/instance/`*`my_instance.node2`*`/error` respectivamente. Los flujos de registro no cambian durante una conmutación por error y el flujo de registro de errores de cada nodo puede contener registros de errores de la instancia principal

o secundaria. Con multi-AZ, se crea automáticamente un flujo de registro para que `/aws/rds/instance/my_instance/rds-events` almacene los datos de eventos, como las conmutaciones por error de instancias de base de datos.

> **Note**
>
> La publicación de registros de SQL Server en CloudWatch Logs no está habilitado de manera predeterminada. La publicación de archivos de seguimiento y volcado no es compatible.
> La publicación de registro de SQL Server en CloudWatch Logs es compatible en todas las regiones, excepto en Asia Pacífico (Hong Kong).

Consola

Para publicar registros de base de datos de SQL Server en CloudWatch Logs desde AWS Management Console

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify.
4. En la sección Logs exports (Exportaciones de registros), elija los registros que desea comenzar a publicar en CloudWatch Logs.

   Puede elegir Agent log (Registro de agentes), Error log (Registro de errores) o ambos.
5. Elija Continue, seguido de Modify DB Instance en la página de resumen.

AWS CLI

Para publicar registros de SQL Server, puede utilizar el comando `modify-db-instance` con los siguientes parámetros:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Los cambios en la opción `--cloudwatch-logs-export-configuration` siempre se aplican a la instancia de base de datos inmediatamente. Por lo tanto, las opciones `--apply-immediately` y `--no-apply-immediately` no tienen ningún efecto.

También puede publicar registros de SQL Server utilizando los siguientes comandos:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Example

En el siguiente ejemplo se crea una instancia de base de datos de SQL Server con la publicación de registros de CloudWatch Logs habilitada. El valor `--enable-cloudwatch-logs-exports` es una matriz de cadenas JSON que puede incluir `error`, `agent` o ambos.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["error","agent"]' \
    --db-instance-class db.m4.large \
    --engine sqlserver-se
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports "[\"error\",\"agent\"]" ^
    --db-instance-class db.m4.large ^
    --engine sqlserver-se
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Example

En el siguiente ejemplo se modifica una instancia de base de datos SQL Server existente para publicar archivos de registro en CloudWatch Logs. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `EnableLogTypes` y su valor es una matriz de cadenas que puede incluir `error`, `agent` o ambos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":["error","agent"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"EnableLogTypes\":[\"error\",\"agent\"]}"
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Example

En el siguiente ejemplo se modifica una instancia de base de datos SQL Server existente para deshabilitar la publicación de archivos de registro del agente en CloudWatch Logs. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `DisableLogTypes` y su valor es una matriz de cadenas que puede incluir `error`, `agent` o ambos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"DisableLogTypes":["agent"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration "{\"DisableLogTypes\":[\"agent\"]}"
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

Archivos de registro de base de datos de MySQL

Puede supervisar los registros de MySQL directamente desde la consola de Amazon RDS, la API de Amazon RDS, AWS CLI o los SDK de AWS. También es posible el acceso a los registros de MySQL dirigiéndolos a una tabla de la base de datos principal y consultando esa tabla. Puede usar la utilidad mysqlbinlog para descargar un registro binario.

Para obtener más información acerca de la visualización, descarga y vigilancia de los registros de bases de datos basados en archivos, consulte Supervisión de archivos de registro de Amazon RDS.

Temas

- Información general de los registros de bases de datos de RDS para MySQL
- Publicación de registros de MySQL en Amazon CloudWatch Logs
- Envío de la salida del registro de MySQL a las tablas
- Configuración del registro binario de RDS para MySQL para bases de datos de Single-AZ
- Configuración del registro binario de MySQL para clústeres de bases de datos multi-AZ
- Acceso a los registros binarios de MySQL

Información general de los registros de bases de datos de RDS para MySQL

Puede supervisar los siguientes tipos de archivos de registro de RDS para MySQL:

- Registro de errores
- Registro de consultas lentas
- Registro general
- Registro de auditoría
- Registro de instancias
- Registro de errores de autenticación de base de datos de IAM

El registro de errores de RDS para MySQL se genera de forma predeterminada. Puede generar la consulta lenta y los registros generales estableciendo parámetros en su grupo de parámetros de base de datos.

Temas

- Registros de errores de RDS para MySQL

- Registros generales y de consultas lentas de RDS para MySQL
- Registro de auditoría de MySQL
- Rotación y retención de registros en RDS para MySQL
- Límites de tamaño en registro REDO

Registros de errores de RDS para MySQL

RDS para MySQL escribe los errores en el archivo `mysql-error.log`. Cada archivo de registro tiene la hora a la que se generó (en UTC) agregada a su nombre. Los archivos de registro también tienen una marca temporal que ayuda a determinar cuándo se escribieron las entradas del registro.

RDS for MySQL solo escribe en el registro de errores durante el inicio, el cierre y cuando encuentra errores. Una instancia de base de datos puede pasar horas o días sin que se escriban nuevas entradas en el registro de errores. Si no hay entradas recientes, se debe a que el servidor no ha encontrado ningún error que genere una entrada en el registro.

Por diseño, los registros de errores se filtran para que solo se muestren los eventos inesperados, por ejemplo, los errores. No obstante, los registros de errores también contienen información adicional sobre la base de datos, por ejemplo, el progreso de la consulta, que no se muestra. Por lo tanto, incluso sin ningún error real, el tamaño de los registros de errores podría aumentar debido a las actividades continuas de la base de datos. Y, aunque puede que vea un tamaño determinado en bytes o kilobytes en los registros de error de la AWS Management Console, es posible que tengan 0 bytes al descargarlos.

RDS para MySQL escribe `mysql-error.log` en disco cada 5 minutos. Adjunta el contenido del registro a `mysql-error-running.log`.

RDS para MySQL rota el archivo `mysql-error-running.log` cada hora. Retiene los registros generados durante las dos últimas semanas.

> **Note**
>
> Tenga en cuenta que el periodo de retención es diferente entre Amazon RDS y Aurora.

Registros generales y de consultas lentas de RDS para MySQL

Puede escribir el registro de consultas lentas de RDS para MySQL y el registro general en un archivo o en una tabla de la base de datos. Para hacerlo, establezca los parámetros en el grupo

de parámetros de la base de datos. Para obtener información acerca de cómo crear y modificar un grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS. Debe definir estos parámetros para poder ver el registro de consultas lentas o el registro general en la consola de Amazon RDS o a través de la API de Amazon RDS, la CLI de Amazon RDS o los SDK de AWS.

Puede controlar lo que registra RDS para MySQL con los parámetros de esta lista:

- `slow_query_log`: para crear el registro de consultas lentas, use el valor 1. El valor predeterminado es 0.
- `general_log`: para crear el registro general, use el valor 1. El valor predeterminado es 0.
- `long_query_time`: para evitar que se registren consultas rápidas en el registro de consultas lentas, especifique el valor del tiempo de ejecución mínimo de una consulta, en segundos, para que se registre. El valor predeterminado es 10 segundos y el mínimo es 0. Si log_output = FILE, puede especificar un valor de punto flotante que llega a una resolución de microsegundos. Si log_output = TABLE, debe especificar un valor entero con resolución de segundos. Solo se registran las consultas cuyo tiempo de ejecución exceda el valor de `long_query_time`. Por ejemplo, si configura `long_query_time` como 0,1, evitará que se registren las consultas que tarden menos de 100 milisegundos en ejecutarse.
- `log_queries_not_using_indexes`: para incluir en el registro de consultas lentas todas las consultas que no usen un índice, use el valor 1. Las consultas que no usen un índice se registran incluso si su tiempo de ejecución es inferior al valor del parámetro `long_query_time`. El valor predeterminado es 0.
- `log_output` *`option`*: puede especificar una de las opciones siguientes para el parámetro `log_output`.
  - TABLE (predeterminada): las consultas generales se escriben en la tabla `mysql.general_log` y las consultas lentas en la tabla `mysql.slow_log`.
  - FILE: tanto los registros de las consultas generales como los de las consultas lentas se escriben en el sistema de archivos.
  - NONE: deshabilitar registro.

Para que los datos de consultas lentas aparezcan en Registros de Amazon CloudWatch, se deben cumplir las siguientes condiciones:

- Registros de CloudWatch debe configurarse para incluir registros de consultas lentas.
- `slow_query_log` debe estar habilitado.

- `log_output` se debe establecer en `FILE`.
- La consulta debe tardar más tiempo que el tiempo configurado para `long_query_time`.

Para obtener más información sobre la el registro de consultas lentas y el registro general, consulte los siguientes temas de la documentación de MySQL:

- El registro de consultas lentas
- El registro de consultas generales

Registro de auditoría de MySQL

Para acceder al registro de auditoría, la instancia de base de datos debe usar un grupo de opciones personalizado con la opción `MARIADB_AUDIT_PLUGIN`. Para obtener más información, consulte Compatibilidad con el complemento de auditoría de MariaDB para MySQL.

Rotación y retención de registros en RDS para MySQL

Cuando el registro está habilitado, Amazon RDS rota los registros de las tablas o elimina los archivos de registro a intervalos regulares. Esta medida es una precaución para reducir el riesgo de que un archivo de registro grande bloquee el uso de la base de datos o afecte al desempeño. RDS para MySQL gestiona la rotación y la eliminación de la siguiente manera:

- El tamaño de los archivos de registro de consultas lentas, registro de errores y registro general de MySQL está limitado al 2 por ciento del espacio de almacenamiento asignado a una instancia de base de datos. Para mantener este umbral, los registros se rotan automáticamente cada hora. MySQL elimina los archivos de registro de más de dos semanas de antigüedad. Si el tamaño combinado de los archivos de registro sobrepasa el umbral después de eliminar los archivos de registro antiguos, los archivos de registro más grandes se eliminan hasta que el tamaño del archivo de registro deje de sobrepasar el umbral.
- Cuando se habilita el registro `FILE`, los archivos de registro se examinan cada hora y se eliminan los archivos de registro de más de dos semanas de antigüedad. En algunos casos, el tamaño restante del archivo de registro combinado después de la eliminación puede superar el umbral del 2 por ciento del espacio asignado a una instancia de base de datos. En estos casos, los archivos de registro más antiguos se eliminan hasta que el tamaño del archivo de registro no sobrepase el umbral.
- Cuando el registro de tipo `TABLE` está habilitado, en algunos casos, las tablas de registro se rotan cada 24 horas. Esta rotación de produce cuando el espacio ocupado por los registros de tabla

es superior al 20% del espacio de almacenamiento asignado. También ocurre si el tamaño de todos los registros combinados es superior a 10 GB. Si la cantidad de espacio utilizada para una instancia de base de datos es superior al 90 % del espacio de almacenamiento asignado a la instancia de base de datos, se reducen los umbrales de la rotación de registros. Las tablas de registro se rotan si el espacio ocupado por los registros de tabla es superior al 10 % del espacio de almacenamiento asignado. También rotan si el tamaño de todos los registros combinados es superior a 5 GB. Puede suscribirse a la categoría de evento `low storage` para recibir una notificación cuando roten las tablas de registro para liberar espacio. Para obtener más información, consulte Uso de notificaciones de eventos de Amazon RDS.

Cuando se rotan las tablas de registro, la tabla de registro actual se copia primero en una tabla de registro de copia de seguridad. A continuación, se eliminan las entradas de la tabla de registro actual. Si la tabla de registro de copia de seguridad ya existe, se elimina antes de copiar la tabla del registro actual en la copia de seguridad. Puede consultar la tabla de registro de copia de seguridad si es necesaria. La tabla de registro de copia de seguridad para la tabla `mysql.general_log` se llama `mysql.general_log_backup`. La tabla de registro de copia de seguridad para la tabla `mysql.slow_log` se llama `mysql.slow_log_backup`.

Para rotar la tabla `mysql.general_log` puede ejecutar el procedimiento `mysql.rds_rotate_general_log`. Para rotar la tabla `mysql.slow_log` puede ejecutar el procedimiento `mysql.rds_rotate_slow_log`.

Los registros de tabla se rotan durante una actualización de la versión de la base de datos.

Para trabajar con los registros desde la consola de Amazon RDS, la API de Amazon RDS, la CLI de Amazon RDS o los SDK de AWS, configure el parámetro `log_output` en FILE. Al igual que el registro de errores de MySQL, estos archivos de registro rotan cada hora. Se retienen los archivos de registro que se generaron durante las dos semanas anteriores. Tenga en cuenta que el período de retención es diferente entre Amazon RDS y Aurora.

Límites de tamaño en registro REDO

Para la versión 8.0.32 y anteriores de RDS para MySQL, el valor predeterminado de este parámetro es 256 MB. Esta cantidad se obtiene multiplicando el valor predeterminado del parámetro `innodb_log_file_size` (128 MB) por el valor predeterminado del parámetro `innodb_log_files_in_group` (2). Para obtener más información, consulte Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance.

Para la versión 8.0.33 de RDS para MySQL y versiones menores posteriores, Amazon RDS utiliza el parámetro `innodb_redo_log_capacity` en lugar del parámetro `innodb_log_file_size`. El valor predeterminado en Amazon RDS del parámetro `innodb_redo_log_capacity` es 2 GB. Para obtener más información, consulte Cambios en MySQL 8.0.30, en la documentación de MySQL.

A partir de MySQL 8.4, Amazon RDS habilita el parámetro `innodb_dedicated_server` de forma predeterminada. Con el parámetro `innodb_dedicated_server`, el motor de base de datos calcula los parámetros `innodb_buffer_pool_size` y `innodb_redo_log_capacity`. Para obtener más información, consulte Configuración del tamaño del grupo de búferes y la capacidad de registros redo en MySQL 8.4.

Publicación de registros de MySQL en Amazon CloudWatch Logs

Se puede configurar una instancia de base de datos MySQL para publicar datos de registro en un grupo de registros en Amazon CloudWatch Logs. Con CloudWatch Logs, puede realizar análisis en tiempo real de los datos de registro y utilizar CloudWatch para crear alarmas y ver métricas. Puede utilizar CloudWatch Logs para almacenar los registros de registros en almacenamiento de larga duración.

Amazon RDS publica cada registro de base de datos de MySQL como un flujo de base de datos independiente en el grupo de registros. Por ejemplo, si configura la función de exportación para que incluya el registro de consultas lentas, los datos de consultas lentas se almacenan en un flujo de registros de consultas lentas en el grupo de registros `/aws/rds/instance/`*`my_instance`*`/slowquery`.

El registro de errores están habilitados de forma predeterminada. La tabla siguiente resume los requisitos para los otros registros de MySQL.

Registro	Requisito
Registro de auditoría	La instancia de base de datos debe usar un grupo de opciones personalizado con la opción `MARIADB_AUDIT_PLUGIN` .
Registro general	La instancia de base de datos debe usar un grupo de parámetros personalizado con la configuración del parámetro `general_log = 1` para habilitar el registro general.

Registro	Requisito
Registro de consultas lentas	La instancia de base de datos debe usar un grupo de parámetros personalizado con la configuración del parámetro `slow_query_log = 1` para habilitar el registro de consultas lentas.
Registro de errores de autenticación de base de datos de IAM	Debe habilitar el tipo de registro `iam-db-auth-error` para una instancia de base de datos mediante la creación o modificación de una instancia de base de datos.
Resultado de registro	La instancia de base de datos debe usar un grupo de parámetros personalizado con la configuración del parámetro `log_output = FILE` para escribir registros en el sistema de archivos y publicarlos en CloudWatch Logs.

Consola

Para publicar registros de base de datos MySQL en CloudWatch Logs con la consola

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify.
4. En la sección Logs exports (Exportaciones de registros), elija los registros que desea comenzar a publicar en CloudWatch Logs.
5. Elija Continue, seguido de Modify DB Instance en la página de resumen.

AWS CLI

Puede publicar registros de MySQL con la AWS CLI. Puede llamar al comando `modify-db-instance` con los parámetros siguientes:

- `--db-instance-identifier`

- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Los cambios en la opción `--cloudwatch-logs-export-configuration` siempre se aplican a la instancia de base de datos inmediatamente. Por lo tanto, las opciones `--apply-immediately` y `--no-apply-immediately` no tienen ningún efecto.

También puede publicar registros de MySQL llamando a los siguientes comandos de AWS CLI:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Ejecute uno de estos comandos de la AWS CLI con las siguientes opciones:

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

Podrían ser necesarias otras opciones en función del comando de la AWS CLI que ejecute.

Example

En el siguiente ejemplo se modifica una instancia de base de datos MySQL DB para publicar archivos de registro en CloudWatch Logs. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `EnableLogTypes` y su valor es una matriz de cadenas con cualquier combinación de `audit`, `error`, `general` y `slowquery`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
```

```
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["audit","error","general","slowquery"]}'
```

Example

En el siguiente ejemplo se crea una instancia de base de datos MySQL y se publican archivos de registro en CloudWatch Logs. El valor `--enable-cloudwatch-logs-exports` es una matriz de cadenas JSON. Las cadenas pueden ser cualquier combinación de `audit`, `error`, `general` y `slowquery`.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["audit","error","general","slowquery"]' \
    --db-instance-class db.m4.large \
    --engine MySQL
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports '["audit","error","general","slowquery"]' ^
    --db-instance-class db.m4.large ^
    --engine MySQL
```

API de RDS

Puede publicar registros de MySQL con la API de RDS. Puede llamar a la acción `ModifyDBInstance` con los parámetros siguientes:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Los cambios en el parámetro `CloudwatchLogsExportConfiguration` siempre se aplican a la instancia de base de datos inmediatamente. Por tanto, el parámetro `ApplyImmediately` no tiene efecto.

También puede publicar registros de MySQL llamando a las siguientes operaciones de la API de RDS:

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`

Ejecute una de estas operaciones de la API de RDS con los siguientes parámetros:

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

Podrían ser necesarios otros parámetros en función del comando de la AWS CLI que ejecute.

Envío de la salida del registro de MySQL a las tablas

Para dirigir los registros general y de consultas lentas a tablas de la instancia de base de datos, cree un grupo de parámetros de base de datos y asigne al parámetro `log_output` del servidor el valor `TABLE`. Las consultas generales se registrarán entonces en la tabla `mysql.general_log` y las consultas lentas en la tabla `mysql.slow_log`. Puede consultar las tablas para obtener acceso a la información del registro. Al habilitar este registro, se incrementa la cantidad de datos que se escribe en la base de datos, lo que puede degradar el desempeño.

Tanto el registro general como los registros de consultas lentas están deshabilitados de manera predeterminada. Para habilitar el registro en tablas, también debe asignar a los parámetros `general_log` y `slow_query_log` del servidor el valor `1`.

Las tablas de registro seguirán creciendo hasta que las actividades de registro respectivas se desactiven cambiando el valor del parámetro a `0`. A menudo, se acumula una gran cantidad de datos, lo que puede consumir un porcentaje elevado del espacio de almacenamiento asignado. Amazon RDS no permite truncar las tablas de registro, pero sí mover su contenido. Al rotar una tabla, su contenido se guarda en una tabla de copia de seguridad y se crea una nueva tabla de registro vacía. Puede aplicar manualmente la rotación de las tablas de registro con los procedimientos de línea de comandos siguientes, en los que el símbolo del sistema se representa por:`PROMPT>`

```
PROMPT> CALL mysql.rds_rotate_slow_log;
PROMPT> CALL mysql.rds_rotate_general_log;
```

Para eliminar por completo los datos antiguos y recuperar el espacio del disco, llame al procedimiento correspondiente dos veces consecutivas.

Configuración del registro binario de RDS para MySQL para bases de datos de Single-AZ

El registro binario es un conjunto de archivos de registro que contienen información acerca de las modificaciones de datos hechas en una instancia de servidor de MySQL. El registro binario contiene información como la siguiente:

- Eventos que describen cambios en la base de datos, como la creación de tablas o las modificaciones de filas.
- Información sobre la duración de cada instrucción que actualizó los datos.
- Eventos para instrucciones que podrían haber actualizado datos, pero que no lo hicieron.

El registro binario registra las instrucciones que se envían durante la replicación. También es necesario para algunas operaciones de recuperación. Para obtener más información, consulte The Binary Log en la documentación de MySQL.

La característica de copias de seguridad automatizadas determina si el registro binario se activa o desactiva para MySQL. Dispone de las opciones siguientes:

Activar el registro binario.

Establecer el periodo de retención de copia de seguridad en un valor positivo distinto de cero.

Desactivar el registro binario.

Establecer el periodo de retención de copia de seguridad en cero.

Para obtener más información, consulte Habilitar las copias de seguridad automatizadas.

MySQL en Amazon RDS admite los formatos de registro binario basado en filas, basado en instrucciones y mixto. Recomendamos mezclarlos, a menos que necesite un formato binlog concreto. Para obtener información detallada acerca de los formatos de registro binarios de MySQL, consulte Binary logging formats en la documentación de MySQL.

Si tiene pensado utilizar la replicación, el formato de registro binario es importante porque determina el registro de los cambios de datos que se registra en la fuente y se envía a los objetivos de replicación. Para obtener más información acerca de las ventajas y desventajas de distintos tipos de formatos de registro binarios para la replicación, consulte Advantages and Disadvantages of Statement-Based and Row-Based Replication en la documentación de MySQL.

Important

Con MySQL 8.0.34, MySQL ha dejado de utilizar el parámetro `binlog_format`. En versiones posteriores de MySQL, MySQL planea eliminar el parámetro y admitir únicamente la replicación basada en filas. Por ello, recomendamos utilizar el registro basado en filas para las nuevas configuraciones de replicación de MySQL. Para obtener más información, consulte binlog_format en la documentación de MySQL.

Las versiones 8.0 y 8.4 de MySQL aceptan el parámetro `binlog_format`. Al usar este parámetro, MySQL emite una advertencia de obsolescencia. En una futura versión principal, MySQL eliminará el parámetro `binlog_format`.

La replicación basada en instrucciones puede causar incoherencias entre el de la instancia de base de datos de origen y la réplica de lectura. Para obtener más información, consulte Determination of Safe and Unsafe Statements in Binary Logging en la documentación de MySQL.

Habilitar el registro binario aumenta el número de operaciones de E/S de escritura en el disco en la instancia de base de datos. Puede supervisar el uso de IOPS con la métrica de CloudWatch `WriteIOPS`.

Para configurar el formato de registro binario de MySQL

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Grupos de parámetros.
3. Seleccione el grupo de parámetros del de base de datos asociado con la instancia de base de datos que quiera modificar.

   No puede modificar un grupo de parámetros predeterminado. Si el de la instancia de base de datos emplea un grupo de parámetros predeterminado, cree un nuevo grupo de parámetros y asócielo con el de la instancia de base de datos.

   Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.
4. En Acciones, elija Editar.
5. Establezca el parámetro `binlog_format` en el formato de registro binario de su elección (`ROW`, `STATEMENT` o `MIXED`).

   Para desactivar el registro binario establezca el período de retención de copias de seguridad de una instancia de base de datos en cero. Tenga en cuenta que esto deshabilita las copias de seguridad automatizadas diarias. Al deshabilitar las copias de seguridad automatizadas, se desactiva o deshabilita la variable de sesión `log_bin`. Esto deshabilita el registro binario en la instancia de base de datos de RDS para MySQL, lo que a su vez restablece la variable de sesión `binlog_format` al valor predeterminado de `ROW` en la base de datos. Se recomienda no deshabilitar las copias de seguridad. Para obtener más información acerca de la configuración del Período de retención de copia de seguridad, consulte Configuración de instancias de base de datos.
6. Elija Guardar cambios para guardar los cambios realizados en el grupo de parámetros del de la base de datos.

Dado que el parámetro `binlog_format` es dinámico en RDS para MySQL, no es necesario reiniciar la instancia de base de datos para que se apliquen los cambios. (Tenga en cuenta que en Aurora MySQL, este parámetro es estático. Para obtener más información, consulte Configuración del registro binario de Aurora MySQL.)

> **Important**
>
> El cambio de un grupo de parámetros de base de datos afecta a todas las instancias de base de datos que utilizan ese grupo de parámetros. Si desea especificar diferentes formatos de registro binario para diferentes instancias de base de datos MySQL en una región AWS, las instancias de base de datos deben utilizar diferentes grupos de parámetros de base de datos. Estos grupos de parámetros identifican diferentes formatos de registro. Asigne el grupo de parámetros de base de datos apropiado a cada instancia de base de datos.

Configuración del registro binario de MySQL para clústeres de bases de datos multi-AZ

El registro binario en los clústeres de bases de datos multi-AZ de Amazon RDS para MySQL registra todos los cambios en la base de datos para facilitar la replicación, la recuperación en un momento dado y la auditoría. En los clústeres de bases de datos multi-AZ, los registros binarios sincronizan los nodos secundarios con el nodo principal, lo que garantiza la coherencia de datos en todas las zonas de disponibilidad y permite realizar conmutaciones por error perfectas.

Para optimizar el registro binario, Amazon RDS admite la compresión de transacciones de registros binarios, lo que reduce los requisitos de almacenamiento de los registros binarios y mejora la eficacia de la replicación.

Temas

- Compresión de transacciones de registros binarios para clústeres de bases de datos multi-AZ
- Configuración de la compresión de transacciones de registros binarios para clústeres de bases de datos multi-AZ

Compresión de transacciones de registros binarios para clústeres de bases de datos multi-AZ

La compresión de transacciones de registros binarios utiliza el algoritmo zstd para reducir el tamaño de los datos de transacciones almacenados en los registros binarios. Cuando está habilitado, el motor de base de datos MySQL comprime las cargas útiles de las transacciones en un solo evento, lo que minimiza la sobrecarga de E/S y almacenamiento. Esta característica mejora el rendimiento de la base de datos, reduce el tamaño de los registros binarios y optimiza el uso de recursos para administrar y replicar los registros en clústeres de bases de datos multi-AZ.

Amazon RDS proporciona compresión de transacciones de registros binarios para clústeres de base de datos multi-AZ de RDS para MySQL mediante los parámetros siguientes:

- `binlog_transaction_compression`: cuando está activado (1), el motor de base de datos comprime las cargas útiles de las transacciones y las graba en el registro binario como un evento único. Esto reduce el uso de almacenamiento y la sobrecarga de E/S. Este parámetro está deshabilitado de forma predeterminada.
- `binlog_transaction_compression_level_zstd`: configura el nivel de compresión estándar para las transacciones de registros binarios. Los valores más altos aumentan la relación de compresión, lo que reduce aún más los requisitos de almacenamiento, pero incrementan el uso de CPU y memoria para la compresión. El valor predeterminado es 3, con un rango de 1 a 22.

Estos parámetros le permiten afinar la compresión de registros binarios en función de las características de la carga de trabajo y la disponibilidad de los recursos. Para obtener más información, consulte Binary Log Transaction Compression en la documentación de MySQL.

La compresión de transacciones de registros binarios tiene las siguientes ventajas principales:

- La compresión reduce el tamaño de los registros binarios, especialmente en el caso de cargas de trabajo con transacciones grandes o volúmenes de escritura elevados.
- Los registros binarios más pequeños reducen la sobrecarga de red y de E/S, lo que mejora el rendimiento de la replicación.
- El parámetro `binlog_transaction_compression_level_zstd` permite controlar el equilibrio entre la relación de compresión y el consumo de recursos.

Configuración de la compresión de transacciones de registros binarios para clústeres de bases de datos multi-AZ

Para configurar la compresión de transacciones de registros binarios para un clúster de base de datos multi-AZ de RDS para MySQL, modifique la configuración de los parámetros del clúster correspondiente para adaptarla a sus requisitos de carga de trabajo.

Consola

Habilitación de la compresión de transacciones de registros binarios

1. Modifique el grupo de parámetros del clúster de bases de datos para establecer el parámetro `binlog_transaction_compression` en 1.

2. (Opcional) Ajuste el valor del parámetro `binlog_transaction_compression_level_zstd` en función de los requisitos de carga de trabajo y la disponibilidad de los recursos.

Para obtener más información, consulte the section called “Modificación de parámetros de un grupo de parámetros de clúster de base de datos”.

AWS CLI

Para configurar la compresión de transacciones de registros binarios mediante la AWS CLI, utilice el comando modify-db-cluster-parameter-group.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-cluster-parameter-group \
  --db-cluster-parameter-group-name your-cluster-parameter-group \
  --parameters
 "ParameterName=binlog_transaction_compression,ParameterValue=1,ApplyMethod=pending-
reboot"
```

Para Windows:

```
aws rds modify-db-cluster-parameter-group ^
  --db-cluster-parameter-group-name your-cluster-parameter-group ^
  --parameters
 "ParameterName=binlog_transaction_compression,ParameterValue=1,ApplyMethod=pending-
reboot"
```

API de RDS

Para configurar la compresión de transacciones de registros binarios mediante la API de Amazon RDS, utilice la operación `ModifyDBClusterParameterGroup`.

Acceso a los registros binarios de MySQL

Puede usar la herramienta mysqlbinlog para descargar o transmitir los registros binarios desde las instancias de Amazon RDS para MySQL. El registro binario se descarga en el equipo local, donde puede ejecutar acciones tales como reproducirlo con la utilidad mysql. Para obtener más información acerca del uso de la herramienta mysqlbinlog, consulte Using mysqlbinlog to Back Up Binary Log

Files (Uso de mysqlbinlog para realizar copias de seguridad de archivos de registro binarios) en la documentación de MySQL.

Para ejecutar la utilidad mysqlbinlog en una instancia de Amazon RDS, use las siguientes opciones:

- `--read-from-remote-server`: obligatorio.
- `--host`: el nombre de DNS del punto de conexión de la instancia.
- `--port`: el puerto que utiliza la instancia.
- `--user`: un usuario de MySQL al que se le concede el permiso `REPLICATION SLAVE`.
- `--password`: la contraseña del usuario de MySQL, o bien no indique ninguna para que la herramienta le pida una.
- `--raw`: descargue el archivo en formato binario.
- `--result-file`: el archivo local en que se guardará la salida sin procesar.
- `--stop-never`: transmita los archivos de registro binarios.
- `--verbose`: cuando utilice el formato binlog de `ROW`, incluya esta opción para ver los eventos de fila como instrucciones pseudo-SQL. Para obtener más información acerca de la opción `--verbose`, consulte mysqlbinlog row event display (Visualización de eventos de fila mysqlbinlog) en la documentación de MySQL.
- Especifique los nombres de uno o varios de los archivos de registro binarios. Para obtener una lista de los registros disponibles, use el comando de SQL `SHOW BINARY LOGS`.

Para obtener más información acerca de las opciones de mysqlbinlog, consulte mysqlbinlog - Utility for Processing Binary Log Files (mysqlbinlog - Utilidad para procesar archivos de registro binarios) en la documentación de MySQL.

En los siguientes ejemplos, se muestra cómo utilizar la herramienta mysqlbinlog.

Para Linux, macOS o Unix:

```
mysqlbinlog \
    --read-from-remote-server \
    --host=MySQLInstance1.cg034hpkmmjt.region.rds.amazonaws.com \
    --port=3306  \
    --user ReplUser \
    --password \
    --raw \
    --verbose \
```

```
    --result-file=/tmp/ \
    binlog.00098
```

Para Windows:

```
mysqlbinlog ^
    --read-from-remote-server ^
    --host=MySQLInstance1.cg034hpkmmjt.region.rds.amazonaws.com ^
    --port=3306  ^
    --user ReplUser ^
    --password ^
    --raw ^
    --verbose ^
    --result-file=/tmp/ ^
    binlog.00098
```

Los registros binarios deben permanecer disponibles en la instancia de base de datos para que la utilidad mysqlbinlog pueda acceder a ellos. Para garantizar su disponibilidad, utilice el procedimiento mysql.rds_set_configuration almacenado y especifique un periodo con tiempo suficiente para descargar los registros. Si esta configuración no está establecida, Amazon RDS purga los registros binarios lo antes posible, lo que genera huecos en los registros binarios que recupera la utilidad mysqlbinlog.

En el siguiente ejemplo se define el periodo de retención en 1 día.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Para mostrar el valor actual, utilice el procedimiento almacenado mysql.rds_show_configuration.

```
call mysql.rds_show_configuration;
```

Archivos de registro de base de datos de Amazon RDS para Oracle

Puede obtener acceso a los registros de alertas, archivos de auditoría y archivos de seguimiento de Oracle mediante la API o la consola de Amazon RDS. Para obtener más información acerca de la visualización, descarga y vigilancia de los registros de bases de datos basados en archivos, consulte Supervisión de archivos de registro de Amazon RDS.

Los archivos de auditoría de Oracle proporcionados son los de auditoría estándar de Oracle. Amazon RDS admite la característica fine-grained auditing (FGA) de Oracle. Sin embargo, el acceso al registro no proporciona acceso a los eventos de FGA que se almacenan en la tabla `SYS.FGA_LOG$`, disponibles en la vista `DBA_FGA_AUDIT_TRAIL`.

La operación de la API `DescribeDBLogFiles`, que muestra una lista de los archivos de registro de Oracle que están disponibles para una instancia de base de datos, no tiene en cuenta el parámetro `MaxRecords` y devuelve hasta 1000 registros. La llamada devuelve `LastWritten` como una fecha POSIX en milisegundos.

Temas

- Calendario de retención
- Uso de los archivos de seguimiento de Oracle
- Publicación de registros de Oracle en Amazon CloudWatch Logs
- Acceso a los registros de alertas y de oyentes

Calendario de retención

El motor de base de datos de Oracle podría rotar los archivos de registros si alcanzan un tamaño muy grande. Para conservar los archivos de auditoría o de seguimiento, descárguelos. Si almacena los archivos localmente, reducirá los costos de almacenamiento de Amazon RDS y hará que haya más espacio disponible para los datos.

La tabla siguiente muestra el calendario de retención para los registros de alertas, los archivos de auditoría y los archivos de seguimiento de Oracle en Amazon RDS.

Log type (Tipo de registro)	Calendario de retención
Registros de alertas	El registro de alertas de texto se rota diariamente con una retención de 30 días administrada por Amazon RDS. El registro de alertas XML se

Log type (Tipo de registro)	Calendario de retención
	conserva durante al menos siete días. Puede acceder a este registro con la vista `ALERTLOG`.
Archivos de auditoría	El periodo de retención predeterminado para los archivos de auditoría es de siete días. Amazon RDS podría eliminar los archivos de auditoría que tienen más de siete días.
Archivos de seguimiento	El periodo de retención predeterminado para los archivos de seguimiento es de siete días. Amazon RDS podría eliminar los archivos de seguimien to que tienen más de siete días.
Registros de escuchas	El periodo de retención predeterminado para los registros de agente de escucha es de siete días. Amazon RDS podría eliminar los registros de agente de escucha que tienen más de siete días.

> **Note**
>
> Los archivos de auditoría y archivos de seguimiento comparten la misma configuración de retención.

Uso de los archivos de seguimiento de Oracle

Puede encontrar, a continuación, descripciones de procedimientos de Amazon RDS para crear, actualizar, obtener acceso y eliminar archivos de seguimiento.

Temas

- Descripción de archivos
- Generación de archivos de seguimiento y seguimiento de una sesión
- Recuperación de archivos de seguimiento
- Depuración de archivos de seguimiento

Descripción de archivos

Puede usar cualquiera de estos dos procedimientos para permitir el acceso a cualquier archivo en la ruta `background_dump_dest`. El primer procedimiento actualiza una vista que contiene una lista de todos los archivos existentes en `background_dump_dest`.

```
EXEC rdsadmin.manage_tracefiles.refresh_tracefile_listing;
```

Una vez actualizada la vista, consulte la siguiente vista para acceder a los resultados.

```
SELECT * FROM rdsadmin.tracefile_listing;
```

Una alternativa al proceso anterior consiste en utilizar `FROM table` para transmitir datos no relacionales con un formato similar al de una tabla con el fin de mostrar el contenido del directorio de bases de datos.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('BDUMP'));
```

La consulta siguiente muestra el texto de un archivo de registro.

```
SELECT text FROM
 TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP','alert_dbname.log.date'));
```

En una réplica de lectura, obtenga el nombre del directorio BDUMP consultando `V$DATABASE.DB_UNIQUE_NAME`. Si el nombre único es `DATABASE_B`, entonces el directorio BDUMP es `BDUMP_B`. En el ejemplo siguiente se consulta el nombre de BDUMP en una réplica y, a continuación, se utiliza este nombre para consultar el contenido de `alert_DATABASE.log.2020-06-23`.

```
SELECT 'BDUMP' || (SELECT regexp_replace(DB_UNIQUE_NAME,'.*(_[A-Z])', '\1') FROM V
$DATABASE) AS BDUMP_VARIABLE FROM DUAL;

BDUMP_VARIABLE
--------------
BDUMP_B

SELECT TEXT FROM
 table(rdsadmin.rds_file_util.read_text_file('BDUMP_B','alert_DATABASE.log.2020-06-23'));
```

Generación de archivos de seguimiento y seguimiento de una sesión

Dado que no existen restricciones sobre `ALTER SESSION`, muchos métodos estándar para generar archivos de seguimiento en Oracle permanecen disponibles para una instancia de base de datos de Amazon RDS. Los siguientes procedimientos están disponibles para los archivos de seguimiento que necesitan un acceso mayor.

Método de Oracle	Método de Amazon RDS
`oradebug hanganalyze 3`	`EXEC rdsadmin.manage_tracefiles.hanganalyze;`
`oradebug dump systemstate 266`	`EXEC rdsadmin.manage_tracefiles.dump_systemstate;`

Puede utilizar varios métodos estándar para realizar el seguimiento de sesiones individuales conectadas a una instancia de base de datos de Oracle en Amazon RDS. Para habilitar el seguimiento de una sesión, puede ejecutar subprogramas en paquetes PL/SQL suministrados por Oracle, como `DBMS_SESSION` y `DBMS_MONITOR`. Para obtener más información, consulte Enabling Tracing for a Session en la documentación de Oracle.

Recuperación de archivos de seguimiento

Puede recuperar cualquier archivo de seguimiento de `background_dump_dest` utilizando una consulta SQL estándar de una tabla externa administrada por Amazon RDS. Para utilizar este método, debe ejecutar un procedimiento para establecer la ubicación de esta tabla en el archivo de seguimiento específico.

Por ejemplo, puede utilizar la vista `rdsadmin.tracefile_listing` mencionada anteriormente para obtener la lista de los archivos de seguimiento del sistema. A continuación, puede utilizar el siguiente procedimiento para configurar la vista `tracefile_table` para que haga referencia al archivo de seguimiento que desee.

```
EXEC
 rdsadmin.manage_tracefiles.set_tracefile_table_location('CUST01_ora_3260_SYSTEMSTATE.trc');
```

En el siguiente ejemplo se crea una tabla externa en el esquema actual con la ubicación establecida en el archivo indicado. Puede recuperar el contenido en un archivo local utilizando una consulta SQL.

```
SPOOL /tmp/tracefile.txt
SELECT * FROM tracefile_table;
SPOOL OFF;
```

Depuración de archivos de seguimiento

Los archivos de seguimiento pueden acumular y consumir espacio en el disco. De forma predeterminada, Amazon RDS limpia los archivos de seguimiento y registro que tienen más de siete días. Puede ver y establecer el periodo de retención de los archivos de seguimiento mediante el procedimiento `show_configuration`. Debe ejecutar el comando `SET SERVEROUTPUT ON` para ver los resultados de la configuración.

En el siguiente ejemplo se muestra el período actual de retención de archivos de seguimiento y, a continuación, se establece un período nuevo de retención para dichos archivos.

```
# Show the current tracefile retention
SQL> EXEC rdsadmin.rdsadmin_util.show_configuration;
NAME:tracefile retention
VALUE:10080
DESCRIPTION:tracefile expiration specifies the duration in minutes before tracefiles in
 bdump are automatically deleted.

# Set the tracefile retention to 24 hours:
SQL> EXEC rdsadmin.rdsadmin_util.set_configuration('tracefile retention',1440);
SQL> commit;

#show the new tracefile retention
SQL> EXEC rdsadmin.rdsadmin_util.show_configuration;
NAME:tracefile retention
VALUE:1440
DESCRIPTION:tracefile expiration specifies the duration in minutes before tracefiles in
 bdump are automatically deleted.
```

Además del proceso de purga periódica, puede eliminar manualmente los archivos de `background_dump_dest`. En el siguiente ejemplo se muestra cómo purgar todos los archivos que tienen más de cinco minutos.

```
EXEC rdsadmin.manage_tracefiles.purge_tracefiles(5);
```

También puede purgar todos los archivos que coincidan con un patrón específico (si lo hace, no incluya la extensión de archivo, como .trc). En el siguiente ejemplo se muestra cómo purgar todos los archivos que comienzan por `SCHPOC1_ora_5935`.

```
EXEC rdsadmin.manage_tracefiles.purge_tracefiles('SCHPOC1_ora_5935');
```

Publicación de registros de Oracle en Amazon CloudWatch Logs

Se puede configurar una instancia de base de datos de RDS para Oracle para publicar datos de registro en un grupo de registro en Registros de Amazon CloudWatch. Con CloudWatch Logs, puede analizar los datos de registro y utilizar CloudWatch para crear alarmas y ver métricas. Puede utilizar CloudWatch Logs para almacenar los registros de registros en almacenamiento de larga duración.

Amazon RDS publica cada registro de base de datos de Oracle como un flujo de base de datos independiente en el grupo de registros. Por ejemplo, si configura la función de exportación para que incluya el registro de auditoría, los datos de auditoría se almacenan en un flujo de registros de auditorías en el grupo de registros `/aws/rds/instance/my_instance/audit`. En la tabla siguiente, se resumen los requisitos para que RDS para Oracle publique registros en Registros de Amazon CloudWatch.

Nombre de registro	Requisito	Predeterminado
Registro de alerta	Ninguna. No puede deshabilitar este registro.	Habilitado
Registro de seguimiento	Defina el parámetro `trace_enabled` en `TRUE` o déjelo establecido en el valor predeterminado.	`TRUE`
Registro de auditoría	Establezca el parámetro `audit_trail` en uno de los siguientes valores permitidos: `{ none | os | db [, extended] | xml [, extended] }`	`none`
Registro de escucha	Ninguna. No puede deshabilitar este registro.	Habilitado

Nombre de registro	Requisito	Predeterminado
Registro de Oracle Management Agent	Ninguna. No puede deshabilitar este registro.	Habilitado

Este registro de Oracle Management Agent consta de los grupos de registro que se muestran en la siguiente tabla.

Nombre de registro	Grupo de registro de CloudWatch
emctl.log	oemagent-emctl
emdctlj.log	oemagent-emdctlj
gcagent.log	oemagent-gcagent
gcagent_errors.log	oemagent-gcagent-errors
emagent.nohup	oemagent-emagent-nohup
secure.log	oemagent-secure

Para obtener más información, consulte Localización de archivos de seguimiento y registros de agentes de administración en la documentación de Oracle.

Consola

Para publicar registros de base de datos de Oracle en CloudWatch Logs desde AWS Management Console

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify.
4. En la sección Logs exports (Exportaciones de registros), elija los registros que desea comenzar a publicar en CloudWatch Logs.
5. Elija Continue, seguido de Modify DB Instance en la página de resumen.

AWS CLI

Para publicar registros de Oracle, puede utilizar el comando `modify-db-instance` con los siguientes parámetros:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Los cambios en la opción `--cloudwatch-logs-export-configuration` siempre se aplican a la instancia de base de datos inmediatamente. Por lo tanto, las opciones `--apply-immediately` y `--no-apply-immediately` no tienen ningún efecto.

También puede publicar registros de Oracle utilizando los siguientes comandos:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-from-s3`
- `restore-db-instance-to-point-in-time`

Example

En el siguiente ejemplo se crea una instancia de base de datos con la publicación de registros de CloudWatch Logs habilitada. El valor `--cloudwatch-logs-export-configuration` es una matriz de cadenas JSON. Las cadenas pueden ser cualquier combinación de `alert`, `audit`, `listener` y `trace`.

Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration
 '["trace","audit","alert","listener","oemagent"]' \
    --db-instance-class db.m5.large \
    --allocated-storage 20 \
    --engine oracle-ee \
    --engine-version 19.0.0.0.ru-2024-04.rur-2024-04.r1 \
```

```
    --license-model bring-your-own-license \
    --master-username myadmin \
    --manage-master-user-password
```

En:Windows

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration trace alert audit listener oemagent ^
    --db-instance-class db.m5.large ^
    --allocated-storage 20 ^
    --engine oracle-ee ^
    --engine-version 19.0.0.0.ru-2024-04.rur-2024-04.r1 ^
    --license-model bring-your-own-license ^
    --master-username myadmin ^
    --manage-master-user-password
```

Example

En el siguiente ejemplo se modifica una instancia de base de datos de Oracle existente para publicar archivos de registro en CloudWatch Logs. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `EnableLogTypes` y su valor es una matriz de cadenas con cualquier combinación de `alert`, `audit`, `listener` y `trace`.

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["trace","alert","audit","listener","oemagent"]}'
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration EnableLogTypes=\"trace\",\"alert\",\"audit
\",\"listener\",\"oemagent\"
```

Example

En el siguiente ejemplo se modifica una instancia de base de datos de Oracle existente para deshabilitar la publicación de archivos de registro en CloudWatch Logs. El valor `--`

`cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `DisableLogTypes` y su valor es una matriz de cadenas con cualquier combinación de `alert`, `audit`, `listener` y `trace`.

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"DisableLogTypes":["audit","listener"]}'
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration DisableLogTypes=\"audit\",\"listener\"
```

API de RDS

Puede publicar registros de base de datos Oracle con la API de RDS. Puede llamar a la acción `ModifyDBInstance` con los parámetros siguientes:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Los cambios en el parámetro `CloudwatchLogsExportConfiguration` siempre se aplican a la instancia de base de datos inmediatamente. Por tanto, el parámetro `ApplyImmediately` no tiene efecto.

También puede publicar registros de Oracle llamando a las siguientes operaciones de la API de RDS:

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`

Ejecute una de estas operaciones de la API de RDS con los siguientes parámetros:

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

Podrían ser necesarios otros parámetros en función de la operación de la RDS que ejecute.

Acceso a los registros de alertas y de oyentes

Puede ver el archivo de alertas mediante la consola de Amazon RDS. También puede utilizar la siguiente instrucción SQL.

```
SELECT message_text FROM alertlog;
```

Acceda al registro de oyentes mediante Amazon CloudWatch Logs.

> **Note**
>
> Oracle rota los registros de alertas y de escuchas cuando superan los 10 MB, momento en el que dejan de estar disponibles en las vistas de Amazon RDS.

Archivos de registro de bases de datos de RDS para PostgreSQL

Puede supervisar los siguientes tipos de archivos de registro de :

- Registro de PostgreSQL
- Registro de actualización
- Registro de errores de autenticación de base de datos de IAM

> **Note**
>
> Para habilitar los registros de errores de autenticación de base de datos de IAM, primero debe habilitar la autenticación de base de datos de IAM para la instancia de base de datos de RDS para PostgreSQL. Para obtener más información sobre la habilitación de la autenticación de bases de datos de IAM, consulte Activación y desactivación de la autenticación de bases de datos de IAM.

RDS para PostgreSQL registra las actividades de la base de datos en el archivo de registro de PostgreSQL predeterminado. En el caso de una instancia de base de datos de PostgreSQL en las instalaciones, estos mensajes se almacenan localmente en `log/postgresql.log`. Para una instancia de base de datos de RDS para PostgreSQL, el archivo de registro está disponible en , la instancia de Amazon RDS. También puede acceder a estos registros a través de la AWS Management Console, donde podrá verlos o descargarlos. El nivel de registro predeterminado captura los errores de inicio de sesión, los errores graves del servidor, los bloqueos y los errores de consulta.

Para obtener más información sobre cómo puede ver, descargar y observar los registros de la base de datos basados en archivos, consulte Supervisión de archivos de registro de Amazon RDS. Para saber más sobre los registros de PostgreSQL, consulte Trabajo con registros de Amazon RDS y Aurora PostgreSQL: parte 1 y Trabajo con registros de Amazon RDS y Aurora PostgreSQL: parte 2.

Además de los registros estándar de PostgreSQL que se describen en este tema, RDS para PostgreSQL también admite la extensión de auditoría de PostgreSQL (`pgAudit`). La mayoría de los sectores regulados y las agencias gubernamentales necesitan mantener un registro de auditoría o registro de auditoría de los cambios realizados en los datos para cumplir con los requisitos legales. Para obtener información acerca del modo de instalar y usar pgAudit, consulte Uso de pgAudit para registrar la actividad de la base de datos.

Temas

- Parámetros de registro en RDS para PostgreSQL
- Activación de registro de consultas para su instancia de base de datos de RDS para PostgreSQL
- Publicación de registros de PostgreSQL en Amazon CloudWatch Logs

Parámetros de registro en RDS para PostgreSQL

Puede personalizar el comportamiento de registro de su instancia de base de datos de RDS para PostgreSQL modificando varios parámetros. En la siguiente tabla, puede encontrar los parámetros que afectan al tiempo que se almacenan los registros, cuándo se debe rotar el registro y si se debe generar el registro en formato CSV (valor separado por comas). También puede encontrar la salida de texto enviada a STDERR, entre otras configuraciones. Para cambiar la configuración de los parámetros que se pueden modificar, use un grupo de parámetros de base de datos personalizado para su Instancia de base de datos RDS para PostgreSQL. Para obtener más información, consulte Grupos de parámetros de base de datos para instancias de Amazon RDS.

Parámetro	Predeterminado/a	Descripción
log_destination	stderr	Establece el formato de salida para el registro. El valor predeterminado es `stderr`, pero también puede especificar un valor separado por comas (CSV) agregándolo `csvlog` al ajuste. Para obtener más información, consulte Configuración del destino del registro (`stderr`, `csvlog`).
log_filename	postgresql.log.%Y-%m-%d-%H	Especifica el patrón del nombre del archivo de registro. Además del valor predeterminado, este parámetro admite `postgresql.log.%Y-%m-%d` y `postgresql.log.%Y-%m-%d-%H%M` para el patrón del nombre de archivo.
log_line_prefix	%t:%r:%u@%d:[%p]:	Define el prefijo de cada línea de registro que se escribe en `stderr`, para anotar la hora (%t),

Parámetro	Predeterminado/a	Descripción
		el host remoto (%r), el usuario (%u), la base de datos (%d) y el ID del proceso (%p).
log_rotation_age	60	Minutos después de los cuales el archivo de registro rota automáticamente. Puede cambiar este valor dentro del intervalo de 1 a 1440 minutos. Para obtener más informaci ón, consulte Configuración de la rotación del archivo de registro.
log_rotation_size	–	El tamaño (kB) con el que se rota automátic amente el registro. De forma predeterminada, este parámetro no se usa porque los registros rotan en función del parámetro `log_rotat ion_age` . Para obtener más información, consulte Configuración de la rotación del archivo de registro.
rds.log_retention_ period	4320	Los registros de PostgreSQL que superan el número de minutos especificado se eliminará n. El valor predeterminado de 4320 minutos elimina los archivos de registro transcurridos 3 días. Para obtener más información, consulte Configuración de periodo de retención de registros.

Para identificar problemas de aplicaciones, puede buscar errores de consulta, errores de inicio de sesión, interbloqueos y errores de servidor graves en el registro. Por ejemplo, suponga que ha convertido una aplicación heredada de Oracle a Amazon RDS PostgreSQL, pero no todas las consultas se han convertido correctamente. Estas consultas con formato incorrecto generan mensajes de error que se pueden encontrar en los registros para ayudar a identificar los problemas. Para más información sobre el registro de consultas, consulte Activación de registro de consultas para su instancia de base de datos de RDS para PostgreSQL.

En los temas siguientes, encontrará información sobre cómo configurar varios parámetros que controlan los detalles básicos de sus registros de PostgreSQL.

Temas

- Configuración de periodo de retención de registros
- Configuración de la rotación del archivo de registro
- Configuración del destino del registro (stderr, csvlog)
- Descripción del parámetro log_line_prefix

Configuración de periodo de retención de registros

El parámetro `rds.log_retention_period` especifica cuánto tiempo su instancia de base de datos de RDS para PostgreSQL mantiene sus archivos de registro. La configuración predeterminada es de 3 días (4320 minutos), pero puede configurarla entre 1 día (1440 minutos) y 7 días (10 080 minutos). Asegúrese de que su instancia de base de datos de RDS para PostgreSQL tenga suficiente almacenamiento para almacenar los archivos de registro durante ese período de tiempo.

Le recomendamos que publique sus registros de forma rutinaria en Registros de Amazon CloudWatch, de modo que pueda ver y analizar los datos del sistema mucho tiempo después de que los registros se hayan eliminado de su . Instancia de base de datos RDS para PostgreSQL. Para obtener más información, consulte Publicación de registros de PostgreSQL en Amazon CloudWatch Logs.

Configuración de la rotación del archivo de registro

Amazon RDS crea los nuevos archivos de registro cada hora de forma predeterminada. El tiempo lo controla el parámetro `log_rotation_age`. Este parámetro tiene un valor predeterminado de 60 (minutos), pero puede configurarlo entre 1 minuto y 24 horas (1440 minutos). Cuando llega el momento de la rotación, se crea un nuevo archivo de registro distinto. Al archivo se le asigna un nombre de conformidad con el patrón especificado por el parámetro `log_filename`.

Los archivos de registro también se pueden rotar según su tamaño, tal y como se especifica en el parámetro `log_rotation_size`. Este parámetro especifica que el registro debe rotarse cuando alcance el tamaño especificado (en kilobytes). Para una instancia de base de datos de RDS para PostgreSQL, `log_rotation_size` no está establecido, es decir, no se ha especificado ningún valor. Sin embargo, puede establecer el parámetro entre 0 y 2 097 151 kB (kilobytes).

Los nombres de archivo de registro se basan en el patrón de nombre de archivo especificado en el parámetro `log_filename`. La configuración disponible para este parámetro es la siguiente:

- `postgresql.log.%Y-%m-%d`: formato predeterminado para el nombre del archivo de registro. Incluye el año, el mes y la fecha en el nombre del archivo de registro.
- `postgresql.log.%Y-%m-%d-%H`: incluye la hora en el formato del nombre del archivo de registro.

Para obtener más información, consulte `log_rotation_age` y `log_rotation_size` en la documentación de PostgreSQL.

Configuración del destino del registro (**`stderr`**, **`csvlog`**)

De forma predeterminada, Amazon RDS PostgreSQL genera registros en formato de error estándar (stderr). Esta es la configuración predeterminada del parámetro `log_destination`. Cada mensaje lleva el prefijo según el patrón especificado en el parámetro `log_line_prefix`. Para obtener más información, consulte Descripción del parámetro log_line_prefix.

RDS para PostgreSQL también puede generar los registros con el formato `csvlog`. `csvlog` resulta útil para analizar los datos de registro como valores separados con coma (CSV). Por ejemplo, supongamos que utiliza la extensión `log_fdw` para trabajar con los registros como tablas extranjeras. La tabla extranjera creada en los archivos de registro `stderr` contienen una sola columna con datos de eventos de registro. Al añadir `csvlog` al parámetro `log_destination`, se obtiene el archivo de registro en formato CSV con demarcaciones para las múltiples columnas de la tabla externa. Esto le permite ordenar y analizar los registros con mayor facilidad. Para obtener información sobre cómo usar `log_fdw` con `csvlog`, consulte Uso de la extensión log_fdw para acceder al registro de base de datos mediante SQL.

Si especifica `csvlog` para este parámetro, tenga en cuenta que se generan los archivos `stderr` y `csvlog`. Asegúrese de supervisar el almacenamiento consumido por los registros, teniendo en cuenta `rds.log_retention_period` y otras configuraciones que afectan al almacenamiento de registros y a los análisis. Usar `stderr` y `csvlog` duplica de sobra el almacenamiento consumido por los registros.

Si añade `csvlog` a `log_destination` y quiere volver solo a `stderr` solo, debe restablecer el parámetro. Para ello, utilice la consola de Amazon RDS y abra el grupo de parámetros de la base de datos personalizado para su instancia. Elija el parámetro `log_destination`, elija Edit parameter (Editar parámetro) y, a continuación, seleccione Reset (Restablecer).

Para obtener más información acerca de la configuración de los registros, consulte la entrada del blog sobre trabajar con registros de Amazon RDS y Aurora PostgreSQL: parte 1.

Descripción del parámetro log_line_prefix

El formato de registro de `stderr` prefija cada mensaje de registro con los detalles especificados por el parámetro `log_line_prefix`. El valor predeterminado es:

```
%t:%r:%u@%d:[%p]:t
```

A partir de la versión 16 de Aurora PostgreSQL, también puede elegir:

```
%m:%r:%u@%d:[%p]:%l:%e:%s:%v:%x:%c:%q%a
```

Cada entrada de registro enviada a stderr incluye la siguiente información en función del valor seleccionado:

- `%t`: hora de entrada del registro sin milisegundos
- `%m`: hora de entrada del registro con milisegundos
- `%r`: dirección del host remoto.
- `%u@%d`: nombre de usuario @ nombre de base de datos.
- `[%p]`: ID del proceso si está disponible.
- `%l`: Número de línea de registro por sesión
- `%e`: Código de error SQL
- `%s`: Marca temporal de inicio de proceso
- `%v`: ID de transacción virtual
- `%x`: ID de transacción
- `%c`: ID de sesión
- `%q`: Terminador que no sea de sesión
- `%a`: Nombre de la aplicación

Activación de registro de consultas para su instancia de base de datos de RDS para PostgreSQL

Puede recopilar información más detallada sobre las actividades de la base de datos, incluidas las consultas, las consultas en espera de bloqueos, los puntos de control y muchos otros detalles

configurando algunos de los parámetros que se enumeran en la tabla siguiente. Este tema se centra en el registro de consultas.

Parámetro	Predeterminado/a	Descripción
log_connections	–	Registra cada conexión realizada correctam ente.
log_disconnections	–	Registra el final de cada sesión y su duración.
log_checkpoints	1	Registra cada punto de comprobación.
log_lock_waits	–	Registra las esperas de bloqueo largas. Por defecto, este parámetro no está configurado.
log_min_duration_s ample	–	(ms) Establece el tiempo mínimo de ejecución a partir del cual se registra una muestra de instrucciones. El tamaño de la muestra se establece mediante el parámetro `log_state ment_sample_rate` .
log_min_duration_s tatement	–	Se registra cualquier instrucción SQL que se ejecute al menos durante el período de tiempo especificado o durante más tiempo. Por defecto, este parámetro no está configurado. Si se activa este parámetro, puede resultar más sencillo encontrar consultas no optimizadas.
log_statement	–	Define el tipo de declaraciones que se deben registrar. De forma predeterminada, este parámetro no está configurado, pero puede cambiarlo a `all`, `ddl` o `mod` para especific ar los tipos de instrucciones SQL que desea que se registren. Si especifica algo que no sea `none` para este parámetro, también debe adoptar medidas adicionales para evitar que las contraseñas aparezcan en los archivos de registro. Para obtener más información,

Parámetro	Predeterminado/a	Descripción
		consulte Mitigar el riesgo de exposición de contraseñas al utilizar el registro de consultas.
log_statement_sample_rate	–	El porcentaje de sentencias que superan el tiempo especificado en `log_min_duration_sample` se registrarán, expresado como un valor de coma flotante entre 0.0 y 1.0.
log_statement_stats	–	Escribe las estadísticas de rendimiento acumulativas en el registro del servidor.

Uso del registro para encontrar consultas con un rendimiento lento

Puede registrar instrucciones y consultas SQL para ayudar a encontrar consultas que se den con resultados lentos. Para activar esta función, modifique la configuración de los parámetros `log_statement` y `log_min_duration`, tal como se describe en esta sección. Antes de activar el registro de consultas para su instancia de base de datos de RDS para PostgreSQL, debe conocer la posible exposición de contraseñas en los registros y cómo mitigar los riesgos. Para obtener más información, consulte Mitigar el riesgo de exposición de contraseñas al utilizar el registro de consultas.

A continuación, encontrará información de referencia sobre los parámetros `log_statement` y `log_min_duration`.

log_statement

Este parámetro especifica el tipo de instrucciones SQL que deben enviarse al registro. El valor predeterminado es `none`. Si cambia este parámetro a `all`, `ddl` o `mod`, asegúrese de aplicar algunas de las medidas recomendadas para reducir el riesgo de exponer las contraseñas en los registros. Para obtener más información, consulte Mitigar el riesgo de exposición de contraseñas al utilizar el registro de consultas.

all

Registra todas las instrucciones. Para depuración, se recomienda esta configuración.

ddl

Registra todas las instrucciones del lenguaje de definición de datos (DDL), como CREATE, ALTER, DROP, etc.

MOD

Registra todas las instrucciones DDL y las instrucciones de lenguaje de manipulación de datos (DML), como INSERT, UPDATE y DELETE, que modifican los datos.

none

No se registra ninguna instrucción SQL. Recomendamos esta configuración para evitar el riesgo de exponer las contraseñas en los registros.

log_min_duration_statement

Se registra cualquier instrucción SQL que se ejecute al menos durante el período de tiempo especificado o durante más tiempo. Por defecto, este parámetro no está configurado. Si se activa este parámetro, puede resultar más sencillo encontrar consultas no optimizadas.

–1–2147483647

El número de milisegundos (ms) de tiempo de ejecución durante los cuales se registra una instrucción.

Para configurar el registro de consultas

Estos pasos suponen que su instancia de base de datos de RDS para PostgreSQL utiliza un grupo personalizado de parámetros de base de datos.

1. Establezca el parámetro `log_statement` como `all`. En el siguiente ejemplo se muestra la información que se escribe en el archivo con esta configuración de parámetros.

```
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:LOG: statement:
 SELECT feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:LOG: QUERY
 STATISTICS
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:DETAIL: ! system
 usage stats:
```

```
! 0.017355 s user, 0.000000 s system, 0.168593 s elapsed
! [0.025146 s user, 0.000000 s system total]
! 36644 kB max resident size
! 0/8 [0/8] filesystem blocks in/out
! 0/733 [0/1364] page faults/reclaims, 0 [0] swaps
! 0 [0] signals rcvd, 0/0 [0/0] messages rcvd/sent
! 19/0 [27/0] voluntary/involuntary context switches
2022-10-05 22:05:52 UTC:52.95.4.1(11335):postgres@labdb:[3639]:STATEMENT: SELECT
 feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-05 22:05:56 UTC:52.95.4.1(11335):postgres@labdb:[3639]:ERROR: syntax error
 at or near "ORDER" at character 1
2022-10-05 22:05:56 UTC:52.95.4.1(11335):postgres@labdb:[3639]:STATEMENT: ORDER BY
 s.confidence DESC;
---------------------- END OF LOG ----------------------
```

2. Establezca el parámetro `log_min_duration_statement`. En el siguiente ejemplo se muestra la información que se escribe en el archivo `postgresql.log`cuando se establece el parámetro en:1

   Se registran las consultas que superan la duración especificada en el parámetro `log_min_duration_statement`. A continuación se muestra un ejemplo. Puede ver el archivo de registro de su instancia de base de datos de RDS para PostgreSQL en la consola de Amazon RDS.

```
2022-10-05 19:05:19 UTC:52.95.4.1(6461):postgres@labdb:[6144]:LOG: statement: DROP
 table comments;
2022-10-05 19:05:19 UTC:52.95.4.1(6461):postgres@labdb:[6144]:LOG: duration:
 167.754 ms
2022-10-05 19:08:07 UTC::@:[355]:LOG: checkpoint starting: time
2022-10-05 19:08:08 UTC::@:[355]:LOG: checkpoint complete: wrote 11 buffers
 (0.0%); 0 WAL file(s) added, 0 removed, 0 recycled; write=1.013 s, sync=0.006 s,
 total=1.033 s; sync files=8, longest=0.004 s, average=0.001 s; distance=131028 kB,
 estimate=131028 kB
---------------------- END OF LOG ----------------------
```

Mitigar el riesgo de exposición de contraseñas al utilizar el registro de consultas

Le recomendamos que mantenga `log_statement` establecido en `none` para evitar exponer las contraseñas. Si establece `log_statement` en `all`, `ddl` o `mod`, le recomendamos que siga uno o más de los siguientes pasos.

- Para el cliente, cifre la información confidencial. Para obtener más información, consulte Encryption Options en la documentación de PostgreSQL. Utilice las opciones `ENCRYPTED` (y `UNENCRYPTED`) de las instrucciones `CREATE` y `ALTER`. Para obtener más información, consulte CREATE USER en la documentación de PostgreSQL.
- Para su instancia de base de datos de RDS para PostgreSQL, configure y utilice la extensión de auditoría de PostgreSQL (pgAudit). Esta extensión redacta la información confidencial de las instrucciones CREATE y ALTER enviadas al registro. Para obtener más información, consulte Uso de pgAudit para registrar la actividad de la base de datos.
- Restrinja el acceso a los Registros de CloudWatch.
- Utilice mecanismos de autenticación más sólidos como IAM.

Publicación de registros de PostgreSQL en Amazon CloudWatch Logs

Para almacenar los registros de PostgreSQL en un almacenamiento de larga duración, se puede usar Amazon CloudWatch Logs. Con CloudWatch Logs, también puede realizar análisis en tiempo real de los datos de registro y utilizar CloudWatch para ver métricas y crear alarmas. Por ejemplo, si establece `log_statement` en `ddl`, puede configurar una alarma para que avise siempre que se ejecute una instrucción DDL. Puede elegir cargar los registros de PostgreSQL en CloudWatch Logs durante el proceso de creación de su instancia de base de datos de RDS para PostgreSQL. Si optó por no subir registros en ese momento, puedes modificar tu instancia más adelante para empezar a subir los registros a partir de ese momento. En otras palabras, los registros existentes no se cargan. Solo los registros nuevos se cargan a medida que se crean en la instancia de base de datos de RDS para PostgreSQL modificada.

Todas las versiones de RDS para PostgreSQL disponibles actualmente permiten publicar archivos de registro en CloudWatch Logs. Para obtener información detallada sobre la versión, consulte las actualizaciones de Amazon RDS para PostgreSQL en las notas de la versión de Amazon RDS para PostgreSQL.

Para trabajar con CloudWatch Logs, configure la instancia de base de datos de RDS para PostgreSQL para que publique datos de registro en un grupo de registros.

Puede publicar los siguientes tipos de registro en CloudWatch Logs para RDS para PostgreSQL:

- Registro de PostgreSQL
- Registro de actualización
- Registro de errores de autenticación de base de datos de IAM

Tras completar la configuración, Amazon RDS publica los eventos de registro en los flujos de registro con un grupo de registros de CloudWatch. Por ejemplo, los datos de registro de PostgreSQL se almacenan en el grupo de registro `/aws/rds/instance/my_instance/postgresql`. Para ver los registros, abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.

Consola

Para publicar registros de base de datos PostgreSQL en CloudWatch Logs con la consola

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione la instancia de base de datos que quiera modificar y seleccione Modify (Modificar).
4. En la sección Logs exports (Exportaciones de registros), elija los registros que desea comenzar a publicar en CloudWatch Logs.

   La sección Log exports (Exportaciones de registros) está disponible para versiones de PostgreSQL que admiten la publicación en CloudWatch Logs.
5. Elija Continue, seguido de Modify DB Instance en la página de resumen.

AWS CLI

Puede publicar registros de PostgreSQL con la AWS CLI. Puede llamar al comando `modify-db-instance` con los parámetros siguientes:

- `--db-instance-identifier`
- `--cloudwatch-logs-export-configuration`

> **Note**
>
> Los cambios en la opción `--cloudwatch-logs-export-configuration` siempre se aplican a la instancia de base de datos inmediatamente. Por lo tanto, las opciones `--apply-immediately` y `--no-apply-immediately` no tienen ningún efecto.

También puede publicar registros de PostgreSQL llamando a los siguientes comandos de la CLI:

- `create-db-instance`
- `restore-db-instance-from-db-snapshot`
- `restore-db-instance-to-point-in-time`

Ejecute uno de estos comandos de la CLI con las siguientes opciones:

- `--db-instance-identifier`
- `--enable-cloudwatch-logs-exports`
- `--db-instance-class`
- `--engine`

Podrían ser necesarias otras opciones en función del comando de la CLI que ejecute.

Example Modificar una instancia para publicar registros en CloudWatch Logs

En el siguiente ejemplo se modifica una instancia de base de datos de PostgreSQL existente para publicar archivos de registro en CloudWatch Logs. El valor `--cloudwatch-logs-export-configuration` es un objeto JSON. La clave de este objeto es `EnableLogTypes` y su valor es una matriz de cadenas con cualquier combinación de `postgresql` y `upgrade`.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":["postgresql",
 "upgrade"]}'
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --cloudwatch-logs-export-configuration '{"EnableLogTypes":
["postgresql","upgrade"]}'
```

Example Crear una instancia para publicar registros en CloudWatch Logs

En el siguiente ejemplo se crea una instancia de base de datos PostgreSQL y se publican archivos de registro en CloudWatch Logs. El valor `--enable-cloudwatch-logs-exports` es una matriz de cadenas JSON. Las cadenas pueden ser cualquier combinación de `postgresql` y `upgrade`.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --enable-cloudwatch-logs-exports '["postgresql","upgrade"]' \
    --db-instance-class db.m4.large \
    --engine postgres
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --enable-cloudwatch-logs-exports '["postgresql","upgrade"]' ^
    --db-instance-class db.m4.large ^
    --engine postgres
```

API de RDS

Puede publicar registros de PostgreSQL con la API de RDS. Puede llamar a la acción `ModifyDBInstance` con los parámetros siguientes:

- `DBInstanceIdentifier`
- `CloudwatchLogsExportConfiguration`

> **Note**
>
> Los cambios en el parámetro `CloudwatchLogsExportConfiguration` siempre se aplican a la instancia de base de datos inmediatamente. Por tanto, el parámetro `ApplyImmediately` no tiene efecto.

También puede publicar registros de PostgreSQL llamando a las siguientes operaciones de la API de RDS:

- `CreateDBInstance`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceToPointInTime`

Ejecute una de estas operaciones de la API de RDS con los siguientes parámetros:

- `DBInstanceIdentifier`
- `EnableCloudwatchLogsExports`
- `Engine`
- `DBInstanceClass`

Podrían ser necesarios otros parámetros en función de la operación que ejecute.

Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail

AWS CloudTrail es un servicio de AWS que ayuda a auditar la cuenta de AWS. AWS CloudTrail se activa en la cuenta de AWS cuando esta se crea. Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Temas

- Integración de CloudTrail con Amazon RDS
- Entradas de archivos de registro de Amazon RDS

Integración de CloudTrail con Amazon RDS

Todas las acciones de Amazon RDS se registran en CloudTrail. CloudTrail proporciona un registro de las acciones que realiza un usuario, un rol o un servicio de AWS en Amazon RDS.

Eventos de CloudTrail

CloudTrail captura las llamadas a la API de Amazon RDS como eventos. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los eventos incluyen las llamadas realizadas desde la consola de Amazon RDS y las llamadas desde el código a las operaciones de la API de Amazon RDS.

La actividad de Amazon RDS se registra en un evento de CloudTrail de Event history (Historial de eventos). Puede utilizar la consola de CloudTrail para ver los últimos 90 días de actividad y eventos de API registrados en una región de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Registros de seguimiento de CloudTrail

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de Amazon RDS, cree una traza. Un seguimiento es una configuración que permite la entrega de eventos en un bucket de Amazon S3 especificado. CloudTrail normalmente entrega archivos de registro en el plazo de 15 minutos después de producirse la actividad de la cuenta.

> **Note**
>
> Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos).

Puede crear dos tipos de registros de seguimiento en una cuenta de AWS : uno que se aplique a todas las regiones o uno que se aplique a una región específica. De manera predeterminada, cuando crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones.

También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail desde varias regiones y Recibir archivos de registro de CloudTrail desde varias cuentas

Entradas de archivos de registro de Amazon RDS

Los archivos log de CloudTrail pueden contener una o varias entradas de log. Los archivos de registro de CloudTrail no son un rastro de la stack ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail que ilustra la acción `CreateDBInstance`.

```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/johndoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
```

```
        "userName": "johndoe"
    },
    "eventTime": "2018-07-30T22:14:06Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "CreateDBInstance",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.15.42 Python/3.6.1 Darwin/17.7.0 botocore/1.10.42",
    "requestParameters": {
        "enableCloudwatchLogsExports": [
            "audit",
            "error",
            "general",
            "slowquery"
        ],
        "dBInstanceIdentifier": "test-instance",
        "engine": "mysql",
        "masterUsername": "myawsuser",
        "allocatedStorage": 20,
        "dBInstanceClass": "db.m1.small",
        "masterUserPassword": "****"
    },
    "responseElements": {
        "dBInstanceArn": "arn:aws:rds:us-east-1:123456789012:db:test-instance",
        "storageEncrypted": false,
        "preferredBackupWindow": "10:27-10:57",
        "preferredMaintenanceWindow": "sat:05:47-sat:06:17",
        "backupRetentionPeriod": 1,
        "allocatedStorage": 20,
        "storageType": "standard",
        "engineVersion": "8.0.28",
        "dbInstancePort": 0,
        "optionGroupMemberships": [
            {
                "status": "in-sync",
                "optionGroupName": "default:mysql-8-0"
            }
        ],
        "dBParameterGroups": [
            {
                "dBParameterGroupName": "default.mysql8.0",
                "parameterApplyStatus": "in-sync"
            }
        ],
```

```
        "monitoringInterval": 0,
        "dBInstanceClass": "db.m1.small",
        "readReplicaDBInstanceIdentifiers": [],
        "dBSubnetGroup": {
            "dBSubnetGroupName": "default",
            "dBSubnetGroupDescription": "default",
            "subnets": [
                {
                    "subnetAvailabilityZone": {"name": "us-east-1b"},
                    "subnetIdentifier": "subnet-cbfff283",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1e"},
                    "subnetIdentifier": "subnet-d7c825e8",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1f"},
                    "subnetIdentifier": "subnet-6746046b",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1c"},
                    "subnetIdentifier": "subnet-bac383e0",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1d"},
                    "subnetIdentifier": "subnet-42599426",
                    "subnetStatus": "Active"
                },
                {
                    "subnetAvailabilityZone": {"name": "us-east-1a"},
                    "subnetIdentifier": "subnet-da327bf6",
                    "subnetStatus": "Active"
                }
            ],
            "vpcId": "vpc-136a4c6a",
            "subnetGroupStatus": "Complete"
        },
        "masterUsername": "myawsuser",
        "multiAZ": false,
        "autoMinorVersionUpgrade": true,
```

```
        "engine": "mysql",
        "cACertificateIdentifier": "rds-ca-2015",
        "dbiResourceId": "db-ETDZIIXHEWY5N7GXVC4SH7H5IA",
        "dBSecurityGroups": [],
        "pendingModifiedValues": {
            "masterUserPassword": "****",
            "pendingCloudwatchLogsExports": {
                "logTypesToEnable": [
                    "audit",
                    "error",
                    "general",
                    "slowquery"
                ]
            }
        },
        "dBInstanceStatus": "creating",
        "publiclyAccessible": true,
        "domainMemberships": [],
        "copyTagsToSnapshot": false,
        "dBInstanceIdentifier": "test-instance",
        "licenseModel": "general-public-license",
        "iAMDatabaseAuthenticationEnabled": false,
        "performanceInsightsEnabled": false,
        "vpcSecurityGroups": [
            {
                "status": "active",
                "vpcSecurityGroupId": "sg-f839b688"
            }
        ]
    },
    "requestID": "daf2e3f5-96a3-4df7-a026-863f96db793e",
    "eventID": "797163d3-5726-441d-80a7-6eeb7464acd4",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


Tal y como se muestra en el elemento `userIdentity` del ejemplo anterior, cada evento o entrada del registro contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.

- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información sobre `userIdentity`, consulte Elemento userIdentity de CloudTrail. Para obtener más información sobre `CreateDBInstance` y otras acciones de Amazon RDS, consulte la Referencia de la API de Amazon RDS.

Supervisión de Amazon RDS con flujos de actividad de la base de datos

Mediante la característica de flujos de actividad de la base de datos, puede supervisar flujos de actividad de la base de datos prácticamente en tiempo real.

Temas

- Información general sobre flujos de actividad de la base de datos
- Configuración de la auditoría unificada para Oracle Database
- Configuración de la política de auditoría para Amazon RDS para Microsoft SQL Server
- Inicio de una secuencia de actividades de la base de datos
- Modificación de una secuencia de actividades de la base de datos para Amazon RDS
- Obtención del estado de un flujo de actividad de la base de datos
- Detención de un flujo de actividad de la base de datos
- Monitoreo de secuencias de actividades de la base de datos
- Ejemplos de políticas de IAM para flujos de actividad de base de datos

Información general sobre flujos de actividad de la base de datos

Como administrador de base de datos de Amazon RDS, debe proteger su base de datos y cumplir los requisitos normativos y de conformidad. Una estrategia es integrar flujos de actividad de la base de datos con sus herramientas de monitoreo. De esta manera, monitoriza y configura alarmas para la actividad de auditoría en su base de datos.

Las amenazas de seguridad son tanto externas como internas. Para protegerse contra amenazas internas, puede controlar el acceso del administrador a los flujos de datos mediante la configuración de la característica de flujos de actividad de la base de datos. Los DBA de Amazon RDS no tienen acceso a la recopilación, transmisión, almacenamiento ni procesamiento de los flujos.

Contenido

- Cómo funcionan los flujos de actividad de la base de datos
- Auditoría en Oracle Database y Microsoft SQL Server Database
  - Auditoría unificada en la base de datos de Oracle
  - Auditoría en Microsoft SQL Server

  - Campos de auditoría no nativos para Oracle Database y SQL Server
  - Anulación del grupo de parámetros de base de datos
- Modo asíncrono para flujos de actividad de la base de datos
- Requisitos y limitaciones de los flujos de actividad de la base de datos
- Disponibilidad en regiones y versiones
- Clases de instancia de base de datos admitidas para los flujos de actividad de la base de datos

Cómo funcionan los flujos de actividad de la base de datos

Amazon RDS envía actividades a un flujo de datos de Amazon Kinesis prácticamente en tiempo real. El flujo de Kinesis se crea automáticamente. Desde Kinesis, puede configurar servicios de AWS como Amazon Data Firehose y AWS Lambda para utilizar el flujo y almacenar los datos.

> **Important**
>
> La característica de flujo de actividad de la base de datos en Amazon RDS se puede utilizar de forma gratuita, pero Amazon Kinesis cobra por un flujo de datos. Para obtener más información, consulte los Precios de Amazon Kinesis Data Streams.

Puede configurar aplicaciones para administrar la conformidad para consumir los flujos de actividad de la base de datos. Esas aplicaciones pueden utilizar el flujo para generar alertas y auditar la actividad la base de datos.

Amazon RDS admite flujos de actividad de bases de datos en implementaciones multi-AZ. En este caso, los flujos de actividad de la base de datos auditan tanto las instancias principales como en espera.

Auditoría en Oracle Database y Microsoft SQL Server Database

La auditoría es el monitoreo y registro de acciones de base de datos configuradas. Amazon RDS no captura las actividades de la base de datos de forma predeterminada. Cree y administre usted mismo políticas de auditoría en la base de datos.

Temas

- Auditoría unificada en la base de datos de Oracle
- Auditoría en Microsoft SQL Server

- Campos de auditoría no nativos para Oracle Database y SQL Server
- Anulación del grupo de parámetros de base de datos

Auditoría unificada en la base de datos de Oracle

En una base de datos de Oracle, una política de auditoría unificada es un grupo con nombre de configuración de auditoría que se puede utilizar para auditar un aspecto del comportamiento del usuario. Una política puede ser tan simple como auditar las actividades de un solo usuario. También puede crear políticas de auditoría complejas que utilicen condiciones.

Una base de datos de Oracle escribe registros de auditoría, incluidos registros de auditoría `SYS`, en los seguimientos de auditoría unificada. Por ejemplo, si se produce un error durante una instrucción `INSERT`, la auditoría estándar indica el número de error y el SQL que se ejecutó. El seguimiento de auditoría reside en una tabla de solo lectura en el esquema `AUDSYS`. Para acceder a estos registros, consulte la vista `UNIFIED_AUDIT_TRAIL` del diccionario de datos.

Por lo general, se configuran flujos de actividad de la base de datos de la siguiente manera:

1. Cree una política de auditoría de base de datos de Oracle mediante el comando `CREATE AUDIT POLICY`.

   La base de datos de Oracle genera registros de auditoría.
2. Habilite la política de auditoría mediante el comando `AUDIT POLICY`.
3. Configure los flujos de actividad de la base de datos.

   Solo las actividades que coincidan con las políticas de auditoría de la base de datos de Oracle se capturan y envían al flujo de datos de Amazon Kinesis. Cuando se habilitan los flujos de actividad de la base de datos, un administrador de base de datos de Oracle no puede modificar la política de auditoría ni eliminar registros de auditoría.

Para obtener más información sobre las políticas de auditoría unificadas, consulte la sección acerca de las actividades de auditoría con políticas de auditoría unificadas y AUDIT en la guía de seguridad de la base de datos de Oracle.

Auditoría en Microsoft SQL Server

El flujo de actividad de la base de datos utiliza la característica SQLAudit para auditar la base de datos de SQL Server.

La instancia de RDS para SQL Server contiene lo siguiente:

- Auditoría de servidor: la auditoría de SQL server recopila una sola instancia de acciones a nivel de servidor o base de datos y un grupo de acciones para supervisar. Las auditorías a nivel de servidor `RDS_DAS_AUDIT` y `RDS_DAS_AUDIT_CHANGES` las administra RDS.
- Especificación de auditoría del servidor: la especificación de auditoría del servidor registra los eventos a nivel de servidor. Puede modificar la especificación `RDS_DAS_SERVER_AUDIT_SPEC`. Esta especificación está vinculada a la auditoría del servidor `RDS_DAS_AUDIT`. La especificación `RDS_DAS_CHANGES_AUDIT_SPEC` la administra RDS.
- Especificación de auditoría de base de datos: la especificación de auditoría de base de datos registra los eventos a nivel de base de datos. Puede crear una especificación de auditoría de base de datos `RDS_DAS_DB_<name>` y vincularla a la auditoría del servidor `RDS_DAS_AUDIT`.

Puede configurar los flujos de actividad de la base de datos mediante la consola o la CLI. Por lo general, se configuran flujos de actividad de la base de datos de la siguiente manera:

1. (Opcional) Cree una especificación de auditoría de base de datos con el comando `CREATE DATABASE AUDIT SPECIFICATION` y vincúlela a la auditoría `RDS_DAS_AUDIT` del servidor.
2. (Opcional) Modifique la especificación de auditoría del servidor con el comando `ALTER SERVER AUDIT SPECIFICATION` y defina las políticas.
3. Active las políticas de auditoría de base de datos y servidor. Por ejemplo:

   ```
   ALTER DATABASE AUDIT SPECIFICATION [<Your database specification>] WITH
   (STATE=ON)

   ALTER SERVER AUDIT SPECIFICATION [RDS_DAS_SERVER_AUDIT_SPEC] WITH
   (STATE=ON)
   ```

4. Configure los flujos de actividad de la base de datos.

   Solo las actividades que coincidan con las políticas de auditoría de base de datos y servidor se capturan y envían a Amazon Kinesis Data Streams. Cuando se habilitan los flujos de actividad de base de datos y las políticas están bloqueadas, un administrador de base de datos no puede modificar la política de auditoría ni eliminar registros de auditoría.

> **Important**
>
> Si la especificación de auditoría de base de datos para una base de datos específica está habilitada y la política está bloqueada, no se puede eliminar la base de datos.

Para obtener más información sobre la auditoría de SQL Server, consulte SQL Server Audit Components (Componentes de auditoría de SQL Server) en la documentación de Microsoft SQL Server.

Campos de auditoría no nativos para Oracle Database y SQL Server

Cuando inicia un flujo de actividad de la base de datos, cada evento de base de datos genera un evento de flujo de actividad correspondiente. Por ejemplo, un usuario de base de datos puede ejecutar las instrucciones `SELECT` y `INSERT`. La base de datos audita estos eventos y los envía a un flujo de datos de Amazon Kinesis.

Los eventos se representan como objetos JSON en el flujo. Un objeto JSON contiene un `DatabaseActivityMonitoringRecord`, que contiene una matriz `databaseActivityEventList`. Los campos predefinidos en la matriz incluyen `class`, `clientApplication` y `command`.

De forma predeterminada, un flujo de actividad no incluye campos de auditoría nativos del motor. Puede configurar Amazon RDS para Oracle y SQL Server para que incluyan estos campos adicionales en el objeto JSON `engineNativeAuditFields`.

En Oracle Database, la mayoría de los eventos del seguimiento de auditoría unificado se asignan a campos del flujo de actividad de datos de RDS. Por ejemplo, el campo `UNIFIED_AUDIT_TRAIL.SQL_TEXT` en los mapas unificados de auditoría al campo `commandText` en un flujo de actividad de la base de datos. Sin embargo, los campos de auditoría de la base de datos de Oracle, como `OS_USERNAME`, no se asignan a campos predefinidos en un flujo de actividad de la base de datos.

En SQL Server, la mayoría de los campos del evento que registra SQLAudit se asignan a los campos del flujo de actividad de la base de datos de RDS. Por ejemplo, el campo `code` de `sys.fn_get_audit_file` en la auditoría se asigna al campo `commandText` en un flujo de actividad de la base de datos. Sin embargo, los campos de auditoría de la base de datos de SQL

Server, como `permission_bitmask`, no se asignan a campos predefinidos en un flujo de actividad de la base de datos.

Para obtener más información acerca de databaseActivityEventList, consulte Matriz JSON databaseActivityEventList para flujos de actividad de base de datos.

Anulación del grupo de parámetros de base de datos

Por lo general, se adjunta un grupo de parámetros para activar la auditoría unificada en RDS para Oracle. Sin embargo, los flujos de actividad de la base de datos requieren una configuración adicional. Para mejorar la experiencia del cliente, Amazon RDS realiza lo siguiente:

- Si activa un flujo de actividad, RDS para Oracle ignora los parámetros de auditoría del grupo de parámetros.
- Si desactiva un flujo de actividad, RDS para Oracle deja de ignorar los parámetros de auditoría.

El flujo de actividad de la base de datos para SQL Server es independiente de los parámetros que establezca en la opción de auditoría de SQL.

Modo asíncrono para flujos de actividad de la base de datos

Los flujos de actividad en Amazon RDS siempre son asíncronos. Cuando una sesión de la base de datos genere un evento de flujo de actividad, la sesión volverá de inmediato a las actividades normales. En segundo plano, Amazon RDS convierte el evento de flujo de actividad en un registro permanente.

Si se produce un error en la tarea en segundo plano, Amazon RDS generará un evento. Dicho evento marca el principio y el fin de todo período de tiempo en el que podrían haberse perdido registros de eventos de la secuencia de actividades. El modo asíncrono favorece el rendimiento de la base de datos con respecto a la precisión de la secuencia de actividades.

Requisitos y limitaciones de los flujos de actividad de la base de datos

En RDS, los flujos de actividad de la base de datos tienen los límites y los requisitos siguientes:

- Los flujos de actividad de la base de datos requieren Amazon Kinesis.
- Se requiere AWS Key Management Service (AWS KMS) porque los flujos de actividad de la base de datos siempre están cifrados.
- La aplicación de cifrado adicional al flujo de datos de Amazon Kinesis no es compatible con los flujos de actividad de la base de datos, que ya están cifrados con su clave AWS KMS.

- Usted mismo debe crear y administrar las políticas de auditoría. A diferencia de Amazon Aurora, RDS para Oracle no captura las actividades de la base de datos de forma predeterminada.
- Usted mismo debe crear y administrar las políticas o especificaciones de la auditoría. A diferencia de Amazon Aurora, Amazon RDS no captura las actividades de la base de datos de forma predeterminada.
- En una implementación multi-AZ, inicie el flujo de actividad de la base de datos solo en la instancia de base de datos principal. El flujo de actividad audita automáticamente las instancias de base de datos principal y en espera. No hace falta realizar ningún otro paso durante una conmutación por error.
- Al cambiar el nombre de una instancia de base de datos, no se crea un flujo de Kinesis nuevo.
- No se admiten CDB en RDS para Oracle.
- No se admiten réplicas de lectura.

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad de versiones y regiones de los flujos de actividades de base de datos, consulte Regiones y motores de base de datos admitidos para los flujos de actividad de bases de datos en Amazon RDS.

Clases de instancia de base de datos admitidas para los flujos de actividad de la base de datos

Para RDS para Oracle, puede utilizar flujos de actividad de bases de datos con las siguientes clases de instancias de base de datos:

- db.m4.*large
- db.m5.*large
- db.m5d.*large
- db.m6i.*large
- db.r4.*large
- db.r5.*large
- db.r5.*large.tpc*.mem*x
- db.r5b.*large
- db.r5b.*large.tpc*.mem*x

- db.r5d.*large
- db.r6i.*large
- db.r6i.*large.tpc*.mem*x
- db.x2idn.*large
- db.x2iedn.*large
- db.x2iezn.*large
- db.z1d.*large

Para RDS para SQL Server, puede utilizar flujos de actividad de bases de datos con las siguientes clases de instancias de base de datos:

- db.m4.*large
- db.m5.*large
- db.m5d.*large
- db.m6i.*large
- db.r4.*large
- db.r5.*large
- db.r5b.*large
- db.r5d.*large
- db.r6i.*large
- db.x1e.*large
- db.x2iedn.*large
- db.z1d.*large

Para obtener más información sobre los tipos de clases de instancia, consulte Clases de instancia de base de datos de .

Configuración de la auditoría unificada para Oracle Database

Al configurar la auditoría unificada para usarse con flujos de actividad de la base de datos, son posibles las siguientes situaciones:

- La auditoría unificada no está configurada para la base de datos de Oracle.

En este caso, cree nuevas políticas con el comando `CREATE AUDIT POLICY` y, después, actívelas con el comando `AUDIT POLICY`. En el ejemplo siguiente, se crea y activa una política para supervisar usuarios con privilegios y roles específicos.

```
CREATE AUDIT POLICY table_pol
PRIVILEGES CREATE ANY TABLE, DROP ANY TABLE
ROLES emp_admin, sales_admin;

AUDIT POLICY table_pol;
```

Para obtener instrucciones completas, consulte Configuring Audit Policies en la documentación de Oracle Database.

- La auditoría unificada está configurada para la base de datos de Oracle.

  Al activar un flujo de actividad de la base de datos, RDS for Oracle borra automáticamente los datos de auditoría existentes. También revoca los privilegios de seguimiento de auditoría. RDS for Oracle ya no puede hacer lo siguiente:

  - Depure registros de traza de auditoría unificados.
  - agregar, eliminar ni modificar la política de auditoría unificada
  - actualizar la última marca temporal archivada.

  > **Important**
  >
  > Le recomendamos realizar una copia de seguridad de los datos de auditoría antes de activar un flujo de actividad de la base de datos.

  Para obtener una descripción de la vista `UNIFIED_AUDIT_TRAIL`, consulte UNIFIED_AUDIT_TRAIL. Si tiene una cuenta con Oracle Support, consulte How To Purge The UNIFIED AUDIT TRAIL.

Configuración de la política de auditoría para Amazon RDS para Microsoft SQL Server

Una instancia de base de datos de SQL Server tiene la auditoría del servidor `RDS_DAS_AUDIT`, que administra Amazon RDS. Puede definir políticas para registrar los eventos del servidor en

la especificación de auditoría del servidor RDS_DAS_SERVER_AUDIT_SPEC. Puede crear una especificación de auditoría de base de datos, por ejemplo RDS_DAS_DB_<name>, y definir políticas para registrar eventos de la base de datos. Para obtener la lista de grupos de acciones de auditoría a nivel de servidor y base de datos, consulte SQL Server Audit Action Groups and Actions (Grupos de acciones y acciones de auditoría de SQL Server) en la documentación de Microsoft SQL Server.

La política de servidor predeterminada solo supervisa los inicios de sesión fallidos y los cambios en cualquier especificación de auditoría de bases de datos o servidores para los flujos de actividad de las bases de datos.

Estas son algunas de las limitaciones de la auditoría y las especificaciones de auditoría:

- No puede modificar las especificaciones de auditoría del servidor o la base de datos cuando el flujo de actividad de la base de datos esté bloqueado.
- No puede modificar la especificación de auditoría RDS_DAS_AUDIT del servidor.
- No puede modificar la auditoría de SQL Server RDS_DAS_CHANGES ni su especificación de auditoría de servidor relacionada RDS_DAS_CHANGES_AUDIT_SPEC.
- Al crear una especificación de auditoría de base de datos, debe utilizar el formato RDS_DAS_DB_<name>; por ejemplo,RDS_DAS_DB_databaseActions.

> **Important**
>
> Para clases de instancias más pequeñas, recomendamos que solo audite los datos necesarios. Esto ayuda a reducir el impacto en el rendimiento de los flujos de actividad de las bases de datos en estas clases de instancias.

El siguiente código de ejemplo modifica la especificación de auditoría del servidor RDS_DAS_SERVER_AUDIT_SPEC y audita todas las acciones de cierre de sesión y de inicio de sesión que se realizan correctamente:

```
ALTER SERVER AUDIT SPECIFICATION [RDS_DAS_SERVER_AUDIT_SPEC]
      WITH (STATE=OFF);
ALTER SERVER AUDIT SPECIFICATION [RDS_DAS_SERVER_AUDIT_SPEC]
      ADD (LOGOUT_GROUP),
      ADD (SUCCESSFUL_LOGIN_GROUP)
      WITH (STATE = ON );
```

El siguiente código de ejemplo crea una especificación de auditoría de base de datos `RDS_DAS_DB_database_spec` y la asocia a la auditoría del servidor `RDS_DAS_AUDIT`:

```
USE testDB;
CREATE DATABASE AUDIT SPECIFICATION [RDS_DAS_DB_database_spec]
     FOR SERVER AUDIT [RDS_DAS_AUDIT]
     ADD ( INSERT, UPDATE, DELETE
          ON testTable BY testUser )
     WITH (STATE = ON);
```

Una vez configuradas las especificaciones de auditoría, asegúrese de que las especificaciones `RDS_DAS_SERVER_AUDIT_SPEC` y `RDS_DAS_DB_<name>` estén configuradas en el estado `ON`. Ahora pueden enviar los datos de auditoría al flujo de actividad de su base de datos.

Inicio de una secuencia de actividades de la base de datos

Cuando inicie un flujo de actividad para la instancia de base de datos, todos los eventos de actividad de la base de datos que haya configurado en la política de auditoría generarán un evento del flujo de actividad. Los eventos de acceso se generan a partir de comandos SQL como `CONNECT` y `SELECT`. Los eventos de cambio se generan a partir de comandos SQL como `CREATE` y `INSERT`.

> **Important**
>
> La activación de un flujo de actividad para una instancia de Oracle Database borra los datos de auditoría existentes. También revoca los privilegios de seguimiento de auditoría. Cuando el flujo está habilitado, RDS para Oracle ya no puede hacer lo siguiente:
>
> - Depure registros de traza de auditoría unificados.
> - agregar, eliminar ni modificar la política de auditoría unificada
> - actualizar la última marca temporal archivada

Console

Inicio de un flujo de actividad de la base de datos

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).

3. Elija la instancia de base de datos de Amazon RDS en la que desea iniciar un flujo de actividad. En una implementación Multi-AZ, inicie el flujo solo en la instancia principal. El flujo de actividad audita automáticamente las instancias de base de datos principal y en espera.
4. En Actions (Acciones), elija Start activity stream (Iniciar secuencia de actividades).

   Aparecerá la ventana Start database activity stream: *name* (Iniciar el flujo de actividad de la base de datos: nombre), donde *name* (nombre) equivale a su instancia de RDS.
5. Ingrese la siguiente configuración:

   - En AWS KMS key, seleccione una clave de la lista de AWS KMS keys.

     Amazon RDS utiliza la clave de KMS para cifrar la clave que, a su vez, cifra la actividad de la base de datos. Elija una clave de KMS distinta de la clave predeterminada. Para obtener más información sobre las claves de cifrado y AWS KMS, consulte ¿Qué es AWS Key Management Service? en la guía para desarrolladores de AWS Key Management Service.
   - En Eventos de actividades de base de datos, elija Habilitar campos de auditoría nativos de Oracle para incluir campos de auditoría específicos del motor.
   - Elija Immediately (De inmediato).

     Cuando elige Immediately (De inmediato), la instancia de RDS se reinicia de inmediato. Si elige During the next maintenance window (Durante el siguiente periodo de mantenimiento), la instancia de RDS no se reinicia de inmediato. En este caso, la secuencia de actividades de la base de datos no se inicia hasta la siguiente ventana de mantenimiento.
6. Seleccione Start database activity stream (Iniciar secuencia de actividades de base de datos).

   El estado la base de datos muestra que el flujo de actividad se está iniciando.

> **Note**
>
> Si aparece el error `You can't start a database activity stream in this configuration`, compruebe Clases de instancia de base de datos admitidas para los flujos de actividad de la base de datos para ver si su instancia de RDS utiliza una clase de instancia compatible.

AWS CLI

Para empezar a transmitir la actividad de la base de datos de una instancia de base de datos, configure la base de datos mediante el comando start-activity-stream de la AWS CLI.

- `--resource-arn` *arn*: especifica el nombre de recurso de Amazon (ARN) de la instancia de base de datos.
- `--kms-key-id` *key*: especifica el identificador de clave KMS para cifrar mensajes en el flujo de actividad de la base de datos. El identificador de clave de KMS AWS es el ARN clave, el ID de clave, el ARN de alias o el nombre de alias de la AWS KMS key.
- `--engine-native-audit-fields-included`: incluye campos de auditoría unificados específicos del motor en el flujo de datos. Para excluir estos campos, especifique `--no-engine-native-audit-fields-included` (predeterminada).

El siguiente ejemplo inicia un flujo de actividad de la base de datos para una instancia de base de datos en modo asíncrono.

Para Linux, macOS o Unix:

```
aws rds start-activity-stream \
    --mode async \
    --kms-key-id my-kms-key-arn \
    --resource-arn my-instance-arn \
    --engine-native-audit-fields-included \
    --apply-immediately
```

Para Windows:

```
aws rds start-activity-stream ^
    --mode async ^
    --kms-key-id my-kms-key-arn ^
    --resource-arn my-instance-arn ^
    --engine-native-audit-fields-included ^
    --apply-immediately
```

Amazon RDS API

Para iniciar flujos de actividad de base de datos de una instancia de base de datos, configure la instancia mediante la operación StartActivityStream.

Llame a la acción con los siguientes parámetros:

- `Region`
- `KmsKeyId`
- `ResourceArn`
- `Mode`
- `EngineNativeAuditFieldsIncluded`

Modificación de una secuencia de actividades de la base de datos para Amazon RDS

Es posible que desee personalizar la política de auditoría de Amazon RDS cuando se inicie el flujo de actividad. Si no quiere perder tiempo ni datos deteniendo la secuencia de actividades, puede cambiar el estado de la política de auditoría a cualquiera de las siguientes opciones:

Locked (Bloqueado) (predeterminado)

Las políticas de auditoría de la base de datos son de solo lectura.

Unlocked (Desbloqueado)

Las políticas de auditoría de la base de datos son de lectura/escritura.

Los pasos básicos son los siguientes:

1. Cambie el estado de la política de auditoría a desbloqueado.
2. Personalice su política de auditoría.
3. Cambie el estado de la política de auditoría a bloqueado.

Consola

Para cambiar el estado de la política de auditoría de la secuencia de actividades

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. En Actions (Acciones), elija Modify database activity stream (Modificar secuencia de actividades de la base de datos).

Aparece la ventana Modify database activity stream: ***name***(Modificar secuencia de actividad de la base de datos: nombre), donde *name* es su instancia de RDS.

4. Elija cualquiera de las siguientes opciones:

   Locked (Bloqueado)

   Cuando se bloquea la política de auditoría, pasa a ser de solo lectura. No puede editar la política de auditoría a menos que la desbloquee o detenga la secuencia de actividades.

   Unlocked (Desbloqueado)

   Al desbloquear la política de auditoría, pasa a ser de lectura/escritura. Puede editar su política de auditoría mientras se inicia el flujo de actividades.

5. Elija Modify DB activity stream (Modificar flujo de actividades de la base de datos).

   El estado de Amazon RDS muestra Configurando el flujo de actividad.

6. (Opcional) Elija el enlace de la instancia de base de datos. A continuación, elija la pestaña Configuration (Configuración).

   El campo Audit policy status (Estado de política de auditoría) muestra uno de los siguientes valores:

   - Locked (Bloqueado)
   - Unlocked (Desbloqueado)
   - Locking policy (Política de bloqueo)
   - Unlocking policy (Política de desbloqueo)

AWS CLI

Para modificar el estado del flujo de actividad de una instancia de base de datos, utilice el comando modify-activity-stream de la AWS CLI.

Opción	¿Obligatorio?	Descripción
`--resource-arn` *my-instance-ARN*	Sí	El nombre de recurso de Amazon (ARN) de la instancia de base de datos de RDS.

Opción	¿Obligatorio?	Descripción
`--audit-policy-state`	No	El nuevo estado de la política de auditoría para el flujo de actividades de la base de datos en su instancia: `locked` o `unlocked`.

El siguiente ejemplo desbloquea la política de auditoría de la secuencia de actividades iniciada en *my-instance-ARN*.

Para Linux, macOS o:Unix

```
aws rds modify-activity-stream \
    --resource-arn my-instance-ARN \
    --audit-policy-state unlocked
```

En:Windows

```
aws rds modify-activity-stream ^
    --resource-arn my-instance-ARN ^
    --audit-policy-state unlocked
```

En el siguiente ejemplo, se describe la instancia *my-instance*. El resultado de ejemplo parcial muestra que la política de auditoría está desbloqueada.

```
aws rds describe-db-instances --db-instance-identifier my-instance

{
    "DBInstances": [
        {
            ...
            "Engine": "oracle-ee",
            ...
            "ActivityStreamStatus": "started",
            "ActivityStreamKmsKeyId": "ab12345e-1111-2bc3-12a3-ab1cd12345e",
            "ActivityStreamKinesisStreamName": "aws-rds-das-db-
AB1CDEFG23GHIJK4LMNOPQRST",
            "ActivityStreamMode": "async",
            "ActivityStreamEngineNativeAuditFieldsIncluded": true,
            "ActivityStreamPolicyStatus": "unlocked",
```

```
            ...
        }
    ]
}
```

API de RDS

Para modificar el estado de la política de flujo de actividades de la base de datos, utilice la operación ModifyActivityStream.

Llame a la acción con los siguientes parámetros:

- `AuditPolicyState`
- `ResourceArn`

Obtención del estado de un flujo de actividad de la base de datos

Puede obtener el estado de un flujo de actividad para su instancia de base de datos de Amazon RDS mediante la consola o AWS CLI.

Consola

Obtención del estado de un flujo de actividad de la base de datos

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, luego, el enlace de la instancia de base de datos.
3. Elija la pestaña Configuración y consulte el estado en Secuencia de actividades de base de datos.

AWS CLI

Puede usar la configuración del flujo de actividad para una instancia de base de datos como respuesta a una solicitud describe-db-instances de la CLI.

En el siguiente ejemplo, se describe *my-instance*.

```
aws rds --region my-region describe-db-instances --db-instance-identifier my-db
```

El ejemplo siguiente muestra una respuesta JSON. Se muestran los siguientes campos:

- `ActivityStreamKinesisStreamName`
- `ActivityStreamKmsKeyId`
- `ActivityStreamStatus`
- `ActivityStreamMode`
- `ActivityStreamPolicyStatus`

```
{
    "DBInstances": [
        {
            ...
            "Engine": "oracle-ee",
            ...
            "ActivityStreamStatus": "starting",
            "ActivityStreamKmsKeyId": "ab12345e-1111-2bc3-12a3-ab1cd12345e",
            "ActivityStreamKinesisStreamName": "aws-rds-das-db-
AB1CDEFG23GHIJK4LMNOPQRST",
            "ActivityStreamMode": "async",
            "ActivityStreamEngineNativeAuditFieldsIncluded": true,
            "ActivityStreamPolicyStatus": locked",
            ...
        }
    ]
}
```

API de RDS

Puede usar la configuración del flujo de actividad de un una base de datos como respuesta a una operación DescribeDBInstances.

Detención de un flujo de actividad de la base de datos

Puede detener una secuencia de actividades mediante la consola o AWS CLI.

Si elimina su instancia de base de datos de Amazon RDS, el flujo de actividad se detiene y el flujo subyacente de Amazon Kinesis se elimina automáticamente.

Consola

Para desactivar una secuencia de actividades

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija una base de datos cuyo flujo de actividad de la base de datos quiera detener.
4. En Actions (Acciones), elija Stop activity stream (Detener secuencia de actividades). Se visualizará la ventana Database Activity Stream (Secuencia de actividades de base de datos).

    a. Elija Immediately (De inmediato).

        Cuando elige Immediately (De inmediato), la instancia de RDS se reinicia de inmediato. Si elige During the next maintenance window (Durante el siguiente periodo de mantenimiento), la instancia de RDS no se reinicia de inmediato. En este caso, el flujo de actividad de la base de datos no se detiene hasta el siguiente periodo de mantenimiento.

    b. Elija Continue.

AWS CLI

Para detener flujos de actividad de la base de datos de su base de datos, configure la instancia de base de datos ejecutando el comando stop-activity-stream de AWS CLI. Identifique la región de AWS de la instancia de base de datos mediante el parámetro `--region`. El parámetro `--apply-immediately` es opcional.

Para Linux, macOS o:Unix

```
aws rds --region MY_REGION \
    stop-activity-stream \
    --resource-arn MY_DB_ARN \
    --apply-immediately
```

En:Windows

```
aws rds --region MY_REGION ^
    stop-activity-stream ^
    --resource-arn MY_DB_ARN ^
    --apply-immediately
```

API de RDS

Para detener los flujos de actividad la base de datos, configure el la instancia de base de datos mediante la operación StopActivityStream. Identifique la región de AWS de la instancia de base de datos mediante el parámetro `Region`. El parámetro `ApplyImmediately` es opcional.

Monitoreo de secuencias de actividades de la base de datos

Los flujos de actividad de la base de datos monitorean y notifican las actividades. La secuencia de actividades se recopila y se transmite a Amazon Kinesis. Desde Kinesis, puede monitorear la secuencia de actividad, o bien otros servicios y aplicaciones pueden consumir la secuencia de actividades para un análisis posterior. Puede encontrar el nombre del flujo de Kinesis subyacente mediante el comando `describe-db-instances` de la AWS CLI o la operación de la API de RDS `DescribeDBInstances`.

Amazon RDS administra el flujo de Kinesis de la siguiente manera:

- Amazon RDS crea el flujo de Kinesis automáticamente con un periodo de retención de 24 horas.
- Amazon RDS escala el flujo de Kinesis si es necesario.
- Si detiene el flujo de actividad de la base de datos o elimina la instancia de base de datos, Amazon RDS elimina el flujo de Kinesis.

Las categorías de actividad siguientes se monitorizan y se ponen en el registro de auditoría de secuencias de actividades:

- Comandos SQL: todos los comandos SQL se auditan, así como las instrucciones preparadas, las funciones integradas y las funciones en lenguaje de procedimientos para SQL (PL/SQL). Las llamadas a procedimientos almacenados se auditan. Cualquier instrucción SQL emitida dentro de procedimientos o funciones almacenados también se auditan.
- Otra información de la base de datos: la actividad monitoreada incluye la instrucción SQL completa, el recuento de las filas afectadas de los comandos DML, los objetos a los que se accede y el nombre único de la base de datos. Los flujos de actividad de la base de datos también monitorean las variables de enlace y los parámetros del procedimiento almacenados.

> **Important**
>
> El texto SQL completo de cada instrucción está visible en el registro de auditoría de secuencia de actividades, incluida la información confidencial. Sin embargo, las

contraseñas de usuario de base de datos se redactan siOracle las puede determinar a partir del contexto, tal y como pasa con la siguiente instrucción SQL.

```
ALTER ROLE role-name WITH password
```

- Información de conexión: la actividad monitorizada incluye la información de sesión y de red, el ID de proceso del servidor y los códigos de salida.

Si un flujo de actividad tiene un error mientras monitorea una instancia de base de datos, se lo notificará mediante eventos RDS.

En las siguientes secciones, puede acceder a los flujos de actividad de base de datos, auditarlos y procesarlos.

Temas

- Acceso a un flujo de actividad desde Amazon Kinesis
- Ejemplos y contenido sobre el registro de auditoría en flujos de actividad de bases de datos
- Matriz JSON databaseActivityEventList para flujos de actividad de base de datos
- Procesamiento de un flujo de actividad de la base de datos mediante SDK de AWS

Acceso a un flujo de actividad desde Amazon Kinesis

Cuando habilite un flujo de actividad para una base de datos, se creará un flujo de Kinesis para usted. En Kinesis podrá monitorizar la actividad de la base de datos en tiempo real. Para profundizar en el análisis de la actividad de la base de datos, puede conectar su secuencia de Kinesis a aplicaciones de consumidor. También puede conectar el flujo de datos con aplicaciones de administración de conformidad como Security Guardium de IBM o SecureSphere Database Audit and Protection de Imperva.

Puede acceder a su transmisión de Kinesis desde la consola de RDS o la consola de Kinesis.

Para acceder a una secuencia de actividades desde Kinesis utilizando la consola de RDS

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija la instancia de base de datos de Amazon RDS en la que desea iniciar un flujo de actividad.

4. Elija Configuration (Configuración).
5. En Database activity stream (Secuencia de actividad de base de datos), seleccione el enlace en Kinesis stream (Secuencia de Kinesis).
6. En la colsola de Kinesis, elija Monitoring (Supervisión) para empezar a observar la actividad de la base de datos.

Para acceder a una secuencia de actividades desde Kinesis utilizando la consola de Kinesis

1. Abra la consola de Kinesis en https://console.aws.amazon.com/kinesis.
2. Elija la secuencia de actividades en la lista de secuencias de Kinesis.

   El nombre de un flujo de actividad consta de un prefijo `aws-rds-das-db-` seguido del ID de recurso de la base datos. A continuación se muestra un ejemplo.

   ```
   aws-rds-das-db-NHVOV4PCLWHGF52NP
   ```

   Para utilizar la consola de Amazon RDS para encontrar el ID de recurso del la base de datos, elija su instancia de base de datos en la lista de bases de datos y, luego, elija la pestaña Configuration (Configuración).

   Para utilizar la AWS CLI para encontrar el nombre completo del flujo de Kinesis de un flujo de actividad, utilice una solicitud describe-db-instances de la CLI y anote el valor de `ActivityStreamKinesisStreamName` en la respuesta.
3. Elija Monitoring (Monitorización) para empezar a observar la actividad de la base de datos.

Para obtener más información acerca del uso de Amazon Kinesis, consulte ¿Qué es Amazon Kinesis Data Streams?.

Ejemplos y contenido sobre el registro de auditoría en flujos de actividad de bases de datos

Los eventos monitoreados se representan en el flujo de actividad de la base de datos como cadenas JSON. La estructura está formada por un objeto JSON que contiene un `DatabaseActivityMonitoringRecord`, el cual, a su vez, contiene una matriz `databaseActivityEventList` de eventos de actividad.

> **Note**
>
> Para los flujos de actividad de la base de datos, la matriz JSON de `paramList` no incluye valores nulos de las aplicaciones de Hibernate.

Temas

- Ejemplos de un registro de auditoría de flujo de actividad de la base de datos
- Objeto JSON DatabaseActivityMonitoringRecords
- Objeto JSON databaseActivityEvents

Ejemplos de un registro de auditoría de flujo de actividad de la base de datos

A continuación mostramos registros de auditoría JSON descifrados de muestra de registros de eventos de actividad.

Example Registro de eventos de actividad de una instrucción CONNECT SQL

El siguiente registro de eventos de actividad muestra un inicio de sesión con el uso de una instrucción SQL `CONNECT` (`command`) por parte de un JDBC Thin Client (`clientApplication`) para su base de datos Oracle.


```
{
    "class": "Standard",
    "clientApplication": "JDBC Thin Client",
    "command": "LOGON",
    "commandText": null,
    "dbid": "0123456789",
    "databaseName": "ORCL",
    "dbProtocol": "oracle",
    "dbUserName": "TEST",
    "endTime": null,
    "errorMessage": null,
    "exitCode": 0,
    "logTime": "2021-01-15 00:15:36.233787",
    "netProtocol": "tcp",
    "objectName": null,
    "objectType": null,
    "paramList": [],
    "pid": 17904,
```

```
    "remoteHost": "123.456.789.012",
    "remotePort": "25440",
    "rowCount": null,
    "serverHost": "987.654.321.098",
    "serverType": "oracle",
    "serverVersion": "19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3",
    "serviceName": "oracle-ee",
    "sessionId": 987654321,
    "startTime": null,
    "statementId": 1,
    "substatementId": null,
    "transactionId": "0000000000000000",
    "engineNativeAuditFields": {
        "UNIFIED_AUDIT_POLICIES": "TEST_POL_EVERYTHING",
        "FGA_POLICY_NAME": null,
        "DV_OBJECT_STATUS": null,
        "SYSTEM_PRIVILEGE_USED": "CREATE SESSION",
        "OLS_LABEL_COMPONENT_TYPE": null,
        "XS_SESSIONID": null,
        "ADDITIONAL_INFO": null,
        "INSTANCE_ID": 1,
        "DBID": 123456789
        "DV_COMMENT": null,
        "RMAN_SESSION_STAMP": null,
        "NEW_NAME": null,
        "DV_ACTION_NAME": null,
        "OLS_PROGRAM_UNIT_NAME": null,
        "OLS_STRING_LABEL": null,
        "RMAN_SESSION_RECID": null,
        "OBJECT_PRIVILEGES": null,
        "OLS_OLD_VALUE": null,
        "XS_TARGET_PRINCIPAL_NAME": null,
        "XS_NS_ATTRIBUTE": null,
        "XS_NS_NAME": null,
        "DBLINK_INFO": null,
        "AUTHENTICATION_TYPE": "(TYPE\u003d(DATABASE));(CLIENT ADDRESS\u003d((ADDRESS
\u003d(PROTOCOL\u003dtcp)(HOST\u003d205.251.233.183)(PORT\u003d25440))));",
        "OBJECT_EDITION": null,
        "OLS_PRIVILEGES_GRANTED": null,
        "EXCLUDED_USER": null,
        "DV_ACTION_OBJECT_NAME": null,
        "OLS_LABEL_COMPONENT_NAME": null,
        "EXCLUDED_SCHEMA": null,
        "DP_TEXT_PARAMETERS1": null,
```

```
        "XS_USER_NAME": null,
        "XS_ENABLED_ROLE": null,
        "XS_NS_ATTRIBUTE_NEW_VAL": null,
        "DIRECT_PATH_NUM_COLUMNS_LOADED": null,
        "AUDIT_OPTION": null,
        "DV_EXTENDED_ACTION_CODE": null,
        "XS_PACKAGE_NAME": null,
        "OLS_NEW_VALUE": null,
        "DV_RETURN_CODE": null,
        "XS_CALLBACK_EVENT_TYPE": null,
        "USERHOST": "a1b2c3d4e5f6.amazon.com",
        "GLOBAL_USERID": null,
        "CLIENT_IDENTIFIER": null,
        "RMAN_OPERATION": null,
        "TERMINAL": "unknown",
        "OS_USERNAME": "sumepate",
        "OLS_MAX_READ_LABEL": null,
        "XS_PROXY_USER_NAME": null,
        "XS_DATASEC_POLICY_NAME": null,
        "DV_FACTOR_CONTEXT": null,
        "OLS_MAX_WRITE_LABEL": null,
        "OLS_PARENT_GROUP_NAME": null,
        "EXCLUDED_OBJECT": null,
        "DV_RULE_SET_NAME": null,
        "EXTERNAL_USERID": null,
        "EXECUTION_ID": null,
        "ROLE": null,
        "PROXY_SESSIONID": 0,
        "DP_BOOLEAN_PARAMETERS1": null,
        "OLS_POLICY_NAME": null,
        "OLS_GRANTEE": null,
        "OLS_MIN_WRITE_LABEL": null,
        "APPLICATION_CONTEXTS": null,
        "XS_SCHEMA_NAME": null,
        "DV_GRANTEE": null,
        "XS_COOKIE": null,
        "DBPROXY_USERNAME": null,
        "DV_ACTION_CODE": null,
        "OLS_PRIVILEGES_USED": null,
        "RMAN_DEVICE_TYPE": null,
        "XS_NS_ATTRIBUTE_OLD_VAL": null,
        "TARGET_USER": null,
        "XS_ENTITY_TYPE": null,
        "ENTRY_ID": 1,
```

```
        "XS_PROCEDURE_NAME": null,
        "XS_INACTIVITY_TIMEOUT": null,
        "RMAN_OBJECT_TYPE": null,
        "SYSTEM_PRIVILEGE": null,
        "NEW_SCHEMA": null,
        "SCN": 5124715
    }
}
```

El siguiente registro de eventos de actividad muestra un error de inicio de sesión en la base de datos de SQL Server.

```
{
    "type": "DatabaseActivityMonitoringRecord",
    "clusterId": "",
    "instanceId": "db-4JCWQLUZVFYP7DIWP6JVQ77O3Q",
    "databaseActivityEventList": [
        {
            "class": "LOGIN",
            "clientApplication": "Microsoft SQL Server Management Studio",
            "command": "LOGIN FAILED",
            "commandText": "Login failed for user 'test'. Reason: Password did not
 match that for the login provided. [CLIENT: local-machine]",
            "databaseName": "",
            "dbProtocol": "SQLSERVER",
            "dbUserName": "test",
            "endTime": null,
            "errorMessage": null,
            "exitCode": 0,
            "logTime": "2022-10-06 21:34:42.7113072+00",
            "netProtocol": null,
            "objectName": "",
            "objectType": "LOGIN",
            "paramList": null,
            "pid": null,
            "remoteHost": "local machine",
            "remotePort": null,
            "rowCount": 0,
            "serverHost": "172.31.30.159",
            "serverType": "SQLSERVER",
            "serverVersion": "15.00.4073.23.v1.R1",
            "serviceName": "sqlserver-ee",
            "sessionId": 0,
```

```
            "startTime": null,
            "statementId": "0x1eb0d1808d34a94b9d3dcf5432750f02",
            "substatementId": 1,
            "transactionId": "0",
            "type": "record",
            "engineNativeAuditFields": {
                "target_database_principal_id": 0,
                "target_server_principal_id": 0,
                "target_database_principal_name": "",
                "server_principal_id": 0,
                "user_defined_information": "",
                "response_rows": 0,
                "database_principal_name": "",
                "target_server_principal_name": "",
                "schema_name": "",
                "is_column_permission": false,
                "object_id": 0,
                "server_instance_name": "EC2AMAZ-NFUJJNO",
                "target_server_principal_sid": null,
                "additional_information": "<action_info "xmlns=\"http://
schemas.microsoft.com/sqlserver/2008/sqlaudit_data\"><pooled_connection>0</
pooled_connection><error>0x00004818</error><state>8</state><address>local machine</
address><PasswordFirstNibbleHash>B</PasswordFirstNibbleHash></action_info>"-->,
                "duration_milliseconds": 0,
                "permission_bitmask": "0x00000000000000000000000000000000",
                "data_sensitivity_information": "",
                "session_server_principal_name": "",
                "connection_id": "98B4F537-0F82-49E3-AB08-B9D33B5893EF",
                "audit_schema_version": 1,
                "database_principal_id": 0,
                "server_principal_sid": null,
                "user_defined_event_id": 0,
                "host_name": "EC2AMAZ-NFUJJNO"
            }
        }
    ]
}
```


> **Note**
>
> Si un flujo de actividad de la base de datos no está habilitado, el último campo del documento JSON es `"engineNativeAuditFields": { }`.

Example Registro de evento de actividad de una instrucción CREATE TABLE

En el siguiente ejemplo, se muestra un evento `CREATE TABLE` para su base de datos Oracle.


```
{
    "class": "Standard",
    "clientApplication": "sqlplus@ip-12-34-5-678 (TNS V1-V3)",
    "command": "CREATE TABLE",
    "commandText": "CREATE TABLE persons(\n    person_id NUMBER GENERATED BY DEFAULT AS
 IDENTITY,\n    first_name VARCHAR2(50) NOT NULL,\n    last_name VARCHAR2(50) NOT NULL,
\n    PRIMARY KEY(person_id)\n)",
    "dbid": "0123456789",
    "databaseName": "ORCL",
    "dbProtocol": "oracle",
    "dbUserName": "TEST",
    "endTime": null,
    "errorMessage": null,
    "exitCode": 0,
    "logTime": "2021-01-15 00:22:49.535239",
    "netProtocol": "beq",
    "objectName": "PERSONS",
    "objectType": "TEST",
    "paramList": [],
    "pid": 17687,
    "remoteHost": "123.456.789.0",
    "remotePort": null,
    "rowCount": null,
    "serverHost": "987.654.321.01",
    "serverType": "oracle",
    "serverVersion": "19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3",
    "serviceName": "oracle-ee",
    "sessionId": 1234567890,
    "startTime": null,
    "statementId": 43,
    "substatementId": null,
    "transactionId": "090011007F0D0000",
    "engineNativeAuditFields": {
        "UNIFIED_AUDIT_POLICIES": "TEST_POL_EVERYTHING",
        "FGA_POLICY_NAME": null,
        "DV_OBJECT_STATUS": null,
        "SYSTEM_PRIVILEGE_USED": "CREATE SEQUENCE, CREATE TABLE",
        "OLS_LABEL_COMPONENT_TYPE": null,
        "XS_SESSIONID": null,
        "ADDITIONAL_INFO": null,
```

```
        "INSTANCE_ID": 1,
        "DV_COMMENT": null,
        "RMAN_SESSION_STAMP": null,
        "NEW_NAME": null,
        "DV_ACTION_NAME": null,
        "OLS_PROGRAM_UNIT_NAME": null,
        "OLS_STRING_LABEL": null,
        "RMAN_SESSION_RECID": null,
        "OBJECT_PRIVILEGES": null,
        "OLS_OLD_VALUE": null,
        "XS_TARGET_PRINCIPAL_NAME": null,
        "XS_NS_ATTRIBUTE": null,
        "XS_NS_NAME": null,
        "DBLINK_INFO": null,
        "AUTHENTICATION_TYPE": "(TYPE\u003d(DATABASE));(CLIENT ADDRESS\u003d((PROTOCOL
\u003dbeq)(HOST\u003d123.456.789.0)));",
        "OBJECT_EDITION": null,
        "OLS_PRIVILEGES_GRANTED": null,
        "EXCLUDED_USER": null,
        "DV_ACTION_OBJECT_NAME": null,
        "OLS_LABEL_COMPONENT_NAME": null,
        "EXCLUDED_SCHEMA": null,
        "DP_TEXT_PARAMETERS1": null,
        "XS_USER_NAME": null,
        "XS_ENABLED_ROLE": null,
        "XS_NS_ATTRIBUTE_NEW_VAL": null,
        "DIRECT_PATH_NUM_COLUMNS_LOADED": null,
        "AUDIT_OPTION": null,
        "DV_EXTENDED_ACTION_CODE": null,
        "XS_PACKAGE_NAME": null,
        "OLS_NEW_VALUE": null,
        "DV_RETURN_CODE": null,
        "XS_CALLBACK_EVENT_TYPE": null,
        "USERHOST": "ip-10-13-0-122",
        "GLOBAL_USERID": null,
        "CLIENT_IDENTIFIER": null,
        "RMAN_OPERATION": null,
        "TERMINAL": "pts/1",
        "OS_USERNAME": "rdsdb",
        "OLS_MAX_READ_LABEL": null,
        "XS_PROXY_USER_NAME": null,
        "XS_DATASEC_POLICY_NAME": null,
        "DV_FACTOR_CONTEXT": null,
        "OLS_MAX_WRITE_LABEL": null,
```

```
        "OLS_PARENT_GROUP_NAME": null,
        "EXCLUDED_OBJECT": null,
        "DV_RULE_SET_NAME": null,
        "EXTERNAL_USERID": null,
        "EXECUTION_ID": null,
        "ROLE": null,
        "PROXY_SESSIONID": 0,
        "DP_BOOLEAN_PARAMETERS1": null,
        "OLS_POLICY_NAME": null,
        "OLS_GRANTEE": null,
        "OLS_MIN_WRITE_LABEL": null,
        "APPLICATION_CONTEXTS": null,
        "XS_SCHEMA_NAME": null,
        "DV_GRANTEE": null,
        "XS_COOKIE": null,
        "DBPROXY_USERNAME": null,
        "DV_ACTION_CODE": null,
        "OLS_PRIVILEGES_USED": null,
        "RMAN_DEVICE_TYPE": null,
        "XS_NS_ATTRIBUTE_OLD_VAL": null,
        "TARGET_USER": null,
        "XS_ENTITY_TYPE": null,
        "ENTRY_ID": 12,
        "XS_PROCEDURE_NAME": null,
        "XS_INACTIVITY_TIMEOUT": null,
        "RMAN_OBJECT_TYPE": null,
        "SYSTEM_PRIVILEGE": null,
        "NEW_SCHEMA": null,
        "SCN": 5133083
    }
}
```

En el siguiente ejemplo, se muestra un evento `CREATE TABLE` de la base de datos SQL Server.

```
{
    "type": "DatabaseActivityMonitoringRecord",
    "clusterId": "",
    "instanceId": "db-4JCWQLUZVFYP7DIWP6JVQ77O3Q",
    "databaseActivityEventList": [
        {
            "class": "SCHEMA",
            "clientApplication": "Microsoft SQL Server Management Studio - Query",
            "command": "ALTER",
```

```
            "commandText": "Create table [testDB].[dbo].[TestTable2](\r\ntextA
 varchar(6000),\r\n    textB varchar(6000)\r\n)",
            "databaseName": "testDB",
            "dbProtocol": "SQLSERVER",
            "dbUserName": "test",
            "endTime": null,
            "errorMessage": null,
            "exitCode": 1,
            "logTime": "2022-10-06 21:44:38.4120677+00",
            "netProtocol": null,
            "objectName": "dbo",
            "objectType": "SCHEMA",
            "paramList": null,
            "pid": null,
            "remoteHost": "local machine",
            "remotePort": null,
            "rowCount": 0,
            "serverHost": "172.31.30.159",
            "serverType": "SQLSERVER",
            "serverVersion": "15.00.4073.23.v1.R1",
            "serviceName": "sqlserver-ee",
            "sessionId": 84,
            "startTime": null,
            "statementId": "0x5178d33d56e95e419558b9607158a5bd",
            "substatementId": 1,
            "transactionId": "4561864",
            "type": "record",
            "engineNativeAuditFields": {
                "target_database_principal_id": 0,
                "target_server_principal_id": 0,
                "target_database_principal_name": "",
                "server_principal_id": 2,
                "user_defined_information": "",
                "response_rows": 0,
                "database_principal_name": "dbo",
                "target_server_principal_name": "",
                "schema_name": "",
                "is_column_permission": false,
                "object_id": 1,
                "server_instance_name": "EC2AMAZ-NFUJJNO",
                "target_server_principal_sid": null,
                "additional_information": "",
                "duration_milliseconds": 0,
                "permission_bitmask": "0x00000000000000000000000000000000",
```

```
                "data_sensitivity_information": "",
                "session_server_principal_name": "test",
                "connection_id": "EE1FE3FD-EF2C-41FD-AF45-9051E0CD983A",
                "audit_schema_version": 1,
                "database_principal_id": 1,
                "server_principal_sid":
 "0x0105000000000005150000000bdc2795e2d0717901ba6998cf4010000",
                "user_defined_event_id": 0,
                "host_name": "EC2AMAZ-NFUJJNO"
            }
        }
    ]
}
```

Example Registro de evento de actividad de una instrucción SELECT de Aurora PostgreSQL

En el siguiente ejemplo, se muestra un evento `SELECT` para su base de datos Oracle.

```
{
    "class": "Standard",
    "clientApplication": "sqlplus@ip-12-34-5-678 (TNS V1-V3)",
    "command": "SELECT",
    "commandText": "select count(*) from persons",
    "databaseName": "1234567890",
    "dbProtocol": "oracle",
    "dbUserName": "TEST",
    "endTime": null,
    "errorMessage": null,
    "exitCode": 0,
    "logTime": "2021-01-15 00:25:18.850375",
    "netProtocol": "beq",
    "objectName": "PERSONS",
    "objectType": "TEST",
    "paramList": [],
    "pid": 17687,
    "remoteHost": "123.456.789.0",
    "remotePort": null,
    "rowCount": null,
    "serverHost": "987.654.321.09",
    "serverType": "oracle",
    "serverVersion": "19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3",
    "serviceName": "oracle-ee",
    "sessionId": 1080639707,
    "startTime": null,
```

```
    "statementId": 44,
    "substatementId": null,
    "transactionId": null,
    "engineNativeAuditFields": {
        "UNIFIED_AUDIT_POLICIES": "TEST_POL_EVERYTHING",
        "FGA_POLICY_NAME": null,
        "DV_OBJECT_STATUS": null,
        "SYSTEM_PRIVILEGE_USED": null,
        "OLS_LABEL_COMPONENT_TYPE": null,
        "XS_SESSIONID": null,
        "ADDITIONAL_INFO": null,
        "INSTANCE_ID": 1,
        "DV_COMMENT": null,
        "RMAN_SESSION_STAMP": null,
        "NEW_NAME": null,
        "DV_ACTION_NAME": null,
        "OLS_PROGRAM_UNIT_NAME": null,
        "OLS_STRING_LABEL": null,
        "RMAN_SESSION_RECID": null,
        "OBJECT_PRIVILEGES": null,
        "OLS_OLD_VALUE": null,
        "XS_TARGET_PRINCIPAL_NAME": null,
        "XS_NS_ATTRIBUTE": null,
        "XS_NS_NAME": null,
        "DBLINK_INFO": null,
        "AUTHENTICATION_TYPE": "(TYPE\u003d(DATABASE));(CLIENT ADDRESS\u003d((PROTOCOL
\u003dbeq)(HOST\u003d123.456.789.0)));",
        "OBJECT_EDITION": null,
        "OLS_PRIVILEGES_GRANTED": null,
        "EXCLUDED_USER": null,
        "DV_ACTION_OBJECT_NAME": null,
        "OLS_LABEL_COMPONENT_NAME": null,
        "EXCLUDED_SCHEMA": null,
        "DP_TEXT_PARAMETERS1": null,
        "XS_USER_NAME": null,
        "XS_ENABLED_ROLE": null,
        "XS_NS_ATTRIBUTE_NEW_VAL": null,
        "DIRECT_PATH_NUM_COLUMNS_LOADED": null,
        "AUDIT_OPTION": null,
        "DV_EXTENDED_ACTION_CODE": null,
        "XS_PACKAGE_NAME": null,
        "OLS_NEW_VALUE": null,
        "DV_RETURN_CODE": null,
        "XS_CALLBACK_EVENT_TYPE": null,
```

```
        "USERHOST": "ip-12-34-5-678",
        "GLOBAL_USERID": null,
        "CLIENT_IDENTIFIER": null,
        "RMAN_OPERATION": null,
        "TERMINAL": "pts/1",
        "OS_USERNAME": "rdsdb",
        "OLS_MAX_READ_LABEL": null,
        "XS_PROXY_USER_NAME": null,
        "XS_DATASEC_POLICY_NAME": null,
        "DV_FACTOR_CONTEXT": null,
        "OLS_MAX_WRITE_LABEL": null,
        "OLS_PARENT_GROUP_NAME": null,
        "EXCLUDED_OBJECT": null,
        "DV_RULE_SET_NAME": null,
        "EXTERNAL_USERID": null,
        "EXECUTION_ID": null,
        "ROLE": null,
        "PROXY_SESSIONID": 0,
        "DP_BOOLEAN_PARAMETERS1": null,
        "OLS_POLICY_NAME": null,
        "OLS_GRANTEE": null,
        "OLS_MIN_WRITE_LABEL": null,
        "APPLICATION_CONTEXTS": null,
        "XS_SCHEMA_NAME": null,
        "DV_GRANTEE": null,
        "XS_COOKIE": null,
        "DBPROXY_USERNAME": null,
        "DV_ACTION_CODE": null,
        "OLS_PRIVILEGES_USED": null,
        "RMAN_DEVICE_TYPE": null,
        "XS_NS_ATTRIBUTE_OLD_VAL": null,
        "TARGET_USER": null,
        "XS_ENTITY_TYPE": null,
        "ENTRY_ID": 13,
        "XS_PROCEDURE_NAME": null,
        "XS_INACTIVITY_TIMEOUT": null,
        "RMAN_OBJECT_TYPE": null,
        "SYSTEM_PRIVILEGE": null,
        "NEW_SCHEMA": null,
        "SCN": 5136972
    }
}
```

En el siguiente ejemplo, se muestra un evento SELECT para su base de datos SQL Server.


```
{
    "type": "DatabaseActivityMonitoringRecord",
    "clusterId": "",
    "instanceId": "db-4JCWQLUZVFYP7DIWP6JVQ77O3Q",
    "databaseActivityEventList": [
        {
            "class": "TABLE",
            "clientApplication": "Microsoft SQL Server Management Studio - Query",
            "command": "SELECT",
            "commandText": "select * from [testDB].[dbo].[TestTable]",
            "databaseName": "testDB",
            "dbProtocol": "SQLSERVER",
            "dbUserName": "test",
            "endTime": null,
            "errorMessage": null,
            "exitCode": 1,
            "logTime": "2022-10-06 21:24:59.9422268+00",
            "netProtocol": null,
            "objectName": "TestTable",
            "objectType": "TABLE",
            "paramList": null,
            "pid": null,
            "remoteHost": "local machine",
            "remotePort": null,
            "rowCount": 0,
            "serverHost": "172.31.30.159",
            "serverType": "SQLSERVER",
            "serverVersion": "15.00.4073.23.v1.R1",
            "serviceName": "sqlserver-ee",
            "sessionId": 62,
            "startTime": null,
            "statementId": "0x03baed90412f564fad640ebe51f89b99",
            "substatementId": 1,
            "transactionId": "4532935",
            "type": "record",
            "engineNativeAuditFields": {
                "target_database_principal_id": 0,
                "target_server_principal_id": 0,
                "target_database_principal_name": "",
                "server_principal_id": 2,
                "user_defined_information": "",
                "response_rows": 0,
```

```
                "database_principal_name": "dbo",
                "target_server_principal_name": "",
                "schema_name": "dbo",
                "is_column_permission": true,
                "object_id": 581577110,
                "server_instance_name": "EC2AMAZ-NFUJJNO",
                "target_server_principal_sid": null,
                "additional_information": "",
                "duration_milliseconds": 0,
                "permission_bitmask": "0x00000000000000000000000000000001",
                "data_sensitivity_information": "",
                "session_server_principal_name": "test",
                "connection_id": "AD3A5084-FB83-45C1-8334-E923459A8109",
                "audit_schema_version": 1,
                "database_principal_id": 1,
                "server_principal_sid":
 "0x0105000000000005150000000bdc2795e2d0717901ba6998cf4010000",
                "user_defined_event_id": 0,
                "host_name": "EC2AMAZ-NFUJJNO"
            }
        }
    ]
}
```

Objeto JSON DatabaseActivityMonitoringRecords

Los registros de eventos de actividad de la base de datos se encuentran en un objeto JSON que contiene la siguiente información.

Campo JSON	Tipo de datos	Descripción
`type`	string	Tipo de registro JSON. El valor es `DatabaseActivityMonitoringRecords` .
`version`	string	La versión de los registros de monitoreo de actividad de la base de datos. La base de datos Oracle utiliza la versión 1.3 y SQL Server utiliza la versión 1.4. Estas

Campo JSON	Tipo de datos	Descripción
		versiones del motor introducen el objeto JSON `engineNativeAuditFields` .
databaseActivityEvents	cadena	Un objeto JSON que contiene los eventos de actividad.
key	cadena	Una clave de cifrado que se utiliza para descifrar el Matriz de JSON databaseActivityEventList.

Objeto JSON databaseActivityEvents

El objeto JSON `databaseActivityEvents` contiene la siguiente información.

Campos de nivel superior en el registro JSON

Cada evento del registro de auditoría se envuelve dentro de un registro en formato JSON. Este registro contiene los siguientes campos.

type

Este campo siempre tiene el valor `DatabaseActivityMonitoringRecords`.

version

Este campo representa la versión del protocolo o contrato de datos del flujo de actividad de la base de datos. Define los campos que están disponibles.

databaseActivityEvents

Una cadena cifrada que representa uno o más eventos de actividad. Se representa como una matriz de bytes base64. Al descifrar la cadena, el resultado es un registro en formato JSON con campos, tal y como se muestra en los ejemplos de esta sección.

key

Clave de datos cifrada utilizada para cifrar la cadena `databaseActivityEvents`. Esta es la misma AWS KMS key que proporcionó cuando inició la secuencia de actividades de la base de datos.

En el ejemplo siguiente se muestra el formato de este registro.

```
{
  "type":"DatabaseActivityMonitoringRecords",
  "version":"1.3",
  "databaseActivityEvents":"encrypted audit records",
  "key":"encrypted key"
}
```

```
          "type":"DatabaseActivityMonitoringRecords",
          "version":"1.4",
          "databaseActivityEvents":"encrypted audit records",
          "key":"encrypted key"
```

Siga estos pasos para descifrar el contenido del campo:`databaseActivityEvents`

1. Descifrar el valor en el campo JSON `key` mediante la clave de KMS que proporcionó al iniciar la secuencia de actividades de la base de datos. Al hacerlo, se devuelve la clave de cifrado de datos en texto sin cifrar.
2. Decodifique en base64 el valor en el campo JSON `databaseActivityEvents` para obtener el texto cifrado, en formato binario, de la carga útil de auditoría.
3. Descifrar el texto cifrado binario con la clave de cifrado de datos que decodificó en el primer paso.
4. Descomprimir la carga útil descifrada.
   - La carga cifrada está en el campo `databaseActivityEvents`.
   - El campo `databaseActivityEventList` contiene una matriz de registros de auditoría. Los campos `type` de la matriz pueden ser `record` o `heartbeat`.

Un registro de evento de actividad de registro de auditoría es un objeto JSON que contiene la información siguiente.

Campo JSON	Tipo de datos	Descripción
`type`	string	Tipo de registro JSON. El valor es `DatabaseActivityMonitoringRecord` .

Campo JSON	Tipo de datos	Descripción
`instanceId`	string	El identificador del recurso de instancia de base de datos. Corresponde al atributo de instancia de base de datos `DbiResourceId` .
Matriz de JSON databaseActivityEventList	string	Una matriz de registros de auditoría de actividad o mensajes de latido.

Matriz JSON databaseActivityEventList para flujos de actividad de base de datos

La carga de registro de auditoría es una matriz JSON `databaseActivityEventList` cifrada. En la tabla siguiente, se enumeran alfabéticamente los campos de cada evento de actividad de la matriz `DatabaseActivityEventList` descifrada de un registro de auditoría.

Cuando la auditoría unificada está activada en la base de datos de Oracle, los registros de auditoría se rellenan en este nuevo seguimiento de auditoría. La vista `UNIFIED_AUDIT_TRAIL` muestra los registros de auditoría en forma tabular; para ello, recupera los registros de auditoría del seguimiento de auditoría. Cuando inicia un flujo de actividad de la base de datos, una columna en `UNIFIED_AUDIT_TRAIL` corresponde a un campo en la matriz `databaseActivityEventList`.

> **Important**
>
> La estructura de los eventos está sujeta a cambio. Amazon RDS podría agregar nuevos campos a eventos de actividad en el futuro. En las aplicaciones que analizan los datos JSON, asegúrese de que el código puede ignorar o tomar las acciones adecuadas para nombres de campo desconocidos.

Campos databaseActivityEventList para Amazon RDS para Oracle

A continuación, encontrará campos `databaseActivityEventList` para Amazon RDS para Oracle.

Campo	Tipo de datos	Fuente	Descripción
`class`	string	`AUDIT_TYPE` columna en `UNIFIED_AUDIT_TRAIL`	Clase de evento de actividad. Esto se corresponde con la `AUDIT_TYPE` columna de la vista `UNIFIED_AUDIT_TRAIL`. Los valores válidos para Amazon RDS para Oracle son los siguientes: • `Standard` • `FineGrainedAudit` • `XS` • `Database Vault` • `Label Security` • `RMAN_AUDIT` • `Datapump` • `Direct path API` Para obtener más información, consulte UNIFIED_AUDIT_TRAIL en la documentación de Oracle.
`clientApplication`	string	`CLIENT_PROGRAM_NAME` en `UNIFIED_AUDIT_TRAIL`	Aplicación que el cliente ha usado para establecer conexión según notificación del cliente. No es obligatorio que el cliente notifique esta informaci

Campo	Tipo de datos	Fuente	Descripción
			ón, por lo que el valor puede ser nulo. Un valor de muestra es `JDBC Thin Client`.
`command`	string	`ACTION_NAME` columna en `UNIFIED_AUDIT_TRAIL`	Nombre de la acción ejecutada por el usuario. Para comprender la acción completa, lea tanto el nombre del comando como el valor `AUDIT_TYPE` . Un valor de muestra es `ALTER DATABASE`.
`commandText`	string	`SQL_TEXT` columna en `UNIFIED_AUDIT_TRAIL`	La instrucción SQL asociada con el evento Un valor de muestra es `ALTER DATABASE BEGIN BACKUP`.
`databaseName`	string	`NAME` columna en `V $DATABASE`	El nombre de la base de datos.
`dbid`	núme	`DBID` columna en `UNIFIED_AUDIT_TRAIL`	Identificador numérico para la base de datos Un valor de muestra es `1559204751` .
`dbProtocol`	string	N/A	Protocolo de la base de datos. En esta versión beta, el valor es `oracle`.

Campo	Tipo de datos	Fuente	Descripción
`dbUserName`	string	`DBUSERNAME` columna en `UNIFIED_AUDIT_TRAIL`	Nombre del usuario de la base de datos cuyas acciones se auditaron Un valor de muestra es `RDSADMIN`.
`endTime`	string	N/A	Este campo no se utiliza para RDS para Oracle y siempre es nulo.

Campo	Tipo de datos	Fuente	Descripción

`engineNativeAuditFields`	objeto	`UNIFIED_AUDIT_TRAIL`	De forma predeterminada, este objeto está vacío. Cuando inicia el flujo de actividad con la opción `--engine-native-audit-fields-included` , este objeto incluye las siguientes columnas y sus valores:
			`ADDITIONAL_INFO`
			`APPLICATION_CONTEXTS`
			`AUDIT_OPTION`
			`AUTHENTICATION_TYPE`
			`CLIENT_IDENTIFIER`
			`CURRENT_USER`
			`DBLINK_INFO`
			`DBPROXY_USERNAME`
			`DIRECT_PATH_NUM_COLUMNS_LOADED`
			`DP_BOOLEAN_PARAMETERS1`
			`DP_TEXT_PARAMETERS1`
			`DV_ACTION_CODE`
			`DV_ACTION_NAME`
			`DV_ACTION_OBJECT_NAME`
			`DV_COMMENT`
			`DV_EXTENDED_ACTION_CODE`
			`DV_FACTOR_CONTEXT`
			`DV_GRANTEE`
			`DV_OBJECT_STATUS`

Campo	Tipo de datos	Fuente	Descripción
			DV_RETURN_CODE DV_RULE_SET_NAME ENTRY_ID EXCLUDED_OBJECT EXCLUDED_SCHEMA EXCLUDED_USER EXECUTION_ID EXTERNAL_USERID FGA_POLICY_NAME GLOBAL_USERID INSTANCE_ID KSACL_SER VICE_NAME KSACL_SOURCE_LOCA TION KSACL_USER_NAME NEW_NAME NEW_SCHEMA OBJECT_EDITION OBJECT_PRIVILEGES OLS_GRANTEE OLS_LABEL_COM PONENT_NAME OLS_LABEL_COMPO NENT_TYPE OLS_MAX_READ_LABEL OLS_MAX_WRITE_LA BEL OLS_MIN_WRITE_ LABEL OLS_NEW_VALUE OLS_OLD_VALUE OLS_PARENT_ GROUP_NAME OLS_POLICY_NAME OLS_PRIVILEGES_GRA NTED OLS_PRIVILEGE S_USED

Campo	Tipo de datos	Fuente	Descripción
			OLS_PROGRAM _UNIT_NAME OLS_STRING_LABEL OS_USERNAME PROTOCOL_ACTIO N_NAME PROTOCOL_MESSAGE PROTOCOL_RET URN_CODE PROTOCOL_SESSION_I D PROTOCOL_USERHOST PROXY_SESSIONID RLS_INFO RMAN_DEVICE_TYPE RMAN_OBJECT_TYPE RMAN_OPERATION RMAN_SESSION_RECID RMAN_SESSION_STAMP ROLE SCN SYSTEM_PRIVILEGE SYSTEM_PRIVIL EGE_USED TARGET_USER TERMINAL UNIFIED_AUDIT_P OLICIES USERHOST XS_CALLBAC K_EVENT_TYPE XS_COOKIE XS_DATASEC_PO LICY_NAME XS_ENABLED_ROLE XS_ENTITY_TYPE XS_INACTIVITY _TIMEOUT XS_NS_ATTRIBUTE

Campo	Tipo de datos	Fuente	Descripción

			`XS_NS_ATTRIBUTE_NEW_VAL`
			`XS_NS_ATTRIBUTE_OLD_VAL`
			`XS_NS_NAME`
			`XS_PACKAGE_NAME`
			`XS_PROCEDURE_NAME`
			`XS_PROXY_USER_NAME`
			`XS_SCHEMA_NAME`
			`XS_SESSIONID`
			`XS_TARGET_PRINCIPAL_NAME`
			`XS_USER_NAME`
			
			Para obtener más información, consulte UNIFIED_AUDIT_TRAIL en la documentación de Oracle Database.

`errorMessage`	string	N/A	Este campo no se utiliza para RDS para Oracle y siempre es nulo.
`exitCode`	núme	`RETURN_CODE` columna en `UNIFIED_AUDIT_TRAIL`	Código de error de Oracle Database generado por la acción Si la acción se realizó correctamente, el valor es `0`.

Campo	Tipo de datos	Fuente	Descripción
logTime	string	EVENT_TIMESTAMP_UTC columna en UNIFIED_AUDIT_TRAIL	Marca de tiempo de la creación de la entrada de seguimiento de auditoría . Un valor de muestra es 2020-11-27 06:56:14.981404 .
netProtocol	string	AUTHENTICATION_TYPE columna en UNIFIED_AUDIT_TRAIL	Protocolo de comunicación de red Un valor de muestra es TCP.
objectName	string	OBJECT_NAME columna en UNIFIED_AUDIT_TRAIL	El nombre del objeto afectado por la acción Un valor de muestra es employees .
objectType	string	OBJECT_SCHEMA columna en UNIFIED_AUDIT_TRAIL	El nombre del esquema del objeto afectado por la acción Un valor de muestra es hr.
paramList	Lista	SQL_BINDS columna en UNIFIED_AUDIT_TRAIL	La lista de variables de enlace, si las hay, asociadas con SQL_TEXT Un valor de muestra es parameter_1,parameter_2 .
pid	núme	OS_PROCESS columna en UNIFIED_AUDIT_TRAIL	Identificador de proceso del sistema operativo del proceso de base de datos de Oracle Un valor de muestra es 22396.

Campo	Tipo de datos	Fuente	Descripción
`remoteHost`	string	`AUTHENTICATION_TYPE` columna en `UNIFIED_AUDIT_TRAIL`	La dirección IP del cliente o el nombre del anfitrión desde el que se generó la sesión Un valor de muestra es `123.456.789.123` .
`remotePort`	string	`AUTHENTICATION_TYPE` columna en `UNIFIED_AUDIT_TRAIL`	Número de puerto del cliente. Un valor típico en entornos de Oracle Database es `1521`.
`rowCount`	núme	N/A	Este campo no se utiliza para RDS para Oracle y siempre es nulo.
`serverHost`	string	Anfitrión de base de datos	Dirección IP del anfitrión del servidor de base de datos. Un valor de muestra es `123.456.789.123` .
`serverType`	string	N/A	Tipo de servidor de base de datos. Este valor siempre es `ORACLE`.

Campo	Tipo de datos	Fuente	Descripción
`serverVersion`	string	Anfitrión de base de datos	La versión de Amazon RDS para Oracle, la actualización de versión (RU) y la revisión de actualización de versión (RUR) Un valor de muestra es `19.0.0.0.ru-2020-01.rur-2020-01.r1.EE.3` .
`serviceName`	string	Anfitrión de base de datos	Nombre del servicio de Un valor de muestra es `oracle-ee` .
`sessionId`	núme	`SESSIONID` columna en `UNIFIED_AUDIT_TRAIL`	El identificador de sesión de la auditoría Un ejemplo es: `1894327130` .
`startTime`	string	N/A	Este campo no se utiliza para RDS para Oracle y siempre es nulo.
`statementId`	núme	`STATEMENT_ID` columna en `UNIFIED_AUDIT_TRAIL`	ID numérico para cada instrucción ejecutada Una instrucción puede causar muchas acciones. Un valor de muestra es `142197`.
`substatementId`	N/A	N/A	Este campo no se utiliza para RDS para Oracle y siempre es nulo.

Campo	Tipo de datos	Fuente	Descripción
`transactionId`	string	`TRANSACTION_ID` columna en `UNIFIED_AUDIT_TRAIL`	El identificador de la transacción en la que se modifica el objeto Un valor de muestra es `02000800D5030000` .

Campos databaseActivityEventList para Amazon RDS para SQL Server

A continuación, encontrará campos `databaseActivityEventList` para Amazon RDS para SQL Server.

Campo	Tipo de datos	Fuente	Descripción
`class`	cadena	`sys.fn_get_audit_file.class_type` asignado a `sys.dm_audit_class_type_map.class_type_desc`	Clase de evento de actividad . Para obtener más información, consulte SQL Server Audit (Database Engine) (SQL Server Audit [motor de base de datos]) en la documentación de Microsoft SQL Server.
`clientApplication`	cadena	`sys.fn_get_audit_file.application_name`	La aplicación a la que se conecta el cliente según lo que informa el cliente (versión 14 y posteriores de SQL Server). Este campo es nulo en la versión 13 de SQL Server.
`command`	cadena	`sys.fn_get_audit_file.action_id` asignado a `sys.dm_audit_actions.name`	La categoría general de la instrucción SQL. El valor de este

Campo	Tipo de datos	Fuente	Descripción
			campo depende del valor de la clase.
commandText	cadena	sys.fn_get_audit_file.statement	Este campo indica la instrucción SQL.
databaseName	cadena	sys.fn_get_audit_file.database_name	Nombre de la base de datos.
dbProtocol	cadena	N/A	Protocolo de la base de datos. El valor es SQLSERVER .
dbUserName	cadena	sys.fn_get_audit_file.server_principal_name	El usuario de base de datos para la autenticación del cliente.
endTime	cadena	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.
engineNativeAuditFields	objeto	Cada campo de sys.fn_get_audit_file que no aparece en esta columna.	De forma predeterminada, este objeto está vacío. Cuando inicia el flujo de actividad con la opción --engine-native-audit-fields-included , este objeto incluye otros campos de auditoría del motor nativo que este mapa JSON no devuelve.
errorMessage	cadena	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.

Campo	Tipo de datos	Fuente	Descripción
exitCode	entero	sys.fn_get_audit_file.succeeded	Indica si la acción que inició el evento se realizó correctamente. Este campo no puede ser nulo. Para todos los eventos, excepto los eventos de inicio de sesión, este campo indica si la comprobación de permisos se realizó correctamente, pero no si la operación se realizó correctamente. Entre los valores se encuentran: • 0: fallo • 1: correcto
logTime	cadena	sys.fn_get_audit_file.event_time	Marca de tiempo del evento que registra SQL Server.
netProtocol	cadena	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.
objectName	cadena	sys.fn_get_audit_file.object_name	Nombre del objeto de base de datos si la instrucción SQL opera en un objeto.
objectType	cadena	sys.fn_get_audit_file.class_type asignado a sys.dm_audit_class_type_map.class_type_desc	Tipo de objeto de base de datos si la instrucción SQL opera en un tipo de objeto.

Campo	Tipo de datos	Fuente	Descripción
`paramList`	cadena	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.
`pid`	entero	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.
`remoteHost`	cadena	`sys.fn_get_audit_file.client_ip`	La dirección IP o el nombre de host del cliente que emitió la instrucción SQL (versión 14 y posteriores de SQL Server). Este campo es nulo en la versión 13 de SQL Server.
`remotePort`	entero	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.
`rowCount`	entero	`sys.fn_get_audit_file.affected_rows`	El número de filas de la tabla afectadas por la instrucción SQL (versión 14 y posteriores de SQL Server). Este campo está en la versión 13 de SQL Server.
`serverHost`	cadena	Host de base de datos	Dirección IP del servidor de base de datos del host.
`serverType`	cadena	N/A	Tipo de servidor de base de datos. El valor es `SQLSERVER` .

Campo	Tipo de datos	Fuente	Descripción
`serverVersion`	cadena	Host de base de datos	La versión del servidor de base de datos, por ejemplo, 15.00.4073.23.v1.R1 para SQL Server 2017.
`serviceName`	cadena	Host de base de datos	Nombre del servicio de Un valor de ejemplo es `sqlserver-ee` .
`sessionId`	entero	`sys.fn_get_audit_file.session_id`	Identificador único de la sesión.
`startTime`	cadena	N/A	Amazon RDS para SQL Server no utiliza este campo y el valor es nulo.
`statementId`	cadena	`sys.fn_get_audit_file.sequence_group_id`	Identificador único de la instrucción SQL del cliente. El identificador es diferente para cada evento que se genera. Un valor de muestra es `0x38eaf4156267184094bb82071aaab644` .
`substatementId`	entero	`sys.fn_get_audit_file.sequence_number`	Identificador para determinar el número de secuencia de una instrucción. Este identificador es útil cuando los registros grandes se dividen en varios registros.
`transactionId`	entero	`sys.fn_get_audit_file.transaction_id`	Identificador de una transacción. Si no hay ninguna transacción activa, el valor es cero.

Campo	Tipo de datos	Fuente	Descripción
`type`	cadena	Flujo de actividad de la base de datos generado	El tipo de evento. Los valores son `record` o `heartbeat` .

Procesamiento de un flujo de actividad de la base de datos mediante SDK de AWS

Puede procesar una secuencia de actividades mediante programación con AWS SDK. A continuación, mostramos ejemplos de Java y Python totalmente funcionales sobre cómo puede usar registros de flujos de actividad de la base de datos para la habilitación basada en instancias.

Java

```
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.net.InetAddress;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.Security;
import java.util.HashMap;
import java.util.List;
import java.util.Map;
import java.util.UUID;
import java.util.zip.GZIPInputStream;

import javax.crypto.Cipher;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.spec.SecretKeySpec;

import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoInputStream;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;
import
 com.amazonaws.services.kinesis.clientlibrary.exceptions.InvalidStateException;
```

```
import com.amazonaws.services.kinesis.clientlibrary.exceptions.ShutdownException;
import com.amazonaws.services.kinesis.clientlibrary.exceptions.ThrottlingException;
import com.amazonaws.services.kinesis.clientlibrary.interfaces.IRecordProcessor;
import
 com.amazonaws.services.kinesis.clientlibrary.interfaces.IRecordProcessorCheckpointer;
import
 com.amazonaws.services.kinesis.clientlibrary.interfaces.IRecordProcessorFactory;
import
 com.amazonaws.services.kinesis.clientlibrary.lib.worker.InitialPositionInStream;
import
 com.amazonaws.services.kinesis.clientlibrary.lib.worker.KinesisClientLibConfiguration;
import com.amazonaws.services.kinesis.clientlibrary.lib.worker.ShutdownReason;
import com.amazonaws.services.kinesis.clientlibrary.lib.worker.Worker;
import com.amazonaws.services.kinesis.clientlibrary.lib.worker.Worker.Builder;
import com.amazonaws.services.kinesis.model.Record;
import com.amazonaws.services.kms.AWSKMS;
import com.amazonaws.services.kms.AWSKMSClientBuilder;
import com.amazonaws.services.kms.model.DecryptRequest;
import com.amazonaws.services.kms.model.DecryptResult;
import com.amazonaws.util.Base64;
import com.amazonaws.util.IOUtils;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;
import com.google.gson.annotations.SerializedName;
import org.bouncycastle.jce.provider.BouncyCastleProvider;

public class DemoConsumer {

    private static final String STREAM_NAME = "aws-rds-das-[instance-external-
resource-id]"; // aws-rds-das-db-ABCD123456
    private static final String APPLICATION_NAME = "AnyApplication"; //unique
 application name for dynamo table generation that holds kinesis shard tracking
    private static final String AWS_ACCESS_KEY =
 "[AWS_ACCESS_KEY_TO_ACCESS_KINESIS]";
    private static final String AWS_SECRET_KEY =
 "[AWS_SECRET_KEY_TO_ACCESS_KINESIS]";
    private static final String RESOURCE_ID = "[external-resource-id]"; // db-
ABCD123456
    private static final String REGION_NAME = "[region-name]"; //us-east-1, us-
east-2...
    private static final BasicAWSCredentials CREDENTIALS = new
 BasicAWSCredentials(AWS_ACCESS_KEY, AWS_SECRET_KEY);
    private static final AWSStaticCredentialsProvider CREDENTIALS_PROVIDER = new
 AWSStaticCredentialsProvider(CREDENTIALS);
```

```
    private static final AwsCrypto CRYPTO = new AwsCrypto();
    private static final AWSKMS KMS = AWSKMSClientBuilder.standard()
            .withRegion(REGION_NAME)
            .withCredentials(CREDENTIALS_PROVIDER).build();

    class Activity {
        String type;
        String version;
        String databaseActivityEvents;
        String key;
    }

    class ActivityEvent {
        @SerializedName("class") String _class;
        String clientApplication;
        String command;
        String commandText;
        String databaseName;
        String dbProtocol;
        String dbUserName;
        String endTime;
        String errorMessage;
        String exitCode;
        String logTime;
        String netProtocol;
        String objectName;
        String objectType;
        List<String> paramList;
        String pid;
        String remoteHost;
        String remotePort;
        String rowCount;
        String serverHost;
        String serverType;
        String serverVersion;
        String serviceName;
        String sessionId;
        String startTime;
        String statementId;
        String substatementId;
        String transactionId;
        String type;
    }
```

```
   class ActivityRecords {
       String type;
       String clusterId; // note that clusterId will contain an empty string on RDS
Oracle and RDS SQL Server
       String instanceId;
       List<ActivityEvent> databaseActivityEventList;
   }

   static class RecordProcessorFactory implements IRecordProcessorFactory {
       @Override
       public IRecordProcessor createProcessor() {
           return new RecordProcessor();
       }
   }

   static class RecordProcessor implements IRecordProcessor {

       private static final long BACKOFF_TIME_IN_MILLIS = 3000L;
       private static final int PROCESSING_RETRIES_MAX = 10;
       private static final long CHECKPOINT_INTERVAL_MILLIS = 60000L;
       private static final Gson GSON = new
GsonBuilder().serializeNulls().create();

       private static final Cipher CIPHER;
       static {
           Security.insertProviderAt(new BouncyCastleProvider(), 1);
           try {
               CIPHER = Cipher.getInstance("AES/GCM/NoPadding", "BC");
           } catch (NoSuchAlgorithmException | NoSuchPaddingException |
NoSuchProviderException e) {
               throw new ExceptionInInitializerError(e);
           }
       }

       private long nextCheckpointTimeInMillis;

       @Override
       public void initialize(String shardId) {
       }

       @Override
       public void processRecords(final List<Record> records, final
IRecordProcessorCheckpointer checkpointer) {
```

```
            for (final Record record : records) {
                processSingleBlob(record.getData());
            }

            if (System.currentTimeMillis() > nextCheckpointTimeInMillis) {
                checkpoint(checkpointer);
                nextCheckpointTimeInMillis = System.currentTimeMillis() +
CHECKPOINT_INTERVAL_MILLIS;
            }
        }

        @Override
        public void shutdown(IRecordProcessorCheckpointer checkpointer,
ShutdownReason reason) {
            if (reason == ShutdownReason.TERMINATE) {
                checkpoint(checkpointer);
            }
        }

        private void processSingleBlob(final ByteBuffer bytes) {
            try {
                // JSON $Activity
                final Activity activity = GSON.fromJson(new String(bytes.array(),
StandardCharsets.UTF_8), Activity.class);

                // Base64.Decode
                final byte[] decoded =
Base64.decode(activity.databaseActivityEvents);
                final byte[] decodedDataKey = Base64.decode(activity.key);

                Map<String, String> context = new HashMap<>();
                context.put("aws:rds:db-id", RESOURCE_ID);

                // Decrypt
                final DecryptRequest decryptRequest = new DecryptRequest()

.withCiphertextBlob(ByteBuffer.wrap(decodedDataKey)).withEncryptionContext(context);
                final DecryptResult decryptResult = KMS.decrypt(decryptRequest);
                final byte[] decrypted = decrypt(decoded,
getByteArray(decryptResult.getPlaintext()));

                // GZip Decompress
                final byte[] decompressed = decompress(decrypted);
                // JSON $ActivityRecords
```

```
                final ActivityRecords activityRecords = GSON.fromJson(new
String(decompressed, StandardCharsets.UTF_8), ActivityRecords.class);

                // Iterate throught $ActivityEvents
                for (final ActivityEvent event :
activityRecords.databaseActivityEventList) {
                    System.out.println(GSON.toJson(event));
                }
            } catch (Exception e) {
                // Handle error.
                e.printStackTrace();
            }
        }

        private static byte[] decompress(final byte[] src) throws IOException {
            ByteArrayInputStream byteArrayInputStream = new
ByteArrayInputStream(src);
            GZIPInputStream gzipInputStream = new
GZIPInputStream(byteArrayInputStream);
            return IOUtils.toByteArray(gzipInputStream);
        }

        private void checkpoint(IRecordProcessorCheckpointer checkpointer) {
            for (int i = 0; i < PROCESSING_RETRIES_MAX; i++) {
                try {
                    checkpointer.checkpoint();
                    break;
                } catch (ShutdownException se) {
                    // Ignore checkpoint if the processor instance has been shutdown
(fail over).
                    System.out.println("Caught shutdown exception, skipping
checkpoint." + se);
                    break;
                } catch (ThrottlingException e) {
                    // Backoff and re-attempt checkpoint upon transient failures
                    if (i >= (PROCESSING_RETRIES_MAX - 1)) {
                        System.out.println("Checkpoint failed after " + (i + 1) +
"attempts." + e);
                        break;
                    } else {
                        System.out.println("Transient issue when checkpointing -
attempt " + (i + 1) + " of " + PROCESSING_RETRIES_MAX + e);
                    }
                } catch (InvalidStateException e) {
```

```
                    // This indicates an issue with the DynamoDB table (check for
table, provisioned IOPS).
                    System.out.println("Cannot save checkpoint to the DynamoDB table
used by the Amazon Kinesis Client Library." + e);
                    break;
                }
                try {
                    Thread.sleep(BACKOFF_TIME_IN_MILLIS);
                } catch (InterruptedException e) {
                    System.out.println("Interrupted sleep" + e);
                }
            }
        }
    }

    private static byte[] decrypt(final byte[] decoded, final byte[] decodedDataKey)
throws IOException {
        // Create a JCE master key provider using the random key and an AES-GCM
encryption algorithm
        final JceMasterKey masterKey = JceMasterKey.getInstance(new
SecretKeySpec(decodedDataKey, "AES"),
                "BC", "DataKey", "AES/GCM/NoPadding");
        try (final CryptoInputStream<JceMasterKey> decryptingStream =
CRYPTO.createDecryptingStream(masterKey, new ByteArrayInputStream(decoded));
             final ByteArrayOutputStream out = new ByteArrayOutputStream()) {
            IOUtils.copy(decryptingStream, out);
            return out.toByteArray();
        }
    }

    public static void main(String[] args) throws Exception {
        final String workerId = InetAddress.getLocalHost().getCanonicalHostName() +
":" + UUID.randomUUID();
        final KinesisClientLibConfiguration kinesisClientLibConfiguration =
                new KinesisClientLibConfiguration(APPLICATION_NAME, STREAM_NAME,
CREDENTIALS_PROVIDER, workerId);

kinesisClientLibConfiguration.withInitialPositionInStream(InitialPositionInStream.LATEST);
        kinesisClientLibConfiguration.withRegionName(REGION_NAME);
        final Worker worker = new Builder()
                .recordProcessorFactory(new RecordProcessorFactory())
                .config(kinesisClientLibConfiguration)
                .build();
```

```
        System.out.printf("Running %s to process stream %s as worker %s...\n",
 APPLICATION_NAME, STREAM_NAME, workerId);

        try {
            worker.run();
        } catch (Throwable t) {
            System.err.println("Caught throwable while processing data.");
            t.printStackTrace();
            System.exit(1);
        }
        System.exit(0);
    }

    private static byte[] getByteArray(final ByteBuffer b) {
        byte[] byteArray = new byte[b.remaining()];
        b.get(byteArray);
        return byteArray;
    }
}
```

Python

```
import base64
import json
import zlib
import aws_encryption_sdk
from aws_encryption_sdk import CommitmentPolicy
from aws_encryption_sdk.internal.crypto import WrappingKey
from aws_encryption_sdk.key_providers.raw import RawMasterKeyProvider
from aws_encryption_sdk.identifiers import WrappingAlgorithm, EncryptionKeyType
import boto3

REGION_NAME = '<region>'                    # us-east-1
RESOURCE_ID = '<external-resource-id>'      # db-ABCD123456
STREAM_NAME = 'aws-rds-das-' + RESOURCE_ID  # aws-rds-das-db-ABCD123456

enc_client =
 aws_encryption_sdk.EncryptionSDKClient(commitment_policy=CommitmentPolicy.FORBID_ENCRYPT_AL

class MyRawMasterKeyProvider(RawMasterKeyProvider):
    provider_id = "BC"

    def __new__(cls, *args, **kwargs):
```

```
        obj = super(RawMasterKeyProvider, cls).__new__(cls)
        return obj

    def __init__(self, plain_key):
        RawMasterKeyProvider.__init__(self)
        self.wrapping_key =
 WrappingKey(wrapping_algorithm=WrappingAlgorithm.AES_256_GCM_IV12_TAG16_NO_PADDING,
                                        wrapping_key=plain_key,
 wrapping_key_type=EncryptionKeyType.SYMMETRIC)

    def _get_raw_key(self, key_id):
        return self.wrapping_key


def decrypt_payload(payload, data_key):
    my_key_provider = MyRawMasterKeyProvider(data_key)
    my_key_provider.add_master_key("DataKey")
    decrypted_plaintext, header = enc_client.decrypt(
        source=payload,

 materials_manager=aws_encryption_sdk.materials_managers.default.DefaultCryptoMaterialsManag
    return decrypted_plaintext


def decrypt_decompress(payload, key):
    decrypted = decrypt_payload(payload, key)
    return zlib.decompress(decrypted, zlib.MAX_WBITS + 16)


def main():
    session = boto3.session.Session()
    kms = session.client('kms', region_name=REGION_NAME)
    kinesis = session.client('kinesis', region_name=REGION_NAME)

    response = kinesis.describe_stream(StreamName=STREAM_NAME)
    shard_iters = []
    for shard in response['StreamDescription']['Shards']:
        shard_iter_response = kinesis.get_shard_iterator(StreamName=STREAM_NAME,
 ShardId=shard['ShardId'],

 ShardIteratorType='LATEST')
        shard_iters.append(shard_iter_response['ShardIterator'])

    while len(shard_iters) > 0:
```

```
        next_shard_iters = []
        for shard_iter in shard_iters:
            response = kinesis.get_records(ShardIterator=shard_iter, Limit=10000)
            for record in response['Records']:
                record_data = record['Data']
                record_data = json.loads(record_data)
                payload_decoded =
 base64.b64decode(record_data['databaseActivityEvents'])
                data_key_decoded = base64.b64decode(record_data['key'])
                data_key_decrypt_result =
 kms.decrypt(CiphertextBlob=data_key_decoded,

 EncryptionContext={'aws:rds:db-id': RESOURCE_ID})
                print (decrypt_decompress(payload_decoded,
 data_key_decrypt_result['Plaintext']))
            if 'NextShardIterator' in response:
                next_shard_iters.append(response['NextShardIterator'])
        shard_iters = next_shard_iters


if __name__ == '__main__':
    main()
```

Ejemplos de políticas de IAM para flujos de actividad de base de datos

Cualquier usuario que tenga privilegios de rol de AWS Identity and Access Management (IAM) apropiados para los flujos de actividad de la base de datos puede crear, iniciar, detener y modificar la configuración del flujo de actividad de una instancia de base de datos. Estas acciones se incluyen en el registro de auditoría de la secuencia. Como práctica recomendada de cumplimiento, le recomendamos que no proporcione estos privilegios a los DBA.

Establezca el acceso a las secuencias de actividades de base de datos mediante políticas IAM. Para obtener más información acerca de la autenticación de Amazon RDS, consulte Administración de la identidad y el acceso en Amazon RDS. Para obtener más información sobre la creación de políticas de IAM, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM.

Example Política para permitir configurar secuencias de actividades de la base de datos

Para dar a los usuarios un acceso detallado con el fin de modificar flujos de actividad, utilice las claves de contexto de operación específica del servicio `rds:StartActivityStream` y

`rds:StopActivityStream` de una política de IAM. En el siguiente ejemplo de política de IAM el usuario o rol pueden configurar secuencias de actividades.

```
{
   "Version":"2012-10-17",
   "Statement":[
        {
            "Sid":"ConfigureActivityStreams",
            "Effect":"Allow",
            "Action": [
                "rds:StartActivityStream",
                "rds:StopActivityStream"
            ],
            "Resource":"*",
          }
     ]
}
```

Example Política para permitir iniciar secuencias de actividades de la base de datos

En el siguiente ejemplo de política de IAM el usuario o rol pueden iniciar secuencias de actividades.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowStartActivityStreams",
            "Effect":"Allow",
            "Action":"rds:StartActivityStream",
            "Resource":"*"
        }
    ]
}
```

Example Política para permitir detener secuencias de actividades de la base de datos

En el siguiente ejemplo de política de IAM el usuario o rol pueden detener secuencias de actividades.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
```

```
            "Sid":"AllowStopActivityStreams",
            "Effect":"Allow",
            "Action":"rds:StopActivityStream",
            "Resource":"*"
        }
     ]
}
```

Example Política para rechazar iniciar secuencias de actividades de la base de datos

En el siguiente ejemplo de política de IAM se evita que un usuario o rol inicie secuencias de actividades.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"DenyStartActivityStreams",
            "Effect":"Deny",
            "Action":"rds:StartActivityStream",
            "Resource":"*"
        }
     ]
}
```

Example Política para rechazar la detención de secuencias de actividades de la base de datos

En el siguiente ejemplo de política de IAM se evita que un usuario o rol detenga secuencias de actividades.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"DenyStopActivityStreams",
            "Effect":"Deny",
            "Action":"rds:StopActivityStream",
            "Resource":"*"
        }
    ]
}
```

Supervisión de amenazas con Amazon GuardDuty para protección de RDS

Amazon GuardDuty es un servicio de detección de amenazas que ayuda a proteger las cuentas, los contenedores, las cargas de trabajo y los datos de su entorno de AWS. Mediante modelos de machine learning (ML) y capacidades de detección de anomalías y amenazas, GuardDuty supervisa continuamente los diferentes orígenes de registro y la actividad en tiempo de ejecución para identificar y priorizar los posibles riesgos de seguridad y actividades maliciosas en su entorno.

GuardDuty para protección de RDS analiza y perfila los eventos de inicio de sesión para detectar posibles amenazas de acceso a sus bases de datos de Amazon RDS. Al activar Protección de RDS, GuardDuty consume los eventos de inicio de sesión de RDS de sus bases de datos de RDS. RDS Protection supervisa estos eventos y los perfila para detectar posibles amenazas internas o agentes externos.

Para obtener más información sobre la forma de habilitar la protección de RDS de Amazon GuardDuty, consulte GuardDuty RDS Protection (Protección de RDS de Amazon GuardDuty) en la Guía del usuario de Amazon GuardDuty.

Cuando RDS Protection detecta una amenaza potencial, como un patrón inusual de intentos de inicio de sesión con éxito o fallidos, GuardDuty genera un nuevo hallazgo con detalles sobre la base de datos potencialmente comprometida. Puede ver los detalles de los resultados en la sección de resumen de los resultados de la consola de Amazon GuardDuty. Los detalles de los resultados varían según el tipo de resultado. Los detalles principales, el tipo de recurso y el rol del recurso determinan el tipo de información disponible para cualquier resultado. Para obtener más información sobre los detalles más comunes disponibles en los resultados y los tipos de resultados, consulte Finding details (Detalles de resultados) y GuardDuty RDS Protection (Protección de RDS de GuardDuty) respectivamente, en la Guía del usuario de Amazon GuardDuty.

Puede activar o desactivar la característica de protección RDS para cualquier Cuenta de AWS en cualquier Región de AWS donde esté disponible. Cuando Protección de RDS no está habilitado, GuardDuty no detecta las bases de datos de RDS que puedan estar comprometidas ni proporciona detalles sobre el problema.

Una cuenta de GuardDuty existente puede habilitar la protección de RDS con un periodo de prueba de 30 días. En una cuenta nueva de GuardDuty, la protección de RDS ya está habilitada e incluida en el periodo de prueba gratuito de 30 días. Para obtener más información, consulte Estimating GuardDuty cost (Cálculo del coste de GuardDuty) en la Guía del usuario de Amazon GuardDuty.

Para obtener información sobre las Regiones de AWS en las que GuardDuty aún no admite la protección de RDS, consulte Disponibilidad de características específicas para cada región en la Guía del usuario de Amazon GuardDuty.

Para obtener información sobre las versiones de la base de datos de RDS compatibles con GuardDuty RDS Protection, consulte Bases de datos ilimitadas compatibles con Amazon Aurora, Amazon RDS y Aurora en la Guía del usuario de Amazon GuardDuty.

Amazon RDS Custom

Amazon RDS Custom automatiza las tareas y las operaciones de administración de bases de datos. RDS Custom permite que, como administrador de bases de datos, pueda acceder y personalizar el entorno de base de datos y el sistema operativo. Con RDS Custom, puede personalizarlo para cumplir con los requisitos de las aplicaciones heredadas, personalizadas y empaquetadas.

Para ver los webinars y blogs más recientes sobre RDS Custom, consulte Amazon RDS Custom resources (Recursos de Amazon RDS Custom).

Temas

- Abordar el desafío de la personalización de la base de datos
- Modelo de administración y ventajas de Amazon RDS Custom
- Arquitectura de Amazon RDS Custom
- Seguridad de Amazon RDS Custom
- Trabajar con RDS Custom for Oracle
- Trabajar con RDS Custom for SQL Server

Abordar el desafío de la personalización de la base de datos

Amazon RDS Custom aporta los beneficios de Amazon RDS a un mercado que no puede pasar fácilmente a un servicio completamente administrado debido a las personalizaciones requeridas con aplicaciones de terceros. Amazon RDS Custom ahorra tiempo administrativo, es permanente y es escalable según su empresa.

Si necesita que toda la base de datos y el sistema operativo estén completamente administrados porAWS, recomendamos Amazon RDS. Si necesita derechos administrativos sobre la base de datos y el sistema operativo subyacente para que las aplicaciones dependientes estén disponibles, Amazon RDS Custom es la mejor opción. Si desea una plena responsabilidad de administración y simplemente necesita un servicio de computación administrado, la mejor opción es administrar automáticamente sus bases de datos comerciales en Amazon EC2.

Para ofrecer una experiencia de servicio administrado, Amazon RDS no permite acceder al host subyacente. Amazon RDS también restringe el acceso a ciertos procedimientos y objetos del sistema que requieren privilegios avanzados. Sin embargo, para algunas aplicaciones, es posible que deba realizar operaciones como usuario del sistema operativo (SO) con privilegios.

Por ejemplo, es probable que deba realizar algunas de las siguientes tareas:

- Instalar revisiones y paquetes personalizados de bases de datos y SO.
- Configurar ajustes de base de datos específicos.
- Configurar archivos del sistema para compartir archivos directamente con sus aplicaciones.

Anteriormente, si necesitaba personalizar la aplicación, tenía que implementar la base de datos en las instalaciones o en Amazon EC2. En este caso, asume la mayor parte o la totalidad de la responsabilidad de la administración de las bases de datos, tal como se resume en la siguiente tabla.

Característica	Responsabilidad en las instalaciones	Responsabilidad de Amazon EC2	Responsabilidad de Amazon RDS
Optimización de aplicaciones	Cliente	Cliente	Cliente
Escalado	Cliente	Cliente	AWS
Alta disponibilidad	Cliente	Cliente	AWS
Copias de seguridad de bases de datos	Cliente	Cliente	AWS
Revisiones de software de base de datos	Cliente	Cliente	AWS
Instalación de software de base de datos	Cliente	Cliente	AWS
Revisiones de sistema operativo	Cliente	Cliente	AWS
Instalación del sistema operativo	Cliente	Cliente	AWS

Característica	Responsabilidad en las instalaciones	Responsabilidad de Amazon EC2	Responsabilidad de Amazon RDS
Mantenimiento de servidores	Cliente	AWS	AWS
Ciclo de vida del hardware	Cliente	AWS	AWS
Alimentación, red y refrigeración	Cliente	AWS	AWS

Cuando administra el software de base de datos por su cuenta, obtiene más control, pero también es más propenso a los errores del usuario. Por ejemplo, cuando hace cambios de forma manual, podría provocar por accidente el tiempo de inactividad de la aplicación. Es posible que pase horas verificando cada cambio para identificar y solucionar un problema. Idealmente, desea un servicio de base de datos administrada que automatice las tareas comunes de DBA, pero que también admita el acceso privilegiado a la base de datos y al sistema operativo subyacente.

Modelo de administración y ventajas de Amazon RDS Custom

Amazon RDS Custom es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. RDS Custom automatiza la configuración, el funcionamiento y el escalado de las bases de datos en la Nube de AWS al tiempo que le otorga acceso a la base de datos y al sistema operativo subyacente. Con este acceso, puede configurar los ajustes, instalar revisiones y habilitar características nativas para cumplir con los requisitos de la aplicación dependiente. Con RDS Custom, puede ejecutar la carga de trabajo de la base de datos mediante la AWS Management Console o AWS CLI.

RDS Custom solo admite los motores Oracle Database y Microsoft SQL Server.

Temas

- Modelo de responsabilidad compartida en RDS Custom
- Configuraciones no compatibles y compatibilidad perimetral de RDS Custom
- Beneficios clave de RDS Custom

Modelo de responsabilidad compartida en RDS Custom

Con RDS Custom, utiliza las características administradas de Amazon RDS, pero administra el host y personaliza el sistema operativo como lo hace en Amazon EC2. Asume responsabilidades adicionales de administración de bases de datos más allá de lo que hace en Amazon RDS. El resultado es que tiene más control sobre la administración de bases de datos e instancias de base de datos que en Amazon RDS y, al mismo tiempo, se beneficia de la automatización de RDS.

La responsabilidad compartida significa lo siguiente:

1. Cuando utiliza una característica de RDS Custom es dueño de parte del proceso.

   Por ejemplo, en RDS Custom para Oracle, usted controla qué parches de bases de datos de Oracle utilizar y cuándo aplicarlos a sus instancias de base de datos.
2. Usted es responsable de asegurarse de que cualquier personalización de las características de RDS Custom funcione correctamente.

   Para ayudar a proteger frente a personalizaciones no válidas, RDS Custom cuenta con un software de automatización que se ejecuta fuera de la instancia de base de datos. Si la instancia de Amazon EC2 subyacente se deteriora, RDS Custom intenta resolver estos problemas automáticamente reiniciando o reemplazando la instancia EC2. El único cambio visible para el usuario es una nueva dirección IP. Para obtener más información, consulte Sustitución del host de Amazon RDS Custom.

En la siguiente tabla se detalla el modelo de responsabilidad compartida para distintas características de RDS Custom.

Característica	Responsabilidad de Amazon EC2	Responsabilidad de Amazon RDS	Responsabilidad de RDS Custom for Oracle	Responsabilidad de RDS Custom for SQL Server
Optimización de aplicaciones	Cliente	Cliente	Cliente	Cliente
Escalado	Cliente	AWS	Compartido	Compartido
Alta disponibilidad	Cliente	AWS	AWS	AWS

Característica	Responsabilidad de Amazon EC2	Responsabilidad de Amazon RDS	Responsabilidad de RDS Custom for Oracle	Responsabilidad de RDS Custom for SQL Server
Copias de seguridad de bases de datos	Cliente	AWS	Compartido	AWS
Revisiones de software de base de datos	Cliente	AWS	Compartido	AWS para RPEV, cliente para CEV[1]
Instalación de software de base de datos	Cliente	AWS	Compartido	AWS para RPEV, cliente para CEV[1]
Revisiones de sistema operativo	Cliente	AWS	Cliente	AWS para RPEV, cliente para CEV[1]
Instalación del sistema operativo	Cliente	AWS	Compartido	AWS
Mantenimiento de servidores	AWS	AWS	AWS	AWS
Ciclo de vida del hardware	AWS	AWS	AWS	AWS
Alimentación, red y refrigeración	AWS	AWS	AWS	AWS

1 Una versión de motor personalizada (CEV) es una instantánea de volumen binario de una versión de base de datos y una Imagen de máquina de Amazon (AMI). Una versión del motor proporcionada por RDS (RPEV) es la imagen de máquina de Amazon (AMI) predeterminada y la instalación de Microsoft SQL Server.

Puede crear una instancia de base de datos de RDS Custom mediante Microsoft SQL Server. En este caso:

- Puede elegir entre dos modelos de licencia: licencia incluida (LI) y Bring Your Own Media (BYOM).
- Con LI. no es necesario que compre por su cuenta licencias de SQL Server. AWS ya es titular de la licencia del software de base de datos de SQL Server.
- Con BYOM, usted proporciona e instala sus propios binarios y licencias de Microsoft SQL Server.

Puede crear una instancia de base de datos personalizada de RDS mediante Oracle Database. En este caso, haga lo siguiente:

- Administre sus propios medios.

  Al utilizar RDS Custom, cargue sus propios archivos de instalación de bases de datos y revisiones. Puede crear una versión de motor personalizada (CEV) a partir de estos archivos. A continuación, puede crear una instancia de base de datos de RDS Custom con este CEV.
- Administrar sus propias licencias.

  Trae sus propias licencias de Oracle Database y administra las licencias usted mismo.

Configuraciones no compatibles y compatibilidad perimetral de RDS Custom

RDS Custom proporciona una capacidad de monitoreo denominada perímetro de soporte. Esta característica garantiza que el entorno de host y base de datos estén configurados correctamente. Si realiza un cambio que provoca que la instancia de base de datos quede fuera del perímetro de soporte, RDS Custom cambia el estado de la instancia a `unsupported-configuration` hasta que solucione manualmente los problemas de configuración. Para obtener más información, consulte Perímetro de soporte de RDS Custom.

Beneficios clave de RDS Custom

Con RDS Custom puede hacer lo siguiente:

- Automatizar muchas de las mismas tareas administrativas de Amazon RDS, incluidas las siguientes:
  - Administración del ciclo de vida de bases de datos

  - Copias de seguridad automatizadas y recuperación a un momento dado (PITR)
  - Monitorización del estado de las instancias de base de datos de RDS Custom y observación de cambios en la infraestructura, el sistema operativo y los procesos de bases de datos
  - Notificación o acción para solucionar problemas en función de la interrupción de la instancia de base de datos
- Instale aplicaciones de terceros.

  Puede instalar software para ejecutar aplicaciones y agentes personalizados. Dado que tiene acceso privilegiado al host, puede modificar los sistemas de archivos para admitir aplicaciones heredadas.
- Instale revisiones personalizadas.

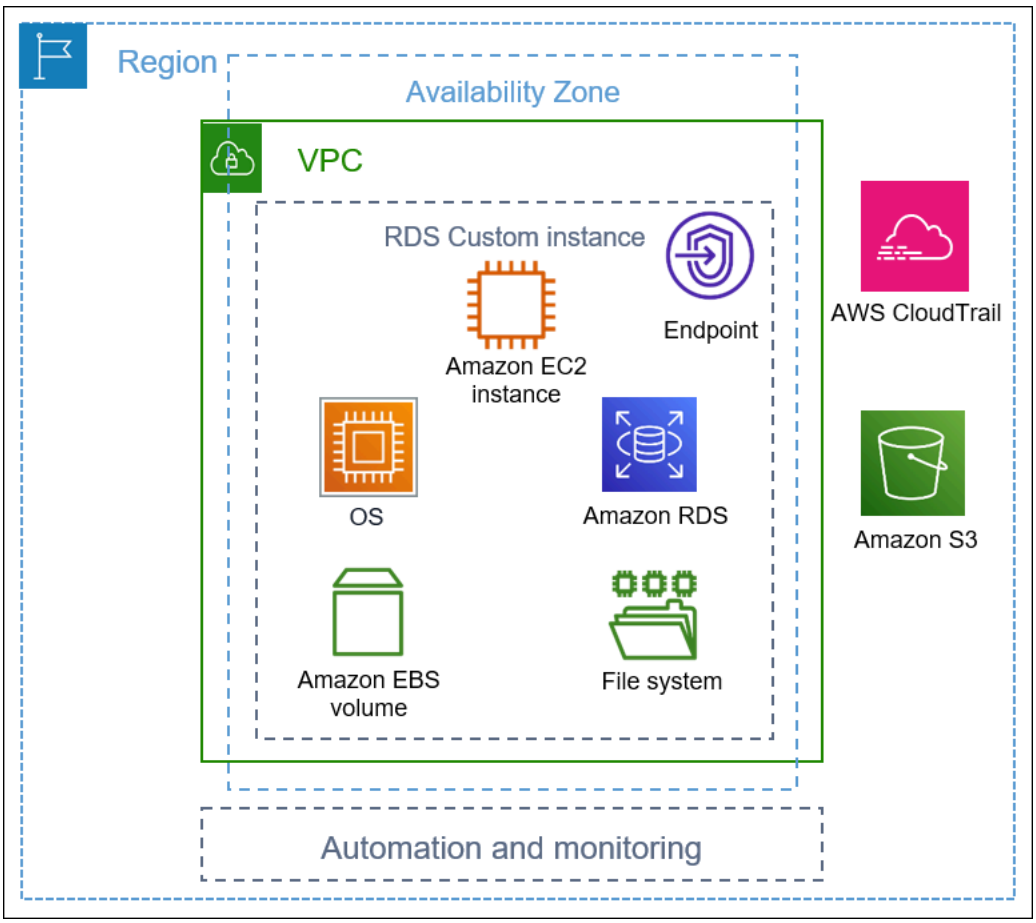
  Puede aplicar revisiones de base de datos personalizadas o modificar paquetes de SO en las instancias de base de datos de RDS Custom.
- Elabore una base de datos en las instalaciones antes de moverla a un servicio completamente administrado.

  Si administra su propia base de datos en las instalaciones, puede organizar la base de datos en RDS Custom tal cual. Después de familiarizarse con el entorno de nube, puede migrar su base de datos a una instancia de base de datos de Amazon RDS completamente administrada.
- Crear su propia automatización.

  Puede crear, programar y ejecutar scripts de automatización personalizados para herramientas de generación de informes, administración o diagnóstico.

Arquitectura de Amazon RDS Custom

La arquitectura de Amazon RDS Custom se basa en Amazon RDS, con diferencias importantes. En el siguiente diagrama se muestran los componentes clave de la arquitectura de RDS Custom.



Temas

- VPC
- Automatización y monitoreo personalizados de RDS
- Amazon S3
- AWS CloudTrail

VPC

Al igual que en Amazon RDS, la instancia de base de datos de RDS Custom reside en una nube virtual privada (VPC).



La instancia de base de datos de RDS Custom consta de los siguientes componentes:

- Instancia de Amazon EC2
- Punto de conexión de instancia
- Sistema operativo instalado en la instancia de Amazon EC2
- Almacenamiento de Amazon EBS, que contiene sistemas de archivos adicionales

Automatización y monitoreo personalizados de RDS

RDS Custom tiene software de automatización que se ejecuta fuera de la instancia de base de datos. Este software se comunica con los agentes de la instancia de base de datos y con otros componentes del entorno de RDS Custom en general.

Las características de monitoreo y recuperación de RDS Custom ofrecen una funcionalidad similar a la de Amazon RDS. De forma predeterminada, RDS Custom está en modo de automatización completa. El software de automatización tiene las siguientes responsabilidades principales:

- Recopilar métricas y enviar notificaciones
- Hacer recuperación automática de instancias

Una responsabilidad importante de la automatización de RDS Custom es responder a los problemas de su instancia de Amazon EC2. Por varios motivos, el host podría verse afectado o inaccesible. Para resolver estos problemas, RDS Custom reinicia o reemplaza la instancia de Amazon EC2.

Temas

- Sustitución del host de Amazon RDS Custom
- Perímetro de soporte de RDS Custom

Sustitución del host de Amazon RDS Custom

Si el host de Amazon EC2 se ve afectado, RDS Custom intenta reiniciarlo. Si hay errores en este esfuerzo, RDS Custom utiliza la misma característica para detención e inicio incluida en Amazon EC2. El único cambio visible por el cliente cuando se reemplaza un host es una nueva dirección IP pública.

Temas

- Detención e inicio del host
- Efectos de la sustitución del host
- Las prácticas recomendadas de Amazon EC2

Detención e inicio del host

RDS Custom efectúa automáticamente los siguientes pasos, sin necesidad de intervención del usuario:

1. Detiene el host de Amazon EC2.

   La instancia EC2 se cierre de forma normal y deja de ejecutarse. Los volúmenes de Amazon EBS siguen adjuntos a la instancia y sus datos persisten. Se pierden los datos almacenados en los volúmenes del almacén de instancias (no compatibles con RDS Custom) o la RAM del ordenador del host.

   Para obtener más información, consulte Detener e iniciar la instancia en la Guía del usuario de Amazon EC2.
2. Inicia el host de Amazon EC2.

   La instancia EC2 migra a un nuevo hardware del host subyacente. En algunos casos, la instancia de base de datos de RDS Custom permanece en el host original.

Efectos de la sustitución del host

En RDS Custom, tiene control total sobre el volumen de dispositivo raíz y los volúmenes de almacenamiento de Amazon EBS. El volumen raíz puede contener datos y configuraciones importantes que no quiere perder.

RDS Custom for Oracle conserva todos los datos de los clientes y la base de datos después de la operación, entre los que se incluyen los datos del volumen raíz. No se requiere intervención de los usuarios. En RDS Custom para SQL Server, se retienen los datos de la base de datos, pero se pierden todos los datos de la unidad `C:`, entre los que se incluyen los datos del sistema operativo y del cliente.

Tras el proceso de sustitución del host, el host de Amazon EC2 tiene una nueva dirección IP pública. El nuevo host conserva los datos y los metadatos que se muestran en la siguiente tabla.

Metadatos o datos	Retención de RDS Custom para Oracle	Retención de RDS Custom para SQL Server
ID de instancia de EC2	Sí	No
Metadatos de la instancia de EC2	Sí	Sí
Los datos del volumen de almacenamiento de datos	Sí	Sí
Datos del volumen raíz	Sí	No
Direcciones IP privadas	Sí	Sí
Direcciones IP elásticas	Sí	Sí

Las prácticas recomendadas de Amazon EC2

La característica de reemplazo de host de Amazon EC2 cubre la mayoría de los escenarios de deterioro de Amazon EC2. Recomendamos que siga las siguientes prácticas recomendadas:

- Antes de cambiar la configuración o el sistema operativo, haga una copia de seguridad de los datos. Si el volumen raíz o el sistema operativo se dañan, la sustitución del host no podrá

repararlo. Las únicas opciones son la restauración a partir de una instantánea de base de datos o una recuperación a un momento dado.

- No detenga ni termine manualmente el host físico de Amazon EC2. Ambas acciones hacen que la instancia se sitúe fuera del perímetro de soporte de RDS Custom.
- (RDS Custom for SQL Server) Si adjunta volúmenes adicionales al host de Amazon EC2, configúrelos para que se vuelvan a subir al reiniciar. Si el host está dañado, RDS Custom podría detenerlo e iniciarlo automáticamente.

Perímetro de soporte de RDS Custom

RDS Custom proporciona una capacidad de monitoreo adicional denominada perímetro de soporte. Este monitoreo adicional garantiza que la instancia de base de datos de RDS Custom utilice infraestructura, sistema operativo y base de datos compatibles con AWS.

El perímetro de soporte comprueba que la instancia de base de datos se ajuste a los requisitos que se indican en Corrección de configuraciones no compatibles en RDS Custom para Oracle y Corrección de configuraciones no compatibles en RDS Custom para SQL Server. Si no se cumple alguno de estos requisitos, RDS Custom considera que la instancia de base de datos está fuera del perímetro de soporte.

Temas

- Configuraciones no admitidas en RDS Custom
- Solución de problemas de configuraciones no admitidas

Configuraciones no admitidas en RDS Custom

Cuando la instancia de base de datos se ve fuera del perímetro de soporte, RDS Custom cambia el estado de la instancia de datos a `unsupported-configuration` y envía notificaciones de eventos. Después de solucionar los problemas de configuración, RDS Custom cambia el estado de la instancia de base de datos a `available`.

Mientras la instancia de base de datos se encuentra en el estado `unsupported-configuration`, se cumple lo siguiente:

- Se puede acceder a su base de datos. La excepción es cuando la instancia de datos está en el estado `unsupported-configuration` porque la base de datos se apagó inesperadamente.
- No puede modificar la instancia de base de datos.

- No puede tomar instantáneas de base de datos.
- No se crean copias de seguridad de forma automática.
- Solo para las instancias de dase de datos de RDS Custom para SQL Server, RDS Custom no sustituye a la instancia de Amazon EC2 subyacente si se ve dañada. Para obtener más información sobre las sustituciones del host, consulte Sustitución del host de Amazon RDS Custom.
- Puede eliminar la instancia de base de datos, pero la mayoría de las demás operaciones de la API de RDS Custom no estarán disponibles.
- RDS Custom sigue admitiendo la recuperación en un momento dado (PITR) al archivar los archivos de registro REDO y cargarlos a Amazon S3. La PITR en un estado `unsupported-configuration` difiere de las siguientes maneras:
  - La PITR puede tardar mucho tiempo en restaurarse por completo en una nueva instancia de base de datos de RDS Custom. Esta situación se produce porque no puede tomar instantáneas automatizadas ni manuales mientras la instancia de base de datos se encuentre en el estado `unsupported-configuration`.
  - La recuperación a un momento dado tiene que volver a reproducir más registros de recuperación de cambios a partir de la instantánea más reciente tomada antes de que la instancia ingresara al estado `unsupported-configuration`.
  - En algunos casos, la instancia de base de datos se encuentra en el estado `unsupported-configuration` porque realizó un cambio que impidió cargar los archivos de registro REDO archivados. Algunos ejemplos son detener la instancia EC2, detener el agente de RDS Custom y desconectar los volúmenes de EBS. En estos casos, la PITR no puede restaurar la instancia de base de datos al último momento restaurable.

Solución de problemas de configuraciones no admitidas

RDS Custom proporciona una guía de solución de problemas para el estado `unsupported-configuration`. Aunque algunas directrices se aplican tanto a RDS Custom para Oracle como a RDS Custom para SQL Server, otras dependen del motor de la base de datos. Para obtener información sobre la solución de problemas específicos del motor, consulte los siguientes temas:

- Corrección de configuraciones no compatibles en RDS Custom para Oracle
- Corrección de configuraciones no compatibles en RDS Custom para SQL Server

Amazon S3

Si utiliza RDS Custom for Oracle, cargará los medios de instalación en un bucket de Amazon S3 creado por el usuario. RDS Custom for Oracle utiliza el medio de este bucket para crear una versión de motor personalizada (CEV). Una CEV es una instantánea de volumen binario de una versión de base de datos y una Amazon Machine Image (AMI). Desde el CEV, puede crear una instancia de base de datos de RDS Custom. Para obtener más información, consulte Trabajar con versiones de motor personalizadas para Amazon RDS Custom for Oracle.

Tanto para RDS Custom for Oracle como para RDS Custom for SQL Server, RDS Custom crea automáticamente un bucket de Amazon S3 con el prefijo de la cadena `do-not-delete-rds-custom-`. RDS Custom utiliza el bucket de S3 `do-not-delete-rds-custom-` para almacenar los siguientes tipos de archivos:

- Registros de AWS CloudTrail para el rastro creado por RDS Custom
- Artefactos perimetrales de compatibilidad (consulte Perímetro de soporte de RDS Custom)
- Archivos de registro de recuperación de cambios de bases de datos (solo para RDS Custom for Oracle)
- Registros de transacciones (solo para RDS Custom for SQL Server)
- Artefactos de versión de motor personalizados (solo para RDS Custom for Oracle)

RDS Custom crea el bucket de S3 `do-not-delete-rds-custom-` al crear cualquiera de los siguientes recursos:

- Su primer CEV for RDS Custom for Oracle
- La primera instancia de base de datos para RDS Custom for SQL Server

RDS Custom crea un bucket para cada combinación de lo siguiente:

- ID de Cuenta de AWS
- Tipo de motor (ya sea de RDS Custom for Oracle o RDS Custom for SQL Server)
- Región de AWS

Por ejemplo, si crea RDS Custom for Oracle CEVs en una única Región de AWS, existe un bucket `do-not-delete-rds-custom-`. Si crea varias instancias de RDS Custom para SQL Server y residen en diferentes Regiones de AWS, existe un bucket `do-not-delete-rds-custom-` en

cada Región de AWS. Si crea una instancia de RDS Custom para Oracle y dos instancias de RDS Custom para SQL Server en una única Región de AWS, existen dos buckets `do-not-delete-rds-custom-`.

AWS CloudTrail

RDS Custom crea automáticamente un rastro de AWS CloudTrail cuyo nombre empieza por `do-not-delete-rds-custom-`. El perímetro de soporte personalizado de RDS se basa en los eventos de CloudTrail para determinar si sus acciones afectan a la automatización de RDS Custom. Para obtener más información, consulte Solución de problemas de configuraciones no admitidas.

RDS Custom creará el rastro cuando cree su primera instancia de base de datos. RDS Custom crea un rastro para cada combinación de lo siguiente:

- ID de Cuenta de AWS
- Tipo de motor (ya sea de RDS Custom for Oracle o RDS Custom for SQL Server)
- Región de AWS

Al eliminar una instancia de base de datos de RDS Custom el CloudTrail de esta instancia no se elimina automáticamente. En este caso, se sigue facturando a su Cuenta de AWS el CloudTrail no eliminado. RDS Custom no se hace responsable de la eliminación de este recurso. Para obtener información sobre cómo eliminar el CloudTrail manualmente, consulte Eliminar una ruta en la Guía del usuario de AWS CloudTrail.

Seguridad de Amazon RDS Custom

Familiarícese con los aspectos de seguridad de RDS Custom.

Para obtener más información sobre la seguridad de RDS Custom, consulte los temas siguientes.

- Protección de su bucket de Amazon S3 contra el problema del suplente confuso
- Rotación de credenciales de RDS Custom para Oracle para programas de conformidad

Cómo gestiona RDS Custom las tareas en su nombre de forma segura

RDS Custom utiliza las siguientes herramientas y técnicas para ejecutar operaciones en su nombre de forma segura:

Rol vinculado al servicio AWSServiceRoleForRDSCustom

Un rol vinculado al servicio está predefinido por el servicio e incluye todos los permisos que requiere el servicio para llamar a otros Servicios de AWS en su nombre. Para RDS Custom, `AWSServiceRoleForRDSCustom` es un rol vinculado al servicio que se define según el principio del privilegio mínimo. RDS Custom utiliza los permisos de `AmazonRDSCustomServiceRolePolicy`, que es la política adjunta a este rol, para realizar la mayoría de las tareas de aprovisionamiento y de administración fuera del host. Para obtener más información, consulte AmazonRDSCustomServiceRolePolicy.

Cuando realiza tareas en el host, la automatización de RDS Custom utiliza las credenciales del rol vinculado al servicio para ejecutar los comandos mediante AWS Systems Manager. Puede auditar el historial de comandos a través del historial de comandos de Systems Manager y AWS CloudTrail. Systems Manager se conecta a su instancia de base de datos de RDS Custom mediante la configuración de red. Para obtener más información, consulte Paso 4: configurar IAM para RDS Custom for Oracle.

Credenciales de IAM temporales

Al aprovisionar o eliminar recursos, RDS Custom a veces utiliza credenciales temporales derivadas de las credenciales de la entidad principal de la IAM que llama. Estas credenciales de la IAM están restringidas por las políticas de IAM adjuntas a esa entidad principal y caducan una vez finalizada la operación. Para obtener más información sobre los permisos necesarios para las entidades principales de IAM que utilizan RDS Custom, consulte Paso 5: otorgar los permisos necesarios al rol o usuario de IAM.

Perfil de instancia de Amazon EC2

Un perfil de instancia de EC2 es un contenedor de un rol de IAM, que puede utilizar para transferir información del rol a una instancia de EC2. Una instancia de EC2 subyace a una instancia de base de datos de RDS Custom. Debe proporcionar un perfil de instancia al crear una instancia de base de datos de RDS Custom. RDS Custom utiliza las credenciales del perfil de instancia de EC2 cuando realiza tareas de administración basadas en el host, como las copias de seguridad. Para obtener más información, consulte Cree manualmente el rol de IAM y el perfil de instancias.

Par de claves SSH

Cuando RDS Custom crea la instancia de EC2 que subyace a una instancia de base de datos, crea un par de claves SSH en su nombre. La clave usa el prefijo del nombre `do-not-delete-rds-custom-ssh-privatekey-db-` o `rds-custom!oracle-do-not-delete-`*`db_resource_id-uuid`*`-ssh-privatekey`. AWS Secrets Manager almacena la clave privada SSH como secreto en la Cuenta de AWS. Amazon RDS no almacena, accede ni usa estas credenciales. Para obtener más información, consulte Pares de claves de Amazon EC2 e instancias Linux.

Certificados de SSL

Las instancias de bases de datos de RDS Custom no admiten certificados SSL administrados. Si desea implementar SSL, puede administrar automáticamente los certificados SSL en su propia cartera y crear un oyente de SSL para proteger las conexiones entre la base de datos del cliente o para la replicación de la base de datos. Para obtener más información, consulte Configuring Transport Layer Security Authentication (Configuración de la autenticación de seguridad de la capa de transporte) en la documentación de Oracle Database.

Protección de su bucket de Amazon S3 contra el problema del suplente confuso

Cuando crea una versión del motor personalizado de Amazon RDS Custom para Oracle o una instancia de base de datos de RDS Custom para SQL Server, RDS Custom crea un bucket de Amazon S3. El bucket de S3 almacena archivos como artefactos CEV, registros REDO (transacciones), elementos de configuración para el perímetro de soporte y registros AWS CloudTrail.

Puede hacer que estos buckets de S3 sean más seguros mediante el uso de las claves de contexto de condición global para evitar el problema del suplente confuso. Para obtener más información, consulte Prevención de los problemas del suplente confuso entre servicios.

El siguiente ejemplo de RDS Custom para Oracle muestra el uso de las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en una política de bucket de S3. Para RDS Custom para Oracle, asegúrese de incluir los nombres de recursos de Amazon (ARN) para los CEV y las instancias de base de datos. Para RDS Custom para SQL Server, asegúrese de incluir el ARN para las instancias de base de datos.

```
...
{
  "Sid": "AWSRDSCustomForOracleInstancesObjectLevelAccess",
  "Effect": "Allow",
  "Principal": {
     "Service": "custom.rds.amazonaws.com"
  },
  "Action": [
     "s3:GetObject",
     "s3:GetObjectVersion",
     "s3:DeleteObject",
     "s3:DeleteObjectVersion",
     "s3:GetObjectRetention",
     "s3:BypassGovernanceRetention"
  ],
  "Resource": "arn:aws:s3:::do-not-delete-rds-custom-123456789012-us-east-2-c8a6f7/
RDSCustomForOracle/Instances/*",
  "Condition": {
     "ArnLike": {
        "aws:SourceArn": [
            "arn:aws:rds:us-east-2:123456789012:db:*",
            "arn:aws:rds:us-east-2:123456789012:cev:*/*"
        ]
     },
     "StringEquals": {
        "aws:SourceAccount": "123456789012"
    }
  }
},
...
```

Rotación de credenciales de RDS Custom para Oracle para programas de conformidad

Algunos programas de conformidad exigen que las credenciales de usuario de la base de datos cambien periódicamente, por ejemplo, cada 90 días. RDS Custom para Oracle rota automáticamente las credenciales de algunos usuarios de bases de datos predefinidos.

Temas

- Rotación automática de credenciales para usuarios predefinidos
- Directrices para rotar las credenciales de usuario
- Rotación manual de credenciales de usuario

Rotación automática de credenciales para usuarios predefinidos

Si su instancia de base de datos de RDS Custom para Oracle está alojada en Amazon RDS, las credenciales de los siguientes usuarios predefinidos de Oracle se rotan automáticamente cada 30 días. Las credenciales de los usuarios anteriores residen en AWS Secrets Manager.

Usuario de base de datos	Creado por	Versiones del motor admitidas	Notas
`SYS`	Oracle	custom-oracle-ee custom-oracle-ee-cdb custom-oracle-se2 custom-oracle-se2-cdb	
`SYSTEM`	Oracle	custom-oracle-ee custom-oracle-ee-cdb custom-oracle-se2 custom-oracle-se2-cdb	
`RDSADMIN`	RDS	custom-oracle-ee	

Usuario de base de datos	Creado por	Versiones del motor admitidas	Notas
		custom-oracle-se2	
C##RDSADMIN	RDS	custom-oracle-ee-cdb custom-oracle-se2-cdb	Los nombres de usuario con un prefijo C## solo existen en las CDB. Para obtener más información acerca de las CDB, consulte Información general de la arquitectura de Amazon RDS Custom para Oracle.
RDS_DATAGUARD	RDS	custom-oracle-ee	Este usuario solo existe en las réplicas de lectura, en las bases de datos de origen para réplicas de lectura y en las bases de datos que haya migrado físicamente a RDS Custom mediante Oracle Data Guard.
C##RDS_DATAGUARD	RDS	custom-oracle-ee-cdb	Este usuario solo existe en las réplicas de lectura, en las bases de datos de origen para réplicas de lectura y en las bases de datos que haya migrado físicamente a RDS Custom mediante Oracle Data Guard. Los nombres de usuario con un prefijo C## solo existen en las CDB. Para obtener más información acerca de las CDB, consulte Información general de la arquitectura de Amazon RDS Custom para Oracle.

Una excepción a la rotación automática de credenciales es una instancia de base de datos de RDS Custom para Oracle que haya configurado manualmente como base de datos en espera. RDS solo rota las credenciales de las réplicas que haya creado mediante el comando de la CLI de `create-db-instance-read-replica` o la API de `CreateDBInstanceReadReplica`.

Directrices para rotar las credenciales de usuario

Para asegurarse de que sus credenciales roten de acuerdo con su programa de conformidad, tenga en cuenta las siguientes directrices:

- Si la instancia de base de datos rota las credenciales automáticamente, no cambie ni elimine manualmente un secreto, un archivo de contraseñas o una contraseña para los usuarios que figuran en Usuarios predefinidos de Oracle. De lo contrario, RDS Custom podría colocar la instancia de base de datos fuera del perímetro de soporte, lo que suspendería la rotación automática.
- El usuario maestro de RDS no está predefinido, por lo que usted es el responsable de cambiar la contraseña manualmente o configurar la rotación automática en Secrets Manager. Para obtener más información, consulte Rotar secretos de AWS Secrets Manager.

Rotación manual de credenciales de usuario

Para las siguientes categorías de bases de datos, RDS no rota automáticamente las credenciales de los usuarios que figuran en Usuarios predefinidos de Oracle:

- Base de datos que configuró manualmente para que funcione como base de datos en espera.
- Base de datos en las instalaciones
- Instancia de base de datos que se encuentra fuera del perímetro de soporte o en un estado en el que no se puede ejecutar la automatización de RDS Custom. En este caso, RDS Custom tampoco rota las claves.

Si la base de datos se encuentra en alguna de las categorías anteriores, debe rotar las credenciales de usuario manualmente.

Para rotar manualmente las credenciales de usuario de una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En Bases de datos, asegúrese de que RDS no esté realizando copias de seguridad de la instancia de base de datos ni operaciones como la configuración de la alta disponibilidad.
3. En la página de detalles de la base de datos, elija Configuración y anote el ID del recurso de la instancia de base de datos. También puede utilizar el comando `describe-db-instances` de la AWS CLI.
4. Abra la consola de Secrets Manager en https://console.aws.amazon.com/secretsmanager/.
5. En el cuadro de búsqueda, ingrese el ID de recurso de la base de datos y busque un secreto mediante una de las siguientes convenciones de nomenclatura:

```
do-not-delete-rds-custom-resource_id-uuid
rds-custom!oracle-do-not-delete-resource_id-uuid
```

Este secreto almacena la contraseña de `RDSADMIN`, `SYS` y `SYSTEM`. Las siguientes claves de ejemplo son para la instancia de base de datos con el ID de recurso `db-ABCDEFG12HIJKLNMNOPQRS3TUVWX` y UUID `123456`:

```
do-not-delete-rds-custom-db-ABCDEFG12HIJKLNMNOPQRS3TUVWX-123456
rds-custom!oracle-do-not-delete-db-ABCDEFG12HIJKLNMNOPQRS3TUVWX-123456
```

> **Important**
>
> Si la instancia de base de datos es una réplica de lectura y usa el motor `custom-oracle-ee-cdb`, existen dos secretos con el sufijo *`db-resource_id-uuid`*: uno para el usuario maestro y otro para `RDSADMIN`, `SYS` y `SYSTEM`. Para encontrar el secreto correcto, ejecute el siguiente comando en el host:
>
> ```
> cat /opt/aws/rdscustomagent/config/database_metadata.json | python3 -c
>  "import sys,json; print(json.load(sys.stdin)['dbMonitoringUserPassword'])"
> ```
>
> El atributo `dbMonitoringUserPassword` indica el secreto para `RDSADMIN`, `SYS` y `SYSTEM`.

6. Si la instancia de base de datos existe en una configuración de Oracle Data Guard, busque un secreto mediante una de las siguientes convenciones de nomenclatura:

```
do-not-delete-rds-custom-resource_id-uuid-dg
```

```
rds-custom!oracle-do-not-delete-resource_id-uuid-dg
```

Este secreto almacena la contraseña de RDS_DATAGUARD. Las siguientes claves de ejemplo son para la instancia de base de datos con el ID de recurso de base de datos db-ABCDEFG12HIJKLNMNOPQRS3TUVWX y UUID 789012:

```
do-not-delete-rds-custom-db-ABCDEFG12HIJKLNMNOPQRS3TUVWX-789012-dg
rds-custom!oracle-do-not-delete-db-ABCDEFG12HIJKLNMNOPQRS3TUVWX-789012-dg
```

7. Para todos los usuarios de bases de datos que se indican en Usuarios predefinidos de Oracle, actualice las contraseñas de acuerdo con las instrucciones de Modificación de un secreto de AWS Secrets Manager.
8. Si su base de datos es una base de datos independiente o una base de datos de origen en una configuración de Oracle Data Guard:

   a. Inicie su cliente de Oracle SQL e inicie sesión como SYS.

   b. Ejecute una instrucción SQL del siguiente modo para cada usuario de base de datos incluido en Usuarios predefinidos de Oracle:

   ```
   ALTER USER user-name IDENTIFIED BY pwd-from-secrets-manager ACCOUNT UNLOCK;
   ```

   Por ejemplo, si la nueva contraseña de RDSADMIN almacenada en Secrets Manager es pwd-123, ejecute la siguiente instrucción:

   ```
   ALTER USER RDSADMIN IDENTIFIED BY pwd-123 ACCOUNT UNLOCK;
   ```

9. Si su instancia de base de datos ejecuta Oracle Database 12c Versión 1 (12.1) y la administra Oracle Data Guard, copie manualmente el archivo de contraseña (orapw) desde la instancia de base de datos principal a cada instancia de base de datos en espera.

   Si la instancia de base de datos está alojada en Amazon RDS, la ubicación del archivo de contraseñas es /rdsdbdata/config/orapw. Para las bases de datos que no están alojadas en Amazon RDS, la ubicación predeterminada es $ORACLE_HOME/dbs/orapw$ORACLE_SID en Linux y UNIX y %ORACLE_HOME%\database\PWD%ORACLE_SID%.ora en Windows.

Trabajar con RDS Custom for Oracle

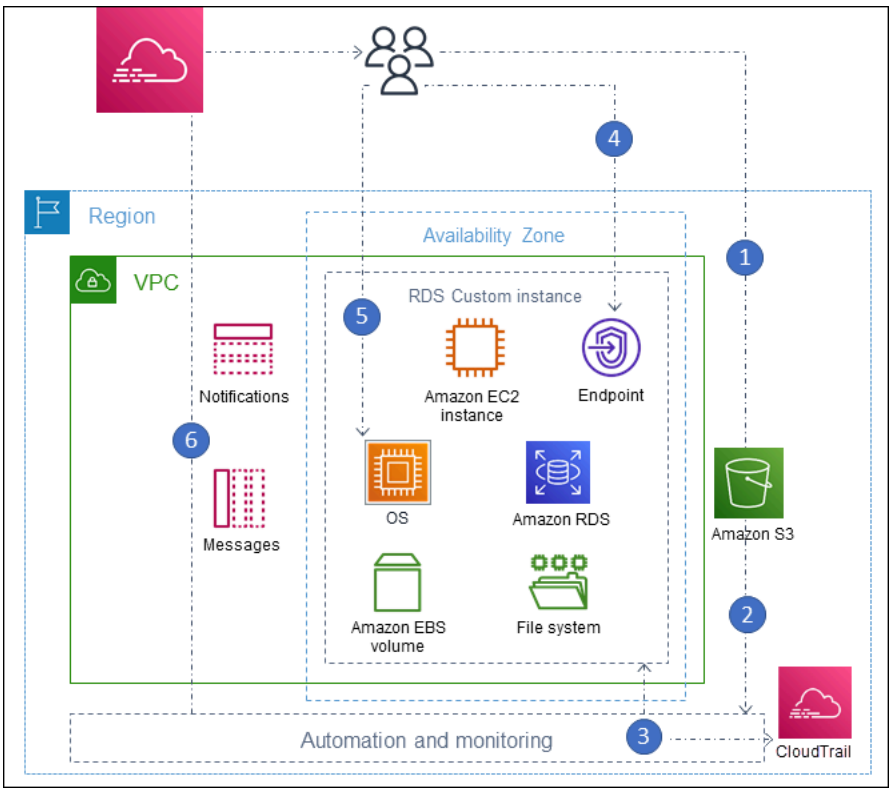
A continuación encontrará instrucciones para crear, administrar y mantener sus instancias de base de datos de RDS Custom for Oracle.

Temas

- Flujo de trabajo de RDS Custom for Oracle
- Arquitectura de base de datos de Amazon RDS Custom para Oracle
- Disponibilidad y compatibilidad de características con RDS Custom para Oracle
- Requisitos y limitaciones de Amazon RDS Custom para Oracle
- Configuración del entorno para Amazon RDS Custom for Oracle
- Trabajar con versiones de motor personalizadas para Amazon RDS Custom for Oracle
- Configuración de una instancia de base de datos para Amazon RDS Custom para Oracle
- Administración de una instancia de base de datos de Amazon RDS Custom para Oracle
- Administración de una implementación multi-AZ de RDS Custom para Oracle
- Trabajar con réplicas de Oracle para RDS Custom para Oracle
- Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS Custom for Oracle
- Trabajar con grupos de opciones en RDS Custom para Oracle
- Migración de una base de datos en las instalaciones a RDS Custom para Oracle
- Actualización de una instancia de base de datos para Amazon RDS Custom for Oracle
- Solución de problemas de base de datos de Amazon RDS Custom para Oracle
- Problemas conocidos de Amazon RDS Custom para Oracle

Flujo de trabajo de RDS Custom for Oracle

En el siguiente diagrama se muestra el flujo de trabajo típico de RDS Custom for Oracle.



Los pasos son los siguientes:

1. Cargue el software de base de datos en su bucket de Amazon S3.

   Para obtener más información, consulte Paso 3: cargar los archivos de instalación en Amazon S3.
2. Cree una versión del motor personalizado (CEV) de RDS Custom para Oracle desde sus medios.

   Elija la arquitectura CDB o la arquitectura no CDB tradicional. Para obtener más información, consulte Creación de una CEV.
3. Cree una instancia de base de datos de RDS Custom para Oracle desde una CEV.

   Para obtener más información, consulte Creación de una instancia de base de datos de RDS Custom for Oracle.
4. Conecte la aplicación al punto de conexión de instancia de base de datos.

   Para obtener más información, consulte Conexión a la instancia de base de datos de RDS Custom mediante SSH y Conexión a su instancia de base de datos de RDS Custom mediante Session Manager.
5. (Opcional) Acceda al host para personalizar el software.
6. Supervise las notificaciones y los mensajes generados por la automatización RDS Custom.

Archivos de instalación de base de datos

Su responsabilidad hacia los medios es una diferencia clave entre Amazon RDS y RDS Custom. Amazon RDS, que es un servicio completamente administrado, suministra el software de base de datos y de Amazon Machine Image (AMI). El software de base de datos de Amazon RDS está preinstalado, por lo que solo necesita elegir un motor y una versión de base de datos y crear la base de datos.

Para RDS Custom, proporciona sus propios medios. Cuando crea una versión de motor personalizada, RDS Custom instala el medio que proporciona. Los medios de RDS Custom contienen los archivos y las revisiones de instalación de la base de datos. Este modelo de servicio se denomina Bring Your Own Media (BYOM) (Traiga sus propios medios).

Versiones de motor personalizadas para RDS Custom para Oracle

Una Versión de motor personalizada de RDS Custom para Oracle (CEV) es una instantánea de volumen binario de una versión de base de datos y una AMI. De forma predeterminada, RDS Custom para Oracle utiliza la AMI más reciente que Amazon EC2 pone a su disposición. También puede elegir reutilizar una AMI existente.

Manifiesto CEV

Tras descargar de Oracle los archivos de instalación de bases de datos Oracle, cárguelos en un bucket de Amazon S3. Al crear su CEV, especificará los nombres de los archivos en un documento JSON denominado Manifiesto CEV. RDS Custom para Oracle utiliza los archivos especificados y la AMI para crear su CEV.

RDS Custom para Oracle proporciona plantillas de manifiestos JSON con los archivos.zip que recomendamos para cada versión compatible de Oracle Database. Por ejemplo, la siguiente plantilla es para la RU 19.17.0.0.0.

```
{
    "mediaImportTemplateVersion": "2020-08-14",
    "databaseInstallationFileNames": [
        "V982063-01.zip"
    ],
    "opatchFileNames": [
        "p6880880_190000_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames": [
        "p34419443_190000_Linux-x86-64.zip",
```

```
        "p34411846_190000_Linux-x86-64.zip"
    ],
    "otherPatchFileNames": [
        "p28852325_190000_Linux-x86-64.zip",
        "p29997937_190000_Linux-x86-64.zip",
        "p31335037_190000_Linux-x86-64.zip",
        "p32327201_190000_Linux-x86-64.zip",
        "p33613829_190000_Linux-x86-64.zip",
        "p34006614_190000_Linux-x86-64.zip",
        "p34533061_190000_Linux-x86-64.zip",
        "p34533150_190000_Generic.zip",
        "p28730253_190000_Linux-x86-64.zip",
        "p29213893_1917000DBRU_Generic.zip",
        "p33125873_1917000DBRU_Linux-x86-64.zip",
        "p34446152_1917000DBRU_Linux-x86-64.zip"
    ]
}
```

También puede especificar los parámetros de instalación en el manifiesto JSON. Por ejemplo, puede configurar valores no predeterminados para la base de Oracle, el directorio raíz de Oracle, y el ID y el nombre del usuario y el grupo de UNIX/Linux. Para obtener más información, consulte Campos JSON en el manifiesto de CEV.

Formato de nomenclatura de CEV

Asígnele un nombre a la CEV de RDS Custom para Oracle mediante una cadena especificada por el cliente. El formato del nombre es el siguiente, según la versión de Oracle Database:

- `19.`*`customized_string`*
- `18.`*`customized_string`*
- `12.2.`*`customized_string`*
- `12.1.`*`customized_string`*

Puede utilizar de 1 a 50 caracteres alfanuméricos, guiones bajos, guiones y puntos. Por ejemplo, podría asignar el nombre `19.my_cev1` a su CEV.

Arquitectura multitenencia de Oracle en RDS Custom para Oracle

La arquitectura multitenencia de Oracle permite que una base de datos de Oracle funcione como base de datos de tipo contenedor (CDB). Una CDB incluye ninguna, uno o muchas bases de datos

conectables (PDB) creadas por el cliente. Una PDB es una colección portátil de esquemas y objetos que una aplicación ve como una base de datos tradicional no CDB.

Al crear una CEV de RDS Custom para Oracle, debe especificar una arquitectura CDB o no CDB. Puede crear una CDB de RDS Custom para Oracle solo cuando la CEV que utilizó para crearla utilice la arquitectura multitenencia de Oracle. Para obtener más información, consulte Trabajar con versiones de motor personalizadas para Amazon RDS Custom for Oracle.

Creación de una instancia de base de datos para RDS Custom for Oracle

Después de crear la CEV, está disponible para su uso. Puede crear varias CEV y luego crear varias instancias de RDS Custom para Oracle desde cualquier CEV. También puede cambiar el estado de una CEV para que esté disponible o inactiva.

Puede crear su instancia de base de datos de RDS Custom para Oracle con la arquitectura multitenencia de Oracle (tipo de motor `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`) o con la arquitectura tradicional que no es CDB (tipo de motor `custom-oracle-ee` o `custom-oracle-se2`). Al crear una base de datos de contenedores (CDB, por sus siglas en inglés), contiene una base de datos conectable (PDB, por sus siglas en inglés) y un origen de PDB. Puede crear PDB adicionales manualmente con Oracle SQL.

Para crear su instancia de base de datos de RDS Custom for Oracle, utilice el comando `create-db-instance`. En este comando, especifique qué CEV se va a utilizar. El procedimiento es similar al que se debe seguir para crear una instancia de base de datos de Amazon RDS. Sin embargo, algunos parámetros son diferentes. Para obtener más información, consulte Configuración de una instancia de base de datos para Amazon RDS Custom para Oracle.

Conexión a la base de datos

Igual que con una instancia de base de datos de Amazon RDS, la instancia de base de datos de RDS Custom reside en una nube privada virtual (VPC). La aplicación se conecta a la base de datos de Oracle mediante un oyente de Oracle.

Si su base de datos es una CDB, puede usar el oyente `L_RDSCDB_001` para conectarse a la raíz de la CDB y a una PDB. Si conecta una base de datos no CDB a una CDB, asegúrese de configurar `USE_SID_AS_SERVICE_LISTENER = ON` para que las aplicaciones migradas mantengan la misma configuración.

Si se conecta a una base de datos no CDB, el usuario maestro es el usuario de una base de datos no CDB. Si se conecta a una CDB, el usuario maestro es el usuario de la PDB. Para conectarse a

la raíz de la CDB, inicie sesión en el host, inicie un cliente SQL y cree un usuario administrativo con comandos SQL.

Personalización de RDS Custom

Puede acceder al host de RDS Custom para instalar o personalizar el software. Para evitar conflictos entre los cambios y la automatización de RDS Custom, puede pausar la automatización durante un periodo determinado. Durante este periodo, RDS Custom no hace monitoreos ni recuperación de instancias. Al final del periodo, RDS Custom reanuda la automatización completa. Para obtener más información, consulte Pausa y reanudación de la instancia de base de datos de RDS Custom.

Arquitectura de base de datos de Amazon RDS Custom para Oracle

RDS Custom para Oracle admite tanto la arquitectura multitenencia de Oracle como la no multitenencia.

Temas

- Arquitecturas de bases de datos de Oracle compatibles
- Motores de bases de datos compatibles
- Características compatibles en la arquitectura multitenencia de Oracle

Arquitecturas de bases de datos de Oracle compatibles

La arquitectura multitenencia de Oracle, también denominada arquitectura CDB, permite que una base de datos Oracle funcione como base de datos de tipo contenedor (CDB). Una CDB incluye bases de datos conectables (PDB). Una PDB es una colección de esquemas y objetos que una aplicación ve como base de datos tradicional de Oracle. Para obtener más información, consulte Introduction to the Multitenant Architecture en la Guía del administrador multitenencia de Oracle.

Las arquitecturas CDB y no CDB se excluyen mutuamente. Si una base de datos de Oracle no es una CDB, es una no CDB y, por lo tanto, no puede contener PDB. En RDS Custom para Oracle, solo Oracle Database 19c admite la arquitectura CDB. Por lo tanto, si crea instancias de base de datos con versiones anteriores de bases de datos de Oracle, solo puede crear instancias que no sean CDB. Para obtener más información, consulte Consideraciones sobre la arquitectura multitenencia.

Motores de bases de datos compatibles

Al crear una instancia de base de datos o un CEV de Amazon RDS Custom para Oracle, elija un tipo de motor CDB o un tipo de motor que no sea CDB:

- `custom-oracle-ee-cdb` y `custom-oracle-se2-cdb`

  Estos tipos de motores especifican la arquitectura multitenencia de Oracle. Esta opción solo está disponible para Oracle Database 19c. Al crear una instancia de base de datos de RDS para Oracle mediante la arquitectura multitenencia, la CDB incluye los siguientes contenedores:

  - Raíz de CDB (`CDB$ROOT`)
  - Origen de PDB (`PDB$SEED`)
  - PDB inicial

Puede crear más PDB mediante el comando `CREATE PLUGGABLE DATABASE` de Oracle SQL. No puede usar las API de RDS para crear o eliminar PDB.

- `custom-oracle-ee` y `custom-oracle-se2`

  Estos tipos de motor especifican la arquitectura tradicional que no es CDB. Una base de datos que no es CDB no puede contener bases de datos conectables (PDB, por sus siglas en inglés).

Para obtener más información, consulte Consideraciones sobre la arquitectura multitenencia.

Características compatibles en la arquitectura multitenencia de Oracle

Una instancia de CDB de RDS Custom para Oracle admite las siguientes características:

- Copias de seguridad
- Restauración y restauración puntual (PITR, por sus siglas en inglés) a partir de copias de seguridad
- Réplicas de lectura
- Actualizaciones de la versión secundaria

Disponibilidad y compatibilidad de características con RDS Custom para Oracle

En este tema, se resumen la disponibilidad y compatibilidad de las características de RDS Custom para Oracle para realizar una consulta rápida.

Temas

- Compatibilidad de Región de AWS y de versiones de base de datos con RDS Custom para Oracle
- Compatibilidad de versiones de bases de datos con RDS Custom para Oracle
- Compatibilidad de ediciones y licencias con RDS Custom para Oracle
- Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle
- Compatibilidad de grupos de opciones con RDS Custom para Oracle

Compatibilidad de Región de AWS y de versiones de base de datos con RDS Custom para Oracle

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad de las versiones y las regiones de RDS Custom para Oracle, consulte Regiones y motores de base de datos admitidos para RDS Custom.

Compatibilidad de versiones de bases de datos con RDS Custom para Oracle

RDS Custom para Oracle es compatible con las siguientes versiones de bases de datos de Oracle:

- Oracle Database 19c
- Oracle Database 18c
- Base de datos Oracle 12c versión 2 (12.2)
- Base de datos Oracle 12c versión 1 (12.1)

Compatibilidad de ediciones y licencias con RDS Custom para Oracle

RDS Custom para Oracle admite Enterprise Edition (EE) y Standard Edition 2 (SE2) en el modelo BYOL.

Observe las siguientes limitaciones para Standard Edition 2:

- No se admite Oracle Data Guard. Por lo tanto, no puede crear réplicas de lectura de Oracle.
- Solo puede usar clases de instancias de base de datos que tengan 16 vCPU o menos (hasta 4xlarge).
- Una instancia de CDB de Standard Edition 2 admite un máximo de 3 bases de datos de inquilinos.
- No puede migrar datos entre Enterprise Edition y Standard Edition 2.

Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle

RDS Custom para Oracle admite las siguientes clases de instancia de base de datos: Si crea una instancia de base de datos en Standard Edition 2, solo podrá usar clases de instancias con 16 vCPU o menos (hasta 4xlarge).

Tipo	Tamaño
db.r7i	db.r7i.large |db.r7i.xlarge |db.r7i.2xlarge |db.r7i.4xlarge |db.r7i.8xlarge |db.r7i.12xlarge |db.r7i.16xlarge |db.r7i.24xlarge |db.r7i.48xlarge
db.r6i	db.r6i.large |db.r6i.xlarge |db.r6i.2xlarge |db.r6i.4xlarge |db.r6i.8xlarge |db.r6i.12xlarge |db.r6i.16xlarge |db.r6i.24xlarge |db.r6i.32xlarge
db.r5b	db.r5b.large |db.r5b.xlarge |db.r5b.2xlarge |db.r5b.4xlarge |db.r5b.8xlarge |db.r5b.12xlarge |db.r5b.16xlarge |db.r5b.24xlarge
db.r5	db.r5.large |db.r5.xlarge |db.r5.2xlarge |db.r5.4xlarge | db.r5.8xlarge |db.r5.12xlarge |db.r5.16xlarge |db.r5.24xlarge
db.x2iec	db.x2iedn.xlarge |db.x2iedn.2xlarge |db.x2iedn.4xlarge | db.x2iedn.8xlarge |db.x2iedn.16xlarge |db.x2iedn.24xlarge | db.x2iedn.32xlarge
db.x2iez	db.x2iezn.2xlarge |db.x2iezn.4xlarge |db.x2iezn.6xlarge | db.x2iezn.8xlarge |db.x2iezn.12xlarge

Tipo	Tamaño
db.m7i	db.m7i.large | db.m7i.xlarge | db.m7i.2xlarge | db.m7i.4xlarge | db.m7i.8xlarge | db.m7i.12xlarge | db.m7i.16xlarge | db.m7i.24xlarge | db.m7i.48xlarge
db.m6i	db.m6i.large | db.m6i.xlarge | db.m6i.2xlarge | db.m6i.4xlarge | db.m6i.8xlarge | db.m6i.12xlarge | db.m6i.16xlarge | db.m6i.24xlarge | db.m6i.32xlarge
db.m5	db.m5.large | db.m5.xlarge | db.m5.2xlarge | db.m5.4xlarge | db.m5.8xlarge | db.m5.12xlarge | db.m5.16xlarge | db.m5.24xlarge
db.t3	db.t3.medium | db.t3.large | db.t3.xlarge | db.t3.2xlarge

Compatibilidad de grupos de opciones con RDS Custom para Oracle

Puede especificar un grupo de opciones al crear o modificar una instancia de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Trabajar con grupos de opciones en RDS Custom para Oracle.

Requisitos y limitaciones de Amazon RDS Custom para Oracle

En este tema, se resumen la disponibilidad de las características y las limitaciones de Amazon RDS Custom para Oracle para realizar una consulta rápida.

Temas

- Requisitos generales de RDS Custom for Oracle
- Limitaciones generales de RDS Custom para Oracle
- Limitaciones de CEV y AMI para RDS Custom for Oracle
- Configuración no compatible para crear y modificar flujos de trabajo
- Cuotas de instancias de base de datos para su Cuenta de AWS

Requisitos generales de RDS Custom for Oracle

Asegúrese de cumplir los siguientes requisitos para Amazon RDS Custom for Oracle:

- Tiene acceso a My Oracle Support y Oracle Software Delivery Cloud para descargar la lista compatible de archivos de instalación y revisión para RDS Custom for Oracle. Si utiliza una revisión desconocida, se produce un error en la creación de la versión de motor personalizada (CEV). En este caso, contacte con el equipo de soporte de RDS Custom y pídale que agregue la revisión que falta. Para obtener más información, consulte Paso 2: descargar revisiones y archivos de instalación de la base de datos desde Oracle Software Delivery Cloud.
- Tiene acceso a Amazon S3. Necesita este servicio por las siguientes razones:
  - Los archivos de instalación de Oracle se cargan en buckets de S3. Los archivos de instalación cargados se utilizan para crear la CEV de RDS Custom.
  - RDS Custom para Oracle utiliza scripts descargados de buckets de S3 definidos internamente para realizar acciones en las instancias de base de datos. Estos scripts son necesarios para la incorporación y la automatización de RDS Custom.
  - RDS Custom para Oracle carga ciertos archivos en los buckets de S3 que se encuentran en su cuenta de cliente. Estos buckets utilizan el siguiente formato de nomenclatura: `do-not-delete-rds-custom-`*`account_id-region-uuid`*. Por ejemplo, es posible que tenga un bucket con el nombre `do-not-delete-rds-custom-123456789012-us-east-1-12a3b4`.

  Para obtener más información, consulte Paso 3: cargar los archivos de instalación en Amazon S3 y Creación de una CEV.

- Debe utilizar las clases de instancia de base de datos que aparecen en Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle para crear sus instancias de base de datos de RDS Custom for Oracle.
- Sus instancias de base de datos de RDS Custom for Oracle ejecutan Oracle Linux 8 (recomendado) u Oracle Linux 7. Si necesita Oracle Linux 7, póngase en contacto con Soporte. Para obtener más información, consulte Consideraciones de las actualizaciones de base de datos de RDS Custom for Oracle.
- Debe especificar las unidades de estado sólido gp2, gp3 o io1 para el almacenamiento de Amazon EBS. El tamaño máximo de almacenamiento es de 64 TiB.
- Tiene una clave AWS KMS para crear una instancia de base de datos de RDS Custom for Oracle. Para obtener más información, consulte Paso 1: crear o reutilizar una clave AWS KMS de cifrado simétrica.
- Tiene el rol de AWS Identity and Access Management (IAM) y el perfil de instancia necesarios para crear instancias de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Paso 4: configurar IAM para RDS Custom for Oracle.
- El usuario AWS Identity and Access Management (IAM) que crea una instancia de base de datos de CEV o RDS Custom tiene los permisos necesarios para IAM, CloudTrail y Amazon S3.

  Para obtener más información, consulte Paso 5: otorgar los permisos necesarios al rol o usuario de IAM.
- Proporciona su propia configuración de nube virtual privada (VPC) y de grupos de seguridad. Para obtener más información, consulte Paso 6: configurar la VPC para RDS Custom for Oracle.
- Debe proporcionar una configuración de redes que RDS Custom for Oracle pueda utilizar para acceder a otros Servicios de AWS. Para conocer los requisitos específicos, consulte Paso 4: configurar IAM para RDS Custom for Oracle.

Limitaciones generales de RDS Custom para Oracle

Las siguientes limitaciones se aplican a RDS Custom for Oracle:

- No puede modificar el identificador de instancia de base de datos de una instancia de base de datos actual de RDS Custom para Oracle.
- No puede especificar la arquitectura multitenencia de Oracle para ninguna versión que no sea Oracle Database 19c.

- No puede crear varias bases de datos Oracle en una única instancia de base de datos de RDS Custom para Oracle.
- No puede detener la instancia de base de datos de RDS Custom para Oracle ni la instancia de Amazon EC2 subyacente. No puede detener la facturación de una instancia de base de datos de RDS Custom para Oracle.
- No puede utilizar la administración de memoria compartida automática porque RDS Custom para Oracle solo admite la administración de memoria automática. Para obtener más información, consulte Automatic Memory Management (Administración de memoria automática) en la Oracle Database Administrator's Guide (Guía del administrador de bases de datos Oracle).
- Asegúrese de no cambiar el `DB_UNIQUE_NAME` de la instancia de base de datos principal. Cambiar el nombre provoca que se bloquee cualquier operación de restauración.
- No puede hacer más de 20 copias de instantáneas al mismo tiempo y en la misma región.
- No puede utilizar la API `describe-reserved-db-instances` para instancias de base de datos de RDS Custom for Oracle.

Para conocer las limitaciones específicas de la modificación de una instancia de base de datos de RDS Custom para Oracle, consulte Modificación de la instancia de base de datos de RDS Custom para Oracle. Para conocer las limitaciones de replicación, consulte Limitaciones generales de la replicación de RDS Custom para Oracle.

Limitaciones de CEV y AMI para RDS Custom for Oracle

Las siguientes limitaciones se aplican a las CEV y AMI de RDS Custom for Oracle:

- No puede proporcionar su propia AMI para utilizarla en una CEV de RDS Custom for Oracle. Puede especificar o bien la AMI predeterminada, que utiliza Oracle Linux 8, o bien una AMI que haya utilizado anteriormente una CEV de RDS Custom for Oracle.

> **Note**
>
> RDS Custom for Oracle lanza una nueva AMI predeterminada cuando se descubren vulnerabilidades y exposiciones comunes. No hay un cronograma fijo disponible ni garantizado. RDS Custom for Oracle suele publicar una nueva AMI predeterminada cada 30 días.

- No se puede modificar una CEV para que use una AMI diferente.

- No puede crear una instancia de CDB a partir de una CEV que utilice los tipos de motor `custom-oracle-ee` o `custom-oracle-se2`. La CEV debe usar `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`.
- Actualmente, RDS Custom for Oracle no le permite actualizar el sistema operativo de su instancia de base de datos de RDS Custom for Oracle con llamadas a la API de RDS. Una alternativa es actualizar manualmente su sistema operativo con el siguiente comando: `sudo yum update --security`.

Configuración no compatible para crear y modificar flujos de trabajo

Al crear o modificar una instancia de base de datos de RDS Custom para Oracle, no puede hacer lo siguiente:

- Cambiar el número de núcleos de CPU y subprocesos por núcleo de la clase de instancia de base de datos.
- Activar el escalado automático del almacenamiento.
- Configurar la retención de copia de seguridad a `0`.
- Configurar la autenticación de Kerberos.
- Especificar su propio grupo de parámetros o grupo de opciones de base de datos.
- Activar la Información sobre rendimiento.
- Activar las actualizaciones automáticas de versiones secundarias.

Cuotas de instancias de base de datos para su Cuenta de AWS

Asegúrese de que el número combinado de instancias de base de datos de RDS Custom y Amazon RDS no supere el límite de cuota. Por ejemplo, si la cuota de Amazon RDS es de 40 instancias de base de datos, puede tener 20 RDS Custom para instancias de base de datos de Oracle y 20 instancias de base de datos de Amazon RDS.

Configuración del entorno para Amazon RDS Custom for Oracle

Antes de crear una instancia de base de datos de Amazon RDS Custom para Oracle, realice las siguientes tareas.

Temas

- Paso 1: crear o reutilizar una clave AWS KMS de cifrado simétrica
- Paso 2: descargar e instalar la AWS CLI
- Paso 3: extraer las plantillas de CloudFormation para RDS Custom for Oracle
- Paso 4: configurar IAM para RDS Custom for Oracle
- Paso 5: otorgar los permisos necesarios al rol o usuario de IAM
- Paso 6: configurar la VPC para RDS Custom for Oracle

Paso 1: crear o reutilizar una clave AWS KMS de cifrado simétrica

Las claves administradas por el cliente son AWS KMS keys en su cuenta de AWS que usted ha creado, posee y administra. Se requiere una clave KMS de cifrado simétrica administrada por el cliente para RDS Custom. Al crear una instancia de base de datos de RDS Custom for Oracle, debe proporcionar el identificador de clave KMS. Para obtener más información, consulte Configuración de una instancia de base de datos para Amazon RDS Custom para Oracle.

Dispone de las opciones siguientes:

- Si ya dispone de una clave KMS administrada por el cliente en su Cuenta de AWS, puede utilizarla con RDS Custom. No hay que hacer nada más.
- Si ya ha creado una clave KMS de cifrado simétrica administrada por el cliente para un motor diferente de RDS Custom, puede reutilizar la misma clave. No hay que hacer nada más.
- Si no tiene una clave KMS de cifrado simétrica administrada por el cliente en su cuenta, cree una clave KMS mediante las instrucciones de Creating keys (Creación de claves) en la Guía para desarrolladores de AWS Key Management Service.
- Si va a crear una instancia de base de datos de CEV o RDS Custom y su clave de KMS está en una Cuenta de AWS diferente, asegúrese de utilizar la AWS CLI. No puede usar la consola de AWScon claves de KMS entre cuentas.

> **Important**
>
> RDS Custom no admite claves KMS administradas por AWS.

Asegúrese de que su clave de cifrado simétrica proporcione acceso a las operaciones `kms:Decrypt` y `kms:GenerateDataKey` al rol de IAM AWS Identity and Access Management en su perfil de instancia de IAM. Si tiene una nueva clave de cifrado simétrica en su cuenta, no se requieren cambios. De lo contrario, asegúrese de que la política de claves de cifrado simétricas proporcione acceso a estas operaciones.

Para obtener más información, consulte Paso 4: configurar IAM para RDS Custom for Oracle.

Para obtener más información sobre la configuración de IAM para RDS Custom para Oracle, consulte Paso 4: configurar IAM para RDS Custom for Oracle.

Paso 2: descargar e instalar la AWS CLI

AWS le proporciona una interfaz de línea de comandos para utilizar las funciones de RDS Custom. Puede utilizar la versión 1 o la versión 2 de la AWS CLI.

Para obtener información acerca de cómo descargar e instalar la AWS CLI, consulte Instalación o actualización de la versión más reciente de AWS CLI.

Omita este paso si se da alguna de estas condiciones:

- Si tiene pensado acceder a RDS Custom solo desde la AWS Management Console.
- Si ya ha descargado la AWS CLI para Amazon RDS o un motor de base de datos RDS Custom diferente.

Paso 3: extraer las plantillas de CloudFormation para RDS Custom for Oracle

Para simplificar la configuración, le recomendamos encarecidamente que utilice plantillas de AWS CloudFormation para crear pilas de CloudFormation. Si planea configurar IAM y la VPC de forma manual, omita este paso.

Temas

- Paso 3a: descargar los archivos de plantilla de CloudFormation
- Paso 3b: extraer custom-oracle-iam.json

- Paso 3c: extraer custom-vpc.json

Paso 3a: descargar los archivos de plantilla de CloudFormation

Una plantilla de CloudFormation es una declaración de los recursos de AWS que componen una pila. La plantilla se almacena como un archivo JSON.

Para descargar los archivos de plantilla de CloudFormation

1. Abra el menú contextual (haga clic con el botón derecho del ratón) del enlace custom-oracle-iam.zip y elija Save Link As (Guardar enlace como).
2. Guarde el archivo en su computadora.
3. Repita los pasos anteriores para el enlace custom-vpc.zip.

   Si ya ha configurado la VPC para RDS Custom, omita este paso.

Paso 3b: extraer custom-oracle-iam.json

Abre el archivo `custom-oracle-iam.zip` que ha descargado y, a continuación, extraiga el archivo `custom-oracle-iam.json`. El principio del archivo tiene el siguiente aspecto.

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "EncryptionKey": {
      "Type": "String",
      "Default": "*",
      "Description": "KMS Key ARN for encryption of data managed by RDS Custom and by
 DB Instances."
    }
  },
  "Resources": {
    "RDSCustomInstanceServiceRole": {
      "Type": "AWS::IAM::Role",
      "Properties": {
        "RoleName": { "Fn::Sub": "AWSRDSCustomInstanceRole-${AWS::Region}" },
        "AssumeRolePolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Action": "sts:AssumeRole",
```

```
            "Effect": "Allow",
            "Principal": {
              "Service": "ec2.amazonaws.com"
            }
          }
        ]
      },...
```

Paso 3c: extraer custom-vpc.json

> **Note**
>
> Si ya ha configurado una VPC existente para RDS Custom for Oracle, omita este paso. Para obtener más información, consulte Configurar la VPC manualmente para RDS Custom for Oracle.

Abra el archivo `custom-vpc.zip` que descargó y, a continuación, extraiga el archivo `custom-vpc.json`. El principio del archivo tiene el siguiente aspecto.

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Parameters": {
    "PrivateVpc": {
      "Type": "AWS::EC2::VPC::Id",
      "Description": "Private VPC Id to use for RDS Custom DB Instances"
    },
    "PrivateSubnets": {
      "Type": "List<AWS::EC2::Subnet::Id>",
      "Description": "Private Subnets to use for RDS Custom DB Instances"
    },
    "RouteTable": {
      "Type": "String",
      "Description": "Route Table that must be associated with the PrivateSubnets and
 used by S3 VPC Endpoint",
      "AllowedPattern": "rtb-[0-9a-z]+"
    }
  },
  "Resources": {
    "DBSubnetGroup": {
      "Type": "AWS::RDS::DBSubnetGroup",
      "Properties": {
```

```
        "DBSubnetGroupName": "rds-custom-private",
        "DBSubnetGroupDescription": "RDS Custom Private Network",
        "SubnetIds": {
          "Ref": "PrivateSubnets"
        }
      }
    },...
```

Paso 4: configurar IAM para RDS Custom for Oracle

Debe utilizar un rol de IAM o un usuario de IAM (denominado entidad de IAM) para crear una instancia de base de datos de RDS Custom mediante la consola o la AWS CLI. Esta entidad de IAM debe tener los permisos necesarios para crear instancias.

Puede configurar IAM mediante CloudFormation o con pasos manuales.

> **Important**
>
> Se recomienda encarecidamente que configure el entorno de RDS Custom para Oracle mediante AWS CloudFormation. Esta técnica es la más sencilla y la menos propensa a errores.

Temas

- Configurar IAM mediante CloudFormation
- Cree manualmente el rol de IAM y el perfil de instancias

Configurar IAM mediante CloudFormation

Cuando utiliza la plantilla de CloudFormation para IAM, se crean los siguientes recursos necesarios:

- Un perfil de instancia llamado `AWSRDSCustomInstanceProfile-`*`region`*
- Un rol de servicio denominado `AWSRDSCustomInstanceRole-`*`region`*
- Una política de acceso denominada `AWSRDSCustomIamRolePolicy` que está asociada al rol de servicio

Para configurar IAM mediante CloudFormation

1. Abra la consola de CloudFormation en https://console.aws.amazon.com/cloudformation.

2. Inicie el Asistente de creación de pila y elija Create Stack (Crear pila).
3. En la página Create stack (Crear pila), proceda del modo siguiente:
   a. En Prepare template (Preparar plantilla), elija Template is ready (La plantilla está lista).
   b. Para Origen de plantilla, elija Cargar un archivo de plantilla.
   c. En Elegir archivo, vaya hasta custom-oracle-iam.json y, a continuación, selecciónelo.
   d. Elija Siguiente.
4. En la página Specify stack Details (Especificar detalles de pila), haga lo siguiente:
   a. En Stack name (Nombre de pila), ingrese **`custom-oracle-iam`**.
   b. Elija Siguiente.
5. En página Configure stack options (Configurar opciones de pila), elija Next (Siguiente).
6. En la página Review custom-oracle-iam (Revisar custom-oracle-iam), haga lo siguiente:
   a. Seleccione la casilla de verificación I acknowledge that AWS CloudFormation might create IAM resources with custom names (Reconozco que AWS CloudFormation podría crear recursos de IAM con nombres personalizados).
   b. Elija Enviar.

   CloudFormation crea los Roles de IAM que requiere RDS Custom for Oracle. En el panel de la izquierda, cuando custom-oracle-iam indique CREATE_COMPLETE, continúe con el paso siguiente.
7. En el panel izquierdo, elija custom-oracle-iam. En el panel de la derecha, haga lo siguiente:
   a. Elija Información de la pila. Su pila tiene un ID con el formato arn:aws:cloudformation:***`region`***:***`account-no`***:stack/custom-oracle-iam/***`identifier`***.
   b. Seleccione Recursos. Debería ver lo siguiente:
      - Un perfil de instancia denominado AWSRDSCustomInstanceProfile-***`region`***
      - Un rol de servicio denominado AWSRDSCustomInstanceRole-***`region`***

      Al crear la instancia de base de datos de RDS Custom, tiene que proporcionar el ID del perfil de instancia.

Cree manualmente el rol de IAM y el perfil de instancias

La configuración es más sencilla cuando se utiliza CloudFormation. Sin embargo, también puede configurar IAM de forma manual. Para la configuración manual, haga lo siguiente:

- Paso 1: crear el rol de IAM AWSRDSCustomInstanceRoleForRdsCustomInstance.
- Paso 2: añadir una política de acceso a AWSRDSCustomInstanceRoleForRdsCustomInstance.
- Paso 2: añadir una política de acceso a AWSRDSCustomInstanceRoleForRdsCustomInstance.
- Paso 4: agregar AWSRDSCustomInstanceRoleForRdsCustomInstance a AWSRDSCustomInstanceProfile.

Paso 1: crear el rol de IAM AWSRDSCustomInstanceRoleForRdsCustomInstance

En este paso, se crea el rol con el formato de nomenclatura `AWSRDSCustomInstanceRole-`*`region`*. Mediante la política de confianza, Amazon EC2 puede asumir el rol. En el ejemplo siguiente, se supone que ha establecido la variable de entorno `$REGION` en la Región de AWS en la que desea crear la instancia de base de datos.

```
aws iam create-role \
  --role-name AWSRDSCustomInstanceRole-$REGION \
  --assume-role-policy-document '{
    "Version": "2012-10-17",
      "Statement": [
        {
          "Action": "sts:AssumeRole",
          "Effect": "Allow",
          "Principal": {
              "Service": "ec2.amazonaws.com"
          }
        }
      ]
    }'
```

Paso 2: añadir una política de acceso a AWSRDSCustomInstanceRoleForRdsCustomInstance

Al integrar una política en línea en un Rol de IAM, la política en línea se utiliza como parte de la política de acceso del rol (permisos). Usted crea la política `AWSRDSCustomIamRolePolicy` que permite a Amazon EC2 enviar y recibir mensajes y realizar diversas acciones.

En el siguiente ejemplo, se crea la política de acceso denominada `AWSRDSCustomIamRolePolicy`, y lo agrega al Rol de IAM `AWSRDSCustomInstanceRole-`*`region`*. En este ejemplo, se presupone que ha establecido las variables de entorno siguientes:

`$REGION`

Defina esta variable en la Región de AWS en la que tiene pensado crear la instancia de base de datos.

`$ACCOUNT_ID`

Defina esta variable en su número de Cuenta de AWS.

`$KMS_KEY`

Defina esta variable en el Nombre de recurso de Amazon (ARN) de la AWS KMS key que desea utilizar para las instancias de base de datos de RDS Custom. Para especificar más de una clave KMS, agréguela a la sección `Resources` del estado de cuenta ID (Sid) 11.

```
aws iam put-role-policy \
  --role-name AWSRDSCustomInstanceRole-$REGION \
  --policy-name AWSRDSCustomIamRolePolicy \
  --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:GetDeployablePatchSnapshotForInstance",
                "ssm:GetDocument",
                "ssm:DescribeDocument",
                "ssm:GetManifest",
                "ssm:GetParameter",
                "ssm:GetParameters",
                "ssm:ListAssociations",
                "ssm:ListInstanceAssociations",
                "ssm:PutInventory",
                "ssm:PutComplianceItems",
                "ssm:PutConfigurePackageResult",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
```

```
                "ssm:UpdateInstanceInformation",
                "ssm:GetConnectionStatus",
                "ssm:DescribeInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
                "ssmmessages:OpenDataChannel"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "2",
            "Effect": "Allow",
            "Action": [
                "ec2messages:AcknowledgeMessage",
                "ec2messages:DeleteMessage",
                "ec2messages:FailMessage",
                "ec2messages:GetEndpoint",
                "ec2messages:GetMessages",
                "ec2messages:SendReply"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "3",
            "Effect": "Allow",
            "Action": [
                "logs:PutRetentionPolicy",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams",
                "logs:DescribeLogGroups",
                "logs:CreateLogStream",
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:'$REGION':'$ACCOUNT_ID':log-group:rds-custom-instance*"
            ]
        },
        {
            "Sid": "4",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::do-not-delete-rds-custom-*/*"
            ]
        },
        {
            "Sid": "5",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "RDSCustomForOracle/Agent"
                    ]
                }
            }
        },
        {
            "Sid": "6",
            "Effect": "Allow",
            "Action": [
                "events:PutEvents"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "7",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
```

```
            "Resource": [
                "arn:aws:secretsmanager:'$REGION':'$ACCOUNT_ID':secret:do-not-delete-
rds-custom-*",
                "arn:aws:secretsmanager:'$REGION':'$ACCOUNT_ID':secret:rds-custom!
oracle-do-not-delete-*"
            ]
        },
        {
           "Sid": "8",
           "Effect": "Allow",
           "Action": [
             "s3:ListBucketVersions"
           ],
           "Resource": [
             "arn:aws:s3:::do-not-delete-rds-custom-*"
           ]
         },
         {
            "Sid": "9",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/AWSRDSCustom": "custom-oracle"
                }
            }
          },
          {
            "Sid": "10",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*"
            ]
          },
          {
            "Sid": "11",
            "Effect": "Allow",
            "Action": [
              "kms:Decrypt",
```

```
              "kms:GenerateDataKey"
            ],
            "Resource": [
              "arn:aws:kms:'$REGION':'$ACCOUNT_ID':key/'$KMS_KEY'"
            ]
          },
          {
            "Sid": "12",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:CreateAction": [
                        "CreateSnapshots"
                    ]
                }
            }
        },
        {
            "Sid": "13",
            "Effect": "Allow",
            "Action": [
                "sqs:SendMessage",
                "sqs:ReceiveMessage",
                "sqs:DeleteMessage",
                "sqs:GetQueueUrl"
            ],
            "Resource": "arn:aws:sqs:'$REGION':'$ACCOUNT_Id':do-not-delete-rds-custom-
*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AWSRDSCustom": "custom-oracle"
                }
            }
        }
    ]
}'
```

Paso 3: crear el perfil de instancia de RDS Custom AWSRDSCustomInstanceProfile

Un perfil de instancia es un contenedor que incluye un rol de IAM único. RDS Custom usa el perfil de instancia para pasar el rol a la instancia.

Si utiliza la CLI para crear un rol, debe crear el rol y el perfil de instancia de forma independiente, con nombres potencialmente diferentes. Cree su perfil de instancia de IAM de la siguiente manera y utilice el formato `AWSRDSCustomInstanceProfile-`*`region`* para el nombre. En el ejemplo siguiente, se supone que ha establecido la variable de entorno `$REGION` en la Región de AWS en la que desea crear la instancia de base de datos.

```
aws iam create-instance-profile \
    --instance-profile-name AWSRDSCustomInstanceProfile-$REGION
```

Paso 4: agregar AWSRDSCustomInstanceRoleForRdsCustomInstance a AWSRDSCustomInstanceProfile

Añada el rol de IAM al perfil de instancia que ha creado anteriormente. En el ejemplo siguiente, se supone que ha establecido la variable de entorno `$REGION` en la Región de AWS en la que desea crear la instancia de base de datos.

```
aws iam add-role-to-instance-profile \
    --instance-profile-name AWSRDSCustomInstanceProfile-$REGION \
    --role-name AWSRDSCustomInstanceRole-$REGION
```

Paso 5: otorgar los permisos necesarios al rol o usuario de IAM

Asegúrese de que la entidad principal de IAM (usuario o rol) que crea la instancia de base de datos de RDS Custom o CEV tenga una de las siguientes políticas:

- La política `AdministratorAccess`
- La política `AmazonRDSFullAccess` con permisos necesarios para Amazon S3 y AWS KMS, creación de CEV y creación de instancias de base de datos

Temas

- Permisos de IAM necesarios para Amazon S3 y AWS KMS
- Permisos de IAM necesarios para crear una CEV
- Permisos de IAM necesarios para crear una instancia de base de datos desde una CEV

Permisos de IAM necesarios para Amazon S3 y AWS KMS

Para crear una CEV o instancias de base de datos de RDS Custom for Oracle, su entidad principal de IAM necesita acceder a Amazon S3 y AWS KMS. La siguiente política de JSON de muestra otorga los permisos necesarios.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateS3Bucket",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::do-not-delete-rds-custom-*"
        },
        {
            "Sid": "CreateKmsGrant",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información acerca del permiso de `kms:CreateGrant`, consulte Administración de AWS KMS key.

Permisos de IAM necesarios para crear una CEV

Para crear una CEV, su entidad principal de IAM necesita los siguientes permisos adicionales:

```
s3:GetObjectAcl
s3:GetObject
s3:GetObjectTagging
s3:ListBucket
mediaimport:CreateDatabaseBinarySnapshot
```

La siguiente política de JSON de ejemplo otorga permisos adicionales para acceder al bucket *my-custom-installation-files* y su contenido.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AccessToS3MediaBucket",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::my-custom-installation-files",
                "arn:aws:s3:::my-custom-installation-files/*"
            ]
        },
        {
            "Sid": "PermissionForByom",
            "Effect": "Allow",
            "Action": [
                "mediaimport:CreateDatabaseBinarySnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

También puede conceder permisos similares para Amazon S3 a las cuentas del autor de la llamada mediante una política de bucket de S3.

Permisos de IAM necesarios para crear una instancia de base de datos desde una CEV

Para crear una instancia de base de datos de RDS Custom para Oracle desde una CEV existente, la entidad principal de IAM necesita los siguientes permisos adicionales.

```
iam:SimulatePrincipalPolicy
cloudtrail:CreateTrail
cloudtrail:StartLogging
```

La siguiente política de JSON de ejemplo otorga los permisos necesarios para validar un rol de IAM y registrar la información en un AWS CloudTrail.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateIamRole",
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
            "Resource": "*"
        },
        {
            "Sid": "CreateCloudTrail",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:StartLogging"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
        }
    ]
}
```

Paso 6: configurar la VPC para RDS Custom for Oracle

La instancia de base de datos de RDS Custom se encuentra en una nube privada virtual (VPC) basada en el servicio Amazon VPC, tal como lo es una instancia de Amazon EC2 o una instancia de Amazon RDS. Proporcione y configure su propia VPC. A diferencia de RDS Custom para SQL Server, RDS Custom para Oracle no crea listas de control de acceso ni grupos de seguridad. Debe asociar su propio grupo de seguridad, subredes y tablas de enrutamiento.

Puede configurar la nube privada virtual (VPC) mediante CloudFormation o un proceso manual.

> **Important**
>
> Se recomienda encarecidamente que configure el entorno de RDS Custom para Oracle mediante AWS CloudFormation. Esta técnica es la más sencilla y la menos propensa a errores.

Temas

- Configuración de la VPC mediante CloudFormation (recomendado)
- Configurar la VPC manualmente para RDS Custom for Oracle

Configuración de la VPC mediante CloudFormation (recomendado)

Si ya ha configurado la VPC para otro motor de RDS Custom y desea reutilizar la VPC existente, omita este paso. En esta sección se presupone lo siguiente:

- Ya ha utilizado CloudFormation para crear el rol y el perfil de instancia de IAM.
- Conoce el ID de tabla de enrutamiento.

  Para que una instancia de base de datos sea privada, debe estar en una subred privada. Para que una subred sea privada, no debe estar asociada a una tabla de enrutamiento que tenga una puerta de enlace de Internet predeterminada. Para obtener más información, consulte Configurar tablas de enrutamiento en la Guía del usuario de Amazon VPC.

Cuando utiliza la plantilla de CloudFormation para su VPC, se crean los siguientes recursos:

- Una VPC privada

- Un grupo de subred denominado `rds-custom-private`
- Los siguientes puntos de conexión de VPC, que su instancia de base de datos usa para comunicarse con los Servicios de AWS dependientes:
  - `com.amazonaws.region.ec2messages`
  - `com.amazonaws.region.events`
  - `com.amazonaws.region.logs`
  - `com.amazonaws.region.monitoring`
  - `com.amazonaws.region.s3`
  - `com.amazonaws.region.secretsmanager`
  - `com.amazonaws.region.ssm`
  - `com.amazonaws.region.ssmmessages`

  Si está creando una implementación multi-AZ:

  - `com.amazonaws.region.sqs`

> **Note**
>
> Para una configuración de red compleja con cuentas existentes, le recomendamos que configure el acceso a los servicios dependientes manualmente si el acceso aún no existe. Para obtener más información, consulte Asegúrese de que su VPC pueda acceder a los Servicios de AWS dependientes.

Para configurar la VPC mediante CloudFormation

1. Abra la consola de CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Inicie el asistente Crear pila, seleccione Crear pila y, a continuación, Con recursos nuevos (estándar).
3. En la página Create stack (Crear pila), proceda del modo siguiente:
   a. En Prepare template (Preparar plantilla), elija Template is ready (La plantilla está lista).
   b. Para Template source (Origen de plantilla), elija Upload a template file (Cargar un archivo de plantilla).
   c. Para Choose file (Elegir un archivo), navegue hasta y, a continuación, elija `custom-vpc.json`.

d. Elija Siguiente.

4. En la página Specify stack Details (Especificar detalles de pila), haga lo siguiente:

   a. En Stack name (Nombre de pila), ingrese **`custom-vpc`**.
   b. Para Parameters (Parámetros), elija las subredes privadas que desea utilizar para las instancias de base de datos de RDS Custom.
   c. Elija el ID de VPC privado que se utilizará para las instancias de base de datos de RDS Custom.
   d. Ingrese la tabla de enrutamiento principal asociada a las subredes privadas.
   e. Elija Siguiente.

5. En la página Configurar opciones de pila, elija Siguiente.
6. En la página Revisar custom-vpc, elija Enviar.

   CloudFormation configura la VPC privada. En el panel de la izquierda, cuando custom-vpc indique CREATE_COMPLETE, continúe con el paso siguiente.

7. (Opcional) Revise los detalles de la VPC. En el panel Pilas, seleccione custom-vpc. En el panel de la derecha, haga lo siguiente:

   a. Elija Información de la pila. Su pila tiene un ID con el formato arn:aws:cloudformation:***`region`***:***`account-no`***:stack/custom-vpc/***`identifier`***.
   b. Seleccione Recursos. Debería ver un grupo de subredes denominado rds-custom-private y varios puntos de conexión de VPC que utilizan el formato de nomenclatura vpce-***`string`***. Cada punto de conexión se corresponde con un Servicio de AWS con el que RDS Custom necesita comunicarse. Para obtener más información, consulte Asegúrese de que su VPC pueda acceder a los Servicios de AWS dependientes.
   c. Elija Agregar parámetro. Debería ver las subredes privadas, la VPC privada y la tabla de enrutamiento que especificó al crear la pila. Al crear una instancia de base de datos, tiene que proporcionar el ID de VPC y el grupo de subred.

Configurar la VPC manualmente para RDS Custom for Oracle

Como alternativa a la creación de VPC de forma automática con AWS CloudFormation, puede configurar la VPC de forma manual. Esta opción puede ser la mejor cuando se tiene una configuración de red compleja que utilice los recursos existentes.

Temas

- Asegúrese de que su VPC pueda acceder a los Servicios de AWS dependientes
- Configurar el servicio de metadatos de instancia

Asegúrese de que su VPC pueda acceder a los Servicios de AWS dependientes

RDS Custom envía la comunicación desde la instancia de base de datos a otros Servicios de AWS. Asegúrese de que se pueda acceder a los siguientes servicios desde la subred en la que creó las instancias de base de datos de RDS Custom:

- Amazon CloudWatch (`com.amazonaws.`*`region`*`.monitoring`)
- Registros de Amazon CloudWatch (`com.amazonaws.`*`region`*`.logs`)
- Eventos de Amazon CloudWatch (`com.amazonaws.`*`region`*`.events`)
- Amazon EC2 (`com.amazonaws.`*`region`*`.ec2` y `com.amazonaws.`*`region`*`.ec2messages`)
- Amazon EventBridge (`com.amazonaws.`*`region`*`.events`)
- Amazon S3 (`com.amazonaws.`*`region`*`.s3`)
- AWS Secrets Manager (`com.amazonaws.`*`region`*`.secretsmanager`)
- AWS Systems Manager (`com.amazonaws.`*`region`*`.ssm` y `com.amazonaws.`*`region`*`.ssmmessages`)

Si se crean implementaciones multi-AZ

- Amazon Simple Queue Service (`com.amazonaws.`*`region`*`.sqs`)

Si RDS Custom no puede comunicarse con los servicios necesarios, publica los siguientes eventos:

```
Database instance in incompatible-network. SSM Agent connection not available. Amazon
 RDS can't connect to the dependent AWS services.
```

```
Database instance in incompatible-network. Amazon RDS can't connect to dependent AWS
 services. Make sure port 443 (HTTPS) allows outbound connections, and try again.
 "Failed to connect to the following services: s3 events"
```

Para evitar errores `incompatible-network`, asegúrese de que los componentes de la VPC que intervienen en la comunicación entre la instancia de base de datos de RDS Custom y Servicios de AWS cumplen los siguientes requisitos:

- La instancia de base de datos puede realizar conexiones salientes en el puerto 443 a otros Servicios de AWS.
- La VPC permite respuestas entrantes a solicitudes originadas en la instancia de base de datos de RDS Custom.
- RDS Custom puede resolver correctamente los nombres de dominio de los puntos de conexión de cada Servicio de AWS.

Si ya ha configurado una VPC para otro motor de base de datos de RDS Custom, puede reutilizar esa VPC y omitir este proceso.

Configurar el servicio de metadatos de instancia

Asegúrese de que la instancia pueda hacer lo siguiente:

- Acceda al servicio de metadatos de la instancia mediante la versión 2 del servicio de metadatos de la instancia (IMDSv2).
- Permitir comunicaciones salientes a través del puerto 80 (HTTP) a la dirección IP del enlace IMDS.
- Solicitar metadatos de instancia de `http://169.254.169.254`, el enlace IMDSv2.

Para obtener más información, consulte Utilizar IMDSv2 en la Guía del usuario de Amazon EC2.

RDS Custom para automatización de Oracle utiliza IMDSv2 de forma predeterminada, configurando `HttpTokens=enabled` en la instancia de Amazon EC2 subyacente. Sin embargo, puede usar IMDSv1 si lo desea. Para obtener más información, consulte Configurar las opciones de metadatos de instancia en la Guía del usuario de Amazon EC2.

Trabajar con versiones de motor personalizadas para Amazon RDS Custom for Oracle

Una versión de motor personalizado (CEV) para Amazon RDS Custom for Oracle es una instantánea de volumen binario de un motor de base de datos y una Amazon Machine Image (AMI) específica. De forma predeterminada, RDS Custom para Oracle usa la última AMI disponible administrada por RDS Custom, pero puede especificar una AMI que se usó en una CEV anterior. Almacena los archivos de instalación de la base de datos en Amazon S3. RDS Custom utiliza los archivos de instalación y la AMI para crear la CEV en su nombre.

Temas

- Preparación para crear una CEV
- Creación de una CEV
- Modificación del estado de CEV
- Visualización de detalles de la CEV de Amazon RDS Custom para Oracle
- Eliminación de una CEV

Preparación para crear una CEV

Para crear un CEV, acceda a los archivos de instalación y a los parches que están almacenados en su bucket de Amazon S3 para cualquiera de las siguientes versiones:

- Oracle Database 19c
- Oracle Database 18c
- Base de datos Oracle 12c versión 2 (12.2)
- Base de datos Oracle 12c versión 1 (12.1)

Por ejemplo, puede usar la RU/RUR de abril de 2021 para Oracle Database 19c o cualquier combinación válida de archivos de instalación y parches. Para obtener más información sobre las regiones y regiones compatibles con RDS Custom para Oracle, consulta RDS Custom con RDS para Oracle.

Temas

- Paso 1 (opcional): descargar las plantillas del manifiesto

- Paso 2: descargar revisiones y archivos de instalación de la base de datos desde Oracle Software Delivery Cloud
- Paso 3: cargar los archivos de instalación en Amazon S3
- Paso 4 (opcional): compartir los medios de instalación en S3 en Cuentas de AWS
- Paso 5: preparar el manifiesto de la CEV
- Paso 6 (opcional): validar el manifiesto de CEV
- Paso 7: añadir los permisos de IAM necesarios

Paso 1 (opcional): descargar las plantillas del manifiesto

Un manifiesto CEV es un documento JSON que incluye la lista de archivos.zip de instalación de la base de datos para su CEV. Para crear una CEV, haga lo siguiente:

1. Identifique los archivos de instalación de la base de datos Oracle que desea incluir en su CEV.
2. Descargue los archivos de instalación.
3. Cree un manifiesto JSON que enumere los archivos de instalación.

RDS Custom para Oracle proporciona plantillas de manifiestos JSON con los archivos.zip que recomendamos para cada versión compatible de Oracle Database. Por ejemplo, la siguiente plantilla es para la RU 19.17.0.0.0.

```
{
    "mediaImportTemplateVersion": "2020-08-14",
    "databaseInstallationFileNames": [
        "V982063-01.zip"
    ],
    "opatchFileNames": [
        "p6880880_190000_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames": [
        "p34419443_190000_Linux-x86-64.zip",
        "p34411846_190000_Linux-x86-64.zip"
    ],
    "otherPatchFileNames": [
        "p28852325_190000_Linux-x86-64.zip",
        "p29997937_190000_Linux-x86-64.zip",
        "p31335037_190000_Linux-x86-64.zip",
        "p32327201_190000_Linux-x86-64.zip",
```

```
        "p33613829_190000_Linux-x86-64.zip",
        "p34006614_190000_Linux-x86-64.zip",
        "p34533061_190000_Linux-x86-64.zip",
        "p34533150_190000_Generic.zip",
        "p28730253_190000_Linux-x86-64.zip",
        "p29213893_1917000DBRU_Generic.zip",
        "p33125873_1917000DBRU_Linux-x86-64.zip",
        "p34446152_1917000DBRU_Linux-x86-64.zip"
    ]
}
```

Cada plantilla tiene un archivo readme asociado que incluye instrucciones para descargar las revisiones, las URL de los archivos.zip y las sumas de verificación de los archivos. Puede utilizar estas plantillas tal como están o modificarlas con sus propias revisiones. Para revisar las plantillas, descargue custom-oracle-manifest.zip en el disco local y, a continuación, ábralo con una aplicación de archivado de archivos. Para obtener más información, consulte Paso 5: preparar el manifiesto de la CEV.

Paso 2: descargar revisiones y archivos de instalación de la base de datos desde Oracle Software Delivery Cloud

Cuando haya identificado los archivos de instalación que desea para su CEV, descárguelos en su sistema local. Los archivos y las revisiones de instalación de Oracle Database se alojan en Oracle Software Delivery Cloud. Cada CEV requiere una versión básica, como Oracle Database 19c u Oracle Database 12c Versión 2 (12.2), y una lista de revisiones opcional.

Para descargar los archivos de instalación de Oracle Database

1. Vaya a https://edelivery.oracle.com/ e inicie sesión.
2. En el cuadro de búsqueda, introduzca **`Oracle Database Enterprise Edition`** o **`Oracle Database Standard Edition 2`** y elija Search.
3. Elija una de las siguientes versiones básicas:

Versión de base de datos	Enterprise Edition	Standard Edition 2
Oracle Database 19c	DLP: Oracle Database 19c Enterprise	DLP: Oracle Database 19c Standard

Versión de base de datos	Enterprise Edition	Standard Edition 2
	Edition 19.3.0.0.0 (Oracle Database Enterprise Edition)	Edition 2 19.3.0.0.0 (Oracle Database Standard Edition 2)
Oracle Database 18c	DLP: Oracle Database 18c Enterprise Edition 18.0.0.0.0 (Oracle Database Enterprise Edition)	DLP: Oracle Database Standard Edition 2 18.0.0.0.0 (Oracle Database Standard Edition 2)
Oracle Database 12c versión 2 (12.2.0.1)	DLP: Oracle Database 12c Enterprise Edition 12.2.0.1.0 (Oracle Database Enterprise Edition)	DLP: Oracle Database Standard Edition 2 12.2.0.1.0 (Oracle Database Standard Edition 2)
Oracle Database 12c versión 1 (12.1.0.2)	DLP: Oracle Database 12c Enterprise Edition 12.1.0.2.0 (Oracle Database Enterprise Edition)	DLP: Oracle Database Standard Edition 2 12.1.0.2.0 (Oracle Database Standard Edition 2)

4. Elija Continuar.
5. Borre la casilla de verificación Download Queue (Descargar cola).
6. Elija la opción que corresponda a su versión básica:
   - Oracle Database 19,3.0.0.0 - Versión a largo plazo.
   - Oracle Database 18.0.0.0.0
   - Oracle Database 12.2.0.1.0.
   - Oracle Database 12.1.0.2.0.
7. Elija Linux x86-64 en Plataforma/Idiomas.
8. Seleccione Continuar y firme el contrato de licencia de Oracle.
9. Elija el archivo .zip que corresponda a su versión de la base de datos:

Versión y edición de la base de datos	Archivos zip	Hash SHA-256
19c EE y SE2	V982063-01.zip	BA8329C757133DA313ED3B6D7F86C5AC42CD9970A28BF2E6233F3235233AA8D8
18c EE y SE2	V978967-01.zip	C96A4FD768787AF98272008833FE10B172691CF84E42816B138C12D4DE63AB96
12.2.0.1 EE y SE2	V839960-01.zip	96ED97D21F15C1AC0CCE3749DA6C3DAC7059BB60672D76B008103FC754D22DDE
12.1.0.2 EE	V46095-01_1of2.zip V46095-01_2of2.zip	31FDC2AF41687B4E547A3A18F796424D8C1AF36406D2160F65B0AF6A9CD47355 for V46095-01_1of2.zip 03DA14F5E875304B28F0F3BB02AF0EC33227885B99C9865DF70749D1E220ACCD for V46095-01_2of2.zip
12.1.0.2 SE2	V77388-01_1of2.zip V77388-01_2of2.zip	73873369753230F5A0921F95ACEADB591388CB06ED72A7F3AEA7BCBCEA2403BC para V77388-01_1of2.zip 2492E1BE1E3E3531DA83D0843C09C08E435AC8CEFD9A00C0DF56BE4F15CEEBF3 para V77388-01_2of2.zip

10. Descargue las revisiones de Oracle que desee desde `updates.oracle.com` o `support.oracle.com` en su sistema local. Puede encontrar las URL de las revisiones en las siguientes ubicaciones:

    - Los archivos readme del archivo .zip que ha descargado en Paso 1 (opcional): descargar las plantillas del manifiesto
    - Las revisiones que se enumeran en cada actualización de la versión (RU) en Notas de versión de Amazon Relational Database Service (Amazon RDS) para Oracle.

Paso 3: cargar los archivos de instalación en Amazon S3

Cargue los archivos de revisión y de instalación de Oracle en Amazon S3 mediante la AWS CLI. El bucket de S3 que contiene los archivos de instalación debe estar en la misma Región AWS como CEV.

En los ejemplos de esta sección se utilizan los siguientes marcadores de posición:

- *`install-or-patch-file.zip`*: archivo multimedia de instalación de Oracle. Por ejemplo, p32126828_190000_Linux-x86-64.zip es una revisión.
- *`amzn-s3-demo-destination-bucket`*: el bucket de Amazon S3 designado para los archivos de instalación cargados.
- *`123456789012/cev1`*: prefijo opcional en el bucket de Amazon S3.
- *`amzn-s3-demo-source-bucket`*: bucket de Amazon S3 en el que puede organizar archivos de forma opcional.

Temas

- Paso 3a: compruebe que el bucket de S3 esté en la Región de AWS correcta
- Paso 3b: asegúrese de que su política de buckets de S3 tenga los permisos correctos
- Paso 3c: cargue sus archivos mediante los comandos cp o sync
- Paso 3d: enumere los archivos en su bucket de S3

Paso 3a: compruebe que el bucket de S3 esté en la Región de AWS correcta

Compruebe que el bucket de S3 esté en la Región AWS en la que planea ejecutar el comando `create-custom-db-engine-version`.

```
aws s3api get-bucket-location --bucket amzn-s3-demo-destination-bucket
```

Paso 3b: asegúrese de que su política de buckets de S3 tenga los permisos correctos

Puede crear una CEV desde cero o desde una CEV de origen. Si planea crear una CEV nueva a partir de las CEV de origen, asegúrese de que su política de bucket de S3 tenga los permisos correctos:

1. Identifique el bucket de S3 reservado por RDS Custom. El nombre del bucket tiene el formato `do-not-delete-rds-custom-`*`account`*`-`*`region`*`-`*`string`*. Por ejemplo, el nombre del bucket puede ser `do-not-delete-rds-custom-`*`123456789012`*`-`*`us-east-1`*`-`*`abc123EXAMPLE`*.
2. Asegúrese de que el siguiente permiso esté adjunto a la política de bucket de S3. Reemplace `do-not-delete-rds-custom-`*`123456789012`*`-`*`us-east-1`*`-`*`abc123EXAMPLE`* con el nombre de su bucket.

```
{
    "Sid": "AWSRDSCustomForOracleCustomEngineVersionGetObject",
    "Effect": "Allow",
    "Principal": {
        "Service": "custom.rds.amazonaws.com"
    },
    "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging"
    ],
    "Resource": "arn:aws:s3:::do-not-delete-rds-custom-123456789012-us-
east-1-abc123EXAMPLE/CustomEngineVersions/*"
}, ...
```

Paso 3c: cargue sus archivos mediante los comandos cp o sync

Elija cualquiera de las siguientes opciones:

- Utilice `aws s3 cp` para cargar un solo archivo .zip.

  Cargue cada archivo .zip de instalación por separado. No combine los archivos .zip en un solo archivo .zip.
- Use `aws s3 sync` para cargar un directorio.

Example

El siguiente ejemplo carga *`install-or-patch-file.zip`* en la carpeta *`123456789012/cev1`* en el bucket de Amazon S3 de RDS Custom. Ejecute un comando `aws s3` separado para cada .zip que desee cargar.

Para Linux, macOS o:Unix

```
aws s3 cp install-or-patch-file.zip \
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

En:Windows

```
aws s3 cp install-or-patch-file.zip ^
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

Example

El siguiente ejemplo carga los archivos en su carpeta *cev1* local a la carpeta *123456789012/cev1* en su bucket de Amazon S3.

Para Linux, macOS o:Unix

```
aws s3 sync cev1 \
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

En:Windows

```
aws s3 sync cev1 ^
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

Example

El siguiente ejemplo carga todos los archivos *amzn-s3-demo-source-bucket* en la carpeta *123456789012/cev1* en el bucket de Amazon S3.

Para Linux, macOS o:Unix

```
aws s3 sync s3://amzn-s3-demo-source-bucket/ \
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

En:Windows

```
aws s3 sync s3://amzn-s3-demo-source-bucket/ ^
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

Paso 3d: enumere los archivos en su bucket de S3

El siguiente ejemplo utiliza el comando `s3 ls` para enumerar los archivos de su bucket de Amazon S3 de RDS Custom.

```
aws s3 ls \
    s3://amzn-s3-demo-destination-bucket/123456789012/cev1/
```

Paso 4 (opcional): compartir los medios de instalación en S3 en Cuentas de AWS

Para la finalidad de esta sección, el bucket de Amazon S3 que contiene los archivos de instalación de Oracle está en su bucket de medios. Es posible que su organización utilice varias Cuentas de AWS en una Región de AWS. Si es así, puede usar una Cuenta de AWS para rellenar el bucket de medios y una Cuenta de AWS diferente para crear CEV. Si no desea compartir el bucket de medios, vaya a la siguiente sección.

En esta sección se presupone lo siguiente:

- Puede acceder a la cuenta que creó su bucket de medios y a otra cuenta en la que tiene pensado crear CEV.
- Tiene pensado crear CEV en una sola Región de AWS. Si tiene pensado usar varias regiones, cree un bucket de medios en cada región.
- Está usando la CLI. Si utiliza la consola de Amazon S3, siga estos pasos:

Para configurar su bucket de medios para compartirlo entre Cuentas de AWS

1. Inicie sesión en la Cuenta de AWS que contiene el bucket de S3 en el que ha cargado los medios de instalación.
2. Comience con una plantilla de política JSON en blanco o una política existente que pueda adaptar.

   El siguiente comando recupera una política existente y la guarda como *my-policy.json*. En este ejemplo, el bucket de S3 que contiene los archivos de instalación se denomina *amzn-s3-demo-bucket*.

   ```
   aws s3api get-bucket-policy \
       --bucket amzn-s3-demo-bucket \
       --query Policy \
   ```

```
    --output text > my-policy.json
```

3. Edite los permisos del bucket de medios de la siguiente manera:

   - En el elemento `Resource` de la plantilla, especifique el bucket de S3 en el que ha cargado los archivos de instalación de Oracle Database.
   - En el elemento `Principal`, especifique los ARN para todas las Cuentas de AWS que pretende usar para crear CEV. Puede añadir la raíz, un usuario o un rol a la lista de buckets de S3 permitidos. Para obtener más información, consulte Identificadores de IAM en la Guía del usuario de AWS Identity and Access Management.

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "GrantAccountsAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-1:root",
                    "arn:aws:iam::account-2:user/user-name-with-path",
                    "arn:aws:iam::account-3:role/role-name-with-path",
                    ...
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

4. Adjunte la política a su bucket de medios.

En el siguiente ejemplo, *amzn-s3-demo-bucket* es el nombre del bucket de S3 que contiene los archivos de instalación, y *my-policy.json* es el nombre del archivo JSON.

```
aws s3api put-bucket-policy \
    --bucket amzn-s3-demo-bucket \
    --policy file://my-policy.json
```

5. Inicie sesión en una Cuenta de AWS en la que piensa crear CEV.
6. Verifique que esta cuenta pueda acceder al bucket de medios en la Cuenta de AWS que lo creó.

```
aws s3 ls --query "Buckets[].Name"
```

Para obtener más información, consulte aws s3 ls en la referencia de comandos de la AWS CLI.

7. Cree un CEV siguiendo los pasos de Creación de una CEV.

Paso 5: preparar el manifiesto de la CEV

Un manifiesto de CEV es un documento JSON que incluye lo siguiente:

- (Obligatorio) La lista de archivos de instalación .zip que ha cargado en Amazon S3. RDS Custom aplica los parches en el orden en que aparecen en el manifesto.
- (Opcional) Parámetros de instalación que establecen valores no predeterminados para la base de Oracle, el directorio raíz Oracle y el ID y el nombre del usuario y el grupo de UNIX/Linux. Tenga en cuenta que no puede modificar los parámetros de instalación de una CEV existente o una instancia de base de datos existente. Tampoco puede actualizar de una CEV a otra si los parámetros de instalación tienen configuraciones diferentes.

Para ver ejemplos de manifiestos de CEV, consulte las plantillas de JSON que ha descargado en Paso 1 (opcional): descargar las plantillas del manifiesto. También puede revisar los ejemplos en Ejemplos de manifiestos CEV.

Temas

- Campos JSON en el manifiesto de CEV
- Creación del manifiesto de CEV
- Ejemplos de manifiestos CEV

Campos JSON en el manifiesto de CEV

La siguiente tabla describe los campos JSON en el manifiesto.

Campo JSON	Descripción
`MediaImportTemplateVersion`	Versión del manifiesto de CEV. La fecha tiene el formato `YYYY-MM-DD` .
`databaseInstallationFileNames`	Lista ordenada de archivos de instalación para la base de datos.
`opatchFileNames`	Lista ordenada de instaladores de OPatch utilizados para el motor de base de datos de Oracle. Solo es válido un valor. Los valores de `opatchFileNames` deben comenzar con `p6880880_` .
`psuRuPatchFileNames`	Las revisiones de PSU y RU para esta base de datos. **Important** Si incluye `psuRuPatchFileNames` , `opatchFileNames` es necesario. Los valores de `opatchFileNames` deben comenzar con `p6880880_` .
`OtherPatchFileNames`	Las revisiones que no figuran en la lista de revisiones de PSU y RU. RDS Custom aplica estas revisiones después de aplicar las revisiones de PSU y RU. **Important** Si incluye `OtherPatchFileNames` , `opatchFileNames` es necesario. Los valores de `opatchFileNames` deben comenzar con `p6880880_` .
`installationParameters`	Configuración no predeterminada para la base de Oracle, el directorio raíz de Oracle, y el ID y el nombre del usuario y el grupo de UNIX/Linux. Puede definir los siguientes parámetros:

Campo JSON	Descripción
	oracleBase El directorio en el que están instalados los archivos binarios de Oracle. Es el punto de montaje del volumen binario que almacena los archivos. El directorio raíz de Oracle puede incluir varias páginas de inicio de Oracle. Por ejemplo, si `/home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1` es uno de sus directorios de directorio raíz de Oracle, entonces `/home/oracle` es el directorio base de Oracle. Un directorio base de Oracle especificado por el usuario no es un enlace simbólico. Si no especifica la base de Oracle, el directorio predeterminado es `/rdsdbbin` . oracleHome El directorio en el que están instalados los archivos binarios de Oracle. Por ejemplo, si especifica `/home/oracle/` como base de Oracle, podría especificar `/home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1/` como su directorio raíz de Oracle. Un directorio raíz de Oracle especificado por el usuario no es un enlace simbólico. La variable de entorno `$ORACLE_HOME` hace referencia al valor de directorio raíz de Oracle. Si no especifica el directorio raíz de Oracle, el formato predeterminado es `/rdsdbbin/oracle.` *`major-engine-version`* `.custom.r1.` *`engine-edition`* `.1`. unixUname Es el nombre del usuario de UNIX que posee el software de Oracle. RDS Custom asume este usuario al ejecutar comandos de bases de datos locales. Si especifica ambos valores `unixUid` y `unixUname` , RDS Custom crea el usuario si no existe y, a continuación, asigna el UID al usuario si no es el mismo que el UID inicial.

Campo JSON	Descripción
	El nombre de usuario predeterminado es `rdsdb`. unixUid Es el ID (UID) del usuario de UNIX que posee el software de Oracle. Si especifica ambos valores `unixUid` y `unixUname`, RDS Custom crea el usuario si no existe y, a continuación, asigna el UID al usuario si no es el mismo que el UID inicial. El UID predeterminado es `61001`. Este es el UID del usuario `rdsdb`. unixGroupName Es el nombre del grupo de UNIX. El usuario de UNIX que posee el software de Oracle pertenece a este grupo. El nombre predeterminado del grupo es `rdsdb`. unixGroupId Es el ID del grupo de UNIX al que pertenece el usuario de UNIX. El ID predeterminado del grupo es `1000`. Este es el ID del grupo `rdsdb`.

Cada versión de Oracle Database tiene una lista diferente de archivos de instalación compatibles. Cuando cree el manifiesto de CEV, asegúrese de especificar solo los archivos compatibles con RDS Custom para Oracle. De lo contrario, se produce un error en la creación de CEV. Las revisiones que se enumeran en cada actualización de la versión (RU) en Notas de versión de Amazon Relational Database Service (Amazon RDS) para Oracle.

Creación del manifiesto de CEV

Para crear un manifiesto CEV

1. Enumere todos los archivos de instalación que va a aplicar, en el orden en que desea aplicarlos.

2. Correlacione los archivos de instalación con los campos JSON que se describen en Campos JSON en el manifiesto de CEV.
3. Haga una de estas dos operaciones:
   - Cree el manifiesto CEV como un archivo de texto JSON.
   - Edite la plantilla de manifiesto CEV cuando cree el CEV en la consola. Para obtener más información, consulte Creación de una CEV.

Ejemplos de manifiestos CEV

Los siguientes ejemplos muestran archivos de manifiesto CEV para diferentes versiones de Oracle Database. Si incluye un campo JSON en el manifiesto, asegúrese de que no esté vacío. Por ejemplo, el siguiente manifiesto CEV no es válido porque `otherPatchFileNames` está vacío.

```
{
    "mediaImportTemplateVersion": "2020-08-14",
    "databaseInstallationFileNames": [
        "V982063-01.zip"
    ],
    "opatchFileNames": [
        "p6880880_190000_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames": [
        "p32126828_190000_Linux-x86-64.zip"
    ],
    "otherPatchFileNames": [
    ]
}
```

Temas

- Sample CEV manifest for Oracle Database 12c Release 1 (12.1)
- Sample CEV manifest for Oracle Database 12c Release 2 (12.2)
- Sample CEV manifest for Oracle Database 18c
- Sample CEV manifest for Oracle Database 19c

Example Manifiesto CEV de ejemplo para Oracle Database 12c versión 1 (12.1)

En el siguiente ejemplo para PSU de julio de 2021 para Oracle Database 12c, versión 1 (12.1), RDS Custom aplica los parches en el orden especificado. Por lo tanto, RDS Custom aplica p32768233; luego, p18759211 y así sucesivamente. El ejemplo establece valores nuevos para el usuario y el grupo de UNIX, así como para el directorio raíz y la base de Oracle.

```
{
    "mediaImportTemplateVersion":"2020-08-14",
    "databaseInstallationFileNames":[
        "V46095-01_1of2.zip",
        "V46095-01_2of2.zip"
    ],
    "opatchFileNames":[
        "p6880880_121010_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames":[
        "p32768233_121020_Linux-x86-64.zip"
    ],
    "otherPatchFileNames":[
        "p32876425_121020_Linux-x86-64.zip",
        "p18759211_121020_Linux-x86-64.zip",
        "p19396455_121020_Linux-x86-64.zip",
        "p20875898_121020_Linux-x86-64.zip",
        "p22037014_121020_Linux-x86-64.zip",
        "p22873635_121020_Linux-x86-64.zip",
        "p23614158_121020_Linux-x86-64.zip",
        "p24701840_121020_Linux-x86-64.zip",
        "p25881255_121020_Linux-x86-64.zip",
        "p27015449_121020_Linux-x86-64.zip",
        "p28125601_121020_Linux-x86-64.zip",
        "p28852325_121020_Linux-x86-64.zip",
        "p29997937_121020_Linux-x86-64.zip",
        "p31335037_121020_Linux-x86-64.zip",
        "p32327201_121020_Linux-x86-64.zip",
        "p32327208_121020_Generic.zip",
        "p17969866_12102210119_Linux-x86-64.zip",
        "p20394750_12102210119_Linux-x86-64.zip",
        "p24835919_121020_Linux-x86-64.zip",
        "p23262847_12102201020_Linux-x86-64.zip",
        "p21171382_12102201020_Generic.zip",
        "p21091901_12102210720_Linux-x86-64.zip",
        "p33013352_12102210720_Linux-x86-64.zip",
```

```
        "p25031502_12102210720_Linux-x86-64.zip",
        "p23711335_12102191015_Generic.zip",
        "p19504946_121020_Linux-x86-64.zip"
    ],
    "installationParameters": {
        "unixGroupName": "dba",
        "unixGroupId": 12345,
        "unixUname": "oracle",
        "unixUid": 12345,
        "oracleHome": "/home/oracle/oracle.12.1.0.2",
        "oracleBase": "/home/oracle"
    }
}
```

Example Manifiesto CEV de ejemplo para Oracle Database 12c versión 2 (12.2)

En el siguiente ejemplo para PSU de octubre de 2021 para Oracle Database 12c, versión 2 (12.2), RDS Custom aplica p33261817; luego, p33192662; luego, p29213893 y así sucesivamente. El ejemplo establece valores nuevos para el usuario y el grupo de UNIX, así como para el directorio raíz y la base de Oracle.

```
{
    "mediaImportTemplateVersion":"2020-08-14",
    "databaseInstallationFileNames":[
        "V839960-01.zip"
    ],
    "opatchFileNames":[
        "p6880880_122010_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames":[
        "p33261817_122010_Linux-x86-64.zip"
    ],
    "otherPatchFileNames":[
        "p33192662_122010_Linux-x86-64.zip",
        "p29213893_122010_Generic.zip",
        "p28730253_122010_Linux-x86-64.zip",
        "p26352615_12201211019DBOCT2021RU_Linux-x86-64.zip",
        "p23614158_122010_Linux-x86-64.zip",
        "p24701840_122010_Linux-x86-64.zip",
        "p25173124_122010_Linux-x86-64.zip",
        "p25881255_122010_Linux-x86-64.zip",
        "p27015449_122010_Linux-x86-64.zip",
        "p28125601_122010_Linux-x86-64.zip",
```

```
        "p28852325_122010_Linux-x86-64.zip",
        "p29997937_122010_Linux-x86-64.zip",
        "p31335037_122010_Linux-x86-64.zip",
        "p32327201_122010_Linux-x86-64.zip",
        "p32327208_122010_Generic.zip"
    ],
    "installationParameters": {
        "unixGroupName": "dba",
        "unixGroupId": 12345,
        "unixUname": "oracle",
        "unixUid": 12345,
        "oracleHome": "/home/oracle/oracle.12.2.0.1",
        "oracleBase": "/home/oracle"
    }
}
```

Example Manifiesto CEV de ejemplo para Oracle Database 18c

En el siguiente ejemplo para PSU de octubre de 2021 para Oracle Database 18c, RDS Custom aplica p32126855; luego, p28730253; luego, p27539475 y así sucesivamente. El ejemplo establece valores nuevos para el usuario y el grupo de UNIX, así como para el directorio raíz y la base de Oracle.

```
{
    "mediaImportTemplateVersion":"2020-08-14",
    "databaseInstallationFileNames":[
        "V978967-01.zip"
    ],
    "opatchFileNames":[
        "p6880880_180000_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames":[
        "p32126855_180000_Linux-x86-64.zip"
    ],
    "otherPatchFileNames":[
        "p28730253_180000_Linux-x86-64.zip",
        "p27539475_1813000DBRU_Linux-x86-64.zip",
        "p29213893_180000_Generic.zip",
        "p29374604_1813000DBRU_Linux-x86-64.zip",
        "p29782284_180000_Generic.zip",
        "p28125601_180000_Linux-x86-64.zip",
        "p28852325_180000_Linux-x86-64.zip",
        "p29997937_180000_Linux-x86-64.zip",
```

```
        "p31335037_180000_Linux-x86-64.zip",
        "p31335142_180000_Generic.zip"
    ]
    "installationParameters": {
        "unixGroupName": "dba",
        "unixGroupId": 12345,
        "unixUname": "oracle",
        "unixUid": 12345,
        "oracleHome": "/home/oracle/18.0.0.0.ru-2020-10.rur-2020-10.r1",
        "oracleBase": "/home/oracle/"
    }
}
```

Example Manifiesto CEV de ejemplo para Oracle Database 19c

En el siguiente ejemplo para Oracle Database 19c, RDS Custom aplica p32126828; luego, p29213893; luego, p29782284 y así sucesivamente. El ejemplo establece valores nuevos para el usuario y el grupo de UNIX, así como para el directorio raíz y la base de Oracle.

```
{
    "mediaImportTemplateVersion": "2020-08-14",
    "databaseInstallationFileNames": [
        "V982063-01.zip"
    ],
    "opatchFileNames": [
        "p6880880_190000_Linux-x86-64.zip"
    ],
    "psuRuPatchFileNames": [
        "p32126828_190000_Linux-x86-64.zip"
    ],
    "otherPatchFileNames": [
        "p29213893_1910000DBRU_Generic.zip",
        "p29782284_1910000DBRU_Generic.zip",
        "p28730253_190000_Linux-x86-64.zip",
        "p29374604_1910000DBRU_Linux-x86-64.zip",
        "p28852325_190000_Linux-x86-64.zip",
        "p29997937_190000_Linux-x86-64.zip",
        "p31335037_190000_Linux-x86-64.zip",
        "p31335142_190000_Generic.zip"
    ],
    "installationParameters": {
        "unixGroupName": "dba",
        "unixGroupId": 12345,
```

```
        "unixUname": "oracle",
        "unixUid": 12345,
        "oracleHome": "/home/oracle/oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1",
        "oracleBase": "/home/oracle"
    }
}
```

Paso 6 (opcional): validar el manifiesto de CEV

Opcionalmente, compruebe que el manifiesto es un archivo JSON válido al ejecutar el Script de Python `json.tool`. Por ejemplo, si cambia al directorio que contiene un manifiesto CEV denominado `manifest.json`, ejecute el siguiente comando.

```
python -m json.tool < manifest.json
```

Paso 7: añadir los permisos de IAM necesarios

Asegúrese de que la entidad principal de IAM que crea el CEV tenga las políticas necesarias descritas en Paso 5: otorgar los permisos necesarios al rol o usuario de IAM.

Creación de una CEV

Puede crear un CEV mediante el AWS Management Console o el AWS CLI. Especifique la arquitectura multitenencia o no multitenencia. Para obtener más información, consulte Consideraciones sobre la arquitectura multitenencia.

Normalmente, crear una CEV lleva aproximadamente dos horas. Una vez creada la CEV, puede utilizarla para usarla para crear o actualizar una instancia de base de datos de RDS Custom. Para obtener más información, consulte Creación de una instancia de base de datos de RDS Custom for Oracle y Actualización de una instancia de base de datos de RDS Custom para Oracle.

> **Note**
>
> Si su instancia de base de datos utiliza actualmente Oracle Linux 7.9, cree un nuevo CEV que utilice la AMI más reciente, que utilice Oracle Linux 8. A continuación, modifique su instancia para usar el nuevo CEV.

Tome nota de los siguientes requisitos y limitaciones para crear una CEV:

- El bucket de Amazon S3 que incluye los archivos de instalación debe estar en la misma Región de AWS que la CEV. De lo contrario, el proceso de creación producirá un error.
- El nombre de la CEV debe estar en el formato *major-engine-version*.*customized_string*, como en `19.cdb_cev1`.
- El nombre de la CEV debe contener de 1 a 50 caracteres alfanuméricos, guiones bajos, guiones o puntos.
- El nombre de la CEV no puede contener puntos consecutivos, como en `19..cdb_cev1`.

Consola

Para crear una CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).

   La página de Custom engine versions (Versiones de motor personalizadas) muestra todos las CEV que existen actualmente. Si no ha creado ninguna CEV, la página está vacía.
3. Elija Crear versión de motor personalizada.
4. En Opciones del motor, haga lo siguiente:

   a. En Engine type (Tipo de motor), elija Oracle.

   b. En Configuración de la arquitectura, elija Arquitectura multitenencia para crear una CEV multiinquilino de Oracle que utilice el motor de base de datos `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`. Puede crear una CDB de RDS Custom para Oracle únicamente con una CEV de varios inquilinos. Si no elige esta opción, su CEV no será una CDB que usa el motor `custom-oracle-ee` o `custom-oracle-se2`.

   > **Note**
   >
   > La arquitectura que elija será una característica permanente de su CEV. No puede modificar su CEV para usar una arquitectura diferente más adelante.

   c. Elija cualquiera de las siguientes opciones:

   - Crear nueva CEV: cree una CEV desde cero. En este caso, debe especificar un manifiesto de JSON que especifique los binarios de la base de datos.

- Crear CEV a partir de origen: en Especificar la CEV que se desea copiar, seleccione una CEV existente para usarla como la CEV de origen. En este caso, puede especificar una nueva imagen de máquina de Amazon (AMI), pero no puede especificar binarios de base de datos diferentes.

d. En Versión del motor, elija la versión principal del motor.

5. En Detalles de la versión, realice lo siguiente:

a. Introduzca un nombre válido en Nombre de la versión del motor personalizada. Por ejemplo, puede ingresar el nombre **`19.cdb_cev1`**.

b. (Opcional) Escriba una descripción para la CEV.

6. En Instalación de medios, haga lo siguiente:

a. (Opcional) En ID de AMI, deje el campo en blanco para utilizar la AMI más reciente proporcionada por el servicio o introduzca una AMI que haya utilizado anteriormente para crear una CEV. Para obtener ID de AMI válidos, utilice cualquiera de las siguientes técnicas:

- En la consola, seleccione Versiones de motor personalizadas en el panel de navegación izquierdo y elija el nombre de una CEV. El ID de AMI utilizado por la CEV aparece en la pestaña Configuración.
- En la AWS CLI, utilice el comando `describe-db-engine-versions`. Busque en la salida de `ImageID`.

b. Para S3 location of manifest files (Ubicación S3 de los archivos de manifiesto), ingrese la ubicación del bucket de Amazon S3 que especificó en Paso 3: cargar los archivos de instalación en Amazon S3. Por ejemplo, escriba **`s3://my-custom-installation-files/123456789012/cev1/`**.

> **Note**
>
> La Región de AWS en la que crea la CEV debe ser la misma que la del bucket de S3.

c. (Solo para Crear nueva CEV) En Manifiesto de la CEV, introduzca el manifiesto de JSON que ha creado en Creación del manifiesto de CEV.

7. En la sección Clave de KMS, seleccione Escriba un ARN de clave para ver las claves AWS KMS disponibles. A continuación, seleccione la clave de KMS de la lista.

Se requiere una clave AWS KMS para RDS Custom. Para obtener más información, consulte Paso 1: crear o reutilizar una clave AWS KMS de cifrado simétrica.

8. (Opcional) Seleccione Añadir una etiqueta nueva para crear un par clave-valor para su CEV.
9. Elija Crear versión de motor personalizada.

   Si el manifiesto de JSON tiene un formulario no válido, la consola mostrará Error al validar el manifiesto de la CEV. Corrija los problemas e inténtelo de nuevo.

Aparece la página de Custom engine versions (Versiones de motor personalizadas). Su CEV se muestra con el estado Create (Crear). El proceso para crear la CEV toma aproximadamente dos horas.

AWS CLI

Para crear una CEV mediante la AWS CLI, ejecute el comando create-custom-db-engine-version.

Se requieren las siguientes opciones:

- `--engine`: especifique el tipo de motor. Para una CDB, especifique `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`. Para no CDB, especifique `custom-oracle-ee` o `custom-oracle-se2`. Solo puede crear CDB a partir de una CEV creada con `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`. Solo puede crear no CDB a partir de una CEV creada con `custom-oracle-ee` o `custom-oracle-se2`.
- `--engine-version`: especifique la versión del motor. El formato es *`major-engine-version.customized_string`*. El nombre de la CEV debe contener de 1 a 50 caracteres alfanuméricos, guiones bajos, guiones o puntos. El nombre de la CEV no puede contener puntos consecutivos, como en `19..cdb_cev1`.
- `--kms-key-id`: especifique un AWS KMS key.
- `--manifest`: especifique *`manifest_json_string`* o `--manifest file:`*`file_name`*. No se permiten caracteres de nueva línea en *`manifest_json_string`*. Asegúrese de escapar de las comillas dobles (") en el código JSON prefijándolos con una barra invertida (\).

  En el siguiente ejemplo, se muestra *`manifest_json_string`* para 19c desde Paso 5: preparar el manifiesto de la CEV. El ejemplo establece valores nuevos para la base de Oracle, la página de inicio de Oracle, y el ID y el nombre del usuario y el grupo de UNIX/Linux. Si copia esta cadena, elimine todos los caracteres de nueva línea antes de pegarla en el comando.

```
"{\"mediaImportTemplateVersion\": \"2020-08-14\",
\"databaseInstallationFileNames\": [\"V982063-01.zip\"],
\"opatchFileNames\": [\"p6880880_190000_Linux-x86-64.zip\"],
\"psuRuPatchFileNames\": [\"p32126828_190000_Linux-x86-64.zip\"],
\"otherPatchFileNames\": [\"p29213893_1910000DBRU_Generic.zip\",
\"p29782284_1910000DBRU_Generic.zip\",\"p28730253_190000_Linux-
x86-64.zip\",\"p29374604_1910000DBRU_Linux-x86-64.zip\",
\"p28852325_190000_Linux-x86-64.zip\",\"p29997937_190000_Linux-x86-64.zip
\",\"p31335037_190000_Linux-x86-64.zip\",\"p31335142_190000_Generic.zip
\"]\"installationParameters\":{ \"unixGroupName\":\"dba\",
\ \"unixUname\":\"oracle\", \ \"oracleHome\":\"/home/oracle/
oracle.19.0.0.0.ru-2020-04.rur-2020-04.r1.EE.1\", \ \"oracleBase\":\"/
home/oracle/\"}}"
```

- `--database-installation-files-s3-bucket-name`: ponga el mismo nombre de bucket que haya puesto en Paso 3: cargar los archivos de instalación en Amazon S3. La Región de AWS donde ejecute `create-custom-db-engine-version` debe estar en la misma región que el bucket de Amazon S3.

También puede especificar las siguientes opciones:

- `--description`: ponga una descripción de la CEV.
- `--database-installation-files-s3-prefix`: ponga el mismo nombre de carpeta que haya puesto en Paso 3: cargar los archivos de instalación en Amazon S3.
- `--image-id`: especifique el ID de AMI que desea reutilizar. Para encontrar ID válidos, ejecute el comando `describe-db-engine-versions` y, a continuación, busque el resultado de `ImageID`. De forma predeterminada, RDS Custom para Oracle utiliza la AMI más reciente disponible.

El siguiente ejemplo crea una CEV multitenencia de Oracle denominada `19.cdb_cev1`. En el ejemplo, se reutiliza una AMI existente en lugar de utilizar la AMI más reciente disponible. Asegúrese de que el nombre de la CEV comience con el número de versión principal del motor.

Example

Para Linux, macOS o Unix:

```
aws rds create-custom-db-engine-version \
```

```
    --engine custom-oracle-se2-cdb \
    --engine-version 19.cdb_cev1 \
    --database-installation-files-s3-bucket-name us-east-1-123456789012-custom-
installation-files \
    --database-installation-files-s3-prefix 123456789012/cev1 \
    --kms-key-id my-kms-key \
    --description "test cev" \
    --manifest manifest_string \
    --image-id ami-012a345678901bcde
```

Para Windows:

```
aws rds create-custom-db-engine-version ^
    --engine custom-oracle-se2-cdb ^
    --engine-version 19.cdb_cev1 ^
    --database-installation-files-s3-bucket-name us-east-1-123456789012-custom-
installation-files ^
    --database-installation-files-s3-prefix 123456789012/cev1 ^
    --kms-key-id my-kms-key ^
    --description "test cev" ^
    --manifest manifest_string ^
    --image-id ami-012a345678901bcde
```

Example

Obtenga detalles acerca de su CEV mediante el comando `describe-db-engine-versions`.

```
aws rds describe-db-engine-versions \
    --engine custom-oracle-se2-cdb \
    --include-all
```

El siguiente resultado de ejemplo parcial muestra el motor, los grupos de parámetros, el manifiesto y otra información.

```
{
    "DBEngineVersions": [
        {
            "Engine": "custom-oracle-se2-cdb",
            "EngineVersion": "19.cdb_cev1",
            "DBParameterGroupFamily": "custom-oracle-se2-cdb-19",
            "DBEngineDescription": "Containerized Database for Oracle Custom SE2",
```

```
            "DBEngineVersionDescription": "test cev",
            "Image": {
                "ImageId": "ami-012a345678901bcde",
                "Status": "active"
            },
            "ValidUpgradeTarget": [],
            "SupportsLogExportsToCloudwatchLogs": false,
            "SupportsReadReplica": true,
            "SupportedFeatureNames": [],
            "Status": "available",
            "SupportsParallelQuery": false,
            "SupportsGlobalDatabases": false,
            "MajorEngineVersion": "19",
            "DatabaseInstallationFilesS3BucketName": "us-east-1-123456789012-custom-
installation-files",
            "DatabaseInstallationFilesS3Prefix": "123456789012/cev1",
            "DBEngineVersionArn": "arn:aws:rds:us-east-1:123456789012:cev:custom-
oracle-se2-cdb/19.cdb_cev1/abcd12e3-4f5g-67h8-i9j0-k1234l56m789",
            "KMSKeyId": "arn:aws:kms:us-
east-1:732027699161:key/1ab2345c-6d78-9ef0-1gh2-3456i7j89k01",
            "CreateTime": "2023-03-07T19:47:58.131000+00:00",
            "TagList": [],
            "SupportsBabelfish": false,
...
```

No se ha creado una CEV

Si la creación de CEV falla, RDS Custom emite `RDS-EVENT-0198` con el mensaje `Creation failed for custom engine version` *`major-engine-version.cev_name`* e incluye detalles sobre el error. Por ejemplo, el evento imprime los archivos que faltan.

No puede modificar una CEV que haya fallado. Solo puede eliminarlo y, a continuación, volver a intentar crear una CEV después de corregir las causas del error. Para obtener información sobre la solución de problemas de los motivos del error de creación de CEV, consulte Solución de problemas de creación de versiones de motores personalizados para RDS Custom for Oracle.

Modificación del estado de CEV

Puede modificar una CEV mediante la AWS Management Console o la AWS CLI. Puede modificar la descripción de la CEV o su estado de disponibilidad. La CEV tiene uno de los siguientes valores de estado:

- `available` – Puede utilizar esta CEV para crear una nueva instancia de base de datos de RDS Custom o actualizar una instancia de base de datos. Este es el estado predeterminado de una CEV recién creada.
- `inactive` – No se puede crear ni actualizar una instancia de RDS Custom con esta CEV. No puede restaurar una instantánea de base de datos para crear una nueva instancia de base de datos de RDS Custom con esta CEV.

Puede cambiar la CEV de cualquier estado compatible a cualquier otro estado admitido. Puede cambiar el estado para evitar el uso accidental de un CEV o hacer que un CEV interrumpido pueda utilizarse de nuevo. Por ejemplo, puede cambiar el estado de su CEV desde `available` a `inactive`, y `inactive` de vuelta a `available`.

Consola

Para modificar una CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).
3. Elija una CEV cuya descripción o estado desee modificar.
4. Para Actions (Acciones), elija Modify (Modificar).
5. Realice cualquiera de los siguientes cambios:
   - Para CEV status settings (Configuración del estado de CEV), elija un nuevo estado de disponibilidad.
   - Para Version description (Descripción de la versión), ingrese una nueva descripción.
6. Elija Modify CEV (Modificar CEV).

   Si la CEV está en uso, la consola muestra You can't modify the CEV status (No se puede modificar el estado de la CEV). Corrija los problemas e inténtelo de nuevo.

Aparece la página de Custom engine versions (Versiones de motor personalizadas).

AWS CLI

Para modificar una CEV mediante la AWS CLI, ejecute el comando modify-custom-db-engine-version. Puede encontrar las CEV para modificarlas al ejecutar el comando describe-db-engine-versions.

Se requieren las siguientes opciones:

- `--engine` *`engine-type`*, donde *`engine-type`* es `custom-oracle-ee`, `custom-oracle-se2`, `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`
- `--engine-version` *`cev`*, donde *`cev`* es el nombre de la versión del motor personalizada que desea modificar
- `--status` *`status`*, donde *`status`* es el estado de disponibilidad que desea asignar a la CEV

En el siguiente ejemplo se cambia una CEV denominada `19.my_cev1` de su estado actual a `inactive`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-custom-db-engine-version \
    --engine custom-oracle-se2 \
    --engine-version 19.my_cev1 \
    --status inactive
```

En:Windows

```
aws rds modify-custom-db-engine-version ^
    --engine custom-oracle-se2 ^
    --engine-version 19.my_cev1 ^
    --status inactive
```

Visualización de detalles de la CEV de Amazon RDS Custom para Oracle

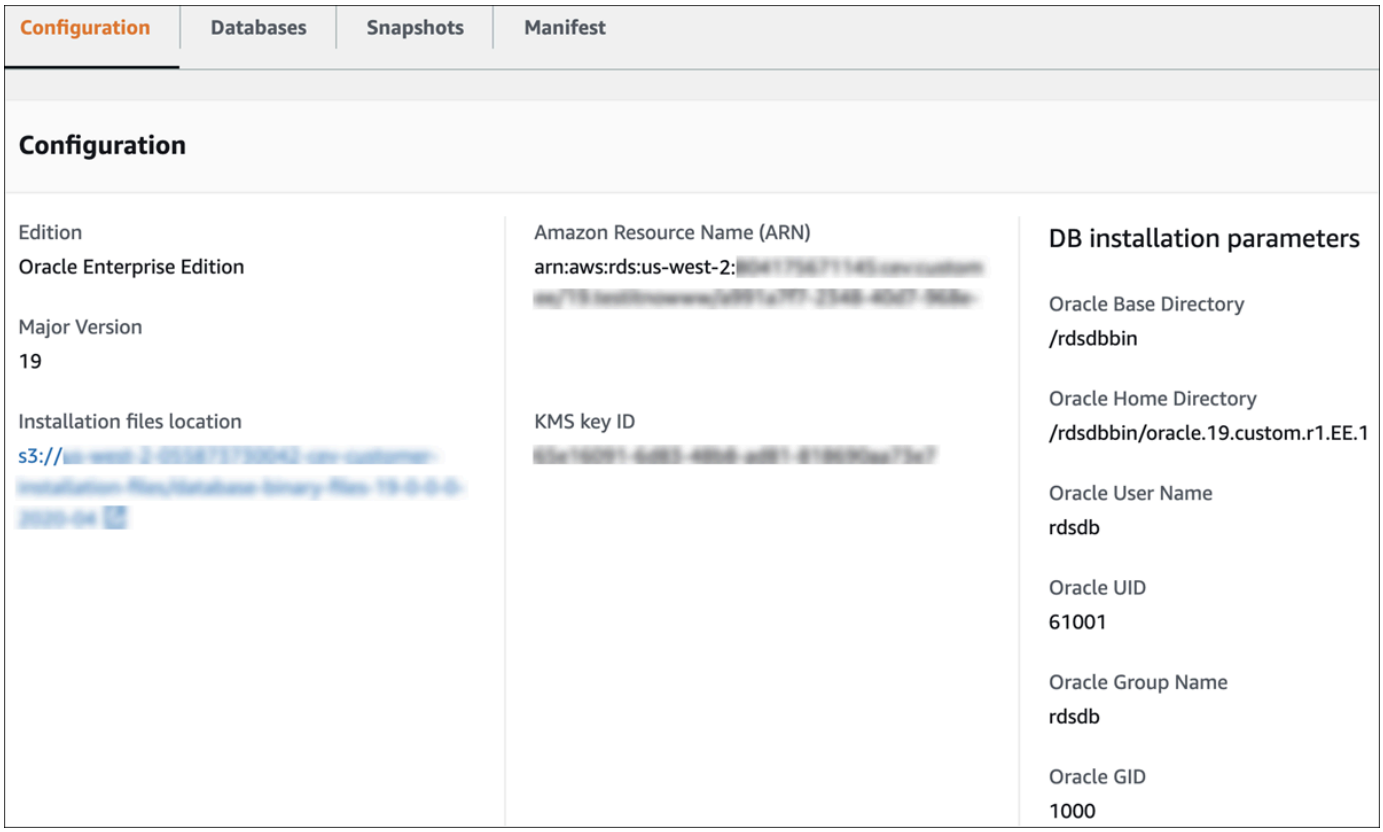
Puede ver los detalles sobre su manifiesto CEV y el comando utilizado para crear su CEV mediante la AWS Management Console o la AWS CLI.

Consola

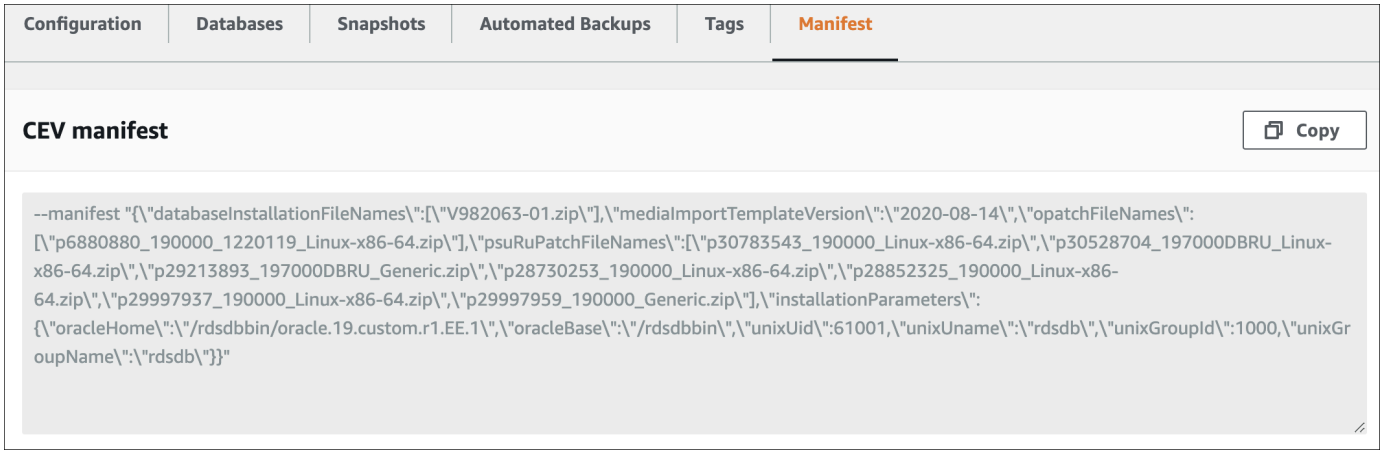
Para ver los detalles de la CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).

   La página de Custom engine versions (Versiones de motor personalizadas) muestra todos las CEV que existen actualmente. Si no ha creado ninguna CEV, la página está vacía.
3. Elija el nombre de la CEV que desea ver.
4. Elija Configuration (Configuración) para ver los parámetros de instalación especificados en el manifiesto.



5. Elija Manifest (Manifiesto) para ver los parámetros de instalación especificados en la opción `--manifest` del comando `create-custom-db-engine-version`. Puede copiar este texto, reemplazar los valores según sea necesario y utilizarlos en un comando nuevo.



AWS CLI

Para ver detalles acerca de una CEV mediante la AWS CLI, ejecute el comando describe-db-engine-versions.

Se requieren las siguientes opciones:

- `--engine` *`engine-type`*, donde *`engine-type`* es `custom-oracle-ee`, `custom-oracle-se2`, `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`
- `--engine-version` *`major-engine-version.customized_string`*

En el siguiente ejemplo, se crea una CEV que no es CDB y que utiliza Enterprise Edition. El nombre de la CEV `19.my_cev1` comienza con el número de versión principal del motor, que es obligatorio.

Example

Para Linux, macOS o:Unix

```
aws rds describe-db-engine-versions \
    --engine custom-oracle-ee \
    --engine-version 19.my_cev1
```

En:Windows

```
aws rds describe-db-engine-versions ^
    --engine custom-oracle-ee ^
    --engine-version 19.my_cev1
```

El siguiente resultado de ejemplo parcial muestra el motor, los grupos de parámetros, el manifiesto y otra información.


```
"DBEngineVersions": [
    {
        "Engine": "custom-oracle-ee",
        "MajorEngineVersion": "19",
        "EngineVersion": "19.my_cev1",
        "DatabaseInstallationFilesS3BucketName": "us-east-1-123456789012-cev-customer-
installation-files",
        "DatabaseInstallationFilesS3Prefix": "123456789012/cev1",
        "CustomDBEngineVersionManifest": "{\n\"mediaImportTemplateVersion\":
 \"2020-08-14\",\n\"databaseInstallationFileNames\": [\n\"V982063-01.zip\"\n],
\n\"installationParameters\": {\n\"oracleBase\":\"/tmp\",\n\"oracleHome\":\"/
tmp/Oracle\"\n},\n\"opatchFileNames\": [\n\"p6880880_190000_Linux-x86-64.zip
\"\n],\n\"psuRuPatchFileNames\": [\n\"p32126828_190000_Linux-x86-64.zip
\"\n],\n\"otherPatchFileNames\": [\n\"p29213893_1910000DBRU_Generic.zip\",\n
\"p29782284_1910000DBRU_Generic.zip\",\n\"p28730253_190000_Linux-x86-64.zip\",\n
\"p29374604_1910000DBRU_Linux-x86-64.zip\",\n\"p28852325_190000_Linux-x86-64.zip\",
\n\"p29997937_190000_Linux-x86-64.zip\",\n\"p31335037_190000_Linux-x86-64.zip\",\n
\"p31335142_190000_Generic.zip\"\n]\n}\n",
        "DBParameterGroupFamily": "custom-oracle-ee-19",
        "DBEngineDescription": "Oracle Database server EE for RDS Custom",
        "DBEngineVersionArn": "arn:aws:rds:us-west-2:123456789012:cev:custom-oracle-
ee/19.my_cev1/0a123b45-6c78-901d-23e4-5678f901fg23",
        "DBEngineVersionDescription": "test",
        "KMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/ab1c2de3-f4g5-6789-h012-
h3ijk4567l89",
        "CreateTime": "2022-11-18T09:17:07.693000+00:00",
        "ValidUpgradeTarget": [
        {
            "Engine": "custom-oracle-ee",
            "EngineVersion": "19.cev.2021-01.09",
            "Description": "test",
            "AutoUpgrade": false,
            "IsMajorVersionUpgrade": false
        }
]
```


Eliminación de una CEV

Puede eliminar una CEV con la AWS Management Console o la AWS CLI. Por lo general, la eliminación tarda unos minutos.

Para eliminar una CEV, no puede estar en uso por ninguno de los siguientes:

- Una instancia de base de datos de RDS Custom
- Instantánea de una instancia de base de datos de RDS Custom
- Una copia de seguridad automatizada de su instancia de base de datos de RDS Custom

Consola

Para eliminar una CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).
3. Elija una CEV cuya descripción o estado desea eliminar.
4. En Actions (Acciones), seleccione Delete (Eliminar).

   Aparece el cuadro de diálogo Delete ***cev_name***? (¿Desea eliminar cev_name?).
5. Introduzca **`delete me`** y luego escriba Delete (Eliminar).

   En la página de Custom engine versions (Versiones de motor personalizadas), el banner muestra que se está eliminando su CEV.

AWS CLI

Para eliminar una CEV mediante la AWS CLI, ejecute el comando delete-custom-db-engine-version.

Se requieren las siguientes opciones:

- `--engine` *`engine-type`*, donde *`engine-type`* es `custom-oracle-ee`, `custom-oracle-se2`, `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`
- `--engine-version` *`cev`*, donde *`cev`* es el nombre de la versión del motor personalizada que se va a eliminar

El siguiente ejemplo elimina una CEV denominada `19.my_cev1`.

Example

Para Linux, macOS o:Unix

```
aws rds delete-custom-db-engine-version \
    --engine custom-oracle-ee \
    --engine-version 19.my_cev1
```

En:Windows

```
aws rds delete-custom-db-engine-version ^
    --engine custom-oracle-ee ^
    --engine-version 19.my_cev1
```

Configuración de una instancia de base de datos para Amazon RDS Custom para Oracle

Puede crear una instancia de base de datos de RDS Custom y luego conectarse a ella mediante Secure Shell (SSH) o AWS Systems Manager.

Para obtener más información sobre la conexión y el inicio de sesión en una instancia de base de datos de RDS Custom para Oracle, consulte los siguientes temas.

- Conexión a su instancia de base de datos de RDS Custom mediante Session Manager
- Conexión a la instancia de base de datos de RDS Custom mediante SSH
- Inicio de sesión en la base de datos de RDS Custom para Oracle como SYS

Creación de una instancia de base de datos de RDS Custom for Oracle

Cree una instancia de base de datos de Amazon RDS Custom for Oracle mediante la AWS Management Console o la AWS CLI. El procedimiento es similar al que se debe seguir para crear una instancia de base de datos de Amazon RDS. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

Si ha incluido parámetros de instalación en el manifiesto CEV, la instancia de base de datos utilizará la base de Oracle, el directorio raíz de Oracle y el ID y el nombre del usuario y grupo de UNIX/Linux que especificó. El archivo `oratab`, que Oracle Database crea durante la instalación, apunta a la ubicación real de la instalación en lugar de a un enlace simbólico. Cuando RDS Custom para Oracle ejecuta comandos, los ejecuta como el usuario del sistema operativo configurado en lugar de como el usuario `rdsdb` predeterminado. Para obtener más información, consulte Paso 5: preparar el manifiesto de la CEV.

Antes de que pueda crear o conectarse a una instancia de base de datos de RDS Custom, asegúrese de completar las tareas en Configuración del entorno para Amazon RDS Custom for Oracle.

Consola

Para crear una instancia de base de datos de RDS Custom for Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija Create database (Crear base de datos).
4. En Choose a database creation method (Elegir un método de creación de base de datos), seleccione Standard Create (Creación estándar).
5. En la sección Opciones de motor, haga lo siguiente:

   a. En Engine type (Tipo de motor), elija Oracle.

   b. Para Database management type (Tipo de administración de base de datos), elija Amazon RDS Custom.

   c. En Configuración de la arquitectura, realice una de las siguientes operaciones:

      - Seleccione Arquitectura multiinquilino para crear una base de datos de contenedores (CDB). En el momento de la creación, su CDB contiene un origen de PDB y una PDB inicial.

        > **Note**
        >
        > La configuración Arquitectura multitenencia solo se admite para Oracle Database 19c.

      - Desmarque Arquitectura multiinquilino para crear una arquitectura que no sea CDB. Un producto que no sea CDB no puede contener PDB.

   d. En Edición, elija Oracle Enterprise Edition o Oracle Standard Edition 2.

   e. En Versión del motor personalizada, elija una versión del motor personalizada de RDS Custom (CEV). Una CEV tiene el siguiente formato: *`major-engine-version.customized_string`*. Un identificador de ejemplo es `19.cdb_cev1`.

      Si ha elegido Arquitectura multitenencia en el paso anterior, solo puede especificar una CEV que use el tipo de motor `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`. La consola filtra las CEV que se crearon con los diferentes tipos de motor.

6. En Templates (Plantillas), elija Production (Producción).
7. En la sección Settings, realice lo siguiente:

   a. En Identificador de instancias de bases de datos, escriba el nombre único de la instancia de base de datos.

b. En Nombre de usuario maestro, escriba un nombre de usuario. Puede recuperar este valor de la consola más adelante.

   Si se conecta a una base de datos no CDB, el usuario maestro es el usuario de una base de datos no CDB. Si se conecta a una CDB, el usuario maestro es el usuario de la PDB. Para conectarse a la raíz de la CDB, inicie sesión en el host, inicie un cliente SQL y cree un usuario administrativo con comandos SQL.

c. Desmarque Generar automáticamente una contraseña.

8. Seleccione su Clase de instancia de base de datos.

   Para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.

9. En la sección Almacenamiento, haga lo siguiente:

   a. En Tipo de almacenamiento, elija un tipo de SSD: io1, gp2 o gp3. Dispone de las siguientes opciones adicionales:

      - Para io1 o gp3, elija una tasa para las IOPS aprovisionadas. El valor predeterminado es 1000 para io1 y 12000 para gp3.
      - Para gp3, elija una tasa de Rendimiento de almacenamiento. El valor predeterminado es 500 MiBps.

   b. En Almacenamiento asignado, elija un tamaño de almacenamiento. El valor predeterminado es 40 GiB.

10. En Conectividad, especifique su Nube privada virtual (VPC), el Grupo de subred de base de datos y el Grupo de seguridad de VPC (firewall).

11. Para RDS Custom security (Seguridad de RDS Custom), realice una de las siguientes opciones:

    a. Para IAM instance profile (Perfil de instancias de IAM), elija el perfil de instancias para la instancia de base de datos de RDS Custom for Oracle.

       El perfil de instancias de IAM debe comenzar con `AWSRDSCustom`, por ejemplo, *`WSRDSCustomInstanceProfileForRdsCustomInstance`*.

    b. Para Encryption (Cifrado), elija Enter a key ARN (Ingresar una ARN de clave) para enumerar las claves de AWS KMS disponibles. A continuación, elija la clave de la lista.

       Se requiere una clave AWS KMS para RDS Custom. Para obtener más información, consulte Paso 1: crear o reutilizar una clave AWS KMS de cifrado simétrica.

12. En Opciones de la base de datos, haga lo siguiente:

    a. (Opcional) En ID del sistema (SID), introduzca un valor para el SID de Oracle, que también es el nombre de su CDB. El SID es el nombre de la instancia de base de datos de Oracle que administra los archivos de la base de datos. En este contexto, el término «instancia de base de datos de Oracle» se refiere exclusivamente al área global del sistema (SGA) y a los procesos en segundo plano de Oracle. Si no especifica un valor de SID, se utiliza el valor predeterminado de **`RDSCDB`**.

    b. (Opcional) En Nombre de base de datos inicial, escriba un nombre. El valor predeterminado es **`ORCL`**. En la arquitectura multiinquilino, el nombre de base de datos inicial es el nombre de PDB.

    > **Note**
    >
    > Los nombres de SID y PDB deben ser diferentes.

    c. En Grupo de opciones, elija un grupo de opciones o acepte el predeterminado.

    > **Note**
    >
    > La única opción admitida en RDS Custom para Oracle es `Timezone`. Para obtener más información, consulte Zona horaria Oracle.

    d. En Periodo de retención de copia de seguridad, elija un valor. No se puede elegir 0 días.

    e. Para las secciones restantes, especifique la configuración de la instancia de base de datos de RDS Custom que prefiera. Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos. La siguiente configuración no aparece en la consola y no se admite:

    - Processor features (Características del procesador)
    - Storage autoscaling (Escalado automático de almacenamiento)
    - Opción de Password and Kerberos authentication (autenticación de Contraseña y Kerberos) en la Database authentication (Autenticación de base de datos) (solo se admite Password authentication [Autenticación de contraseña])
    - Performance Insights (Información sobre rendimiento)
    - Log exports (Exportaciones de registros)

- Enable auto minor version upgrade (Habilitar la actualización automática de la versión secundaria)
- Deletion protection (Protección contra eliminación

13. Elija Creación de base de datos.

> **Important**
>
> Al crear una instancia de base de datos de RDS Custom para Oracle, podría recibir el siguiente error: The service-linked role is in the process of being created. (El rol vinculado al servicio está en proceso de creación). Inténtelo de nuevo más tarde. Si lo hace, espere unos minutos e intente crear la instancia de base de datos de nuevo.

El botón View credential details (Ver detalles de la credencial) aparece en la página Databases (Bases de datos).

Para ver el nombre de usuario y la contraseña maestros para la instancia de base de datos de RDS Custom, elija View credential details (Ver detalles de credenciales).

Para conectarse a la instancia de base de datos como usuario maestro, utilice el nombre de usuario y la contraseña que aparecen.

> **Important**
>
> No puede ver la contraseña de usuario maestro de nuevo en la consola. Si no la registra, es posible que tenga que cambiarla. Para cambiar la contraseña del usuario maestro una vez que la instancia de base de datos de RDS Custom esté disponible, inicie sesión en la base de datos y ejecute un comando `ALTER USER`. No puede restablecer la contraseña mediante la opción Modificar en la consola.

14. Elija Databases (Bases de datos) para ver la lista de instancias de base de datos de RDS Custom.
15. Elija la instancia de base de datos de RDS Custom que acaba de crear.

    En la consola de RDS, aparecen los detalles de la nueva instancia de base de datos de RDS Custom:

- La instancia de base de datos tiene un estado de creating (creación) hasta que la instancia de base de datos de RDS Custom se crea y está lista para su uso. Cuando el estado cambie a available (disponible), podrá conectarse a la instancia de base de datos. En función de la clase de instancia y el almacenamiento asignado, la nueva instancia de base de datos puede tardar varios minutos en estar disponible.
- El Role (Rol) tiene el valor Instance (RDS Custom) [Instancia (RDS Custom]).
- El RDS Custom automation mode (Modo de automatización de RDS Custom) tiene el valor Full automation (Automatización completa). Esta configuración significa que la instancia de base de datos proporciona monitoreo automático y recuperación de instancias.

AWS CLI

Puede crear una instancia de base de datos de RDS Custom mediante el comando AWS CLI create-db-instance.

Se requieren las siguientes opciones:

- `--db-instance-identifier`
- `--db-instance-class` (para obtener una lista de clases de instancias admitidas, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle)
- `--engine` *`engine-type`*, donde *`engine-type`* es `custom-oracle-ee`, `custom-oracle-se2`, `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`
- `--engine-version` *`cev`* (donde *`cev`* es el nombre de la versión del motor personalizada que especificó en Creación de una CEV)
- `--kms-key-id` *`my-kms-key`*
- `--backup-retention-period` *`days`* (donde *`days`* es un valor mayor que `0`)
- `--no-auto-minor-version-upgrade`
- `--custom-iam-instance-profile AWSRDSCustomInstanceProfile-`*`us-east-1`* (donde *`region`* es la Región de AWS donde está creando su instancia de base de datos)

El siguiente ejemplo crea una instancia de base de datos de RDS Custom denominada `my-cfo-cdb-instance`. La base de datos es una CDB con el nombre no predeterminado *`MYCDB`*. El nombre de PDB no predeterminado es *`MYPDB`*. El periodo de retención de copia de seguridad es de tres días.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --engine custom-oracle-ee-cdb \
    --db-instance-identifier my-cfo-cdb-instance \
    --engine-version 19.cdb_cev1 \
    --db-name MYPDB \
    --db-system-id MYCDB \
    --allocated-storage 250 \
    --db-instance-class db.m5.xlarge \
    --db-subnet-group mydbsubnetgroup \
    --master-username myuser \
    --master-user-password mypassword \
    --backup-retention-period 3 \
    --port 8200 \
    --kms-key-id my-kms-key \
    --no-auto-minor-version-upgrade \
    --custom-iam-instance-profile AWSRDSCustomInstanceProfile-us-east-1
```

Para Windows:

```
aws rds create-db-instance ^
    --engine custom-oracle-ee-cdb ^
    --db-instance-identifier my-cfo-cdb-instance ^
    --engine-version 19.cdb_cev1 ^
    --db-name MYPDB ^
    --db-system-id MYCDB ^
    --allocated-storage 250 ^
    --db-instance-class db.m5.xlarge ^
    --db-subnet-group mydbsubnetgroup ^
    --master-username myuser ^
    --master-user-password mypassword ^
    --backup-retention-period 3 ^
    --port 8200 ^
    --kms-key-id my-kms-key ^
    --no-auto-minor-version-upgrade ^
    --custom-iam-instance-profile AWSRDSCustomInstanceProfile-us-east-1
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Obtenga detalles sobre la instancia mediante el comando `describe-db-instances`.

Example

```
aws rds describe-db-instances --db-instance-identifier my-cfo-cdb-instance
```

En la siguiente salida parcial se muestra el motor, los grupos de parámetros y otra información.

```
        {
            "DBInstanceIdentifier": "my-cfo-cdb-instance",
            "DBInstanceClass": "db.m5.xlarge",
            "Engine": "custom-oracle-ee-cdb",
            "DBInstanceStatus": "available",
            "MasterUsername": "admin",
            "DBName": "MYPDB",
            "DBSystemID": "MYCDB",
            "Endpoint": {
                "Address": "my-cfo-cdb-instance.abcdefghijkl.us-
east-1.rds.amazonaws.com",
                "Port": 1521,
                "HostedZoneId": "A1B2CDEFGH34IJ"
            },
            "AllocatedStorage": 100,
            "InstanceCreateTime": "2023-04-12T18:52:16.353000+00:00",
            "PreferredBackupWindow": "08:46-09:16",
            "BackupRetentionPeriod": 7,
            "DBSecurityGroups": [],
            "VpcSecurityGroups": [
                {
                    "VpcSecurityGroupId": "sg-0a1bcd2e",
                    "Status": "active"
                }
            ],
            "DBParameterGroups": [
                {
                    "DBParameterGroupName": "default.custom-oracle-ee-cdb-19",
```

```
                    "ParameterApplyStatus": "in-sync"
                }
            ],
...
```

Consideraciones sobre la arquitectura multitenencia

Si crea una instancia de base de datos de Amazon RDS Custom para Oracle con la arquitectura multitenencia de Oracle (tipo de motor `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`), la base de datos es una base de datos de contenedores (CDB). Si no especifica la arquitectura multitenencia de Oracle, la base de datos será una base de datos tradicional no CDB que utiliza el tipo de motor `custom-oracle-ee` o `custom-oracle-se2`. Una base de datos que no es CDB no puede contener bases de datos conectables (PDB, por sus siglas en inglés). Para obtener más información, consulte Arquitectura de base de datos de Amazon RDS Custom para Oracle.

Al crear una instancia de CDB de RDS Custom para Oracle, tenga en cuenta lo siguiente:

- Puede crear una base de datos multitenencia únicamente a partir de un CEV de base de datos Oracle 19c.
- Puede crear una instancia de CDB solo si la CEV usa el tipo de motor `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`.
- Si crea una instancia de CDB con Standard Edition 2, la CDB puede contener un máximo de 3 PDB.
- De forma predeterminada, la CDB se denomina `RDSCDB`, que también es el nombre del ID del sistema de Oracle (SID de Oracle). Puede elegir un nombre diferente.
- Su CDB contiene solo una PDB inicial. El nombre predeterminado de la PDB es `ORCL`. Puede elegir un nombre diferente para su PDB inicial, pero el SID de Oracle y el nombre de PDB no pueden ser idénticos.
- RDS Custom para Oracle no proporciona API para PDB. Para crear PDB adicionales, utilice el comando `CREATE PLUGGABLE DATABASE` de Oracle SQL. RDS Custom para Oracle no restringe la cantidad de PDB que puede crear. En general, usted es responsable de crear y administrar las PDB, como en una implementación local.
- No puede usar las API de RDS para crear, modificar ni eliminar PDB: debe usar instrucciones SQL de Oracle. Al crear una PDB mediante Oracle SQL, se recomienda realizar una instantánea manual después en caso de que tenga que realizar una recuperación en un momento dado (PITR).
- No puede cambiar el nombre de las PDB existentes mediante las API de Amazon RDS. Tampoco puede cambiar el nombre de la CDB con el comando `modify-db-instance`.

- El modo abierto de la raíz de la CDB es `READ WRITE` en la base de datos principal y `MOUNTED` en una base de datos en espera montada. RDS Custom para Oracle intenta abrir todas las PDB al abrir la CDB. Si RDS Custom para Oracle no puede abrir todas las PDB, emite el evento `tenant database shutdown`.

Rol vinculado al servicio de RDS Custom

Un service-linked role (rol vinculado al servicio) le otorga a Amazon RDS Custom acceso a los recursos de su Cuenta de AWS. Facilita el uso de RDS Custom porque no tiene que agregar manualmente los permisos necesarios. RDS Custom define los permisos de sus roles vinculados al servicio y, a menos que se defina lo contrario, solo RDS Custom puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

Cuando crea una instancia de base de datos de RDS Custom, se crean y utilizan los roles vinculados a servicios de Amazon RDS y RDS Custom (si aún no existen). Para obtener más información, consulte Uso de roles vinculados a servicios de Amazon RDS.

La primera vez que crea una instancia de base de datos de RDS Custom for Oracle, podría recibir el siguiente error: he service-linked role is in the process of being created. (El rol vinculado al servicio está en proceso de creación). Inténtelo de nuevo más tarde. Si lo hace, espere unos minutos e intente crear la instancia de base de datos de nuevo.

Instalación de componentes de software adicionales en su instancia de base de datos RDS Custom para Oracle

En una instancia de base de datos recién creada, el entorno de base de datos incluye archivos binarios de Oracle, una base de datos y un oyente de bases de datos. Puede que desee instalar software adicional en el sistema operativo host de la instancia de base de datos. Por ejemplo, puede que desee instalar Oracle Application Express (APEX), el agente Oracle Enterprise Manager (OEM) o el agente Guardium S-TAP. Para obtener pautas e instrucciones detalladas, consulte la entrada de blog AWS detallada Install additional software components on Amazon RDS Custom for Oracle.

Conexión a su instancia de base de datos de RDS Custom mediante Session Manager

Una vez que haya creado la instancia de base de datos de RDS Custom, puede conectarse a ella mediante AWS Systems Manager Session Manager. Esta es la técnica preferida que se utiliza cuando no se puede acceder a la instancia de base de datos de forma pública.

Session Manager permite acceder a las instancias de Amazon EC2 a través de un intérprete de comandos basado en navegador o mediante la AWS CLI. Para obtener más información, consulte AWSSystems Manager Session Manager.

Consola

Para conectarse a su instancia de base de datos mediante Session Manager

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos de RDS Custom que desea detener.
3. Elija Configuration (Configuración).
4. Tenga en cuenta el Resource ID (ID de recurso) para la instancia de base de datos. Por ejemplo, el ID del recurso puede ser `db-ABCDEFGHIJKLMNOPQRS0123456`.
5. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
6. En el panel de navegación, seleccione Instances (Instancia[s]).
7. Busque el nombre de la instancia EC2 y, a continuación, haga clic en el ID de instancia asociado a ella. Por ejemplo, el ID de instancia puede ser `i-abcdefghijklm01234`.
8. Elija Connect (Conectar).
9. Elija Session Manager.
10. Elija Conectar.

    Se abre una ventana para la sesión.

AWS CLI

Puede conectarse a la instancia de base de datos de RDS Custom mediante la AWS CLI. Esta técnica requiere el complemento Session Manager para la AWS CLI. Para obtener información sobre cómo instalar el complemento, consulte Install the Session Manager plugin for the AWS CLI (Instale el complemento Session Manager).

Para encontrar el ID de recurso de base de datos de la instancia de base de datos de RDS Custom, utilice `aws rds describe-db-instances`.

```
aws rds describe-db-instances \
```

```
    --query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
    --output text
```

En el siguiente ejemplo de resultado se muestra el ID de recurso de la instancia de RDS Custom. El prefijo es `db-`.

```
db-ABCDEFGHIJKLMNOPQRS0123456
```

Para buscar el ID de instancia EC2 de la instancia de base de datos, utilice `aws ec2 describe-instances`. El siguiente ejemplo utiliza `db-ABCDEFGHIJKLMNOPQRS0123456` para el ID del recurso.

```
aws ec2 describe-instances \
    --filters "Name=tag:Name,Values=db-ABCDEFGHIJKLMNOPQRS0123456" \
    --output text \
    --query 'Reservations[*].Instances[*].InstanceId'
```

El siguiente ejemplo muestra el ID de instancia EC2.

```
i-abcdefghijklm01234
```

Use el comando `aws ssm start-session`, proporcionando el ID de instancia EC2 en el parámetro `--target`.

```
aws ssm start-session --target "i-abcdefghijklm01234"
```

Una conexión exitosa sería como la siguiente.

```
Starting session with SessionId: yourid-abcdefghijklm1234
[ssm-user@ip-123-45-67-89 bin]$
```

Conexión a la instancia de base de datos de RDS Custom mediante SSH

El protocolo Secure Shell Protocol (SSH) es un protocolo de red que admite la comunicación cifrada a través de una red no segura. Después de crear la instancia de base de datos de RDS Custom, puede conectarse a ella mediante un cliente ssh. Para obtener más información, consulte Connecting to your Linux instance using SSH (Conexión a la instancia de Linux mediante SSH).

La técnica de conexión SSH depende de si la instancia de base de datos es privada, lo que significa que no acepta conexiones de la Internet pública. En este caso, debe usar el túnel SSH para conectar la utilidad ssh a su instancia. Esta técnica transporta datos con un flujo de datos dedicado (túnel) dentro de una sesión SSH existente. Puede configurar los túneles SSH mediante AWS Systems Manager.

> **Note**
>
> Se admiten varias estrategias para acceder a las instancias privadas. Para aprender a conectar un cliente ssh a instancias privadas mediante hosts bastión, consulte Hosts bastión de Linux en AWS. Para obtener información sobre cómo configurar el reenvío de puertos, consulte Port Forwarding Using AWS Systems Manager Session Manager (Reenvío de puertos mediante AWS Systems Manager Session Manager).

Si la instancia de base de datos se encuentra en una subred pública y tiene la configuración de disponibilidad pública, no se requiere ningún túnel SSH. Puede conectarse con SSH del mismo modo que lo haría con una instancia pública de Amazon EC2.

Para conectar un cliente ssh a la instancia de base de datos, siga estos pasos:

1. Paso 1: configurar la instancia de base de datos para permitir conexiones SSH
2. Paso 2: recuperar la clave secreta SSH y el identificador de instancia de EC2
3. Paso 3: conectarse a la instancia de EC2 mediante la utilidad ssh

Paso 1: configurar la instancia de base de datos para permitir conexiones SSH

Para asegurarse de que la instancia de base de datos pueda aceptar conexiones SSH, realice el siguiente procedimiento:

- Asegúrese de que el grupo de seguridad de instancias de base de datos permita conexiones entrantes en el puerto 22 para TCP.

  Para aprender a configurar el grupo de seguridad de la instancia de base de datos, consulte Control de acceso con grupos de seguridad.
- Si no piensa utilizar túneles SSH, asegúrese de que la instancia de base de datos reside en una subred pública y es de acceso público.

En la consola, se puede acceder públicamente al campo correspondiente en la pestaña Conectividad y seguridad de la página de detalles de la base de datos. Para comprobar la configuración en la CLI, ejecute el siguiente comando:

```
aws rds describe-db-instances \
--query 'DBInstances[*].
{DBInstanceIdentifier:DBInstanceIdentifier,PubliclyAccessible:PubliclyAccessible}' \
--output table
```

Para modificar la configuración de accesibilidad de la instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Paso 2: recuperar la clave secreta SSH y el identificador de instancia de EC2

Para conectarse a la instancia de base de datos mediante SSH, necesita el par de claves SSH asociado a la instancia. RDS Custom crea el par de claves SSH automáticamente, mediante la convención de nomenclatura `do-not-delete-rds-custom-ssh-privatekey-`*`resource_id`*`-`*`uuid`* o `rds-custom!oracle-do-not-delete-`*`resource_id`*`-`*`uuid`*`-ssh-privatekey`. AWS Secrets Manager almacena la clave privada SSH como un secreto.

Recupere la clave secreta mediante la AWS Management Console o la AWS CLI. Si su instancia tiene un DNS público y no tiene pensado utilizar túneles SSH, recupere también el nombre de DNS. Especifique el nombre de DNS para las conexiones públicas.

Consola

Para recuperar la clave SSH secreta

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos de RDS Custom que desea detener.
3. Elija Configuración.
4. Tenga en cuenta el valor de Resource ID (ID de recurso). Por ejemplo, el ID del recurso de la instancia de base de datos puede ser `db-ABCDEFGHIJKLMNOPQRS0123456`.
5. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

6. En el panel de navegación, seleccione Instances (Instancias).
7. Busque el nombre de la instancia EC2 y elija el ID de instancia asociado a ella. Por ejemplo, el ID de instancia EC2 puede ser `i-abcdefghijklm01234`.
8. En Details (Detalles), busque el Key pair name (Nombre del par de claves). El nombre del par incluye el ID del recurso de la instancia de base de datos. Por ejemplo, el nombre del par puede ser `do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c` o `rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey`.
9. Si la instancia de EC2 es pública, anote el DNS IPv4 público. Para el ejemplo, la dirección pública del Sistema de nombres de dominio (DNS) puede ser `ec2-12-345-678-901.us-east-2.compute.amazonaws.com`.
10. Abra la consola de AWS Secrets Manager en https://console.aws.amazon.com/secretsmanager/.
11. Elija el secreto que tiene el mismo nombre que su par de claves.
12. Elija Retrieve secret value (Recuperar valor secreto).
13. Copie la clave SSH privada en un archivo de texto y, a continuación, guarde el archivo con la extensión `.pem`. Por ejemplo, guarde el archivo como `/tmp/do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem` o `/tmp/rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey.pem`.

AWS CLI

Para recuperar la clave SSH privada y guardarla en un archivo.pem, puede utilizar la AWS CLI.

1. Busque el ID del recurso de base de datos de la instancia de RDS Custom con `aws rds describe-db-instances`.

```
aws rds describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
    --output text
```

En el siguiente ejemplo de resultado se muestra el ID de recurso de la instancia de RDS Custom. El prefijo es `db-`.

```
db-ABCDEFGHIJKLMNOPQRS0123456
```

2. Busque el ID de instancia de EC2 de la instancia de base de datos con `aws ec2 describe-instances`. El siguiente ejemplo utiliza `db-ABCDEFGHIJKLMNOPQRS0123456` para el ID del recurso.

```
aws ec2 describe-instances \
    --filters "Name=tag:Name,Values=db-ABCDEFGHIJKLMNOPQRS0123456" \
    --output text \
    --query 'Reservations[*].Instances[*].InstanceId'
```

El siguiente ejemplo muestra el ID de instancia EC2.

```
i-abcdefghijklm01234
```

3. Para buscar el nombre de la clave, especifique el ID de instancia EC2. En el siguiente ejemplo, se describe la instancia de EC2 `i-0bdc4219e66944afa`.

```
aws ec2 describe-instances \
    --instance-ids i-0bdc4219e66944afa \
    --output text \
    --query 'Reservations[*].Instances[*].KeyName'
```

En el siguiente ejemplo de salida se muestra el nombre de la clave, que utiliza el formato de nomenclatura `do-not-delete-rds-custom-ssh-privatekey-`*`resource_id`*`-`*`uuid`* o `rds-custom!oracle-do-not-delete-`*`resource_id`*`-`*`uuid`*`-ssh-privatekey`.

```
do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c
rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey
```

4. Guarde la clave privada en un archivo .pem que lleva el nombre de la clave con `aws secretsmanager`.

En el siguiente ejemplo, se guarda la clave `do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c` en un archivo en el directorio `/tmp`.

```
aws secretsmanager get-secret-value \
    --secret-id do-not-delete-rds-custom-ssh-privatekey-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c \
    --query SecretString \
```

```
    --output text >/tmp/do-not-delete-rds-custom-ssh-privatekey-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem
```

En el siguiente ejemplo, se guarda la clave `rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey` en un archivo en el directorio `/tmp`.

```
aws secretsmanager get-secret-value \
    --secret-id rds-custom!oracle-do-not-delete-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey \
    --query SecretString \
    --output text >/tmp/rds-custom!oracle-do-not-delete-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey.pem
```

Paso 3: conectarse a la instancia de EC2 mediante la utilidad ssh

La técnica de conexión depende de si se conecta a una instancia de base de datos privada o pública. Una conexión privada requiere configurar el túnel de SSH mediante AWS Systems Manager.

Para conectarse a una instancia de EC2 mediante la utilidad ssh

1. Para conexiones privadas, modifique su archivo de configuración de SSH para que utilice comandos de proxy en AWS Systems Manager Session Manager. Para las conexiones públicas, vaya al paso 2.

   Añada las líneas siguientes a `~/.ssh/config`. Estas líneas envían comandos SSH a hosts cuyos nombres comienzan por `i-` o `mi-`.

   ```
   Host i-* mi-*
       ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-
   StartSSHSession --parameters 'portNumber=%p'"
   ```

2. Cambie al directorio que contiene el archivo .pem. Mediante `chmod`, establezca los permisos en `400`.

   En el siguiente ejemplo, se cambia al directorio `/tmp` y establece los permisos para el archivo .pem `do-not-delete-rds-custom-ssh-privatekey-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem`.

   ```
   cd /tmp
   ```

```
chmod 400 do-not-delete-rds-custom-ssh-privatekey-db-
ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem
```

En el siguiente ejemplo, se cambia al directorio `/tmp` y establece los permisos para el archivo .pem `rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-privatekey.pem`.

```
cd /tmp
chmod 400 rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-
privatekey.pem
```

3. Ejecute la utilidad ssh y especifique el archivo .pem y el nombre de DNS público (para conexiones públicas) o el identificador de instancia de EC2 (para conexiones privadas). Inicie sesión como el usuario `ec2-user`.

   En el siguiente ejemplo, se conecta a una instancia pública mediante el nombre de DNS `ec2-12-345-678-901.us-east-2.compute.amazonaws.com`.

   ```
   # .pem file using naming prefix do-not-delete
   ssh -i \
     "do-not-delete-rds-custom-ssh-privatekey-db-
   ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem" \
     ec2-user@ec2-12-345-678-901.us-east-2.compute.amazonaws.com

   # .pem file using naming prefix rds-custom!oracle-do-not-delete
   ssh -i \
     "rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-
   privatekey.pem" \
     ec2-user@ec2-12-345-678-901.us-east-2.compute.amazonaws.com
   ```

   En el siguiente ejemplo, se conecta a una instancia privada mediante el ID de instancia de EC2 `i-0bdc4219e66944afa`.

   ```
   # .pem file using naming prefix do-not-delete
   ssh -i \
     "do-not-delete-rds-custom-ssh-privatekey-db-
   ABCDEFGHIJKLMNOPQRS0123456-0d726c.pem" \
     ec2-user@i-0bdc4219e66944afa

   # .pem file using naming prefix rds-custom!oracle-do-not-delete
   ssh -i \
   ```

```
  "rds-custom!oracle-do-not-delete-db-ABCDEFGHIJKLMNOPQRS0123456-0d726c-ssh-
privatekey.pem" \
  ec2-user@i-0bdc4219e66944afa
```

Inicio de sesión en la base de datos de RDS Custom para Oracle como SYS

Después de crear la instancia de base de datos de RDS Custom, puede iniciar sesión en la base de datos Oracle como usuario SYS, lo que le da privilegios SYSDBA. Dispone de estas opciones de inicio de sesión:

- Obtenga la contraseña SYS de Secrets Manager y especifíquela en su cliente SQL.
- Utilice la autenticación del sistema operativo para iniciar sesión en la base de datos. En este caso, no es necesario introducir una contraseña.

Búsqueda de la contraseña de SYS para la base de datos RDS Custom para Oracle

Puede iniciar sesión en su base de datos Oracle como SYS o SYSTEM, o bien especificando el nombre de usuario maestro en una llamada a la API. La contraseña de SYS y SYSTEM se almacena en Secrets Manager.

El secreto usa el formato de nomenclatura `do-not-delete-rds-custom-`*`resource_id`*`-`*`uuid`* o `rds-custom!oracle-do-not-delete-`*`resource_id`*`-`*`uuid`*. Puede encontrar la contraseña utilizando la AWS Management Console.

Consola

Para encontrar la contraseña de SYS de su base de datos en Secrets Manager

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de RDS, realice los siguientes pasos:
   a. En el panel de navegación, elija Databases (Bases de datos).
   b. Elija el nombre de la instancia de base de datos de RDS Custom para Oracle.
   c. Elija Configuración.
   d. Copie el valor debajo de ID de recurso. Por ejemplo, el ID de su recurso podría ser db-abc12cde3fgh4i5jklMno6pqr7.

3. Abra la consola de Secrets Manager en https://console.aws.amazon.com/secretsmanager/.
4. En la consola de Secrets Manager, siga estos pasos:
   a. En el panel de navegación de la izquierda, elija Secretos.
   b. Filtre los secretos por el ID del recurso que copió en el paso 2.d.
   c. Elija el secreto que utilice el formato de nomenclatura do-not-delete-rds-custom-***resource_id*-*uuid*** o rds-custom!oracle-do-not-delete-***resource_id*-*uuid***. El *resource_id* es el ID del recurso que copió en el paso 2.d.

      Por ejemplo, si el ID de recurso es db-ABC12CDE3FGH4I5JKLMNO6PQR7 y el UUID es 1234ab, su secreto se denominará do-not-delete-rds-custom-db-ABC12CDE3FGH4I5JKLMNO6PQR7-1234ab o rds-custom!oracle-do-not-delete-db-ABC12CDE3FGH4I5JKLMNO6PQR7-1234ab.
   d. En la sección Valor del secreto, elija Recuperar valor del secreto.
   e. En Clave-valor, copie el valor de la contraseña.
5. Instale SQL*Plus en su instancia de base de datos e inicie sesión en su base de datos como SYS. Para obtener más información, consulte Paso 3: conectar el cliente de SQL a una instancia de base de datos de Oracle.

Inicio de sesión en la base de datos RDS Custom para Oracle mediante la autenticación del sistema operativo

El usuario del sistema operativo `rdsdb` es propietario de los archivos binarios de la base de datos Oracle. Puede cambiar al usuario `rdsdb` e iniciar sesión en su base de datos RDS Custom para Oracle sin contraseña.

1. Conéctese a la instancia de base de datos con AWS Systems Manager. Para obtener más información, consulte Conexión a su instancia de base de datos de RDS Custom mediante Session Manager.
2. En un navegador web, vaya a https://www.oracle.com/database/technologies/instant-client/linux-x86-64-downloads.html.
3. Para obtener la versión más reciente de la base de datos que aparece en la página web, copie los enlaces .rpm (no los enlaces .zip) del paquete básico de Instant Client y del package de SQL*Plus. Por ejemplo, los siguientes enlaces corresponden a la versión 21.9 de Oracle Database:

- https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-instantclient-basic-21.9.0.0.0-1.el8.x86_64.rpm
- https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-instantclient-sqlplus-21.9.0.0.0-1.el8.x86_64.rpm

4. En su sesión de SSH, ejecute el comando `wget` para descargar los archivos .rpm desde los enlaces que obtuvo en el paso anterior. En el siguiente ejemplo, se descargan los archivos.rpm de la versión 21.9 de Oracle Database:

```
wget https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-instantclient-basic-21.9.0.0.0-1.el8.x86_64.rpm
wget https://download.oracle.com/otn_software/linux/instantclient/219000/oracle-instantclient-sqlplus-21.9.0.0.0-1.el8.x86_64.rpm
```

5. Ejecute el comando `yum` para instalar los paquetes de la manera siguiente:

```
sudo yum install oracle-instantclient-*.rpm
```

6. Cambie al usuario `rdsdb`.

```
sudo su - rdsdb
```

7. Inicie sesión en la base de datos utilizando la autenticación del sistema operativo.

```
$ sqlplus / as sysdba

SQL*Plus: Release 21.0.0.0.0 - Production on Wed Apr 12 20:11:08 2023
Version 21.9.0.0.0

Copyright (c) 1982, 2020, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.10.0.0.0
```

Administración de una instancia de base de datos de Amazon RDS Custom para Oracle

Amazon RDS Custom admite un subconjunto de las tareas de administración habituales para las instancias de base de datos de Amazon RDS. A continuación, encontrará instrucciones para las tareas de administración de RDS Custom for Oracle compatibles con la AWS Management Console y la AWS CLI.

Temas

- Uso de bases de datos de contenedores (CDB) en RDS Custom para Oracle
- Trabajar con funciones de alta disponibilidad para RDS Custom for Oracle
- Personalización del entorno de RDS Custom
- Modificación de la instancia de base de datos de RDS Custom para Oracle
- Cambio de la zona horaria de una instancia de base de datos de RDS Custom para Oracle
- Configuración del valor de NLS_LANG en RDS Custom para Oracle
- Compatibilidad para cifrado de datos transparente
- Etiquetado de recursos de RDS Custom for Oracle
- Eliminación de una instancia de base de datos de RDS Custom for Oracle

Uso de bases de datos de contenedores (CDB) en RDS Custom para Oracle

Puede crear su instancia de base de datos de RDS Custom para Oracle con la arquitectura multitenencia de Oracle (tipo de motor `custom-oracle-ee-cdb` o `custom-oracle-se2-cdb`) o con la arquitectura tradicional que no es CDB (tipo de motor `custom-oracle-ee` o `custom-oracle-se2`). Al crear una base de datos de contenedores (CDB, por sus siglas en inglés), contiene una base de datos conectable (PDB, por sus siglas en inglés) y un origen de PDB. Puede crear PDB adicionales manualmente con Oracle SQL.

Nombres de la PDB y la CDB

Al crear una instancia de RDS Custom para Oracle, especifique un nombre para la PDB inicial. De forma predeterminada, la PDB inicial se denomina `ORCL`. Puede elegir un nombre diferente.

De forma predeterminada, la CDB se llama `RDSCDB`. Puede elegir un nombre diferente. El nombre de la CDB también es el nombre del identificador del sistema (SID) de Oracle, que identifica de forma

exclusiva la memoria y los procesos que administran la CDB. Para obtener más información sobre el SID de Oracle, consulte Oracle System Identifier (SID) en Oracle Database Concepts.

No puede cambiar el nombre de las PDB existentes mediante las API de Amazon RDS. Tampoco puede cambiar el nombre de la CDB con el comando `modify-db-instance`.

Administración de PDB

En el modelo de responsabilidad compartida de RDS Custom para Oracle, usted es responsable de administrar las PDB y de crear las PDB adicionales. RDS Custom no restringe la cantidad de PDB. Para crear, modificar y eliminar PDB manualmente, conéctese a la raíz de la CDB y ejecute una instrucción SQL. Cree PDB en un volumen de datos de Amazon EBS para evitar que la instancia de base de datos salga del perímetro de soporte.

Para modificar sus CDB o PDB, siga los pasos siguientes:

1. Pause la automatización para evitar la interferencia con las acciones de RDS Custom.
2. Modifique su CDB o sus PDB.
3. Realice copias de seguridad de todas las PDB modificadas.
4. Reanudar la automatización personalizada de RDS.

Recuperación automática de la raíz de CDB

RDS Custom mantiene abierta la raíz de CDB de la misma manera que mantiene abierta una que no sea de CDB. Si el estado de la raíz de CDB cambia, la automatización del monitoreo y la recuperación intenta recuperar el estado deseado de la raíz de CDB. Recibe notificaciones de eventos de RDS cuando la raíz de CDB se apaga (`RDS-EVENT-0004`) o se reinicia (`RDS-EVENT-0006`), de forma similar a la arquitectura que no es de CDB. RDS Custom intenta abrir todas las PDB en modo `READ WRITE` al iniciar la instancia de base de datos. Si no se pueden abrir algunas PDB, RDS Custom publica el siguiente evento: `tenant database shutdown`.

Trabajar con funciones de alta disponibilidad para RDS Custom for Oracle

RDS Custom para Oracle proporciona una alta disponibilidad integrada a través de implementaciones multi-AZ. Además, puede utilizar Oracle Data Guard como una opción administrada por el cliente según los casos de uso.

Implementaciones multi-AZ (completamente administradas)

Con implementaciones multi-AZ para RDS Custom para Oracle, Amazon RDS aprovisiona y mantiene automáticamente una réplica síncrona en espera en una zona de disponibilidad (AZ) diferente. La instancia de base de datos principal se replica de forma síncrona en las zonas de disponibilidad en una réplica en espera para la redundancia de datos. La implementación multi-AZ se admite en la Enterprise Edition y en la Standard Edition 2. Para obtener más información, consulte the section called “Administración de una implementación multi-AZ de RDS Custom para Oracle”.

Oracle Data Guard (administrado por el cliente)

Además, puede lograr una alta disponibilidad configurando manualmente Oracle Data Guard para replicar datos entre instancias de base de datos de RDS Custom para Oracle. La instancia de base de datos principal sincroniza automáticamente los datos con las instancias en espera. Oracle Data Guard solo es compatible con Enterprise Edition.

Puede configurar su entorno de alta disponibilidad de las siguientes formas:

- Configure las instancias en espera en diferentes zonas de disponibilidad para que sean resistentes a los errores de las zonas de disponibilidad.
- Coloque las bases de datos en espera en modo montado o de solo lectura. El modo de solo lectura requiere una licencia de Oracle Active Data Guard.
- Conmutación por error o cambio de la base de datos principal a una base de datos en espera sin pérdida de datos.
- Migre los datos configurando la alta disponibilidad para la instancia en las instalaciones y, a continuación, cambiando a la base de datos en espera de RDS Custom para Oracle.

Para obtener información acerca de cómo configurar Oracle Data Guard para alta disponibilidad, consulte el blog de AWS Build high availability for RDS Custom for Oracle using read replicas (Crear alta disponibilidad para RDS Custom para Oracle mediante las réplicas de lectura). Puede llevar a cabo las tareas siguientes:

- Utilice un túnel de Red privada virtual (VPN) para cifrar los datos en tránsito de sus instancias de alta disponibilidad. RDS Custom para Oracle no configura automáticamente el cifrado en tránsito.
- Configure Oracle Fast-Failover Observer (FSFO) para monitorear sus instancias de alta disponibilidad.
- Permita que el observador realice una conmutación por error automática cuando se cumplan las condiciones necesarias.

Personalización del entorno de RDS Custom

RDS Custom para Oracle incluye funciones integradas que le permiten personalizar su entorno de instancias de base de datos sin pausar la automatización. Por ejemplo, puede usar las API de RDS para personalizar el entorno de la siguiente manera:

- Cree y restaure instantáneas de bases de datos para crear un entorno de clonación.
- Cree réplicas de lectura.
- Modifique la configuración de almacenamiento.
- Cambie la CEV para aplicar las actualizaciones de la versión

Para algunas personalizaciones, como cambiar el conjunto de caracteres, no puede usar las API de RDS. En estos casos, debe cambiar el entorno manualmente. Para ello, acceda a su instancia de Amazon EC2 como usuario raíz o inicie sesión en su base de datos Oracle como `SYSDBA`.

Para personalizar la instancia de forma manual, debe pausar y reanudar la automatización de RDS Custom. Esta pausa garantiza que las personalizaciones no interfieran con la automatización de RDS Custom. De esta forma, evita romper el perímetro de soporte, lo que coloca a la instancia en el estado `unsupported-configuration`hasta que se solucionen los problemas subyacentes. La pausa y la reanudación son las únicas tareas de automatización admitidas al modificar una instancia de base de datos de RDS Custom para Oracle.

Pasos generales para personalizar su entorno de RDS Custom

Para personalizar su instancia de base de datos de RDS Custom, siga los pasos que se describen a continuación:

1. Pause la automatización de RDS Custom durante un periodo determinado mediante la consola o la CLI.
2. Identifique la instancia de Amazon EC2 subyacente.
3. Conéctese a la instancia de Amazon EC2 subyacente mediante claves SSH o AWS Systems Manager.
4. Compruebe los ajustes de configuración actuales en la capa de base de datos o del sistema operativo.

   Puede validar los cambios comparando la configuración inicial con la configuración modificada. Según el tipo de personalización que emplee, utilice herramientas del sistema operativo o consultas a la base de datos.

5. Personalice la instancia de base de datos de RDS Custom para Oracle según sea necesario.
6. Reinicie la instancia o la base de datos si es necesario.

> **Note**
>
> En una CDB de Oracle en las instalaciones, puede conservar un modo abierto especificado para las PDB mediante un comando integrado o después de un activador de inicio. Este mecanismo lleva a las PDB a un estado específico cuando se reinicia la CDB. Al abrir su CDB, la automatización de RDS Custom descarta los estados conservados especificados por el usuario e intenta abrir todas las PDB. Si RDS Custom no puede abrir todas las PDB, se emite el siguiente evento: `The following PDBs failed to open: list-of-PDBs`.

7. Compruebe los nuevos ajustes de configuración comparándolos con los ajustes anteriores.
8. Reanude la automatización de RDS Custom de cualquiera de las siguientes formas:
   - Reanude la automatización manualmente.
   - Espere a que finalice el periodo de pausa. En este caso, RDS Custom reanuda el monitoreo y la recuperación de instancias automáticamente.
9. Verifique el marco de automatización de RDS Custom

   Si ha seguido correctamente los pasos anteriores, RDS Custom inicia una copia de seguridad automática. En el estado de la instancia en la consola, se indica Disponible.

Para conocer las prácticas recomendadas y las instrucciones paso a paso, consulte las entradas del blog de AWS Make configuration changes to an Amazon RDS Custom for Oracle instance: Part 1 (Realizar cambios de configuración en una instancia de Amazon RDS Custom para Oracle: parte 1) y Recreate an Amazon RDS Custom for Oracle database: Part 2 (Recrear una base de datos Amazon RDS Custom para Oracle: parte 2).

Pausa y reanudación de la instancia de base de datos de RDS Custom

Puede pausar y reanudar la automatización de la instancia de base de datos mediante la consola o la CLI.

Consola

Para pausar o reanudar la automatización de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y luego elija la instancia de base de datos de RDS Custom que desea modificar.
3. Elija Modify (Modificar). Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. Para RDS Custom automation mode (Modo de automatización de RDS Custom), elija una de las siguientes opciones:
   - Paused (En pausa) pausa el monitoreo y la recuperación de instancias de la instancia de base de datos de RDS Custom. Ingrese la duración de la pausa que desea (en minutos) para Automation mode duration (Duración del modo de automatización). El valor mínimo es 60 minutos (predeterminado). El valor máximo es 1440 minutos.
   - Full automation (Automatización completa) reanuda la automatización.
5. Elija Continue (Continuar) para ver el resumen de las modificaciones.

   Un mensaje indica que RDS Custom aplicará los cambios inmediatamente.
6. Si los cambios son correctos, elija Modify DB instance (Modificar instancia de base de datos). O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

   Los detalles de la modificación aparecen en la consola de RDS. Si ha puesto en pausa la automatización, el Status (Estado) de la instancia de base de datos de RDS Custom indica Automation paused (Automatización en pausa).
7. (Opcional) En el panel de navegación, elija Databases (Bases de datos) y luego la instancia de base de datos de RDS Custom.

   En el panel Summary (Resumen), RDS Custom automation mode (Modo de automatización de RDS Custom) indica el estado de la automatización. Si se pausa la automatización, el valor es Paused (En pausa). La automatización se reanuda en ***num*** minutos.

AWS CLI

Para pausar o reanudar la automatización de RDS Custom, utilice el comando de la AWS CLI `modify-db-instance`. Identifique la instancia de base de datos mediante el parámetro requerido `--db-instance-identifier`. Controle el modo de automatización con los siguientes parámetros:

- `--automation-mode` especifica el estado de pausa de la instancia de base de datos. Los valores válidos son `all-paused`, que pausa la automatización, y `full`, que lo reanuda.
- `--resume-full-automation-mode-minutes` especifica la duración de la pausa. El valor predeterminado es 60 minutos.

> **Note**
>
> Independientemente de que especifique `--no-apply-immediately` o `--apply-immediately`, RDS Custom aplica las modificaciones de forma asíncrona tan pronto como sea posible.

En la respuesta de comando, `ResumeFullAutomationModeTime` indica la hora de reanudación como marca de hora UTC. Cuando el modo de automatización es `all-paused`, puede utilizar `modify-db-instance` para reanudar el modo de automatización o ampliar el periodo de pausa. No se admiten otras opciones de `modify-db-instance`.

En el siguiente ejemplo se pausa la automatización para `my-custom-instance` durante 90 minutos.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --automation-mode all-paused \
    --resume-full-automation-mode-minutes 90
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --automation-mode all-paused ^
```

```
    --resume-full-automation-mode-minutes 90
```

El siguiente ejemplo extiende la duración de la pausa durante 30 minutos adicionales. Los 30 minutos se añaden a la hora original que se muestra en `ResumeFullAutomationModeTime`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --automation-mode all-paused \
    --resume-full-automation-mode-minutes 30
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --automation-mode all-paused ^
    --resume-full-automation-mode-minutes 30
```

En el siguiente ejemplo se reanuda la automatización completa para `my-custom-instance`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --automation-mode full \
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --automation-mode full
```

En la siguiente salida de muestra parcial, el valor pendiente `AutomationMode` es `full`.

```
{
    "DBInstance": {
        "PubliclyAccessible": true,
```

```
        "MasterUsername": "admin",
        "MonitoringInterval": 0,
        "LicenseModel": "bring-your-own-license",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "0123456789abcdefg"
            }
        ],
        "InstanceCreateTime": "2020-11-07T19:50:06.193Z",
        "CopyTagsToSnapshot": false,
        "OptionGroupMemberships": [
            {
                "Status": "in-sync",
                "OptionGroupName": "default:custom-oracle-ee-19"
            }
        ],
        "PendingModifiedValues": {
            "AutomationMode": "full"
        },
        "Engine": "custom-oracle-ee",
        "MultiAZ": false,
        "DBSecurityGroups": [],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.custom-oracle-ee-19",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        ...
        "ReadReplicaDBInstanceIdentifiers": [],
        "AllocatedStorage": 250,
        "DBInstanceArn": "arn:aws:rds:us-west-2:012345678912:db:my-custom-instance",
        "BackupRetentionPeriod": 3,
        "DBName": "ORCL",
        "PreferredMaintenanceWindow": "fri:10:56-fri:11:26",
        "Endpoint": {
            "HostedZoneId": "ABCDEFGHIJKLMNO",
            "Port": 8200,
            "Address": "my-custom-instance.abcdefghijk.us-west-2.rds.amazonaws.com"
        },
        "DBInstanceStatus": "automation-paused",
        "IAMDatabaseAuthenticationEnabled": false,
        "AutomationMode": "all-paused",
```

```
        "EngineVersion": "19.my_cev1",
        "DeletionProtection": false,
        "AvailabilityZone": "us-west-2a",
        "DomainMemberships": [],
        "StorageType": "gp2",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVW",
        "ResumeFullAutomationModeTime": "2020-11-07T20:56:50.565Z",
        "KmsKeyId": "arn:aws:kms:us-west-2:012345678912:key/
aa111a11-111a-11a1-1a11-1111a11a1a1a",
        "StorageEncrypted": false,
        "AssociatedRoles": [],
        "DBInstanceClass": "db.m5.xlarge",
        "DbInstancePort": 0,
        "DBInstanceIdentifier": "my-custom-instance",
        "TagList": []
    }
```


Modificación de la instancia de base de datos de RDS Custom para Oracle

La modificación de una instancia de base de datos de RDS Custom para Oracle es similar a modificar una instancia de base de datos de Amazon RDS. Puede cambiar opciones de configuración como las siguientes:

- Clase de instancia de base de datos
- Asignación y tipo de almacenamiento
- Backup retention period (Periodo de retención de copia de seguridad)
- Protección contra eliminación
- Option group (Grupo de opciones)
- CEV (consulte Actualización de una instancia de base de datos de RDS Custom para Oracle)
- Puerto

Temas

- Requisitos y limitaciones al modificar el almacenamiento de instancias de base de datos
- Requisitos y limitaciones al modificar su clase de instancia de base de datos
- Cómo crea RDS Custom su instancia de base de datos al modificar la clase de instancia
- Modificación de la instancia de base de datos de RDS Custom para Oracle

Requisitos y limitaciones al modificar el almacenamiento de instancias de base de datos

Tenga en cuenta las siguientes limitaciones y requisitos al modificar el almacenamiento de una instancia de base de datos de RDS Custom para Oracle:

- El almacenamiento mínimo asignado para RDS Custom for Oracle es de 40 GiB y el máximo es de 64 TiB.
- Al igual que con Amazon RDS, no es posible reducir el almacenamiento asignado. Se trata de una limitación de los volúmenes de Amazon EBS.
- El escalado automático de almacenamiento no es compatible con las instancias de base de datos de RDS Custom.
- Los volúmenes de almacenamiento que adjunte manualmente a la instancia de base de datos de RDS Custom están fuera del perímetro de soporte.

  Para obtener más información, consulte Perímetro de soporte de RDS Custom.
- El almacenamiento magnético (estándar) de Amazon EBS no es compatible con RDS Custom. Puede elegir solo los tipos de almacenamiento SSD io1, gp2 o gp3.

Para obtener más información sobre el almacenamiento de Amazon EBS, consulte Almacenamiento de instancias de base de datos de Amazon RDS. Para obtener información general sobre la modificación del almacenamiento de información, consulte Uso de almacenamiento para instancias de base de datos de Amazon RDS.

Requisitos y limitaciones al modificar su clase de instancia de base de datos

Tenga en cuenta las siguientes limitaciones y requisitos al modificar la clase de instancia para una instancia de base de datos de RDS Custom para Oracle:

- Su instancia de base de datos debe tener el estado `available`.
- Su instancia de base de datos debe tener un mínimo de 100 MiB de espacio libre en el volumen raíz, el volumen de datos y el volumen binario.
- Solo puede asignar una IP elástica (EIP) a su instancia de base de datos de RDS Custom para Oracle cuando utilice la interfaz de red elástica (ENI) predeterminada. Si adjunta varias ENI a la instancia de base de datos, se producirá un error en la operación de modificación.
- Todas las etiquetas de RDS Custom para Oracle deben estar presentes.
- Si usa RDS Custom para Oracle, tenga en cuenta los siguientes requisitos y limitaciones:

- Para las instancias de base de datos principales y las réplicas de lectura, solo puede cambiar la clase de instancia para una instancia de base de datos a la vez.
- Si su instancia de base de datos de RDS Custom para Oracle tiene una base de datos principal o de réplica en las instalaciones, asegúrese de actualizar manualmente las direcciones IP privadas de la instancia de base de datos en las instalaciones una vez finalizada la modificación. Esta acción es necesaria para preservar la funcionalidad Oracle DataGuard. RDS Custom para Oracle publica un evento cuando la modificación se realiza correctamente.
- No puede modificar su clase de instancia de base de datos de RDS Custom para Oracle cuando las instancias de base de datos principales o de réplica de lectura tengan configurada la FSFO (conmutación por error de inicio rápido).

Cómo crea RDS Custom su instancia de base de datos al modificar la clase de instancia

Al modificar la clase de instancia, RDS Custom crea su instancia de base de datos del siguiente modo:

- Crea la instancia de Amazon EC2.
- Crea el volumen raíz a partir de la última instantánea de base de datos. RDS Custom para Oracle no conserva la información agregada al volumen raíz después de la última instantánea de base de datos.
- Crea alarmas de Amazon CloudWatch.
- Crea un par de claves SSH de Amazon EC2 si ha eliminado el par de claves original. De lo contrario, RDS Custom para Oracle conserva el par de claves original.
- Crea nuevos recursos mediante las etiquetas que se adjuntan a la instancia de base de datos al iniciar la modificación. RDS Custom no transfiere las etiquetas a los nuevos recursos cuando se adjuntan directamente a los recursos subyacentes.
- Transfiere los volúmenes binarios y de datos con las modificaciones más recientes a la nueva instancia de base de datos.
- Transfiere la dirección IP elástica (EIP). Si la instancia de base de datos es de acceso público, RDS Custom adjunta temporalmente una dirección IP pública a la nueva instancia de base de datos antes de transferir la EIP. Si no se puede acceder a la instancia de base de datos de forma pública, RDS Custom no crea direcciones IP públicas.

Modificación de la instancia de base de datos de RDS Custom para Oracle

Puede modificar la clase de instancia de base de datos o el almacenamiento mediante la consola, la AWS CLI o la API de RDS.

Consola

Para modificar una instancia de base de datos de RDS Custom para Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea modificar.
4. Elija Modify.
5. (Opcional) En Configuración de la instancia, elija un valor para la Clase de instancia de base de datos. Para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.
6. (Opcional) En Almacenamiento, realice los siguientes cambios según sea necesario:
   a. Ingrese un nuevo valor para Allocated Storage (Almacenamiento asignado). Debe ser mayor que el valor actual y de 40 GiB a 64 TiB.
   b. Cambie el valor de Tipo de almacenamiento a SSD de uso general (gp2), SSD de uso general (gp3) o IOPS aprovisionadas (io1).
   c. Si usa IOPS aprovisionadas (io1) o SSD de uso general (gp3), puede cambiar el valor de las IOPS aprovisionadas.
7. (Opcional) En Configuración adicional, realice los siguientes cambios según sea necesario:
   - En Grupo de opciones, elija un nuevo grupo de opciones. Para obtener más información, consulte Trabajar con grupos de opciones en RDS Custom para Oracle.
8. Elija Continue (Continuar).
9. Elija Apply immediately (Aplicar inmediatamente) o Apply during the next scheduled maintenance window (Aplicar durante el próximo periodo de mantenimiento programado).
10. Elija Modify DB instance (Modificar la instancia de base de datos).

AWS CLI

Para modificar el almacenamiento de una instancia de base de datos de RDS Custom for Oracle, utilice el comando de la AWS CLI modify-db-instance. Configure los siguientes parámetros según sea necesario:

- `--db-instance-class`: una clase de instancia nueva. Para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.
- `--allocated-storage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes. Debe ser mayor que el valor actual y de 40 a 65 536 GiB.
- `--storage-type`: tipo de almacenamiento: gp2, gp3 o io1.
- `--iops`: IOPS aprovisionadas para la instancia de base de datos, si se utilizan los tipos de almacenamiento io1 o gp3.
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente.

  También puede utilizar `--no-apply-immediately` (valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento.

En el siguiente ejemplo, se cambia la clase de instancia de base de datos de my-cfo-instance a db.m5.16xlarge. El comando también cambia el tamaño de almacenamiento a 1 TiB, el tipo de almacenamiento a io1 y las IOPS aprovisionadas a 3000, y el grupo de opciones a cfo-ee-19-mt.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-cfo-instance \
    --db-instance-class db.m5.16xlarge \
    --storage-type io1 \
    --iops 3000 \
    --allocated-storage 1024 \
    --option-group cfo-ee-19-mt \
    --apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
```

```
    --db-instance-identifier my-cfo-instance ^
    --db-instance-class db.m5.16xlarge ^
    --storage-type io1 ^
    --iops 3000 ^
    --allocated-storage 1024 ^
    --option-group cfo-ee-19-mt ^
    --apply-immediately
```

Cambio de la zona horaria de una instancia de base de datos de RDS Custom para Oracle

RDS Custom para Oracle utiliza de forma predeterminada el conjunto de caracteres US7ASCII. Es recomendable especificar diferentes conjuntos de caracteres para cumplir los requisitos de idioma o de caracteres de varios bytes. Si utiliza RDS Custom para Oracle, puede pausar la automatización y cambiar manualmente el conjunto de caracteres de su base de datos.

El cambio del conjunto de caracteres de una instancia de base de datos de RDS Custom para Oracle tiene los siguientes requisitos:

- Solo puede cambiar el carácter en una instancia RDS Custom recién aprovisionada que tenga una base de datos vacía o inicial sin datos de aplicación. En los demás casos, cambie el conjunto de caracteres mediante DMU (Asistente de migración de bases de datos para Unicode).
- Solo se puede cambiar a un conjunto de caracteres que admita RDS para Oracle. Para obtener más información, consulte Conjuntos de caracteres de base de datos admitidos.

Para cambiar el conjunto de caracteres de una instancia de base de datos de RDS Custom para Oracle

1. Pausa la automatización de RDS Custom. Para obtener más información, consulte Pausa y reanudación de la instancia de base de datos de RDS Custom.
2. Inicie sesión en su base de datos como un usuario con privilegios SYSDBA.
3. Reinicie la base de datos en modo restringido, cambie el conjunto de caracteres y, a continuación, reinicie la base de datos en modo normal.

   Ejecute el siguiente script en cliente SQL:

   ```
   SHUTDOWN IMMEDIATE;
   STARTUP RESTRICT;
   ALTER DATABASE CHARACTER SET INTERNAL_CONVERT AL32UTF8;
   ```

```
SHUTDOWN IMMEDIATE;
STARTUP;
SELECT VALUE FROM NLS_DATABASE_PARAMETERS WHERE PARAMETER = 'NLS_CHARACTERSET';
```

Compruebe que la salida muestre el conjunto de caracteres correcto:

```
VALUE
--------
AL32UTF8
```

4. Reanudar la automatización personalizada de RDS. Para obtener más información, consulte Pausa y reanudación de la instancia de base de datos de RDS Custom.

Configuración del valor de NLS_LANG en RDS Custom para Oracle

Una configuración regional es un conjunto de información que aborda los requisitos lingüísticos y culturales que corresponde a un idioma y país determinados. Para especificar el comportamiento de la configuración regional del software de Oracle, defina la variable de entorno `NLS_LANG` en el host del cliente. Esta variable establece el idioma, el territorio y el conjunto de caracteres utilizados por la aplicación cliente en una sesión de base de datos.

Para RDS Custom para Oracle, solo puede establecer el idioma en la variable `NLS_LANG`; para el territorio y los caracteres se utilizan los valores predeterminados. El idioma se utiliza para los mensajes de la base de datos Oracle, la intercalación, los nombres de los días y los nombres de los meses. Cada idioma admitido tiene un nombre único, por ejemplo, inglés de EE. UU., francés o alemán. Si no se especifica, el valor predeterminado es el inglés de EE. UU.

Tras crear la base de datos RDS Custom para Oracle, puede configurar `NLS_LANG` en el host del cliente en un idioma que no sea el inglés. Para ver una lista de los idiomas que se admiten en Oracle Database, inicie sesión en su base de datos RDS Custom para Oracle y ejecute la siguiente consulta:

```
SELECT VALUE FROM V$NLS_VALID_VALUES WHERE PARAMETER='LANGUAGE' ORDER BY VALUE;
```

Puede configurar `NLS_LANG` en la línea de comandos del host. En el siguiente ejemplo, se establece el idioma en Alemán para la aplicación cliente mediante el intérprete de comandos Z en Linux.

```
export NLS_LANG=German
```

La aplicación lee el valor `NLS_LANG` cuando se inicia y, a continuación, se lo comunica a la base de datos cuando se conecta.

Para obtener más información, consulte Choosing a Locale with the NLS_LANG Environment Variable (Selección de una configuración regional con la variable de entorno NLS_LANG) en la Oracle Database Globalization Support Guide (Guía de soporte para la globalización de bases de datos Oracle).

Compatibilidad para cifrado de datos transparente

RDS Custom admite el cifrado Transparent Data Encryption (TDE) para instancia de base de datos de RDS Custom for Oracle.

Sin embargo, no se puede habilitar TDE mediante una opción de un grupo de opciones personalizado como en RDS for Oracle. Encienda TDE manualmente. Para obtener información sobre cómo utilizar el cifrado de datos transparente de Oracle, consulte Securing stored data using Transparent Data Encryption (Protección de los datos almacenados mediante el cifrado de datos transparente) en la documentación de Oracle.

Etiquetado de recursos de RDS Custom for Oracle

Puede etiquetar recursos de RDS Custom como con los recursos de Amazon RDS, pero con algunas diferencias importantes:

- No cree ni modifique la etiqueta `AWSRDSCustom` necesaria para la automatización de RDS Custom. Si lo hace, podría interrumpir la automatización.
- La etiqueta `Name` se agrega a los recursos de RDS Custom con un valor de prefijo de `do-not-delete-rds-custom` o `rds-custom!oracle-do-not-delete`. Se sobrescribe cualquier valor de la clave que el cliente haya pasado.
- Las etiquetas agregadas a las instancias de base de datos de RDS Custom durante la creación se propagan a todos los demás recursos de RDS Custom relacionados.
- Las etiquetas no se propagan cuando se agregan a los recursos de RDS Custom tras la creación de la instancia de base de datos.

Para obtener información general sobre el etiquetado de recursos, consulte Etiquetado de los recursos de y Amazon RDS.

Eliminación de una instancia de base de datos de RDS Custom for Oracle

Para eliminar una instancia de base de datos de RDS Custom, haga lo siguiente:

- Proporcione el nombre de la instancia de base de datos.
- Desactive la opción para tomar una instantánea de base de datos final de la instancia de base de datos.
- Elija o desactive la opción de retener copias de seguridad automatizadas.

Puede eliminar una instancia de base de datos de RDS Custom a través de la consola o la CLI. El tiempo necesario para eliminar la instancia de base de datos puede variar según el periodo de retención de copia de seguridad (es decir, cuántas copias de seguridad eliminar) y cuántos datos se eliminan.

Consola

Para eliminar una instancia de base de datos de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y luego elija la instancia de base de datos de RDS Custom que desea eliminar. Las instancias de base de datos de RDS Custom muestran el rol Instance (RDS Custom) (Instancia [RDS Custom]).
3. En Actions (Acciones), seleccione Delete (Eliminar).
4. Para conservar las copias de seguridad automatizadas, elija Retain automated backups (Conservar copias de seguridad automatizadas).
5. En el cuadro, escriba **`delete me`**.
6. Elija Eliminar (Delete).

AWS CLI

Elimine una instancia de base de datos de RDS Custom mediante el comando de la AWS CLI delete-db-instance. Identifique la instancia de base de datos mediante el parámetro requerido `--db-instance-identifier`. Los parámetros restantes son los mismos que para una instancia de base de datos de Amazon RDS, con las siguientes excepciones:

- `--skip-final-snapshot` es obligatorio.

- `--no-skip-final-snapshot` no es compatible.
- `--final-db-snapshot-identifier` no es compatible.

En el siguiente ejemplo se elimina la instancia de base de datos de RDS Custom denominada `my-custom-instance` y conserva copias de seguridad automatizadas.

Example

Para Linux, macOS o:Unix

```
aws rds delete-db-instance \
    --db-instance-identifier my-custom-instance \
    --skip-final-snapshot \
    --no-delete-automated-backups
```

En:Windows

```
aws rds delete-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --skip-final-snapshot ^
    --no-delete-automated-backups
```

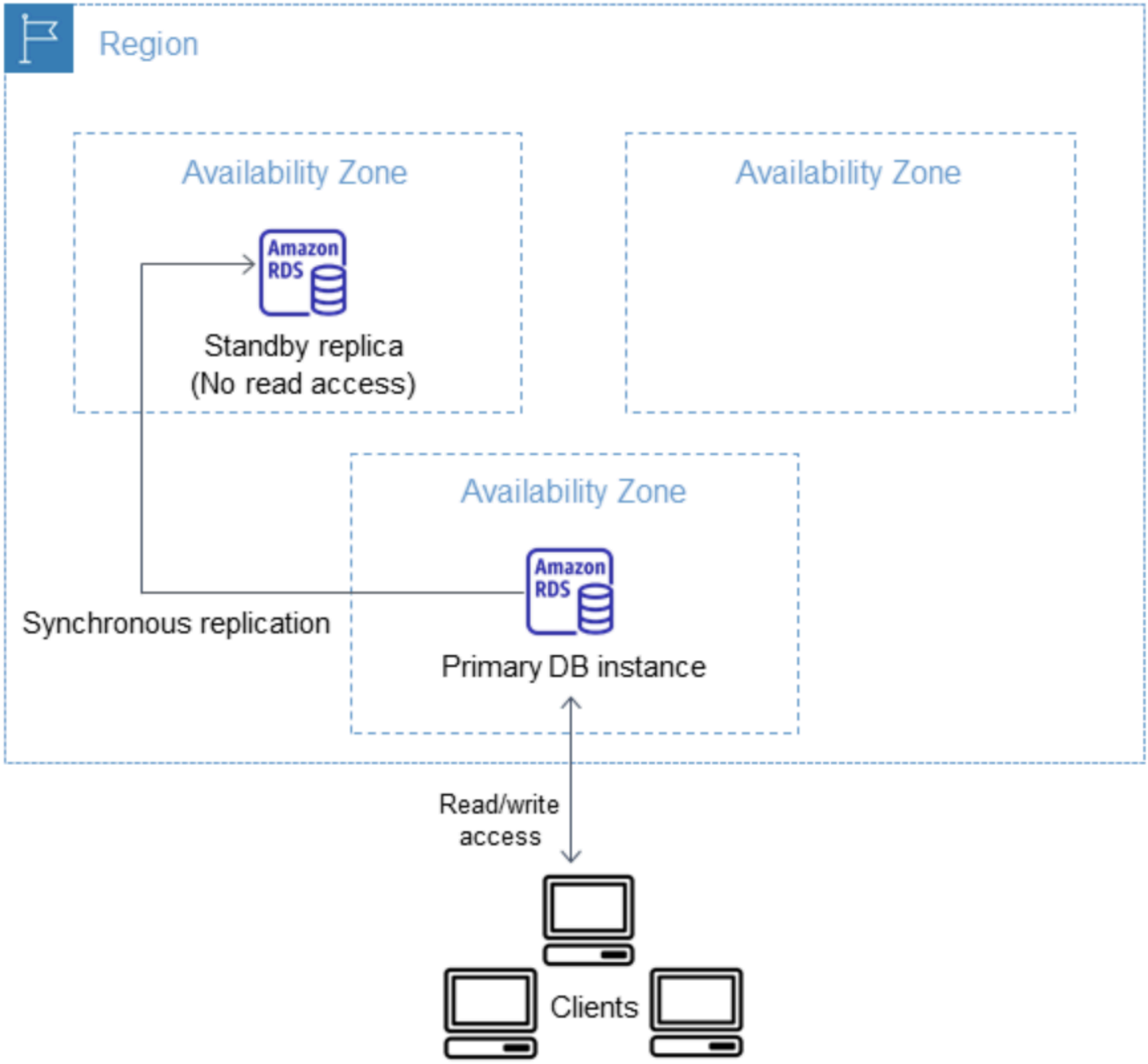
Administración de una implementación multi-AZ de RDS Custom para Oracle

En una implementación de instancias de base de datos multi-AZ para RDS Custom para Oracle, Amazon RDS aprovisiona y mantiene automáticamente una réplica síncrona en espera dentro de una zona de disponibilidad (AZ) diferente. La instancia de base de datos principal se replica de forma síncrona en las zonas de disponibilidad en una réplica en espera para proporcionar redundancia de datos.

> **Important**
>
> Una implementación multi-AZ para RDS Custom para Oracle es diferente a una implementación multi-AZ para RDS para Oracle. A diferencia de multi-AZ para RDS para Oracle, debe cumplir los requisitos previos para RDS Custom para Oracle antes de crear la instancia de base de datos multi-AZ, ya que RDS Custom se ejecuta dentro de su propia cuenta, lo que requiere permisos. Además, debe crear la instancia multi-AZ en la CEV con la AMI proporcionada por el servicio más reciente que admita las implementaciones multi-AZ. Si no cumple los requisitos previos, es posible que su instancia de base de datos multi-AZ no se ejecute o que se revierta automáticamente a una instancia de base de datos Single-AZ. Para obtener más información acerca de los requisitos previos, consulte the section called “Requisitos previos”.

La ejecución de una instancia de base de datos con alta disponibilidad puede mejorar la disponibilidad durante el mantenimiento de sistema planificado. Si se produce una interrupción del servicio no planificada o un mantenimiento planificado de la base de datos, Amazon RDS conmuta automáticamente a la instancia de base de datos en espera. Esta funcionalidad permite que las operaciones de base de datos se reanuden rápidamente sin intervención manual. Las instancias principal y en espera usan el mismo punto de conexión, cuya dirección de red física cambia a la réplica en espera como parte del proceso de conmutación por error. No tiene que volver a configurar su aplicación cuando se produzca una conmutación por error.

En el siguiente diagrama se muestra la arquitectura multi-AZ de RDS Custom para Oracle:



Puede crear una implementación multi-AZ de RDS Custom para Oracle especificando multi-AZ al crear una instancia de base de datos de RDS Custom. Las instancias de base de datos de RDS Custom para Oracle creadas antes del 30 de junio de 2025 no se pueden convertir en implementaciones multi-AZ mediante la modificación de la instancia de base de datos y la especificación de la opción multi-AZ. Debe crear una nueva instancia de base de datos de RDS Custom para Oracle especificando la opción multi-AZ. Las nuevas instancias de base de datos creadas con la AMI proporcionada por el servicio y disponibles después del 30 de junio de 2025

admiten la opción multi-AZ. A continuación, debe migrar la base de datos de RDS Custom para Oracle existente a la instancia de base de datos recién creada. Para obtener más información, consulte the section called “Migración de las CEV anteriores al 30.06.2025”.

La consola de Amazon RDS muestra la zona de disponibilidad de la réplica en espera (la zona de disponibilidad secundaria). También puede usar el comando de la CLI `describe-db-instances` o la operación de la API `DescribeDBInstances` para buscar la AZ secundaria.

Las instancias de base de datos de RDS Custom para Oracle con implementación multi-AZ pueden tener una latencia de escritura y confirmación superior a la de una implementación single-AZ. Este aumento se puede producir debido a la replicación de datos síncrona entre las instancias de base de datos. Puede detectar un cambio en la latencia si la implementación conmuta a la réplica en espera, aunque AWS se ha diseñado con una conectividad de red de baja latencia entre zonas de disponibilidad.

Temas

- Disponibilidad en regiones y versiones
- Limitaciones de una implementación multi-AZ de RDS Custom para Oracle
- Creación de una instancia de base de datos de RDS Custom para Oracle con una implementación multi-AZ
- Requisitos previos de una implementación multi-AZ con RDS Custom para Oracle
- Conversión de una implementación single-AZ de RDS Custom para Oracle en una implementación multi-AZ
- Conversión de una implementación multi-AZ de RDS Custom para Oracle en una implementación single-AZ
- Proceso de conmutación por error para una implementación multi-AZ de RDS Custom para Oracle
- Implementación de RDS Custom para Oracle con AWS CloudFormation

Disponibilidad en regiones y versiones

Las implementaciones multi-AZ de RDS Custom para Oracle son compatibles con las siguientes ediciones de base de datos de Oracle:

- Base de datos Oracle 12c versión 1 (12.1)
- Base de datos Oracle 12c versión 2 (12.2)

- Oracle Database 19c
- Enterprise Edition (EE)
- Standard Edition 2 (SE2)

> **Note**
>
> Las implementaciones multi-AZ de RDS Custom para Oracle no son compatibles con la base de datos de Oracle 18c.

Las implementaciones multi-AZ de RDS Custom para Oracle están disponibles en todas las regiones en las que está disponible RDS Custom para Oracle. Para obtener más información sobre la disponibilidad en las regiones de las implementaciones multi-AZ de RDS Custom para Oracle, consulte the section called “Regiones y motores de base de datos admitidos para RDS Custom para Oracle”.

Limitaciones de una implementación multi-AZ de RDS Custom para Oracle

Las implementaciones multi-AZ de RDS Custom para Oracle tienen las siguientes limitaciones:

- No se admiten implementaciones multi-AZ entre regiones.
- No puede configurar la instancia de base de datos en espera de modo que acepte la actividad de lectura de bases de datos.
- Cuando utilice una versión de motor personalizada (CEV) con una implementación multi-AZ, la instancia de base de datos en espera también utilizará la misma CEV. La instancia de base de datos en espera no puede usar una CEV diferente.
- No puede crear una réplica de lectura en una instancia de implementación multi-AZ y tampoco puede modificar la instancia principal de la réplica de lectura para que tenga una implementación multi-AZ.

Creación de una instancia de base de datos de RDS Custom para Oracle con una implementación multi-AZ

Para crear una instancia de base de datos de RDS Custom para Oracle con una implementación multi-AZ, siga los pasos que se indican en the section called “Configuración del entorno RDS Custom for Oracle” para configurar el entorno con los requisitos previos.

> **Important**
>
> Para simplificar la configuración, le recomendamos que utilice el archivo de plantilla de AWS CloudFormation más reciente que se proporciona en las instrucciones de configuración de red. Para obtener más información, consulte the section called “Implementación con AWS CloudFormation”.

Para crear una instancia de RDS Custom para Oracle con una implementación multi-AZ, elija la opción multi-AZ durante la creación de la instancia de base de datos en la consola de Amazon RDS. Como alternativa, puede especificar el parámetro `--multi-az` en el comando `create-db-instance` de Amazon RDS en la AWS CLI.

Requisitos previos de una implementación multi-AZ con RDS Custom para Oracle

> **Note**
>
> Si creó la instancia de RDS Custom para Oracle antes del 30 de junio de 2025, no podrá modificarla desde una implementación single-AZ a multi-AZ. Su versión de motor personalizado (CEV) subyacente se creó con una AMI anterior proporcionada por el servicio más antigua que no admite la implementación multi-AZ.
> Debe migrar la base de datos a una nueva instancia con una CEV que cree con una AMI proporcionada por el servicio después del 30 de junio de 2025.
> Consulte the section called “Migración de las CEV anteriores al 30.06.2025”.

RDS Custom para Oracle requiere requisitos previos específicos al convertir de una implementación single-AZ a multi-AZ. Los requisitos previos incompletos provocarán un error en la configuración multi-AZ. Utilice la configuración manual o el archivo de plantilla AWS CloudFormation más reciente que se proporciona en las instrucciones de configuración de red. Para obtener más información, consulte the section called “Paso 3: extraer las plantillas de CloudFormation para RDS Custom for Oracle”.

Para completar los requisitos previos manualmente, siga los pasos que se indican en the section called “Single-AZ a multi-AZ” y tenga en cuenta lo siguiente:

- Asegúrese de que la instancia de base de datos de RDS Custom para Oracle utilice una CEV creada después del 30 de junio de 2025 con la última AMI proporcionada por el servicio.

- Actualice las reglas de entrada y salida del grupo de seguridad de Amazon RDS para permitir el puerto 1120.
- Cree nuevos puntos de conexión de VPC de Amazon SQS que permitan a la instancia de base de datos de RDS Custom para Oracle de Amazon RDS comunicarse con Amazon SQS.
- Actualice los permisos de Amazon SQS en el rol del perfil de instancia.

> **Important**
>
> No reinicie manualmente la instancia de base de datos principal multi-AZ iniciando sesión en la instancia sin pausar la automatización de RDS Custom para Oracle.

Pasos de migración para las instancias de base de datos que utilizan CEV creadas antes del 30 de junio de 2025

Si creó la instancia de base de datos de RDS Custom para Oracle antes del 30 de junio de 2025, no podrá modificarla directamente para una implementación multi-AZ porque la CEV subyacente se creó con una AMI proporcionada por el servicio más antigua que no admite multi-AZ. Debe migrar la base de datos a una nueva instancia mediante una CEV que cree después del 30 de junio de 2025. Haga lo siguiente para la migración.

1. Cree una CEV desde el origen con la AMI proporcionada por el servicio más reciente (después del 30 de junio de 2025)
2. Lanzamiento de una nueva instancia de base de datos con la nueva CEV
3. Migre la base de datos desde la instancia de base de datos existente que no admite la implementación multi-AZ a la instancia recién creada utilizando uno de los siguientes métodos:
   - Migración física de bases de datos de Oracle a Amazon RDS Custom mediante Data Guard
   - Migración física de bases de datos de Oracle a Amazon RDS Custom mediante la duplicación de RMAN

Conversión de una implementación single-AZ de RDS Custom para Oracle en una implementación multi-AZ

Puede modificar una instancia de RDS Custom para Oracle compatible de multi-AZ existente para convertirla de una implementación single-AZ en una implementación multi-AZ. Cuando modifica la instancia de base de datos, Amazon RDS realiza varias acciones:

- Realiza una instantánea de la instancia de base de datos principal.
- Crea nuevos volúmenes para la réplica en espera a partir de la instantánea. Estos volúmenes se inicializan en segundo plano y se alcanza el máximo rendimiento del volumen cuando los datos se han inicializado por completo.
- Activa la replicación síncrona en el nivel de bloque entre las instancias de base de datos principal y en espera.

> **Important**
>
> Le recomendamos que evite modificar la instancia de base de datos de RDS Custom para Oracle para convertir la implementación single-AZ en una implementación multi-AZ en una instancia de base de datos de producción durante los periodos de máxima actividad.

AWS usa una instantánea para crear la instancia en espera para evitar el tiempo de inactividad al convertir una implementación single-AZ en multi-AZ, pero el rendimiento podría verse afectado durante y después de la conversión a multi-AZ. Este impacto puede ser significativo para las cargas de trabajo sensibles a la latencia de escritura. Si bien esta capacidad permite restaurar rápidamente grandes volúmenes a partir de instantáneas, puede provocar un aumento considerable de la latencia de las operaciones de E/S debido a la replicación síncrona. Esta latencia puede afectar al rendimiento de la base de datos.

Configuración de requisitos previos para convertir una implementación single-AZ en multi-AZ mediante CloudFormation

Siga the section called “Paso 3: extraer las plantillas de CloudFormation para RDS Custom for Oracle” para volver a configurar el perfil de VPC e IAM para agregar el punto de conexión de VPC de SQS y el permiso de SQS en el perfil de IAM.

Configuración de los requisitos previos para convertir manualmente una implementación single-AZ en multi-AZ

Si decide configurar los requisitos previos manualmente, realice las siguientes tareas.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/
2. Elija Punto de conexión. Aparecerá la página Create Endpoint (Creación de un punto de enlace).
3. En Categoría de servicio, elija Servicios de AWS.

4. En Servicios, busque `SQS`.
5. En VPC, elija la VPC en la que está implementada la instancia de base de datos de RDS Custom para Oracle.
6. En Subredes, elija las subredes en las que está implementada la instancia de base de datos de RDS Custom para Oracle.
7. En Grupos de seguridad, elija el grupo de seguridad en el que está implementada la instancia de base de datos de RDS Custom para Oracle.
8. En Política, elija Personalizada.
9. En la política personalizada, reemplace los valores `AWS partition`, `Region`, `accountId` y `IAM-Instance-role` por sus propios valores.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/AWSRDSCustom": "custom-oracle"
                }
            },
            "Action": [
                "SQS:SendMessage",
                "SQS:ReceiveMessage",
                "SQS:DeleteMessage",
                "SQS:GetQueueUrl"
            ],
            "Resource": "arn:${AWS::Partition}:sqs:${AWS::Region}:${AWS::AccountId}:do-
not-delete-rds-custom-*",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/{IAM-
Instance-role}"
            }
        }
    ]
}
```

Actualice el perfil de instancia con permiso para acceder a Amazon SQS. Reemplace `AWS partition`, `Region` y `accountId` por sus propios valores.

```
{
    "Sid": "13",
    "Effect": "Allow",
    "Action": [
        "SQS:SendMessage",
        "SQS:ReceiveMessage",
        "SQS:DeleteMessage",
        "SQS:GetQueueUrl"
    ],
    "Resource": [
        {
            "Fn::Sub": "arn:${AWS::Partition}:sqs:${AWS::Region}:${AWS::AccountId}:do-
not-delete-rds-custom-*"
        }
    ],
    "Condition": {
        "StringLike": {
            "aws:ResourceTag/AWSRDSCustom": "custom-oracle"
        }
    }
}
```

Actualice las reglas de entrada y salida del grupo de seguridad de Amazon RDS para permitir el puerto 1120.

- En Grupos de seguridad, elija el grupo en el que está implementada la instancia de base de datos de RDS Custom para Oracle.
- En Reglas de entrada, cree una regla TCP personalizada para permitir el puerto `1120` desde el grupo de origen.
- En Reglas de salida, cree una regla TCP personalizada para permitir el puerto `1120` al grupo de destino.

Modificación mediante la consola de RDS, la AWS CLI o la API de RDS

Una vez completados los requisitos previos, puede modificar una instancia de base de datos de RDS Custom para Oracle para convertir una implementación single-AZ en multi-AZ mediante la consola de Amazon RDS, AWS CLI o la API de Amazon RDS.

Consola

Conversión de una implementación single-AZ de RDS Custom para Oracle en una implementación multi-AZ

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos). Aparece el panel Databases (Bases de datos).
3. Elija la instancia de base de datos de RDS Custom para Oracle DB que desea modificar.
4. En Acciones, elija Convertir a implementación multi-AZ.
5. Para aplicar los cambios de forma inmediata, seleccione la opción Aplicar inmediatamente en la página Confirmación. La elección de esta opción no provoca tiempo de inactividad, pero existe un posible impacto en el rendimiento. De forma alternativa, también puede aplicar la actualización durante la siguiente ventana de mantenimiento. Para obtener más información, consulte the section called “Programación de modificaciones”.
6. En la página Confirmación, seleccione Convertir a multi-AZ.

AWS CLI

Para convertirla en una implementación de instancia de base de datos multi-AZ mediante la AWS CLI, llame al comando modify-db-instance y defina la opción `--multi-az`. Especifique el identificador de instancias de base de datos y los valores de las otras opciones que desea modificar. Para obtener más información acerca de cada opción, consulte the section called “Opciones disponibles”.

Example Ejemplo

El código siguiente modifica `mycustomdbinstance` al incluir la opción `--multi-az`. Los cambios se aplican durante el siguiente periodo de mantenimiento si se utiliza el parámetro `--no-apply-immediately`. Utilice `--apply-immediately` para aplicar los cambios inmediatamente. Para obtener más información, consulte the section called “Programación de modificaciones”.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mycustomdbinstance \
```

```
    --multi-az \
    [--no-apply-immediately | --apply-immediately]
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mycustomdbinstance ^
    --multi-az ^
    [--no-apply-immediately | --apply-immediately]
```

API de RDS

Para convertirla en una implementación de instancia de base de datos multi-AZ con la API de Amazon RDS, llame a la operación ModifyDBInstance y defina el parámetro `MultiAZ` en true.

Conversión de una implementación multi-AZ de RDS Custom para Oracle en una implementación single-AZ

Puede modificar una instancia de base de datos de RDS Custom para Oracle existente para convertirla de una implementación multi-AZ en una implementación single-AZ.

Consola

Modificación de una instancia de base de datos de RDS Custom para Oracle para convertirla de una implementación multi-AZ en una implementación single-AZ

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos). Aparece el panel Databases (Bases de datos).
3. Elija la instancia de base de datos de RDS Custom para Oracle DB que desea modificar.
4. En Implementación multi-AZ, elija No.
5. Para aplicar los cambios de forma inmediata, seleccione la opción Aplicar inmediatamente en la página Confirmación. La elección de esta opción no provoca tiempo de inactividad, pero existe un posible impacto en el rendimiento. De forma alternativa, también puede aplicar la actualización durante la siguiente ventana de mantenimiento. Para obtener más información, consulte the section called “Programación de modificaciones”.
6. En la página Confirmación, elija Modificar la instancia de base de datos.

AWS CLI

Para convertir una implementación multi-AZ en una implementación single-AZ mediante la AWS CLI, llame al comando modify-db-instance e incluya la opción `--no-multi-az`. Especifique el identificador de instancias de base de datos y los valores de las otras opciones que desea modificar. Para obtener más información acerca de cada opción, consulte the section called “Opciones disponibles”.

Example Ejemplo

El código siguiente modifica `mycustomdbinstance` al incluir la opción `--no-multi-az`. Los cambios se aplican durante el siguiente periodo de mantenimiento si se utiliza el parámetro `--no-apply-immediately`. Utilice `--apply-immediately` para aplicar los cambios inmediatamente. Para obtener más información, consulte the section called “Programación de modificaciones”.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mycustomdbinstance \
    --no-multi-az \
    [--no-apply-immediately | --apply-immediately]
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mycustomdbinstance ^
    --no-multi-az ^
    [--no-apply-immediately | --apply-immediately]
```

API de RDS

Para convertir una implementación multi-AZ en una implementación single-AZ mediante la API de Amazon RDS, ejecute la operación ModifyDBInstance y defina el parámetro `MultiAZ` en `false`.

Proceso de conmutación por error para una implementación multi-AZ de RDS Custom para Oracle

Si se produce una interrupción planeada o no planeada de la instancia de base de datos a causa de un defecto de la infraestructura, Amazon RDS cambia automáticamente a una réplica en espera

de otra zona de disponibilidad si se ha activado Multi-AZ. El tiempo requerido para completar la conmutación por error dependerá de la actividad de la base de datos y de otras condiciones existentes en el momento en que la instancia de base de datos principal deja de estar disponible. Los tiempos de conmutación por error suelen estar entre los 60 y 120 segundos. Sin embargo, las transacciones grandes o un proceso de recuperación largo pueden aumentar el tiempo de conmutación por error. Cuando la conmutación por error se haya completado, puede hacer falta más tiempo para que la consola de Amazon RDS muestre la nueva zona de disponibilidad.

> **Note**
>
> Puede forzar una conmutación por error manualmente cuando detenga e inicie su host de EC2 principal mientras su instancia de base de datos esté disponible.

Amazon RDS gestiona las conmutaciones por error automáticamente para que sea posible reanudar las operaciones de la base de datos lo antes posible sin intervención administrativa. La instancia de base de datos principal conmuta automáticamente a la réplica en espera si se da cualquiera de las condiciones descritas en la siguiente tabla. Puede ver los motivos de la conmutación por error en el registro de eventos de Amazon RDS.

Motivo de la conmutación por error	Descripción
Se le aplican parches al sistema operativo subyacente a la instancia de base de datos de RDS en una operación sin conexión.	Se ha desencadenado una conmutación por error durante la ventana de mantenimiento para un parche del sistema operativo o una actualización de seguridad. Para obtener más información, consulte the section called “Mantenimiento de una instancia de base de datos”.
El host principal de la instancia multi-AZ de RDS no está en buen estado.	La implementación de una instancia de base de datos Multi-AZ detectó una instancia de base de datos principal deteriorada y se produjo una conmutación por error.
El host principal de la instancia multi-AZ de RDS es inaccesible debido a la pérdida de conectividad de red.	El monitoreo de RDS detectó un error de accesibilidad de la red a la instancia de base de datos principal y desencadenó una conmutación por error.
El cliente modificó la instancia de RDS.	Una modificación de la instancia de base de datos de RDS desencadenó una conmutación por error. Para

Motivo de la conmutación por error	Descripción
	obtener más información, consulte the section called “Modificación de la instancia de base de datos ”.
El volumen de almacenamiento subyacente al host principal de la instancia multi-AZ de RDS tuvo un error.	La implementación de una instancia de base de datos Multi-AZ detectó un problema de almacenamiento en la instancia de base de datos principal y se produjo una conmutación por error.
La instancia principal multi-AZ de RDS está ocupada y no responde.	La instancia de base de datos principal no responde. Recomendamos que haga lo siguiente: examine los registros de eventos y de CloudWatch en busca de uso excesivo de CPU, memoria o espacio de intercambio. Para obtener más información, consulte the section called “Uso de notificaciones de eventos de Amazon RDS” y the section called “Creación de una regla que se desencadena en función de un evento Amazon RDS”. Evalúe su carga de trabajo para determinar si está utilizando la clase de instancia de base de datos adecuada. Para obtener más información, consulte the section called “Clases de instancia de base de datos”.

Para determinar si se produjo una conmutación por error en la instancia de base de datos Multi-AZ, puede hacer lo siguiente:

- Configure suscripciones de eventos de base de datos para notificar por correo electrónico o por SMS que se ha iniciado una conmutación por error. Para obtener más información sobre los eventos, consulte the section called “Uso de notificaciones de eventos de Amazon RDS”.
- Vea sus eventos de base de datos mediante la consola de Amazon RDS o las operaciones de la API.
- Consulte el estado actual de la implementación de una instancia de base de datos multi-AZ de RDS Custom para Oracle mediante la consola de Amazon RDS, la CLI o las operaciones de la API.

Configuración del tiempo de vida (TTL) con aplicaciones que utilizan una implementación multi-AZ de RDS Custom para Oracle

El mecanismo de conmutación por error cambia automáticamente el registro del Sistema de nombres de dominio (DNS) de la instancia de base de datos para que apunte a la instancia de base de datos en espera. Como consecuencia, necesita restablecer las conexiones existentes a la instancia de base de datos. Asegúrese de que cualquier valor de configuración de tiempo de vida (TTL) de la memoria caché de DNS sea bajo y compruebe que la aplicación no almacene el DNS en caché durante un periodo prolongado. Un valor de TTL alto puede impedir que la aplicación se vuelva a conectar rápidamente a la instancia de base de datos tras la conmutación por error.

Implementación de RDS Custom para Oracle con AWS CloudFormation

Automatice la implementación de RDS Custom para Oracle con la plantilla de AWS CloudFormation proporcionada. Complete los siguientes requisitos previos antes de implementar los recursos.

Requisitos previos

Descargar los archivos de Oracle necesarios

Necesita archivos de instalación específicos de Oracle antes de poder crear la plantilla de AWS CloudFormation. Descargue estos archivos antes de implementar.

1. Navegación a Oracle Database 19c (19.3)
2. Localización y descarga del archivo `LINUX.X64_193000_db_home.zip`
3. Cambio de nombre del archivo a `V982063-01.zip`
4. Descarga de los parches restantes, seleccionando Plataforma o Idioma como `Linux x86-64`

Utilidad OPatch más reciente

Parche 6880880

Parches de PSU de enero de 2023

Parches de PSU y RU de bases de datos

- Parche 34765931
- Parche 34786990

Parches adicionales necesarios

- Parche 35099667
- Parche 35099674
- Parche 28730253
- Parche 29213893
- Parche 35012866

Parches de PSU de abril de 2023

Parches de PSU y RU de bases de datos

- Parche 35042068
- Parche 35050341

Parches adicionales necesarios

- Parche 28730253
- Parche 29213893
- Parche 33125873
- Parche 35220732
- Parche 35239280

Configuración de buckets de Amazon S3

1. Cree un bucket de Amazon S3 en la Cuenta de AWS o elija un bucket existente.
2. Cree una estructura de carpetas en el bucket similar al ejemplo siguiente.

```
<bucket-name>/
### oracle_cev/
    ### V982063-01.zip
    ### p6880880_190000_Linux-x86-64.zip
    ### p34765931_190000_Linux-x86-64.zip
    ### p34786990_190000_Linux-x86-64.zip
    ### p35099667_190000_Linux-x86-64.zip
    ### p35099674_190000_Generic.zip
    ### p28730253_190000_Linux-x86-64.zip
    ### p29213893_1918000DBRU_Generic.zip
    ### p35012866_1918000DBRU_Linux-x86-64.zip
```

```
### p35042068_190000_Linux-x86-64.zip
### p35050341_190000_Linux-x86-64.zip
### p29213893_1919000DBRU_Generic.zip
### p33125873_1919000DBRU_Linux-x86-64.zip
### p35220732_190000_Linux-x86-64.zip
### p35239280_190000_Generic.zip
```

3. Cargue todos los archivos de Oracle que descargó anteriormente en las carpetas correspondientes.

Implementación de RDS Custom para Oracle con AWS CloudFormation

Paso 1: preparar la plantilla de AWS CloudFormation

Antes de poder implementar RDS Custom para Oracle, debe descargar y configurar la plantilla de AWS CloudFormation que crea los requisitos previos necesarios.

Copie y guarde la plantilla

1. Vaya a Implementación de RDS Custom para Oracle con una o varias zonas de disponibilidad
2. Copie la plantilla en el formato que prefiera (YAML o JSON)
3. Guarde el archivo en formato YAML o JSON. Por ejemplo, `rds-custom-oracle-prereqs.yaml`

Lance la pila en la consola de AWS

1. Abra la consola de AWS y vaya a AWS CloudFormation
2. Elija Crear pila > Con nuevos recursos (estándar)
3. Seleccione Elegir una plantilla existente
4. Seleccione Cargar un archivo de plantilla > Elegir archivo
5. Seleccione el archivo de plantilla que descargó anteriormente
6. Mantenga los valores de los parámetros predeterminados
7. Seleccione Siguiente para crear la pila

Alternativa: uso de la CLI de AWS

En lugar de utilizar la consola, puede crear la pila con la AWS CLI:

```
aws cloudformation create-stack \
  --stack-name rds-custom-oracle \
  --template-body file://rds-custom-oracle-prereqs.yaml \
  --capabilities CAPABILITY_NAMED_IAM
```

Paso 2: crear las versiones personalizadas del motor (CEV) y las instancias de Amazon RDS

Copie y guarde la plantilla

1. Vaya a Implementación de RDS Custom para Oracle con una o varias zonas de disponibilidad
2. Copie la plantilla en el formato que prefiera (YAML o JSON)
3. Actualice los siguientes parámetros en la plantilla si es necesario:
   - `BucketName`
   - `CEVS3Prefix`
   - Contraseña maestra de la base de datos (sustituya **********)
4. Guarde el archivo en formato YAML o JSON

Paso 3: implementar mediante la consola de AWS

1. Abra la consola de AWS y vaya a AWS CloudFormation
2. Elija Crear pila > Con nuevos recursos (estándar)
3. Seleccione Elegir una plantilla existente
4. Seleccione Cargar un archivo de plantilla > Elegir archivo
5. Seleccione el archivo de plantilla que descargó anteriormente
6. Dejar los parámetros como valores predeterminados
7. Complete los parámetros de la siguiente manera:

   ```
   BucketName: rds-custom-id
   CEVS3Prefix: oracle_cev
   CEVCreation: Yes
   ```

8. Revise la configuración y seleccione Siguiente para crear la pila

Opcional: implementar mediante AWS CLI

```
aws cloudformation create-stack \
```

```
  --stack-name rds-custom-oracle \
  --template-body file://rds-custom-oracle.yaml \
  --parameters \
    ParameterKey=BucketName,ParameterValue=rds-custom-id \
    ParameterKey=CEVS3Prefix,ParameterValue=oracle_cev \
    ParameterKey=CEVCreation,ParameterValue=Yes \
  --capabilities CAPABILITY_NAMED_IAM
```

Se han creado recursos de implementación

La plantilla de crea los siguientes recursos:

- Amazon VPC con subredes públicas y privadas
- Grupos de seguridad
- Puntos de conexión de VPC de Amazon
- Roles y políticas de IAM
- Clave de AWS KMS para el cifrado
- Versiones del motor personalizadas (CEV)
- Instancias de RDS Custom para Oracle en configuraciones de single-AZ y multi-AZ

Supervise el progreso de la implementación

Tras crear la pila de AWS CloudFormation, supervise su progreso para garantizar que la implementación se realice correctamente. El proceso de implementación incluye la creación de versiones de motor personalizadas (CEV) e instancias de RDS.

Para supervisar el progreso de la implementación:

1. Abra la consola de AWS CloudFormation.
2. Elija el nombre de la pila.
3. Elija la pestaña Eventos para ver el progreso e identificar los errores.

> **Note**
>
> La creación de una CEV suele tardar entre 2 y 3 horas. Cuando la creación de la CEV se completa correctamente, Amazon RDS empieza automáticamente a crear la instancia de Amazon RDS.

Posterior a la implementación

Una vez finalizado el proceso de creación de la pila, lleve a cabo los siguientes pasos de verificación y configuración posteriores a la implementación:

1. En la página de la consola de Amazon RDS, vaya a Versiones del motor personalizadas para verificar la creación de la CEV.
2. Confirme que las instancias de Amazon RDS se hayan creado y estén disponibles
3. Pruebe la conectividad a las instancias de Amazon RDS
4. Configure las estrategias de supervisión y respaldo según sea necesario

Limpieza

Para eliminar todos los recursos, ejecute el siguiente comando de la AWS CLI:

```
aws cloudformation delete-stack --stack-name rds-custom-oracle
```

Solución de problemas

Si encuentra problemas durante la implementación, utilice las siguientes soluciones para resolver los problemas comunes.

Error en la creación de CEV

- Compruebe que todos los parches necesarios se hayan cargado en Amazon S3
- Compruebe los permisos de IAM
- Compruebe que las versiones de los parches son correctas; consulte los the section called “Requisitos previos” para obtener la lista de parches necesarios.

Se produce un error al crear la instancia de Amazon RDS

- Compruebe las configuraciones de VPC/subred
- Verifique las reglas del grupo de seguridad
- Confirme que CEV esté disponible

Trabajar con réplicas de Oracle para RDS Custom para Oracle

Puede crear réplicas de Oracle para instancias de base de datos de RDS Custom para Oracle que ejecuten Oracle Enterprise Edition. Se admiten bases de datos de contenedores (CDB) y no CDB. Standard Edition 2 no es compatible con Oracle Data Guard.

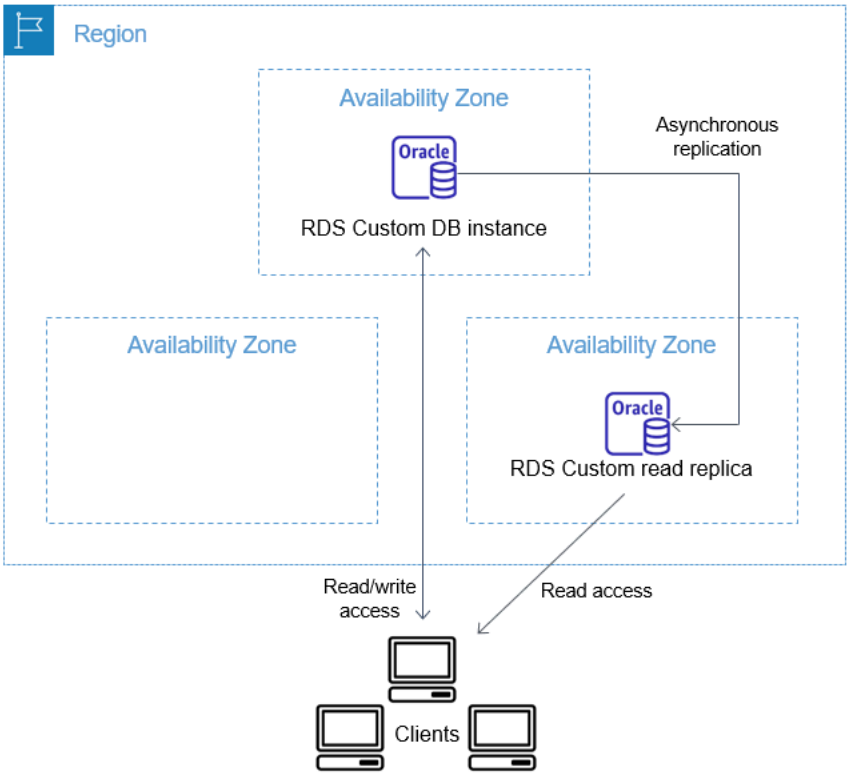
La creación de una réplica de RDS Custom para Oracle es similar a la creación de una réplica de RDS para Oracle, pero con importantes diferencias. Para obtener información general acerca de la creación y administración de réplicas de Oracle, consulte Trabajo con réplicas de lectura de instancias de base de datos y Trabajo con las réplicas de lectura para Amazon RDS para Oracle.

Temas

- Descripción general de la replicación de RDS Custom para Oracle
- Directrices y limitaciones de la replicación de RDS Custom para Oracle
- Promoción de una réplica de RDS Custom para Oracle a una instancia de base de datos independiente
- Configuración de un túnel de VPN entre RDS Custom para instancias principales y réplicas de Oracle

Descripción general de la replicación de RDS Custom para Oracle

La arquitectura de la replicación de RDS Custom para Oracle es análoga a la de RDS para Oracle. Una instancia de base de datos principal se replica de forma asíncrona en una o más réplicas de Oracle.



Número máximo de réplicas

Al igual que con RDS para Oracle, puede crear hasta cinco réplicas de Oracle administradas de la instancia de base de datos primaria de RDS Custom para Oracle. También puede crear sus propias réplicas de Oracle configuradas manualmente (externas). Las réplicas externas no se tienen en cuenta en el límite de instancias de bases de datos. También se encuentran fuera del perímetro de soporte de RDS Custom. Para obtener más información acerca del perímetro de soporte, consulte Perímetro de soporte de RDS Custom.

Convención de nomenclatura de las réplicas

Los nombres de réplica de Oracle se basan en el nombre único de la base de datos El formato es *DB_UNIQUE_NAME_X*, y las letras se adjuntan de forma secuencial. Por ejemplo, si el nombre único de la base de datos es `ORCL`, las dos primeras réplicas se denominan`ORCL_A` y `ORCL_B`. Las seis primeras letras, de la A a la F, están reservadas para RDS Custom. RDS Custom copia los parámetros de la base de datos de la instancia de base de datos principal a las réplicas. Para obtener más información, consulte DB_UNIQUE_NAME en la documentación de Oracle.

Retención de copias de seguridad de las réplicas

De manera predeterminada, las réplicas de Oracle de RDS Custom utilizan el mismo periodo de retención de copias de seguridad que su instancia de base de datos principal. Puede modificar

el periodo de retención de copia de seguridad a 1-35 días. RDS Custom admite la realización de copias de seguridad, restauraciones y recuperaciones en un momento dado (PITR). Para obtener más información sobre la copia de seguridad y la restauración de instancias de base de datos de RDS Custom, consulte Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS Custom for Oracle.

> **Note**
>
> Durante la creación de una réplica de Oracle, RDS Custom pausa temporalmente la limpieza de los archivos de registo REDO. De esta manera, RDS Custom garantiza que puede aplicar estos registros a la nueva réplica de Oracle una vez que esté disponible.

Promoción de las réplicas

Puede promocionar réplicas de Oracle administradas en RDS Custom para Oracle mediante la consola, el comando `promote-read-replica` de la AWS CLI o la API `PromoteReadReplica`. Si elimina la instancia de base de datos primaria y todas las réplicas están en buen estado, RDS Custom para Oracle promociona sus réplicas administradas a instancias independientes automáticamente. Si una réplica ha pausado la automatización o está fuera del perímetro de soporte, debe corregir la réplica para que RDS Custom pueda promocionarla automáticamente. Solo puede promocionar réplicas externas de Oracle manualmente.

Directrices y limitaciones de la replicación de RDS Custom para Oracle

Cuando se crean réplicas de RDS Custom para Oracle, no se admiten todas las opciones de réplica de RDS Oracle.

Temas

- Directrices generales de la replicación de RDS Custom para Oracle
- Limitaciones generales de la replicación de RDS Custom para Oracle
- Requisitos y limitaciones de red de la replicación de RDS Custom para Oracle
- Limitaciones de las réplicas externas para RDS Custom para Oracle

Directrices generales de la replicación de RDS Custom para Oracle

Cuando trabaje con RDS Custom para Oracle, siga estas directrices:

- Puede utilizar la replicación de RDS Custom para Oracle solo en Oracle Enterprise Edition. Standard Edition 2 no es compatible.
- Le recomendamos encarecidamente que implemente un túnel de VPN para cifrar la comunicación entre las instancias principal y en espera. Para obtener más información, consulte Configuración de un túnel de VPN entre RDS Custom para instancias principales y réplicas de Oracle.
- No modifique el usuario `RDS_DATAGUARD`. Este usuario está reservado para la automatización de RDS Custom para Oracle. La modificación de este usuario puede generar resultados no deseados, como la incapacidad de crear réplicas de Oracle para la instancia de base de datos de RDS Custom para Oracle.
- No cambie la contraseña del usuario de replicación. Es necesaria para administrar la configuración de Oracle Data Guard en el host de RDS Custom. Si cambia la contraseña, RDS Custom para Oracle podría situar la réplica de Oracle fuera del perímetro de soporte. Para obtener más información, consulte Perímetro de soporte de RDS Custom.

  La contraseña se almacena en AWS Secrets Manager y se etiqueta con el ID de recurso de base de datos. Cada réplica de Oracle tiene su propio secreto en Secrets Manager. El secreto utiliza uno de los siguientes formatos de nomenclatura.

  ```
  do-not-delete-rds-custom-db-DB_resource_id-uuid-dg
  rds-custom!oracle-do-not-delete-DB_resource_id-uuid-dg
  ```

- No cambie el `DB_UNIQUE_NAME` de la instancia de base de datos principal. Cambiar el nombre provoca que se bloquee cualquier operación de restauración.
- No especifique la cláusula `STANDBYS=NONE` en un comando `CREATE PLUGGABLE DATABASE` de una CDB de RDS Custom. De esta forma, si se produce una conmutación por error, su CDB en espera contiene todas las PDB.

Limitaciones generales de la replicación de RDS Custom para Oracle

Las réplicas de RDS Custom para Oracle tienen las siguientes limitaciones:

- No puede crear réplicas de RDS Custom para Oracle en el modo de solo lectura. Sin embargo, puede cambiar manualmente el modo de las réplicas montadas a solo lectura y viceversa. Para obtener más información, consulte la documentación del comando de la AWS CLI create-db-instance-read-replica.
- No puede crear réplicas de RDS Custom para Oracle entre regiones.

- No puede cambiar el valor del parámetro `CommunicationTimeout` de Oracle Data Guard. Este parámetro se establece en 15 segundos para las instancias de base de datos de RDS Custom para Oracle.

Requisitos y limitaciones de red de la replicación de RDS Custom para Oracle

Asegúrese de que la configuración de red sea compatible con réplicas de RDS Custom para Oracle. Considere lo siguiente:

- Asegúrese de habilitar el puerto 1140 para la comunicación entrante y saliente dentro de nube privada virtual (VPC) para la instancia de base de datos principal y todas sus réplicas. Esto es necesario para la comunicación de Oracle Data Guard entre las réplicas de lectura.
- RDS Custom para Oracle valida la red mientras crea una réplica de Oracle. Si la instancia de base de datos principal y la nueva réplica no pueden conectarse a través de la red, RDS Custom para Oracle no crea la réplica y la coloca en el estado `INCOMPATIBLE_NETWORK`.
- Para réplicas de Oracle externas, como las que crea en Amazon EC2 o en las instalaciones, utilice otro puerto y agente de escucha para la replicación de Oracle Data Guard. Intentar utilizar el puerto 1140 podría provocar conflictos con la automatización de RDS Custom.
- El archivo `/rdsdbdata/config/tnsnames.ora` contiene nombres de servicios de red asignados a direcciones de protocolo de agentes de escucha. Tenga en cuenta los siguientes requisitos y recomendaciones:
  - Las entradas de `tnsnames.ora` con el prefijo `rds_custom_` están reservadas para RDS Custom cuando se manejan operaciones de réplica de Oracle.

    Al crear entradas manuales en `tnsnames.ora`, no use este prefijo.
  - En algunos casos, es posible que desee cambiar o realizar una conmutación por error manualmente, o utilizar tecnologías de conmutación por error, como Fast-Start Failover (FSFO). Si es así, asegúrese de sincronizar manualmente las entradas `tnsnames.ora` de la instancia de base de datos principal a todas las instancias de reserva. Esta recomendación se aplica tanto a las réplicas de Oracle administradas por RDS Custom como a réplicas de Oracle externas.

    La automatización de RDS Custom actualiza las entradas de `tnsnames.ora` solo en la instancia de base de datos principal. Asegúrese de sincronizar también cuando añada o elimine una réplica de Oracle.

Si no sincroniza los archivos `tnsnames.ora` y cambia o conmuta por error manualmente, es posible que Oracle Data Guard en la instancia de base de datos principal no pueda comunicarse con las réplicas de Oracle.

Limitaciones de las réplicas externas para RDS Custom para Oracle

Las réplicas externas de RDS Custom para Oracle, que incluyen réplicas locales, tienen las siguientes limitaciones:

- RDS Custom para Oracle no detecta cambios de rol de instancia tras la conmutación por error manual, como FSFO, para réplicas de Oracle externas.

  RDS Custom para Oracle sí detecta cambios para las réplicas administradas. El cambio de rol se anota en el registro de eventos. También puede ver el nuevo estado mediante el comando de la AWS CLI describe-db-instances.
- RDS Custom para Oracle no detecta un retardo en la replicación elevado para las réplicas de Oracle externas.

  RDS Custom para Oracle sí detecta un retardo para las réplicas administradas. El alto retraso de replicación produce el evento `Replication has stopped`. También puede ver el estado de replicación mediante el comando AWS CLI describe-db-instances, pero podría haber un retraso para que se actualice.
- RDS Custom para Oracle no promueve réplicas externas de Oracle automáticamente si elimina la instancia de base de datos principal.

  La característica de promoción automática solo está disponible para réplicas de Oracle administradas. Para obtener información sobre cómo promocionar réplicas de Oracle manualmente, consulte el documento técnico Enabling high availability with Data Guard on Amazon RDS Custom for Oracle (Habilitación de alta disponibilidad con Data Guard en Amazon RDS Custom para Oracle).

Promoción de una réplica de RDS Custom para Oracle a una instancia de base de datos independiente

Al igual que con RDS para Oracle, puede promover una réplica de RDS Custom para Oracle a una instancia de base de datos independiente. Cuando se promociona una réplica de Oracle, RDS Custom para Oracle reinicia la instancia de base de datos antes de que esté disponible. Para obtener

más información acerca de la promoción de réplicas de Oracle, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Cuando promocione una réplica, tenga en cuenta las siguientes directrices:

- No inicie una conmutación por error mientras RDS Custom para Oracle promociona su réplica. De lo contrario, el flujo de trabajo de la promoción podría estancarse
- No cambie la instancia de base de datos principal mientras RDS Custom para Oracle promociona su réplica de Oracle. De lo contrario, el flujo de trabajo de la promoción podría estancarse
- No cierre la instancia de base de datos principal mientras RDS Custom para Oracle promociona su réplica de Oracle. De lo contrario, el flujo de trabajo de la promoción podría estancarse
- No intente reiniciar la replicación con la instancia de base de datos recién promocionada como destino. Después de que RDS Custom para Oracle promocione su réplica de Oracle, esta se convierte en una instancia de base de datos independiente y deja de tener el rol de réplica.

Tenga en cuenta las siguientes limitaciones para las promociones de réplicas de RDS Custom for Oracle:

- No puede promocionar una réplica mientras RDS Custom para Oracle esté realizando una copia de seguridad.
- No puede cambiar el período de retención de copia de seguridad a `0` cuando promociona su réplica de Oracle.
- No puede promocionar la réplica si esta no está en buen estado.

  Si emite `delete-db-instance` en la instancia de base de datos principal, RDS Custom para Oracle valida que cada réplica de Oracle administrada esté en buen estado y disponible para su promoción. Es posible que una réplica no sea apta para la promoción porque la automatización está en pausa o está fuera del perímetro de soporte. En tales casos, RDS Custom para Oracle publica un evento en el que se explica el problema para que pueda reparar la réplica de Oracle manualmente.

Los siguientes pasos muestran el proceso general para promocionar una réplica de Oracle a instancia de base de datos:

1. Detenga la escritura de transacciones en la instancia de base de datos principal.
2. Espere a que RDS Custom para Oracle aplique todas las actualizaciones a la réplica de Oracle.

3. Para promover la réplica de Oracle, utilice la opción Promote (Promover) de la consola de Amazon RDS, el comando `promote-read-replica` de la AWS CLI o la operación `PromoteReadReplica` de la API de Amazon RDS.

La promoción de una réplica de Oracle tarda unos minutos en completarse. Durante el proceso, RDS Custom para Oracle detiene la replicación y reinicia la réplica. Cuando se completa el reinicio, la réplica de Oracle está disponible como una instancia de base de datos independiente. Para obtener más información sobre la promoción de réplicas de resolución de problemas, consulte Solución de problemas de la promoción de réplicas para RDS Custom para Oracle.

Consola

Para promover una réplica de RDS Custom para Oracle a una instancia de base de datos independiente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos).

   Aparece el panel Databases (Bases de datos). Cada réplica de Oracle muestra Replica (Réplica) en la columna Role (Rol).
3. Elija la réplica de RDS Custom para Oracle que desea promocionar.
4. En Actions (Acciones), seleccione Promote (Promover).
5. En la página Promote Oracle Replica (Promocionar réplica de Oracle), escriba el periodo de retención de copia de seguridad y el periodo de copia de seguridad para la instancia de base de datos recientemente promocionada. No puede establecer este valor en 0.
6. Cuando la configuración sea la deseada, elija Promote Oracle replica (Promocionar réplica de Oracle).

AWS CLI

Para promover una réplica de RDS Custom para Oracle a una instancia de base de datos independiente, use el comando `promote-read-replica` de la AWS CLI.

Example

Para Linux, macOS o Unix:

```
aws rds promote-read-replica \
--db-instance-identifier my-custom-read-replica \
--backup-retention-period 2 \
--preferred-backup-window 23:00-24:00
```

Para Windows:

```
aws rds promote-read-replica ^
--db-instance-identifier my-custom-read-replica ^
--backup-retention-period 2 ^
--preferred-backup-window 23:00-24:00
```

API de RDS

Para promover una réplica de RDS Custom para Oracle a una instancia de base de datos independiente, llame a la operación `PromoteReadReplica` de la API de Amazon RDS con el parámetro `DBInstanceIdentifier` requerido.

Configuración de un túnel de VPN entre RDS Custom para instancias principales y réplicas de Oracle

Un túnel de VPN es una conexión cifrada entre dos o más dispositivos a través de una red. Para garantizar el máximo nivel de seguridad para sus instancias de Oracle Data Guard en RDS Custom for Oracle, le recomendamos encarecidamente que implemente un túnel de VPN para cifrar la comunicación entre las instancias principales y en espera. El túnel protege los datos confidenciales cuando viajan de una instancia a otra por la red. Si bien esta configuración es opcional, aconsejamos su uso como práctica recomendada para garantizar la seguridad de los datos y el cumplimiento de las normas.

Asegúrese de cumplir los siguientes requisitos previos:

- Tiene acceso raíz a los hosts principal y en espera.
- Tiene los conocimientos técnicos necesarios para ejecutar el comando `ipsec`.

Para configurar un túnel de VPN entre un servidor principal y una réplica en RDS Custom para Oracle

1. Agregue los grupos de seguridad de la instancia principal y de la instancia en espera a la lista de permitidos mediante las siguientes reglas:

```
ACTION FLOW SOURCE PROTO PORT

ALLOW ingress this-SG 50 (ESP) all (N/A)
ALLOW egress this-SG 50 (ESP) all (N/A)

ALLOW ingress this-SG 17 (UDP) 500 (IKE)
ALLOW egress this-SG 17 (UDP) 500 (IKE)
```

2. Cambie al usuario raíz.

```
$ sudo su - root
```

3. Ejecute los siguientes comandos tanto en la instancia principal como en la instancia en espera para inicializar la base de datos de los Servicios de Seguridad de Red (NSS) bajo el usuario `root`.

```
ipsec initnss --nssdir /etc/ipsec.d
```

4. Genere las claves RSA de la siguiente manera:

   a. En la instancia principal, genere las claves mediante uno de los siguientes comandos `ipsec`, según la versión del sistema operativo.

   ```
   ipsec newhostkey --nssdir /etc/ipsec.d       ## for Oracle Linux Version 8
   ipsec newhostkey --output /etc/ipsec.secrets ## for Oracle Linux version 7.9
   ```

   b. Obtenga la clave pública, necesaria para crear la configuración. En el siguiente ejemplo, la instancia principal es `left` porque, en términos generales de `ipsec`, `left` se refiere al dispositivo que está configurando actualmente y `right` se refiere al dispositivo que se encuentra en el otro extremo del túnel.

   ```
   ipsec showhostkey --left --ckaid ckaid-returned-in-last-statement
   ```

   c. En la instancia en espera, genere claves para la instancia en espera.

   ```
   ipsec newhostkey --nssdir /etc/ipsec.d       ## for Oracle Linux Version 8
   ipsec newhostkey --output /etc/ipsec.secrets ## for Oracle Linux version 7.9
   ```

d. Obtenga la clave pública de la instancia en espera, necesaria para crear la configuración. En el ejemplo siguiente, la instancia en espera es`right`, ya que hace referencia al dispositivo situado en el otro extremo del túnel.

```
ipsec showhostkey --right --ckaid ckaid-returned-in-last-statement
```

5. En función de las claves RSA que haya obtenido, genere la configuración. La configuración es idéntica tanto para la instancia principal como para la instancia en espera. Puede encontrar la dirección IPv4 de la instancia principal y la dirección IPv4 de la instancia en espera en la consola de AWS.

   Tanto en la instancia principal como en la instancia en espera, guarde la siguiente configuración en el archivo `/etc/ipsec.d/custom-fb-tunnel.conf`.

```
conn custom-db-tunnel
 type=transport
 auto=add
 authby=rsasig
 left=IPV4-for-primary
 leftrsasigkey=RSA-key-generated-on-primary
 right=IPV4-for-standby
 rightrsasigkey=RSA-key-generated-on-standby
```

6. Tanto en la instancia principal como en la instancia en espera, inicie el daemon `ipsec` en ambos hosts.

```
ipsec setup start
```

7. Inicie el túnel en la instancia principal o en la instancia en espera. El resultado de debería parecerse al siguiente.

```
[root@ip-172-31-6-81 ~]# ipsec auto --up custom-db-tunnel
181 "custom-db-tunnel" #1: initiating IKEv2 connection
181 "custom-db-tunnel" #1: sent IKE_SA_INIT request to 172.31.32.196:500
182 "custom-db-tunnel" #1: sent IKE_AUTH request {cipher=AES_GCM_16_256 integ=n/a
 prf=HMAC_SHA2_512 group=DH19}
003 "custom-db-tunnel" #1: initiator established IKE SA; authenticated peer '3584-
bit PKCS#1 1.5 RSA with SHA1' signature using preloaded certificate '172.31.32.196'
004 "custom-db-tunnel" #2: initiator established Child SA using #1; IPsec transport
 [172.31.6.81-172.31.6.81:0-65535 0] -> [172.31.32.196-172.31.32.196:0-65535 0]
 {ESP/ESN=>0xda9c4815 <0xb742ca42 xfrm=AES_GCM_16_256-NONE DPD=passive}
```

```
[root@ip-172-31-6-81 ~]#
```

Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS Custom for Oracle

Al igual que Amazon RDS, RDS Custom crea y guarda copias de seguridad automáticas de la instancia de base de datos de RDS Custom for Oracle durante el periodo de copia de seguridad de su instancia de base de datos. También puede realizar una copia de seguridad de su instancia de base de datos manualmente.

El procedimiento es idéntico a tomar una instantánea de una instancia de base de datos de Amazon RDS. La primera instantánea de una instancia de base de datos de RDS Custom contiene los datos de la instancia de base de datos completa. Las Instantáneas posteriores son progresivas.

Restaure instantáneas de base de datos mediante el AWS Management Console o el AWS CLI.

Temas

- Creación de una instantánea de RDS Custom for Oracle
- Restauración desde una instantánea de base de datos de RDS Custom for Oracle
- Restauración de una instancia de RDS Custom for Oracle a un momento dado
- Eliminación de una instantánea de RDS Custom for Oracle
- Eliminación de copias de seguridad automatizadas de RDS Custom for Oracle

Creación de una instantánea de RDS Custom for Oracle

RDS Custom for Oracle crea una instantánea del volumen de almacenamiento de la instancia de base de datos, al crear una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. Cuando la instancia de base de datos contiene una base de datos de contenedores (CDB, por sus siglas en inglés), la instantánea de la instancia incluye la CDB raíz y todas las PDB.

Cuando cree una instantánea de RDS Custom for Oracle, especifique qué instancia de base de datos personalizada de RDS desea respaldar. Asigne un nombre a la instantánea para poder restaurar desde esta más adelante.

Cuando crea una instantánea, RDS Custom for Oracle crea una instantánea de Amazon EBS para cada volumen adjunto a la instancia de base de datos. RDS Custom for Oracle utiliza la instantánea de EBS del volumen raíz para registrar una nueva Amazon Machine Image (AMI). Para que las

instantáneas sean fáciles de asociar a una instancia de base de datos específica, se etiquetan con `DBSnapshotIdentifier`, `DbiResourceId` y `VolumeType`.

La creación de una instantánea de base de datos da como resultado una breve suspensión de E/S. Esta suspensión puede durar desde unos segundos hasta unos minutos, según el tamaño y la clase de la instancia de base de datos. El tiempo de creación de instantáneas varía según el tamaño de la base de datos. Debido a que la instantánea incluye todo el volumen de almacenamiento, el tamaño de los archivos (como los archivos temporales) también afecta el tiempo de creación de la instantánea. Para obtener más información acerca de la creación de segmentos, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Crear una instantánea de RDS Custom for Oracle mediante la consola o la AWS CLI.

Consola

Para crear una instantánea de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. En la lista de instancias de base de datos de RDS Custom, seleccione la instancia para la que desea tomar una instantánea.
4. En Actions (Acciones), elija Take snapshot (Realizar instantánea).

   Aparece la ventana Take DB Snapshot (Realizar una instantánea de base de datos).
5. En Snapshot name (Nombre de la instantánea), ingrese el nombre de la instantánea.
6. Elija Take Snapshot (Realizar una instantánea).

AWS CLI

Puede crear una instantánea de una instancia de base de datos de RDS Custom mediante el comando AWS CLI create-db-snapshot.

Especifique las opciones siguientes:

- `--db-instance-identifier` – Identifica la instancia de base de datos de RDS Custom de la que va a realizar una copia de seguridad

- `--db-snapshot-identifier` – Nombra su instantánea de RDS Custom para que pueda restaurarla más tarde

En este ejemplo, crea una instantánea de base de datos llamada *`my-custom-snapshot`* para una instancia de base de datos de RDS Custom llamada *`my-custom-instance`*.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-snapshot \
    --db-instance-identifier my-custom-instance \
    --db-snapshot-identifier my-custom-snapshot
```

En:Windows

```
aws rds create-db-snapshot ^
    --db-instance-identifier my-custom-instance ^
    --db-snapshot-identifier my-custom-snapshot
```

Restauración desde una instantánea de base de datos de RDS Custom for Oracle

Al restaurar una instancia de base de datos de RDS Custom for Oracle, debe indicar el nombre de la instantánea de base de datos y un nombre para la nueva instancia. No es posible restaurar desde una instantánea a una instancia de base de datos RDS Custom existente. Al realizar la restauración se crea una nueva instancia de base de datos de RDS Custom for Oracle.

El proceso de restauración difiere de las siguientes formas de restauración en Amazon RDS:

- Antes de restaurar una instantánea, RDS Custom for Oracle realiza una copia de seguridad de los archivos de configuración existentes. Estos archivos están disponibles en la instancia restaurada del directorio `/rdsdbdata/config/backup`. RDS Custom for Oracle restaura la instantánea de base de datos con parámetros predeterminados y sobrescribe los archivos de configuración de base de datos anteriores con los existentes. Por lo tanto, la instancia restaurada no conserva los parámetros personalizados ni los cambios en los archivos de configuración de la base de datos.
- La base de datos restaurada tiene el mismo nombre que en la instantánea. No puede especificar un nombre diferente. (Para RDS Custom for Oracle, el valor predeterminado es `ORCL`).

Consola

Restaure una instancia de base de datos de RDS Custom a partir de una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de base de datos desde la que desea restaurar.
4. En Actions (Acciones), elija Restore snapshot (Restaurar instantánea).
5. En la página Restore DB instance (Restaurar instancia de base de datos), en DB instance identifier (Identificador de instancias de bases de datos), ingrese el nombre de su instancia de base de datos de RDS Custom restaurada.
6. Elija Restore DB Instance (Restaurar instancia de base de datos).

AWS CLI

Restaure una instantánea de base de datos de RDS Custom mediante el comando AWS CLI restore-db-instance-from-db-snapshot.

Si la instantánea desde la que va a restaurar es para una instancia de base de datos privada, asegúrese de especificar el `db-subnet-group-name` y el `no-publicly-accessible` correctos. De lo contrario, la instancia de base de datos pasa a ser de acceso público de manera predeterminada. Se requieren las siguientes opciones:

- `db-snapshot-identifier` – Identifica la instantánea desde la que se va a restaurar
- `db-instance-identifier` – Especifica el nombre de la instancia de base de datos de RDS Custom que se debe crear a partir de la instantánea de base de datos
- `custom-iam-instance-profile` – Especifica el perfil de instancia asociado a la instancia Amazon EC2 subyacente de una instancia de base de datos personalizada de RDS.

El siguiente código restaura la instantánea denominada `my-custom-snapshot` para `my-custom-instance`.

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-instance-from-db-snapshot \
  --db-snapshot-identifier my-custom-snapshot \
  --db-instance-identifier my-custom-instance \
  --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
  --no-publicly-accessible
```

En:Windows

```
aws rds restore-db-instance-from-db-snapshot ^
  --db-snapshot-identifier my-custom-snapshot ^
  --db-instance-identifier my-custom-instance ^
  --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
  --no-publicly-accessible
```

Restauración de una instancia de RDS Custom for Oracle a un momento dado

Al crear una nueva instancia de base de datos puede restaurar una instancia de base de datos a un momento dado (PITR). Para admitir PITR, las instancias de base de datos deben tener una retención de copia de seguridad establecida en un valor distinto de cero.

El último momento en que se puede restaurar para una instancia de base de datos de RDS Custom for Oracle depende de varios factores, pero normalmente se sitúa en los cinco minutos previos a la hora actual. Para ver el último momento que se puede restaurar para una instancia de base de datos, use el comando describe-db-instances de la AWS CLI y compruebe el valor que se devuelve en el campo `LatestRestorableTime` para la instancia de base de datos. Para consultar la hora restaurable más reciente para cada instancia de base de datos en la consola de Amazon RDS, elija Copias de seguridad automatizadas.

Puede restaurar a cualquier punto en el tiempo dentro del periodo de retención de copia de seguridad. Para consultar la hora restaurable más reciente para cada instancia de base de datos, elija Copias de seguridad automatizadas en la consola de Amazon RDS.

Para obtener información general sobre PITR, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Temas

- Consideraciones de PITR para RDS Custom for Oracle

Consideraciones de PITR para RDS Custom for Oracle

En RDS Custom for Oracle, PITR difiere de las siguientes formas importantes de PITR en Amazon RDS:

- La base de datos restaurada tiene el mismo nombre que en la instancia de base de datos de origen. No puede especificar un nombre diferente. El valor predeterminado es `ORCL`.
- `AWSRDSCustomIamRolePolicy` requiere nuevos permisos. Para obtener más información, consulte Paso 2: añadir una política de acceso a AWSRDSCustomInstanceRoleForRdsCustomInstance.
- Todas las instancias de base de datos de RDS Custom for Oracle deben tener la retención de la copia de seguridad establecida en un valor distinto a cero.
- Si cambia el sistema operativo o la zona horaria de la instancia de base de datos, es posible que PITR no funcione. Consulte Zona horaria Oracle para obtener información acerca de cómo cambiar las zonas horarias.
- Si configura la automatización en `ALL_PAUSED`, RDS Custom detiene la carga de registros de recuperación de cambios archivados, incluidos los registros creados antes de la última hora restaurable (LRT). Le recomendamos que ponga en pausa la automatización durante un breve periodo de tiempo.

  Para ilustrarlo, suponga que su LRT es de hace 10 minutos. Pause la automatización. Durante la pausa, RDS Custom no carga los registros de recuperación de cambios archivados. Si la instancia de base de datos se bloquea, solo puede recuperarse hasta un momento anterior al LRT que existía al hacer una pausa. Cuando reanuda la automatización, RDS Custom reanuda la carga de registros. El LRT avanza. Se aplican las reglas normales de PITR.
- En RDS Custom, puede especificar manualmente un número arbitrario de horas para retener los registros de recuperación de cambios archivados antes de que RDS Custom los elimine después de la carga. Especifique el número de horas de la siguiente manera:
  1. Cree un archivo de texto denominado `/opt/aws/rdscustomagent/config/redo_logs_custom_configuration.json`.
  2. Añada un objeto JSON con el siguiente formato: `{"archivedLogRetentionHours" : "num_of_hours"}`. El número debe ser un número entero entre 1 y 840.
- Supongamos que conecta una base de datos que no es CDB a una base de datos de contenedores (CDB) como PDB y, a continuación, intenta la PITR. La operación solo se realiza correctamente si ha realizado previamente una copia de seguridad de la PDB. Después de crear o modificar una PDB, le recomendamos que siempre haga una copia de seguridad de la misma.

- Le recomendamos que no personalice los parámetros de inicialización de la base de datos. Por ejemplo, la modificación de los siguientes parámetros afecta a PITR:
  - `CONTROL_FILE_RECORD_KEEP_TIME` afecta a las reglas de carga y eliminación de registros.
  - `LOG_ARCHIVE_DEST_`*n* no admite varios destinos.
  - `ARCHIVE_LAG_TARGET` afecta a la última hora restaurable. `ARCHIVE_LAG_TARGET` está establecido en `300` porque el objetivo de punto de recuperación (RPO) es de 5 minutos. Para cumplir este objetivo, RDS cambia el registro red en línea cada 5 minutos y lo almacena en un bucket de Amazon S3. Si la frecuencia del cambio de registro provoca un problema de rendimiento en la base de datos de RDS Custom para Oracle, puede escalar la instancia de base de datos y el almacenamiento a una con un rendimiento y un IOPS más altos. Si es necesario para su plan de recuperación, puede ajustar la configuración del parámetro de inicialización `ARCHIVE_LAG_TARGET` a un valor comprendido entre 60 y 7200.
- Si personaliza los parámetros de inicialización de la base de datos, le recomendamos que personalice solo lo siguiente:
  - `COMPATIBLE`
  - `MAX_STRING_SIZE`
  - `DB_FILES`
  - `UNDO_TABLESPACE`
  - `ENABLE_PLUGGABLE_DATABASE`
  - `CONTROL_FILES`
  - `AUDIT_TRAIL`
  - `AUDIT_TRAIL_DEST`

  Para los demás parámetros de inicialización, RDS Custom restaura los valores predeterminados. Si modifica un parámetro que no figura en la lista anterior, podría tener un efecto adverso en el PITR y generar resultados impredecibles. Por ejemplo, `CONTROL_FILE_RECORD_KEEP_TIME` afecta a las reglas para cargar y eliminar registros.

Puede restaurar una instancia de base de datos de RDS Custom a un momento dado mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para restaurar una instancia de base de datos de RDS Custom a un tiempo especificado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Copias de seguridad automáticas.
3. Elija la instancia de base de datos personalizada de RDS que desea restaurar.
4. Para Actions (Acciones), elija Restore to point in time (Restaurar a un momento dado).

   Aparecerá la ventana Restore to point in time (Restaurar a un momento dado).
5. Elija Latest restorable time (Última hora de restauración) para restaurar a la última hora posible o elija Custom (Personalizar) para elegir una hora.

   Si elige Personalizar, ingrese la fecha y la hora a la que desea restaurar la instancia.

   Las horas se muestran en su zona horaria local, que se indica mediante una diferencia de la hora universal coordinada (UTC). Por ejemplo, UTC-5 es la hora estándar del Este/horario de verano central.
6. Para el identificador de instancias de bases de datos, ingrese el nombre de la instancia de base de datos de RDS Custom restaurada de destino. El nombre debe ser único.
7. Elija otras opciones según sea necesario, como la clase de instancia de base de datos.
8. Elija Restore to point in time (Restaurar a un momento dado).

AWS CLI

Puede restaurar una instancia de base de datos a un momento dado mediante el comando restore-db-instance-to-point-in-time AWS CLI para crear una nueva instancia de base de datos de RDS Custom.

Utilice una de las siguientes opciones para especificar la copia de seguridad desde la que restaurar:

- `--source-db-instance-identifier` *`mysourcedbinstance`*
- `--source-dbi-resource-id` *`dbinstanceresourceID`*
- `--source-db-instance-automated-backups-arn` *`backupARN`*

La opción `custom-iam-instance-profile` es obligatoria.

En el siguiente ejemplo se restaura `my-custom-db-instance` a una nueva instancia de base de datos denominada `my-restored-custom-db-instance`, en la hora especificada.

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-identifier my-custom-db-instance\
    --target-db-instance-identifier my-restored-custom-db-instance \
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
    --restore-time 2022-10-14T23:45:00.000Z
```

En:Windows

```
aws rds restore-db-instance-to-point-in-time ^
    --source-db-instance-identifier my-custom-db-instance ^
    --target-db-instance-identifier my-restored-custom-db-instance ^
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
    --restore-time 2022-10-14T23:45:00.000Z
```

Eliminación de una instantánea de RDS Custom for Oracle

Puede eliminar instantáneas de base de datos administradas por RDS Custom for Oracle cuando ya no las necesite. El procedimiento de eliminación es el mismo para las instancias de base de datos de Amazon RDS y RDS Custom.

Las instantáneas de Amazon EBS de los volúmenes binario y raíz permanecen en su cuenta durante más tiempo porque podrían estar vinculadas a algunas instancias que se ejecutan en su cuenta o a otras instantáneas de RDS Custom for Oracle. Estas instantáneas de EBS se eliminan automáticamente después de que ya no están relacionadas con los recursos de RDS Custom for Oracle existentes (instancias de base de datos o copias de seguridad).

Consola

Para eliminar una instantánea de una instancia de base de datos de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).

3. Elija la instantánea de base de datos que desee eliminar.
4. En Actions (Acciones), elija Delete Snapshot (Eliminar instantánea).
5. En la página de confirmación, elija Delete (Eliminar).

AWS CLI

Para eliminar una instantánea de RDS Custom, utilice el comando AWS CLI delete-db-snapshot.

Se requiere la siguiente opción:

- `--db-snapshot-identifier` – La instantánea que se va a eliminar

El siguiente ejemplo elimina la instantánea de base de datos `my-custom-snapshot`.

Example

Para Linux, macOS o:Unix

```
aws rds delete-db-snapshot \
  --db-snapshot-identifier my-custom-snapshot
```

En:Windows

```
aws rds delete-db-snapshot ^
  --db-snapshot-identifier my-custom-snapshot
```

Eliminación de copias de seguridad automatizadas de RDS Custom for Oracle

Puede eliminar las copias de seguridad automáticas retenidas para RDS Custom for Oracle cuando ya no sean necesarias. El procedimiento es el mismo que el procedimiento para eliminar las copias de seguridad de Amazon RDS.

Consola

Para eliminar una copia de seguridad automatizada retenida

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Automated backups (Copias de seguridad automatizadas).

3. Elija Retained (Retenidas).
4. Elija la copia de seguridad automatizada retenida que desea eliminar.
5. En Actions (Acciones), elija Delete (Eliminar).
6. En la página de confirmación, ingrese **`delete me`** y elija Delete (Eliminar).

AWS CLI

Puede eliminar una copia de seguridad automatizada retenida utilizando el comando de la AWS CLI delete-db-instance-automated-backup.

La siguiente opción se utiliza para eliminar una copia de seguridad automática retenida:

- `--dbi-resource-id` – El identificador de recurso para la instancia de base de datos de RDS Custom de origen.

  Puede encontrar el identificador de recursos para la instancia de base de datos de origen de una copia de seguridad automatizada retenida mediante el comando AWS CLI describe-db-instance-automated-backups.

El siguiente ejemplo elimina la copia de seguridad automatizada retenida con el identificador de recursos de la instancia de base de datos `custom-db-123ABCEXAMPLE`.

Example

Para Linux, macOS o:Unix

```
aws rds delete-db-instance-automated-backup \
    --dbi-resource-id custom-db-123ABCEXAMPLE
```

En:Windows

```
aws rds delete-db-instance-automated-backup ^
    --dbi-resource-id custom-db-123ABCEXAMPLE
```

Trabajar con grupos de opciones en RDS Custom para Oracle

RDS Custom utiliza grupos de opciones para habilitar y configurar características adicionales. Un grupo de opciones especifica características, llamadas opciones, que están disponibles para una instancia de RDS Custom para Oracle. Las opciones pueden tener una configuración que especifica el funcionamiento de la opción. Cuando asocia una instancia de base de datos de RDS Custom para Oracle a un grupo de opciones, las opciones especificadas y la configuración de estas se habilitan para dicha instancia. Para obtener información general acerca de los grupos de opciones en Amazon RDS, consulte Trabajo con grupos de opciones.

Temas

- Información general sobre los grupos de opciones en RDS Custom para Oracle
- Zona horaria Oracle

Información general sobre los grupos de opciones en RDS Custom para Oracle

Para habilitar opciones para su base de datos Oracle, puede añadirlas a un grupo de opciones y, a continuación, asociar el grupo de opciones a la instancia de base de datos. Para obtener más información, consulte Trabajo con grupos de opciones.

Temas

- Resumen de las opciones de RDS Custom para Oracle
- Pasos básicos para agregar una opción a una instancia de base de datos de RDS Custom para Oracle
- Creación de un grupo de opciones en RDS Custom para Oracle
- Asociación de un grupo de opciones a una instancia de base de datos de RDS Custom para Oracle

Resumen de las opciones de RDS Custom para Oracle

RDS Custom para Oracle admite las siguientes opciones para una instancia de base de datos.

Opción	ID de la opción	Descripción
Zona horaria Oracle	`Timezone`	La zona horaria que utiliza la instancia de base de datos de RDS Custom para Oracle.

Pasos básicos para agregar una opción a una instancia de base de datos de RDS Custom para Oracle

El proceso general para agregar una opción a su instancia de base de datos de RDS Custom para Oracle es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a su instancia de base de datos al crearlo o modificarlo.

Creación de un grupo de opciones en RDS Custom para Oracle

Puede crear un nuevo grupo de opciones que derive su configuración del grupo de opciones por defecto. Agregue entonces una o más opciones al grupo de opciones. O bien, si ya dispone de un grupo de opciones existente, puede copiarlo con todas sus opciones a un nuevo grupo de opciones. Para aprender cómo copiar un grupo de opciones, consulte Copia de un grupo de opciones.

Los grupos de opciones predeterminados de RDS Custom para Oracle son los siguientes:

- `default:custom-oracle-ee`
- `default:custom-oracle-se2`
- `default:custom-oracle-ee-cdb`
- `default:custom-oracle-se2-cdb`

Al crear un grupo de opciones, la configuración se deriva del grupo de opciones predeterminado. Una vez que haya agregado la opción `TIME_ZONE`, puede asociar el grupo de opciones a la instancia de base de datos.

Consola

Una manera de crear un grupo de opciones es mediante la AWS Management Console.

Para crear un grupo de opciones nuevo mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En la ventana Create option group (Crear grupo de opciones), haga lo siguiente:
   a. En Name, escriba un nombre para el grupo de opciones que sea exclusivo dentro de su cuenta AWS. El nombre solo puede contener letras, dígitos y guiones.
   b. En Description, escriba una breve descripción del grupo de opciones. La descripción se utiliza para fines de visualización.
   c. Para Motor, elija cualquiera de los siguientes motores de base de datos de RDS Custom para Oracle:
      - custom-oracle-ee
      - custom-oracle-se2
      - custom-oracle-ee-cdb
      - custom-oracle-se2-cdb
   d. Para la Versión principal del motor, elija una versión principal del motor compatible con RDS Custom para Oracle. Para obtener más información, consulte Regiones y motores de base de datos admitidos para RDS Custom para Oracle.
5. Para continuar, elija Create (Crear). Para cancelar la operación, elija Cancel.

AWS CLI

Para crear un grupo de opciones, utilice el comando AWS CLI de la `create-option-group` con los siguientes parámetros obligatorios.

- `--option-group-name`
- `--engine-name`
- `--major-engine-version`
- `--option-group-description`

Example

En el siguiente ejemplo, se crea un grupo de opciones llamado `testoptiongroup`, que se asocia con el motor de base de datos Oracle Enterprise Edition. La descripción se proporciona entre comillas.

Para Linux, macOS o:Unix

```
aws rds create-option-group \
    --option-group-name testoptiongroup \
    --engine-name custom-oracle-ee-cdb \
    --major-engine-version 19 \
    --option-group-description "Test option group for a Custom Oracle CDB"
```

En:Windows

```
aws rds create-option-group ^
    --option-group-name testoptiongroup ^
    --engine-name custom-oracle-ee-cdb ^
    --major-engine-version 19 ^
    --option-group-description "Test option group for a Custom Oracle CDB"
```

API de RDS

Para crear un grupo de opciones, llame a la operación `CreateOptionGroup` de la API de Amazon RDS.

Asociación de un grupo de opciones a una instancia de base de datos de RDS Custom para Oracle

Puede asociar su grupo de opciones a una instancia de base de datos nueva o ya existente:

- Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al crear la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de RDS Custom for Oracle.
- Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de la instancia de base de datos de RDS Custom para Oracle.

Zona horaria Oracle

Use la opción de zona horaria para cambiar la zona horaria del sistema empleada por la instancia de base de datos de RDS Custom para Oracle. Por ejemplo, puede cambiar la zona horaria de una instancia de base de datos para que sea compatible con un entorno on-premises o con una aplicación heredada. Esta opción cambia la zona horaria al nivel del host. El cambio de la zona horaria afecta a todas las columnas y valores de fecha, como `SYSDATE` y `SYSTIMESTAMP`.

Temas

- Configuración de la opción de zona horaria en RDS Custom para Oracle
- Zonas horarias disponibles en RDS Custom para Oracle
- Consideraciones para configurar la zona horaria en RDS Custom para Oracle
- Limitaciones para configurar la zona horaria en RDS Custom para Oracle
- Agregar la opción de zona horaria al grupo de opciones
- Eliminación de la opción de zona horaria

Configuración de la opción de zona horaria en RDS Custom para Oracle

Amazon RDS admite los siguientes valores para las opciones de zona horaria.

Ajuste de la opción	Valores válidos	Descripción
`TIME_ZONE`	Una de las zonas horarias disponibles. Puede consultar la lista completa e Zonas horarias disponibles en RDS Custom para Oracle.	Nueva zona horaria para la instancia de base de datos.

Zonas horarias disponibles en RDS Custom para Oracle

Los siguientes son los valores que pueden elegirse para la opción de zona horaria.

Zona	Time zone (Zona horarioa)
África	África/Casablanca, África/El Cairo, África/Harare, África/Lagos, África/Luanda, África/Monrovia, África/Nairobi, África/Trípoli, África/Windhoek

Zona	Time zone (Zona horarioa)
América	América/Araguaína, América/Argentina/Buenos_Aires, América/Asunción, América/Bogotá, América/Caracas, América/Chicago, América/Chihuahua, América/Cuiaba, América/Denver, América/Detroit, América/Fortaleza, América/Godthab, América/Guatemala, América/Halifax, América/Lima, América/Los_Ángeles, América/Manaos, América/Matamoros, América/Ciudad_de_México, América/Monterrey, América/Montevideo, América/Nueva_York, América/Phoenix, América/Santiago, América/São_Paulo, América/Tijuana, América/Toronto
Asia	Asia/Amán, Asia/Asjabad, Asia/Bagdad, Asia/Bakú, Asia/Bangkok, Asia/Beirut, Asia/Calcuta, Asia/Daca, Asia/Damasco, Asia/Ereván, Asia/Hong_Kong, Asia/Irkutsk, Asia/Jerusalén, Asia/Kabul, Asia/Karachi, Asia/Katmandú, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Magadán, Asia/Manila, Asia/Mascate, Asia/Novosibirsk, Asia/Rangún, Asia/Riad, Asia/Seúl, Asia/Shanghái, Asia/Singapur, Asia/Taipéi, Asia/Teherán, Asia/Tokio, Asia/Ulán_Bator, Asia/Vladivostok, Asia/Yakarta, Asia/Yakutsk
Atlántico	Atlántico/Azores, Atlántico/Cabo_Verde
Australia	Australia/Adelaida, Australia/Brisbane, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/Lord_Howe, Australia/Perth, Australia/Sídney
Brasil	Brasil/DeNoronha, Brasil/Este
Canadá	Canadá/Terranova, Canadá/Saskatchewan
etc	Etc/GMT-3
Europa	Europa/Ámsterdam, Europa/Atenas, Europa/Berlín, Europa/Dublín, Europa/Helsinki, Europa/Kaliningrado, Europa/Londres, Europa/Madrid, Europa/Moscú, Europa/París, Europa/Praga, Europa/Roma, Europa/Sarajevo
Pacífico	Pacífico/Apia, Pacífico/Auckland, Pacífico/Chatham, Pacífico/Fiyi, Pacífico/Guam, Pacífico/Honolulu, Pacífico/Kiritimati, Pacífico/Marquesas, Pacífico/Samoa, Pacífico/Tongatapu, Pacífico/Wake

Zona	Time zone (Zona horarioa)
EE. UU.	EE. UU./Alaska, EE. UU./Central, EE. UU./Indiana-Este, EE. UU./Este, EE. UU./Pacífico
UTC	UTC

Consideraciones para configurar la zona horaria en RDS Custom para Oracle

Si decide configurar la zona horaria de su instancia de base de datos, tenga en cuenta lo siguiente:

- Cuando se añade la opción de zona horaria, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente.
- Si configura por accidente la zona horaria de forma incorrecta, debe devolver la instancia de base de datos a su configuración de zona horaria anterior. Por este motivo, le recomendamos que utilice una de las siguientes estrategias antes de añadir la opción de zona horaria a su instancia:
  - Si la instancia de base de datos de RDS Custom para Oracle utiliza el grupo de opciones predeterminado, realice una instantánea de su instancia de base de datos. Para obtener más información, consulte Creación de una instantánea de RDS Custom for Oracle.
  - Si su instancia de base de datos emplea actualmente un grupo de opciones no predeterminado, tome una instantánea de la instancia de base de datos y después cree un nuevo grupo de opciones con la opción de zona horaria.
- Le recomendamos realizar una copia de seguridad de la instancia de base de datos manualmente después de aplicar la opción `Timezone`.
- Recomendamos encarecidamente probar la opción de zona horaria en una instancia de base de datos de prueba antes de agregarla a una instancia de producción. La adición de la opción de zona horaria puede causar problemas en las tablas que utilizan la fecha del sistema para sumar fechas u horas. Le recomendamos que analice sus datos y aplicaciones para evaluar el impacto que puede tener cambiar la zona horaria.

Limitaciones para configurar la zona horaria en RDS Custom para Oracle

Presenta las siguientes limitaciones:

- No puede cambiar la zona horaria directamente en su host sin moverla fuera del perímetro de soporte. Para cambiar la zona horaria de la base de datos, debe crear un grupo de opciones.

- Como la opción de zona horaria es una opción persistente (pero no permanente), no puede hacer lo siguiente:
  - eliminar la opción de un grupo de opciones después de agregarla
  - cambiar el ajuste de zona horaria en la opción por una zona horaria distinta
- No puede asociar varios grupos de opciones a una instancia de base de datos de RDS Custom para Oracle.
- No puede establecer la zona horaria de los PDB individuales dentro de una CDB.

Agregar la opción de zona horaria al grupo de opciones

Los grupos de opciones predeterminados de RDS Custom para Oracle son los siguientes:

- `default:custom-oracle-ee`
- `default:custom-oracle-se2`
- `default:custom-oracle-ee-cdb`
- `default:custom-oracle-se2-cdb`

Al crear un grupo de opciones, la configuración se deriva del grupo de opciones predeterminado. Para obtener información general acerca de los grupos de opciones en Amazon RDS, consulte Trabajo con grupos de opciones.

Consola

Para agregar la opción de zona horaria a un grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que desea modificar y, a continuación, elija Add option (Agregar opción).
4. En la ventana Add option (Añadir opción), haga lo siguiente:
   a. Elija Zona horaria.
   b. En la Configuración de opciones, seleccione una zona horaria.
   c. Para habilitar la opción en todas las instancias de base de datos de RDS Custom para Oracle asociadas en cuanto la agregue, en Aplicar inmediatamente, elija Sí. Si elige No

(valor predeterminado), la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento.

d.

> **Important**
>
> Si añade la opción de zona horaria a un grupo de opciones existente que ya se ha adjuntado a una o varias instancias de bases de datos, se producirá una breve interrupción mientras reinician todas las instancias de bases de datos.

5. Cuando los ajustes sean los deseados, elija Add Option (Agregar opción).
6. Cree una copia de seguridad de las instancias de base de datos de RDS Custom para Oracle cuyas zonas horarias se hayan actualizado. Para obtener más información, consulte Creación de una instantánea de RDS Custom for Oracle.

AWS CLI

En el ejemplo siguiente, se usa el comando add-option-to-option-group de la AWS CLI para añadir la opción `Timezone` y la opción de configuración `TIME_ZONE` a un grupo de opciones denominado `testoptiongroup`. La zona horaria establecida es `America/Los_Angeles`.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name "testoptiongroup" \
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=America/
Los_Angeles}]" \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name "testoptiongroup" ^
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=America/
Los_Angeles}]" ^
    --apply-immediately
```

Eliminación de la opción de zona horaria

La opción de zona horaria es una opción persistente, pero no permanente. Una vez agregada a un grupo de opciones, no es posible retirarla de nuevo. Para desasociar el grupo de opciones anterior de su instancia de base de datos:

1. Cree un nuevo grupo de opciones con una opción de `Timezone` actualizada.
2. Asocie el nuevo grupo de opciones a su instancia de base de datos al modificar la instancia.

Migración de una base de datos en las instalaciones a RDS Custom para Oracle

Antes de migrar una base de datos Oracle en las instalaciones a RDS Custom para Oracle, debe tener en cuenta los siguientes factores:

- La cantidad de tiempo de inactividad que puede permitirse la aplicación
- El tamaño de la base de datos de origen
- La conectividad de red
- Un requisito para un plan alternativo
- La versión de la base de datos Oracle de origen y destino y los tipos de sistema operativos de la instancia de base de datos
- Herramientas de replicación disponibles, como AWS Database Migration Service, Oracle GoldenGate o herramientas de replicación de terceros

En función de estos factores, puede elegir la migración física, la migración lógica o una combinación de las dos. Si elige la migración física, puede utilizar las siguientes técnicas:

Duplicación RMAN

La duplicación activa de bases de datos no requiere una copia de seguridad de la base de datos de origen. Duplica la base de datos de origen activa en el host de destino copiando los archivos de la base de datos a través de la red en la instancia auxiliar. El comando `DUPLICATE` de RMAN copia los archivos necesarios como copias de imágenes o conjuntos de copias de seguridad. Para aprender esta técnica, consulte la entrada del blog de AWS Physical migration of Oracle databases to Amazon RDS Custom using RMAN duplication (Migración física de bases de datos Oracle a Amazon RDS Custom mediante la duplicación RMAN).

Oracle Data Guard

En esta técnica, se realizan copias de seguridad de una base de datos principal en las instalaciones y se copian las copias de seguridad en un bucket de Amazon S3. A continuación, se copian las copias de seguridad en su instancia de base de datos en espera de RDS Custom para Oracle. Tras realizar la configuración necesaria, se cambia manualmente la base de datos principal a la base de datos en espera de RDS Custom para Oracle. Para aprender esta técnica, consulte la entrada del blog de AWS Physical migration of Oracle databases to Amazon RDS

Custom using Data Guard (Migración física de bases de datos Oracle a Amazon RDS Custom mediante Data Guard).

Para obtener información general acerca de la importación lógica de datos a RDS para Oracle, consulte Importación de datos a Oracle en Amazon RDS.

Actualización de una instancia de base de datos para Amazon RDS Custom for Oracle

Puede actualizar una instancia de base de datos personalizada de Amazon RDS Custom al modificarla para utilizar una nueva versión del motor personalizada (CEV). Para obtener información general acerca de las actualizaciones, consulte Actualización de una versión del motor de una instancia de base de datos.

Temas

- Información general sobre las actualizaciones en RDS Custom para Oracle
- Requisitos de las actualizaciones de RDS Custom para Oracle
- Consideraciones de las actualizaciones de base de datos de RDS Custom for Oracle
- Consideraciones de las actualizaciones del sistema operativo de RDS Custom for Oracle
- Visualización de los destinos de actualización de CEV válidos para las instancias de base de datos de RDS Custom para Oracle
- Actualización de una instancia de base de datos de RDS Custom para Oracle
- Visualización de actualizaciones de base de datos pendientes para instancias de base de datos de RDS Custom
- Solución de problemas del error de actualización de una instancia de base de datos de RDS Custom para Oracle

Información general sobre las actualizaciones en RDS Custom para Oracle

Con RDS Custom para Oracle, puede aplicar parches a la base de datos de Oracle o al sistema operativo (SO) de la instancia de base de datos; para ello, cree nuevas CEV y modifique la instancia para que utilice la nueva CEV.

Temas

- Opciones de actualización de CEV
- Aplicación de parches sin CEV
- Pasos generales para parchear la instancia de base de datos con una CEV

Opciones de actualización de CEV

A la hora de crear una CEV para una actualización, tiene las siguientes opciones mutuamente excluyentes:

Solo base de datos

Reutilice la imagen de máquina de Amazon (AMI) que su instancia de base de datos esté usando actualmente, pero especifique diferentes binarios de base de datos. RDS Custom asigna un nuevo volumen binario y lo adjunta a la instancia de Amazon EC2 existente. RDS Custom reemplaza todo el volumen de la base de datos por un nuevo volumen que utiliza la versión de la base de datos de destino.

Solo sistema operativo

Reutilice los binarios de base de datos que utiliza actualmente su instancia de base de datos, pero especifique una AMI distinta. RDS Custom asigna una nueva instancia de Amazon EC2 y adjunta el volumen binario existente a la nueva instancia. Se conserva el volumen de base de datos existente.

Si desea actualizar el sistema operativo y la base de datos, debe actualizar la CEV dos veces. Puede actualizar primero el sistema operativo y, luego, la base de datos o viceversa.

> **Warning**
>
> Al parchear el sistema operativo, se pierden los datos del volumen raíz y cualquier personalización existente del sistema operativo. Por lo tanto, le recomendamos encarecidamente que no utilice el volumen raíz para las instalaciones ni para almacenar datos o archivos permanentes. También le recomendamos que haga una copia de seguridad de los datos antes de la actualización.

Aplicación de parches sin CEV

Le recomendamos encarecidamente que actualice la instancia de base de datos de RDS Custom para Oracle mediante CEV. La automatización de RDS Custom para Oracle sincroniza los metadatos del parche con el binario de base de datos en la instancia de base de datos.

En circunstancias especiales, RDS Custom admite la aplicación de un parche “único” de base de datos directamente en la instancia subyacente de Amazon EC2, mediante la utilidad OPatch. Un

caso de uso válido podría ser cuando desea aplicar de inmediato un parche de base de datos, pero el equipo de RDS Custom está actualizando la característica de CEV, lo que provoca un retraso. Para aplicar un parche de forma manual, siga estos pasos:

1. Pausa la automatización de RDS Custom.
2. Aplique el parche a los binarios de base de datos de la instancia de Amazon EC2.
3. Reanudar la automatización personalizada de RDS.

Una desventaja de la técnica anterior es que debe aplicar el parche de base de datos manualmente a cada instancia que quiera actualizar. Por el contrario, cuando crea una nueva CEV, puede crear o actualizar varias instancias de base de datos con la misma CEV.

Pasos generales para parchear la instancia de base de datos con una CEV

Tanto si aplica parches al SO como a la base de datos, siga estos pasos básicos:

1. Cree una CEV que contenga uno de los siguientes elementos, en función de si va a aplicar parches a la base de datos o al sistema operativo:
   - La actualización de la versión de la base de datos de Oracle que desea aplicar en la instancia de base de datos
   - Una AMI diferente (la última disponible o una que usted especifique) y una CEV existente para usar como fuente

   Siga los pasos de Creación de una CEV.
2. (Opcional para la aplicación de parches en las bases de datos) Compruebe las actualizaciones de versión de motor disponibles ejecutando `describe-db-engine-versions`.
3. Inicie el proceso de aplicación de parches ejecutando `modify-db-instance`.

   El estado de la instancia que se está parcheando varía de la siguiente manera:
   - Mientras RDS aplica parches en la base de datos, el estado de la instancia de base de datos cambia a Actualización.
   - Mientras RDS aplica parches en el SO, el estado de la instancia de base de datos cambia a Modificación.

   Cuando la instancia de base de datos tiene el estado Disponible, la aplicación de parches ha finalizado.

4. Confirme que su instancia de base de datos utiliza la nueva CEV ejecutando `describe-db-instances`.

Requisitos de las actualizaciones de RDS Custom para Oracle

Al actualizar su instancia de base de datos de RDS Custom para Oracle a una CEV de destino, asegúrese de cumplir los siguientes requisitos:

- La CEV de destino a la que va a realizar la actualización debe existir.
- Debe actualizar el sistema operativo o la base de datos en una sola operación. No es posible actualizar el sistema operativo y la base de datos en una sola llamada a la API.
- La CEV de destino debe utilizar los ajustes de los parámetros de instalación que figuran en el manifiesto de la CEV actual. Por ejemplo, no puede actualizar una base de datos que use el directorio raíz de Oracle predeterminado por una CEV que use un directorio raíz de Oracle no predeterminado.
- La CEV de destino debe usar una nueva versión secundaria de la base de datos, no una nueva versión principal. Por ejemplo, no puede actualizar de una CEV de Oracle Database 12c a una CEV de Oracle Database 19c. Sin embargo, puede actualizar de la versión 21.0.0.0.ru-2023-04.rur-2023-04.r1 a la versión 21.0.0.0.ru-2023-07.rur-2023-07.r1.
- Para las actualizaciones del sistema operativo, la CEV de destino debe usar una AMI diferente, pero tener la misma versión principal.

Consideraciones de las actualizaciones de base de datos de RDS Custom for Oracle

Si tiene previsto actualizar la base de datos, tenga en cuenta lo siguiente:

- La versión del sistema operativo (SO) compatible actualmente es Oracle Linux 8. Para seguir recibiendo las últimas actualizaciones y parches de seguridad de RDS Custom para Oracle, actualice sus instancias de base de datos a Oracle Linux 8 especificando un CEV basado en este sistema operativo. Oracle Database 12c versión 1 (12.1), Oracle Database 2 (12.2) y Oracle Database 19c son las únicas versiones compatibles con Oracle Linux 8. Para migrar a la última AMI de Oracle Linux 8, actualice su sistema operativo a la AMI más reciente. Para obtener más información, consulte Actualización de una instancia de base de datos de RDS Custom para Oracle.

  Oracle Linux 7.9 finalizó el soporte el 31 de diciembre de 2024. Para seguir ejecutando Oracle Linux 7 una vez finalizado el soporte, adquiera una licencia de soporte extendido de Oracle. Es

su responsabilidad realizar las actualizaciones de seguridad y parchear las instancias de RDS Custom for Oracle manualmente. Para obtener más información, consulte Lifetime Support Policy: Coverage for Oracle Open Source Service Offerings.

- Al actualizar los binarios de base de datos en la instancia de base de datos principal, RDS Custom para Oracle actualiza las réplicas de lectura automáticamente. Al actualizar el sistema operativo, sin embargo, debe actualizar las réplicas de lectura manualmente.
- Al actualizar una base de datos de contenedores (CDB) a una nueva versión de base de datos, RDS Custom for Oracle comprueba que todas las PDB estén abiertas o puedan abrirse. Si no se cumplen estas condiciones, RDS Custom detiene la comprobación y devuelve la base de datos a su estado original sin intentar la actualización. Si se cumplen las condiciones, RDS Custom aplica el parche primero a la raíz de CDB y, a continuación, a todas las demás PDB (incluida `PDB$SEED`) en paralelo.

  Una vez finalizada la aplicación de parches, RDS Custom intenta abrir todas las PDB. Si alguna PDB no se abre, recibirá el siguiente evento: `The following PDBs failed to open: list-of-PDBs`. Si RDS Custom no logra aplicar el parche a la raíz de CDB ni a ninguna PDB, la instancia pasa al estado `PATCH_DB_FAILED`.
- Es posible que desee realizar, al mismo tiempo, una actualización de versión de base de datos importante y una conversión de una versión que no sea de CDB a CDB. En este caso, le recomendamos que proceda de la siguiente manera:
  1. Cree una nueva instancia de base de datos de RDS Custom for Oracle que utilice la arquitectura multitenencia de Oracle.
  2. Conecte una base de datos que no sea CDB a su raíz de CDB y créela como PDB. Asegúrese de que la versión que no es de CDB sea la misma que la de su CDB.
  3. Convierta la PDB ejecutando el script SQL `noncdb_to_pdb.sql` de Oracle.
  4. Valide su instancia de CDB.
  5. Actualice su instancia de CDB.

Consideraciones de las actualizaciones del sistema operativo de RDS Custom for Oracle

Al planificar una actualización del sistema operativo, tenga en cuenta lo siguiente:

- No puede proporcionar su propia AMI para utilizarla en una CEV de RDS Custom for Oracle. Puede especificar o bien la AMI predeterminada, que utiliza Oracle Linux 8, o bien una AMI que haya utilizado anteriormente una CEV de RDS Custom for Oracle.

  > **Note**
  >
  > RDS Custom for Oracle lanza una nueva AMI predeterminada cuando se descubren vulnerabilidades y exposiciones comunes. No hay un cronograma fijo disponible ni garantizado. RDS Custom for Oracle suele publicar una nueva AMI predeterminada cada 30 días.

- Al actualizar el sistema operativo en la instancia de base de datos principal, debe actualizar las réplicas de lectura asociadas de forma manual.
- Reserve suficiente capacidad de computación de Amazon EC2 para el tipo de instancia en su zona de disponibilidad antes de empezar a aplicar los parches al sistema operativo.

  Al crear una reserva de capacidad, se especifica la zona de disponibilidad, el número de instancias y los atributos de la instancia (lo que incluye el tipo de instancia). Por ejemplo, si su instancia de base de datos utiliza la instancia de EC2 subyacente de tipo r5.large, le recomendamos que reserve la capacidad de EC2 para r5.large en su zona de disponibilidad. Durante la aplicación de parches al sistema operativo, RDS Custom crea un nuevo host de tipo db.r5.large, que puede quedarse atascado si la zona de disponibilidad carece de capacidad de EC2 para este tipo de instancia. Al reservar la capacidad de EC2, se reduce el riesgo de bloqueo de parches por las limitaciones de capacidad. Para obtener más información, consulte On-Demand Capacity Reservations en la Guía del usuario de Amazon EC2.
- Realice una copia de seguridad de la instancia de base de datos antes de actualizar su sistema operativo. La actualización elimina los datos del volumen raíz y cualquier personalización del sistema operativo existente.
- En el modelo de responsabilidad compartida, usted es responsable de mantener su sistema operativo actualizado. RDS Custom for Oracle no exige qué parches debe aplicar a su sistema operativo. Si su RDS Custom for Oracle funciona, puede utilizar la AMI asociada a este CEV de forma indefinida.

Visualización de los destinos de actualización de CEV válidos para las instancias de base de datos de RDS Custom para Oracle

Puede ver las CEV existentes en la página Custom engine versions (Versiones del motor personalizadas) de la AWS Management Console.

También puede utilizar el comando describe-db-engine-versions de la AWS CLI para buscar CEV válidas y usarlas al actualizar las instancias de base de datos, como se muestra en el siguiente ejemplo. En este ejemplo, se da por sentado que ha creado una instancia de base de datos con la versión `19.my_cev1` del motor y que existen las versiones de actualización `19.my_cev2` y `19.my_cev`.

```
aws rds describe-db-engine-versions --engine custom-oracle-ee --engine-version
 19.my_cev1
```

La salida se parece a la siguiente. El campo `ImageId` muestra el ID de la AMI.

```
{
    "DBEngineVersions": [
        {
            "Engine": "custom-oracle-ee",
            "EngineVersion": "19.my_cev1",
            ...
            "Image": {
                "ImageId": "ami-2345",
                "Status": "active"
            },
            "DBEngineVersionArn": "arn:aws:rds:us-west-2:123456789012:cev:custom-
oracle-ee/19.my_cev1/12a34b5c-67d8-90e1-2f34-gh56ijk78lm9"
            "ValidUpgradeTarget": [
                {
                    "Engine": "custom-oracle-ee",
                    "EngineVersion": "19.my_cev2",
                    "Description": "19.my_cev2 description",
                    "AutoUpgrade": false,
                    "IsMajorVersionUpgrade": false
                },
                {
                    "Engine": "custom-oracle-ee",
                    "EngineVersion": "19.my_cev3",
                    "Description": "19.my_cev3 description",
```

```
                "AutoUpgrade": false,
                "IsMajorVersionUpgrade": false
            }
        ]
        ...
```

Actualización de una instancia de base de datos de RDS Custom para Oracle

A fin de actualizar su instancia de base de datos para RDS Custom para Oracle, modifíquela para utilizar una nueva CEV. Esta CEV puede contener binarios de base de datos nuevos o una AMI nueva. Por ejemplo, para actualizar la instancia de base de datos Oracle Linux 7.9 a Oracle Linux 8, especifique la AMI más reciente, que utiliza Oracle Linux 8. Para actualizar la base de datos y el sistema operativo, debe llevar a cabo dos actualizaciones independientes.

> **Note**
>
> Si actualiza la base de datos, RDS Custom actualiza automáticamente las réplicas de lectura después de actualizar la instancia de base de datos principal. Al actualizar el sistema operativo, debe actualizar las réplicas manualmente.

Antes de empezar, revise Requisitos de las actualizaciones de RDS Custom para Oracle y Consideraciones de las actualizaciones de base de datos de RDS Custom for Oracle.

Consola

Para modificar una instancia de base de datos de RDS Custom para Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, luego, elija la instancia de base de datos de RDS Custom para Oracle que desea actualizar.
3. Elija Modify (Modificar). Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. En Versión del motor de base de datos, elija una CEV diferente. Haga lo siguiente:
   - Si va a aplicar parches a la base de datos, asegúrese de que la CEV especifique binarios de base de datos distintos de los que utiliza la instancia de base de datos; además, compruebe

que no especifique una AMI distinta de la AMI que utiliza actualmente la instancia de base de datos.

- Si va a aplicar parches al sistema operativo, asegúrese de que la CEV especifique una AMI distinta de la que utiliza actualmente la instancia de base de datos; además, compruebe que no especifique binarios distintos de base de datos.

> **Warning**
>
> Al parchear el sistema operativo, se pierden los datos del volumen raíz y cualquier personalización existente del sistema operativo.

5. Elija Continue (Continuar) para ver el resumen de las modificaciones.

   Para aplicar los cambios inmediatamente, elija Apply immediately (Aplicar inmediatamente).

6. Si los cambios son correctos, elija Modify DB instance (Modificar instancia de base de datos). O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

En los siguientes ejemplos, se muestran posibles situaciones de actualización. En los ejemplos, se da por sentado que ha creado una instancia de base de datos de RDS Custom para Oracle con las siguientes características:

- Instancia de base de datos denominada `my-custom-instance`
- CEV con el nombre `19.my_cev1`
- Oracle Database 19c con arquitectura no CDB
- Oracle Linux 8 con AMI `ami-1234`

La última AMI proporcionada por el servicio es `ami-2345`. Puede encontrar las AMI ejecutando el comando de la CLI `describe-db-engine-versions`:

Temas

- Actualización del SO
- Actualización de la base de datos

Actualización del SO

En este ejemplo, desea actualizar `ami-1234` a `ami-2345`, que es la AMI más reciente proporcionada por el servicio. Como se trata de una actualización del sistema operativo, los binarios de base de datos para `ami-1234` y `ami-2345` deben ser los mismos. Se crea una nueva CEV con el nombre `19.my_cev2`, basada en `19.my_cev1`.

Example

Para Linux, macOS o Unix:

```
aws rds create-custom-db-engine-version \
    --engine custom-oracle-ee \
    --engine-version 19.my_cev2 \
    --description "Non-CDB CEV based on ami-2345" \
    --kms-key-id key-name \
    --source-custom-db-engine-version-identifer arn:aws:rds:us-
west-2:123456789012:cev:custom-oracle-ee/19.my_cev1/12345678-ab12-1234-cde1-
abcde123456789 \
    --image-id ami-2345
```

Para Windows:

```
aws rds create-custom-db-engine-version ^
    --engine custom-oracle-ee ^
    --engine-version 19.my_cev2 ^
    --description "Non-CDB CEV based on ami-2345" ^
    --kms-key-id key-name ^
    --source-custom-db-engine-version-identifer arn:aws:rds:us-
west-2:123456789012:cev:custom-oracle-ee/19.my_cev1/12345678-ab12-1234-cde1-
abcde123456789 ^
    --image-id ami-2345
```

Para actualizar una instancia de base de datos de RDS Custom, utilice el comando de la AWS CLI modify-db-instance con los siguientes parámetros:

- `--db-instance-identifier`: especifique la instancia de base de datos de RDS Custom para Oracle que se va a actualizar.
- `--engine-version`: especifique la CEV que tiene la nueva AMI.
- `--no-apply-immediately` | `--apply-immediately`: especifique si desea realizar la actualización inmediatamente o esperar hasta el periodo de mantenimiento programado

En el siguiente ejemplo se actualiza `my-custom-instance` a la versión `19.my_cev2`. Solo se actualiza el sistema operativo.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --engine-version 19.my_cev2 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --engine-version 19.my_cev2 ^
    --apply-immediately
```

Actualización de la base de datos

En este ejemplo, desea aplicar el parche p35042068 de Oracle a su instancia de base de datos para RDS para Oracle. Como ha actualizado su sistema operativo en Actualización del SO, la instancia de base de datos está utilizando actualmente `19.my_cev2`, que se basa en `ami-2345`. Ha creado una nueva CEV con el nombre `19.my_cev3` que también utiliza `ami-2345`, pero especifica un nuevo manifiesto JSON en la variable de entorno `$MANIFEST`. Por lo tanto, solo los binarios de la base de datos son diferentes en la nueva CEV y en la CEV que la instancia está utilizando actualmente.

Example

Para Linux, macOS o Unix:

```
aws rds create-custom-db-engine-version \
    --engine custom-oracle-ee \
    --engine-version 19.my_cev3 \
    --description "Non-CDB CEV with p35042068 based on ami-2345" \
    --kms-key-id key-name \
    --image-id ami-2345 \
    --manifest $MANIFEST
```

Para Windows:

```
aws rds create-custom-db-engine-version ^
    --engine custom-oracle-ee ^
    --engine-version 19.my_cev3 ^
    --description "Non-CDB CEV with p35042068 based on ami-2345" ^
    --kms-key-id key-name ^
    --image-id ami-2345 ^
    --manifest $MANIFEST
```

En el siguiente ejemplo, `my-custom-instance` se actualiza a la versión de motor `19.my_cev3`. Solo se actualiza la base de datos.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --engine-version 19.my_cev3 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --engine-version 19.my_cev3 ^
    --apply-immediately
```

Visualización de actualizaciones de base de datos pendientes para instancias de base de datos de RDS Custom

Puede ver las actualizaciones pendientes de base de datos para sus instancias de base de datos de Amazon RDS Custom; para ello, utilice el comando describe-db-instances o describe-pending-maintenance actions de la AWS CLI.

Sin embargo, este enfoque no funciona si utilizó la opción `--apply-immediately` o si la actualización está en curso.

El siguiente comando `describe-db-instances` muestra las actualizaciones pendientes de base de datos para `my-custom-instance`.

```
aws rds describe-db-instances --db-instance-identifier my-custom-instance
```

La salida se parece a la siguiente.

```
{
    "DBInstances": [
        {
           "DBInstanceIdentifier": "my-custom-instance",
            "EngineVersion": "19.my_cev1",
            ...
            "PendingModifiedValues": {
                "EngineVersion": "19.my_cev3"
            ...
            }
        }
    ]
}
```

Solución de problemas del error de actualización de una instancia de base de datos de RDS Custom para Oracle

Si hay errores en la actualización de una instancia de base de datos de RDS Custom, se genera un evento de RDS y el estado de la instancia de base de datos pasa a `upgrade-failed`.

Puede ver este estado mediante el comando de la AWS CLI describe-db-instances, como se muestra en el ejemplo siguiente.

```
aws rds describe-db-instances --db-instance-identifier my-custom-instance
```

La salida se parece a la siguiente.

```
{
    "DBInstances": [
        {
           "DBInstanceIdentifier": "my-custom-instance",
            "EngineVersion": "19.my_cev1",
            ...
            "PendingModifiedValues": {
                "EngineVersion": "19.my_cev3"
            ...
            }
```

```
            "DBInstanceStatus": "upgrade-failed"
        }
    ]
}
```

Tras un error de actualización, se bloquean todas las acciones de la base de datos, excepto aquellas con el fin de modificar la instancia de base de datos para llevar a cabo las siguientes tareas:

- Volver a intentar la misma actualización
- Pausa y reanudación de la automatización de RDS Custom
- Recuperación a un momento dado (PITR)
- Eliminación de una instancia de base de datos

> **Note**
>
> Si se ha pausado la automatización de la instancia de base de datos de RDS Custom, no puede volver a intentar la actualización hasta que reanude la automatización.
> Las mismas acciones se aplican a un error de actualización tanto para una réplica de lectura administrada por RDS como para la principal.

Para obtener más información, consulte Solución de problemas de actualización de RDS Custom para Oracle.

Solución de problemas de base de datos de Amazon RDS Custom para Oracle

El modelo de responsabilidad compartida de RDS Custom proporciona acceso al shell del sistema operativo y acceso como administrador de bases de datos. RDS Custom ejecuta recursos en su cuenta, a diferencia de Amazon RDS, que ejecuta recursos en una cuenta del sistema. Un mayor acceso conlleva una mayor responsabilidad. En las siguientes secciones, puede obtener información sobre cómo solucionar problemas con las instancias de base de datos de Amazon RDS Custom.

> **Note**
>
> En esta sección, se explica cómo solucionar los problemas de RDS Custom para Oracle. Para la solución de problemas de RDS Custom para SQL Server, consulte Solución de problemas de base de datos para Amazon RDS Custom para SQL Server.

Temas

- Visualización de eventos de RDS Custom
- Suscripción a eventos de RDS Custom
- Solución de problemas de creación de versiones de motores personalizados para RDS Custom for Oracle
- Corrección de configuraciones no compatibles en RDS Custom para Oracle
- Solución de problemas de actualización de RDS Custom para Oracle
- Solución de problemas de la promoción de réplicas para RDS Custom para Oracle

Visualización de eventos de RDS Custom

El procedimiento para ver eventos es el mismo para las instancias de base de datos de RDS Custom y Amazon RDS. Para obtener más información, consulte Consulta de eventos de Amazon RDS.

Para ver la notificación de eventos de RDS Custom mediante la AWS CLI, utilice el comando `describe-events`. RDS Custom presenta varios eventos nuevos. Las categorías de eventos son las mismas que para Amazon RDS. Para ver la lista de eventos, consulte Categorías y mensajes de eventos de Amazon RDS.

En el siguiente ejemplo se recuperan los detalles de los eventos que se han producido para la instancia de base de datos de RDS Custom especificada.

```
aws rds describe-events \
    --source-identifier my-custom-instance \
    --source-type db-instance
```

Suscripción a eventos de RDS Custom

El procedimiento para suscribirse a eventos es el mismo para las instancias de base de datos de RDS Custom y Amazon RDS. Para obtener más información, consulte Suscripción a notificaciones de eventos de Amazon RDS.

Para suscribirse a las notificaciones de eventos de RDS Custom con la CLI, utilice el comando `create-event-subscription`. Incluya los siguientes parámetros obligatorios:

- `--subscription-name`
- `--sns-topic-arn`

En el siguiente ejemplo se crea una suscripción para eventos de copia de seguridad y recuperación de una instancia de base de datos de RDS Custom en la cuenta de AWS actual. Las notificaciones se envían a un tema de Amazon Simple Notification Service (Amazon SNS), especificado por `--sns-topic-arn`.

```
aws rds create-event-subscription \
    --subscription-name my-instance-events \
    --source-type db-instance \
    --event-categories '["backup","recovery"]' \
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:interesting-events
```

Solución de problemas de creación de versiones de motores personalizados para RDS Custom for Oracle

Cuando hay errores en la creación de la CEV, RDS Custom emite `RDS-EVENT-0198` con el mensaje `Creation failed for custom engine version` *`major-engine-version.cev_name`* e incluye detalles sobre el error. Por ejemplo, el evento imprime los archivos que faltan.

La creación de la CEV podría tener errores debido a los siguientes problemas:

- El bucket de Amazon S3 que contiene los archivos de instalación no está en la misma región de AWS que su CEV.

- Cuando solicita por primera vez la creación de la CEV en una Región de AWS, RDS Custom crea un bucket de S3 para almacenar recursos de RDS Custom (como artefactos de la CEV, registros AWS CloudTrail y registros de transacciones).

  La creación de la CEV tiene errores si RDS Custom no puede crear el bucket de S3. O bien la persona que llama no tiene permisos de S3 como se describe en Paso 5: otorgar los permisos necesarios al rol o usuario de IAM o el número de buckets de S3 alcanzó el límite.
- La persona que llama no tiene permisos para obtener archivos del bucket de S3 que contiene los archivos multimedia de instalación. Estos permisos se describen en Paso 7: añadir los permisos de IAM necesarios.
- La política de IAM tiene una condición `aws:SourceIp`. Asegúrese de seguir las recomendaciones de la sección AWS: deniega acceso a AWS en función de la dirección IP de origen de la Guía del usuario de AWS Identity and Access Management Asegúrese también de que la persona que llama tenga los permisos de S3 descritos en Paso 5: otorgar los permisos necesarios al rol o usuario de IAM.
- Los archivos multimedia de instalación que aparecen en el manifiesto CEV no se encuentran en el bucket de S3.
- RDS Custom desconoce las sumas de comprobación SHA-256 de los archivos de instalación.

  Confirme que las sumas de comprobación SHA-256 de los archivos proporcionados coinciden con la suma de comprobación SHA-256 del sitio web de Oracle. Si las sumas de comprobación coinciden, contacte a AWS Support y proporcione el nombre de la CEV, el nombre de archivo y la suma de comprobación que tuvieron errores.
- La versión de OPatch no es compatible con sus archivos de revisión. Puede que reciba el siguiente mensaje: `OPatch is lower than minimum required version. Check that the version meets the requirements for all patches, and try again`. Para aplicar una revisión de Oracle, debe utilizar una versión compatible de la utilidad OPatch. Puede encontrar la versión necesaria de la utilidad Opatch en el archivo léame del revisión. Descargue la utilidad OPatch más reciente de My Oracle Support e intente crear el CEV de nuevo.
- Las revisiones especificadas en el manifiesto CEV están en el orden incorrecto.

Puede ver los eventos de RDS en la consola de RDS (en el panel de navegación, elija Events [Eventos]) o mediante el comando `describe-events` de la AWS CLI. La duración predeterminada de la sesión es de 60 minutos. Si no se devuelve ningún evento, especifique una duración más larga, como se muestra en el siguiente ejemplo.

```
aws rds describe-events --duration 360
```

Actualmente, el servicio MediaImport que importa archivos de Amazon S3 para crear las CEV no está integrado con AWS CloudTrail. Por lo tanto, si activa el registro de datos de Amazon RDS en CloudTrail, no se registran las llamadas al servicio MediaImport, como el evento `CreateCustomDbEngineVersion`.

Sin embargo, es posible que vea llamadas de la API Gateway que accede a su bucket de Amazon S3. Estas llamadas provienen del servicio MediaImport para el evento `CreateCustomDbEngineVersion`.

Corrección de configuraciones no compatibles en RDS Custom para Oracle

En el modelo de responsabilidad compartida, es su responsabilidad corregir los problemas de configuración que colocan la instancia de base de datos de RDS Custom para Oracle en el estado `unsupported-configuration`. Si el problema está relacionado con la infraestructura de AWS, puede utilizar la consola o la AWS CLI para solucionarlo. Si el problema está relacionado con el sistema operativo o la configuración de la base de datos, inicie sesión en el host para solucionarlo.

> **Note**
>
> Esta sección explica cómo corregir configuraciones no compatibles en RDS Custom para Oracle. Para obtener información sobre RDS Custom para SQL Server, consulte Corrección de configuraciones no compatibles en RDS Custom para SQL Server.

En las siguientes tablas, se incluyen descripciones de las notificaciones y eventos que envía el perímetro de soporte y cómo solucionarlos. Estas notificaciones y el perímetro de soporte están sujetos a cambios. Para obtener información sobre el perímetro de soporte, consulte Perímetro de soporte de RDS Custom. Para ver las descripciones de los eventos, consulte Categorías y mensajes de eventos de Amazon RDS.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-00000	Configuración	El estado de la instancia de base	Para resolver este problema, cree un caso Soporte.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
	manual no compatible	de datos de RDS Custom está establecido en [Configuración no compatible] debido a *motivo*.	

Recursos de AWS (infraestructura)

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O1001	Volúmenes de Amazon Elastic Block Store (Amazon EBS)	Se agregaron los siguientes volúmenes de EBS a la instancia *ec2_id* de EC2: *volume_id* . Para resolver el problema, separe los volúmenes especificados de la instancia.	RDS Custom crea dos tipos de volumen de EBS, además del volumen raíz creado a partir de la Imagen de máquina de Amazon (AMI), y los asocia a la instancia EC2: • El volumen binario donde se encuentran los binarios de software de base de datos • Los volúmenes de datos donde se encuentran los archivos de base de datos Al crear su instancia de base de datos, las configura ciones de almacenamiento que especifique configuran los volúmenes de datos. El perímetro de soporte monitorea lo siguiente: • Los volúmenes de EBS iniciales creados con la instancia de base de datos siguen asociados a esa instancia.

ID de evento	Configuración	Mensaje de evento de RDS	Acción

			• Los volúmenes de EBS iniciales todavía tienen las mismas configuraciones que se establecieron inicialmente: tipo de almacenamiento, tamaño, IOPS aprovisionadas y rendimiento de almacenamiento.
			• No se adjuntan volúmenes de EBS adicionales a la instancia de base de datos.
			
			Utilice el siguiente comando de la CLI para comparar el tipo de volumen de los detalles del volumen de EBS y los detalles de la instancia de base de datos de RDS Custom para Oracle:
			
			`aws rds describe-db-instances \`
			`--db-instance-identifier db-instance-name | grep StorageType`

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O1002	Volúmenes de Amazon Elastic Block Store (Amazon EBS)	El *volume_id* del volumen EBS se ha separado de la instancia EC2 [*ec2_id*]. No puede separar el volumen original de esta instancia . Para resolver el problema, vuelve a adjuntar *volume_id* a *ec2_id*.	RDS Custom crea dos tipos de volumen de EBS, además del volumen raíz creado a partir de la Imagen de máquina de Amazon (AMI), y los asocia a la instancia EC2: • El volumen binario donde se encuentran los binarios de software de base de datos • Los volúmenes de datos donde se encuentran los archivos de base de datos Al crear su instancia de base de datos, las configuraciones de almacenamiento que especifique configuran los volúmenes de datos. El perímetro de soporte monitorea lo siguiente: • Los volúmenes de EBS iniciales creados con la instancia de base de datos siguen asociados a esa instancia. • Los volúmenes de EBS iniciales todavía tienen las mismas configuraciones que se establecieron inicialmente: tipo de almacenamiento, tamaño, IOPS aprovisionadas y rendimiento de almacenamiento. • No se adjuntan volúmenes de EBS adicionales a la instancia de base de datos. Utilice el siguiente comando de la CLI para comparar el tipo de volumen de los detalles del volumen de EBS y los detalles de la instancia de base de datos de RDS Custom para Oracle:

ID de evento	Configuración	Mensaje de evento de RDS	Acción
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep StorageType`

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O1003	Volúmenes de Amazon Elastic Block Store (Amazon EBS)	El volumen original *volume_id* EBS asociado a la instancia de EC2 *ec2_id* se ha modificado de la siguiente manera: tamaño [*X*] a [*Y*], tipo [*N*] a [*M*] o IOPS [*J*] a [*K*]. Para resolver el problema, revierta la modificación.	RDS Custom crea dos tipos de volumen de EBS, además del volumen raíz creado a partir de la Imagen de máquina de Amazon (AMI), y los asocia a la instancia EC2: • El volumen binario donde se encuentran los binarios de software de base de datos • Los volúmenes de datos donde se encuentran los archivos de base de datos Al crear su instancia de base de datos, las configuraciones de almacenamiento que especifique configuran los volúmenes de datos. El perímetro de soporte monitorea lo siguiente: • Los volúmenes de EBS iniciales creados con la instancia de base de datos siguen asociados a esa instancia. • Los volúmenes de EBS iniciales todavía tienen las mismas configuraciones que se establecieron inicialmente: tipo de almacenamiento, tamaño, IOPS aprovisionadas y rendimiento de almacenamiento. • No se adjuntan volúmenes de EBS adicionales a la instancia de base de datos. Utilice el siguiente comando de la CLI para comparar el tipo de volumen de los detalles del volumen de EBS y los detalles de la instancia de base de datos de RDS Custom para Oracle:

ID de evento	Configuración	Mensaje de evento de RDS	Acción
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep StorageType`
SP-O1004	Estado de la instancia de Amazon EC2	La recuperación automática dejó la instancia EC2 [*ec2_id*] en un estado dañado. Para resolver el problema, consulte Troubleshooting instance recovery failures.	Para comprobar el estado de una instancia de base de datos, utilice la consola o ejecute el siguiente comando de la AWS CLI: `aws rds describe-db-instances \ --db-instance-identifier *db-instance-name* |grep DBInstanceStatus`
SP-O1005	Atributos de la instancia de Amazon EC2	La instancia de EC2 [*ec2_id*] se ha modificado de la siguiente manera: el atributo [*att1*] ha cambiado de [*val-old*] a [*val-new*] y el atributo [*att2*] ha cambiado de [*val-old*] a [*val-new*]. Para resolver el problema, vuelva al valor original.	

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O1006	Estado de la instancia de Amazon EC2	La instancia EC2 [*ec2_id*] se ha cancelado o no se puede encontrar . Para resolver el problema, elimine la instancia de base de datos de RDS Custom.	El perímetro de soporte monitorea las notificaciones del cambio de estado de la instancia EC2. La instancia EC2 siempre tiene que estar siempre en ejecución. Para eliminar la instancia de base de datos 1. Para comprobar el estado de una instancia de base de datos, utilice la consola o ejecute el siguiente comando de la AWS CLI: `aws rds describe-db-instances \ --db-instance-identifier *db-instance-name* |grep DBInstanceStatus` 2. Elimine la instancia de base de datos de RDS Custom para Oracle
SP-O1007	Estado de la instancia de Amazon EC2	La instancia de EC2 [*ec2_id*] se ha detenido. Para resolver el problema, inicie la instancia.	El perímetro de soporte monitorea las notificaciones del cambio de estado de la instancia EC2. La instancia EC2 siempre tiene que estar siempre en ejecución. Para reiniciar la instancia de base de datos 1. Para comprobar el estado de una instancia de base de datos, utilice la consola o ejecute el siguiente comando de la AWS CLI: `aws rds describe-db-instances \ --db-instance-identifier *db-instance-name* |grep DBInstanceStatus` 2. Inicie la instancia de base de datos 3. Vuelva a montar los volúmenes binarios y de datos.

ID de evento	Configuración	Mensaje de evento de RDS	Acción

SP-10	Permiso de Amazon SQS	Faltan permisos para Amazon SQS. Compruebe los permisos del perfil de instancia de IAM, la política de punto de conexión de VPC y las conexiones de servicios dependientes, y vuelva a intentarlo.	Puede resolver este problema asegurándose de que el perfil de IAM asociado al host tiene los siguientes permisos:
			`"SQS:SendMessage"`
			`"SQS:ReceiveMessage"`
			`"SQS:DeleteMessage"`
			`"SQS:GetQueueUrl"`

SP-10	Amazon Simple Queue Service (Amazon SQS)	La cola de SQS [%] se eliminó y no se pudo recuperar. Para resolver este problema, recree la cola.	Recree la cola de Amazon SQS.

Sistema operativo

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O2001	Estado del agente de RDS Custom	El agente de RDS Custom no se está ejecutando en la instancia de EC2 [*ec2_id*]. Asegúrese de que	En RDS Custom for Oracle, la instancia de base de datos sale del perímetro de soporte si se detiene el agente de RDS Custom. Cada 30 segundos, el agente publica la métrica `IamAlive` en Amazon CloudWatch. Se activa una alarma si no se ha publicado la métrica en 30 segundos. Cada 30

ID de evento	Configuración	Mensaje de evento de RDS	Acción

		el agente se esté ejecutando en [*ec2_id*].	minutos, el perímetro de soporte también monitorea el estado del proceso del agente de RDS Custom en el host.
			
			Para reiniciar el agente de RDS Custom
			
			1. Inicie sesión en el host y asegúrese de que el agente de RDS Custom está en ejecución.
			2. Para averiguar el estado del agente, ejecute el comando siguiente.
			
			`service rdscustomagent status`
			
			3. Para iniciar el agente, utilice el comando siguiente.
			
			`service rdscustomagent start`
			
			Cuando el agente de RDS Custom está de nuevo en ejecución, la métrica `IamAlive` se publica en Amazon CloudWatch y la alarma cambia al estado `OK`. Este switch notifica al perímetro de soporte de que el agente está en ejecución.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-02002	Estado del agente de AWS Systems Manager (agente de SSM)	No se puede acceder al agente de Systems Manager en la instancia de EC2 [*ec2_id*]. Asegúrese de haber configurado correctamente los permisos de red, agente e IAM.	El agente de SSM tiene que estar siempre en ejecución. El agente de RDS Custom es responsable de asegurarse de que Systems Manager Agent esté en ejecución. Si el agente de SSM se cancela y se reinicia, el agente de RDS Custom publica una métrica en CloudWatch. El agente de RDS Custom tiene una alarma en la métrica configurada para desencadenarse cuando haya un reinicio en uno de los tres minutos anteriores. Cada 30 minutos, el perímetro de soporte también supervisa el estado del proceso del agente de SSM en el host. Para obtener información, consulte Solución de problemas de SSM Agent.
SP-02003	Estado del agente de AWS Systems Manager (agente de SSM)	El agente de Systems Manager de la instancia de EC2 [*ec2_id*] se ha bloqueado varias veces. Para obtener más información, consulte la documentación sobre la resolución de problemas en el agente de SSM.	Para obtener información, consulte Solución de problemas de SSM Agent.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O2004	Zona horaria del sistema operativo	Se ha cambiado la zona horaria de la instancia de EC2 [*ec2_id*]. Para resolver este problema, restablezca la zona horaria a la configuración anterior de [*previous-time-zone*]. A continuación, utilice un grupo de opciones de RDS para cambiar la zona horaria.	La automatización de RDS detectó que se había cambiado la zona horaria del host sin utilizar un grupo de opciones. Este cambio a nivel de host puede provocar errores en la automatización de RDS, por lo que la instancia EC2 se coloca en el estado `unsupported-configuration`. Para reparar la zona horaria 1. Inicie sesión en su host EC2 y compruebe la zona horaria del sistema operativo de la siguiente manera: `timedatectl` 2. Pausa la automatización de RDS Custom. Para obtener más información, consulte Pausa y reanudación de la instancia de base de datos de RDS Custom. 3. Detenga la instancia de la base de datos. 4. Revierta el cambio de zona horaria en el sistema operativo. 5. Inicie la instancia de base de datos. 6. Reanudar la automatización personalizada de RDS. La instancia de base de datos está disponible en 30 minutos. Para evitar salirse del perímetro en el futuro, modifique su zona horaria mediante un grupo de opciones. Para obtener más información, consulte Zona horaria Oracle.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O2005	Configuraciones de `sudo`	Las configuraciones de Sudo de la instancia EC2 [*`ec2_id`*] carecen de los permisos necesarios. Para resolver este problema, revierta los cambios recientes en las configuraciones de Sudo.	El perímetro de soporte comprueba que determina dos usuarios del sistema operativo puedan ejecutar ciertos comandos en el host. Supervisa las configuraciones de `sudo` y las compara con el estado compatible. Si no se admiten las configuraciones `sudo`, RDS Custom intenta sobrescribirlas y devolverlas al estado admitido anterior. Si el intento se realiza correctamente, RDS Custom envía la siguiente notificación: RDS Custom successfully overwrote your configuration. (RDS Custom sobrescribió correctamente la configuración). Si la sobrescritura no se realiza correctamente, la instancia de base de datos permanece en el estado de configuración no compatible. Para resolver este problema, revierta los cambios del archivo `sudoers.d/` o corrija los permisos. Análisis de los cambios en las configuraciones de **`sudo`** 1. Inicie sesión en el host. 2. Ejecute el siguiente comando. `visudo -c -f /etc/sudoers.d/ individual_sudo_files` 3. Modifique las configuraciones de `sudo` según sea necesario.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
			Después de que el perímetro de soporte determine que las configuraciones de `sudo` son compatibles, la instancia de base de datos de RDS Custom para Oracle estará disponible en 30 minutos.
SP-O2006	Accesibilidad del bucket de S3	La automatización de RDS Custom no puede descargar archivos del bucket de S3 en la instancia EC2 [*ec2_id*]. Compruebe la configuración de red y asegúrese de que la instancia permita conexiones desde S3 y hacia S3.	
SP-20	Versión de la solución de software de alta disponibilidad	La solución HA de la instancia difiere de la versión esperada. Para resolver este problema, cree un caso de AWS Support.	Cree un caso de AWS Support.

Base de datos

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O3001	Objetivo de retraso en el archivo de la base de datos	El parámetro ARCHIVE_LAG_TARGET de la instancia EC2 [*ec2_id*] está fuera del rango *value_range* recomendado. Para resolver el problema, defina el parámetro en un valor dentro de value_range.	El perímetro de soporte supervisa el parámetro de base de datos `ARCHIVE_LAG_TARGET` para verificar que el momento restaurable más reciente de la instancia de base de datos se encuentra dentro de límites razonables. Para cambiar el objetivo de retraso de los archivos de registro REDO 1. Inicie sesión en el host de EC2 2. Conéctese a su instancia de base de datos de RDS Custom para Oracle 3. Cambie el parámetro `ARCHIVE_LAG_TARGET` a un valor entre 60 y 7200. Por ejemplo, utilice la siguiente instrucción SQL. `ALTER SYSTEM SET ARCHIVE_LAG_TARGET=300 SCOPE=BOTH;` La instancia de base de datos está disponible en 30 minutos.
SP-O3002	Rol de Oracle Data Guard	El rol de base de datos [*role_name*] no es compatible con Oracle Data Guard en la instancia EC2 [*ec2_id*]. Para resolver el problema, defina el parámetro	El perímetro de soporte monitorea el rol de base de datos actual cada 15 segundos y envía una notificación de CloudWatch si el rol de base de datos ha cambiado. El parámetro `DATABASE_ROLE` de Oracle Data Guard debe ser `PRIMARY` o `PHYSICAL STANDBY`.

ID de evento	Configuración	Mensaje de evento de RDS	Acción

		DATABASE_ROLE en PRIMARY o PHYSICAL STANDBY.	Para restaurar el rol de base de datos de Oracle Data Guard a un valor compatible
			1. Ejecute la siguiente instrucción para comprobar el rol de Oracle Data Guard:
			`SELECT DATABASE_ROLE FROM V$DATABASE;`
			2. Si la instancia de base de datos es independiente, puede utilizar cualquiera de las siguientes instrucciones para volver a cambiarla al rol PRIMARY:
			`ALTER DATABASE COMMIT TO SWITCHOVER PRIMARY;`
			`ALTER DATABASE ACTIVATE STANDBY DATABASE;`
			Si la instancia de base de datos es una réplica, use la siguiente instrucción para volver a cambiarla al rol PHYSICAL STANDBY:
			`ALTER DATABASE CONVERT TO PHYSICAL STANDBY;`
			Una vez que el perímetro de soporte determine que el rol de base de datos es compatible, la instancia de base de datos de RDS Custom para Oracle estará disponible en 15 segundos.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O3003	Estado de la base de datos	El proceso SMON de la base de datos Oracle se encuentra en estado “zombie”. Para resolver el problema, recupere manualmente la base de datos en la instancia EC2 [*ec2_id*], abra la base de datos y haga inmediata mente una copia de seguridad. Para obtener más ayuda, póngase en contacto con Soporte.	El perímetro de soporte monitorea el estado de la instancia de base de datos. También monitorea cuántos reinicios se produjeron durante la hora y el día anteriores. Se le notifica cuando la instancia se encuentra en un estado en el todavía existe, pero no puede interactuar con ella. Para hacer que el perímetro de soporte evalúe el estado de la instancia 1. Inicie sesión en el host y examine el estado de la base de datos. `ps -eo pid,state,command | grep smon` 2. Si es necesario, reinicie la instancia de la base de datos. Si el reinicio falla, continúe con el siguiente paso. 3. Si es necesario, reinicie el host de EC2. Tras el reinicio de la instancia de base de datos, el agente de RDS Custom detecta que su instancia de base de datos ya no se encuentra en un estado de no respuesta. A continuación, notifica al perímetro de soporte para que vuelva a evaluar el estado de la instancia de base de datos.

ID de evento	Configuración	Mensaje de evento de RDS	Acción

SP-O3004	Modo de registro de base de datos	El modo de registro de la base de datos de la instancia EC2 [*ec2_id*] se ha cambiado a [*value_b*]. Para resolver el problema, ponga el modo de registro en [*value_a*].	Para cambiar el modo de registro de la instancia de base de datos a **`ARCHIVELOG`**
			1. Inicie sesión en el host de EC2
			2. Conéctese a la base de datos y ejecute la siguiente instrucción:
			`SELECT LOG_MODE FROM V$DATABASE;`
			Si lo prefiere, puede ejecutar el siguiente comando en SQL*Plus:
			`ARCHIVE LOG LIST`
			3. Ejecute el siguiente comando de SQL*Plus para iniciar un apagado uniforme.
			`SHUTDOWN IMMEDIATE`
			El agente de RDS Custom reinicia la instancia de base de datos automáticamente y pone el modo de registro en `ARCHIVELOG` . La instancia de base de datos está disponible en 30 minutos.

ID de evento	Configuración	Mensaje de evento de RDS	Acción
SP-O3005	Directorio de inicio de Oracle	El directorio de inicio de Oracle en la instancia de EC2 [*ec2_id*] se ha cambiado a *new_path*. Para resolver el problema, restablezca la configuración a *old_path*.	

SP-O3006	Nombre único de base de datos	El nombre único de base de datos de la instancia de EC2 [*ec2_id*] se ha cambiado a [*new_value*]. Para resolver el problema, cambie el nombre al *old_value* .	Para cambiar el nombre único de la base de datos para su instancia de base de datos
			1. Inicie sesión en el host de EC2
			2. Conéctese a la base de datos y ejecute la siguiente instrucción:
			`SELECT DB_UNIQUE_NAME FROM V$DATABASE;`
			3. Especifique el nombre único de la base de datos original mediante el comando `ALTER SYSTEM SET DB_UNIQUE_NAME` .
			4. Ejecute la siguiente instrucción SQL para iniciar un apagado uniforme.
			`SHUTDOWN IMMEDIATE;`
			El agente de RDS Custom reinicia la instancia de base de datos automáticamente y pone el modo de registro en `ARCHIVELOG` . La instancia de base de datos está disponible en 30 minutos.

Solución de problemas de actualización de RDS Custom para Oracle

Su actualización de una instancia de RDS Custom para Oracle podría fallar. A continuación, encontrará algunas técnicas que puede utilizar durante las actualizaciones de la base de datos de RDS Custom para instancias de base de datos de Oracle:

- Examine los archivos de registro de salida de actualizaciones en el directorio `/tmp` de la instancia de base de datos. Los nombres de los registros dependen de la versión del motor de base de datos. Por ejemplo, es posible que vea registros que contengan las cadenas `catupgrd` o `catup`.
- Examine el archivo `alert.log` que se encuentra en el directorio `/rdsdbdata/log/trace`.
- Ejecute el siguiente comando `grep` en el directorio `root` para llevar a cabo un seguimiento del proceso de actualización del sistema operativo. Este comando muestra dónde se escriben los archivos de registro y determina el estado del proceso de actualización.

  ```
  ps -aux | grep upg
  ```

  A continuación se muestra una salida de ejemplo.

  ```
  root     18884  0.0  0.0 235428  8172 ?        S<   17:03   0:00 /usr/bin/
  sudo -u rdsdb /rdsdbbin/scripts/oracle-control ORCL op_apply_upgrade_sh RDS-
  UPGRADE/2.upgrade.sh
  rdsdb    18886  0.0  0.0 153968 12164 ?        S<   17:03   0:00 /usr/bin/perl -T -
  w /rdsdbbin/scripts/oracle-control ORCL op_apply_upgrade_sh RDS-UPGRADE/2.upgrade.sh
  rdsdb    18887  0.0  0.0 113196  3032 ?        S<   17:03   0:00 /bin/sh /rdsdbbin/
  oracle/rdbms/admin/RDS-UPGRADE/2.upgrade.sh
  rdsdb    18900  0.0  0.0 113196  1812 ?        S<   17:03   0:00 /bin/sh /rdsdbbin/
  oracle/rdbms/admin/RDS-UPGRADE/2.upgrade.sh
  rdsdb    18901  0.1  0.0 167652 20620 ?        S<   17:03   0:07 /rdsdbbin/oracle/
  perl/bin/perl catctl.pl -n 4 -d /rdsdbbin/oracle/rdbms/admin -l /tmp catupgrd.sql
  root     29944  0.0  0.0 112724  2316 pts/0    S+   18:43   0:00 grep --color=auto
   upg
  ```

- Ejecute la siguiente consulta SQL para verificar el estado actual de los componentes y encontrar la versión de la base de datos y las opciones instaladas en la instancia de base de datos.

  ```
  SET LINESIZE 180
  COLUMN COMP_ID FORMAT A15
  COLUMN COMP_NAME FORMAT A40 TRUNC
  COLUMN STATUS FORMAT A15 TRUNC
  SELECT COMP_ID, COMP_NAME, VERSION, STATUS FROM DBA_REGISTRY ORDER BY 1;
  ```

La salida se parece a la siguiente.

```
COMP_NAME                                STATUS               PROCEDURE
---------------------------------------- --------------------
 ------------------------------------------------
Oracle Database Catalog Views            VALID
 DBMS_REGISTRY_SYS.VALIDATE_CATALOG
Oracle Database Packages and Types       VALID
 DBMS_REGISTRY_SYS.VALIDATE_CATPROC
Oracle Text                              VALID                VALIDATE_CONTEXT
Oracle XML Database                      VALID                DBMS_REGXDB.VALIDATEXDB

4 rows selected.
```

- Ejecute la siguiente consulta SQL para verificar si hay objetos no válidos que podrían interferir en el proceso de actualización.

```
SET PAGES 1000 LINES 2000
COL OBJECT FOR A40
SELECT SUBSTR(OWNER,1,12) OWNER,
       SUBSTR(OBJECT_NAME,1,30) OBJECT,
       SUBSTR(OBJECT_TYPE,1,30) TYPE, STATUS,
       CREATED
FROM   DBA_OBJECTS
WHERE  STATUS <>'VALID'
AND    OWNER IN ('SYS','SYSTEM','RDSADMIN','XDB');
```

Solución de problemas de la promoción de réplicas para RDS Custom para Oracle

Puede promocionar réplicas de Oracle administradas en RDS Custom para Oracle mediante la consola, el comando de la AWS CLI `promote-read-replica` o la API `PromoteReadReplica`. Si elimina la instancia de base de datos primaria y todas las réplicas están en buen estado, RDS Custom para Oracle promociona sus réplicas administradas a instancias independientes automáticamente. Si una réplica ha pausado la automatización o está fuera del perímetro de soporte, debe corregir la réplica para que RDS Custom pueda promocionarla automáticamente. Para obtener más información, consulte Promoción de una réplica de RDS Custom para Oracle a una instancia de base de datos independiente.

El flujo de trabajo de promoción de réplicas puede quedarse atascado en la siguiente situación:

- La instancia de base de datos principal se encuentra en el estado `STORAGE_FULL`.
- La base de datos principal no puede archivar todos sus registros redo en línea.
- Existe una brecha entre los archivos de registro REDO archivados en la réplica de Oracle y la base de datos principal.

Respuestas al flujo de trabajo atascado

1. Sincronice la brecha de registros REDO en la instancia de base de datos de réplica de Oracle.
2. Fuerce la promoción de la réplica de lectura al último registro REDO aplicado. Ejecute los siguientes comandos de SQL*Plus:

   ```
   ALTER DATABASE ACTIVATE STANDBY DATABASE;
   SHUTDOWN IMMEDIATE
   STARTUP
   ```

3. Póngase en contacto con Soporte y solicite que se pase la instancia de base de datos al estado `available`.

Problemas conocidos de Amazon RDS Custom para Oracle

Cuando trabaje con RDS Custom para Oracle, tenga en cuenta los siguientes problemas en las instancias de base de datos.

- No se admite el cambio de tamaño de los volúmenes raíz o dbbin.

  > **Warning**
  >
  > Recomendamos encarecidamente que no cambie el tamaño de los volúmenes raíz o dbbin de forma manual. Le recomendamos que almacene todas las configuraciones en el volumen de datos, que persiste después de aplicar los parches, y que cambie el tamaño del volumen utilizando únicamente la API de almacenamiento a escala de RDS.

- Algunas API de RDS se pueden bloquear cuando una instancia de base de datos se encuentra en una AMI anterior, por ejemplo, una AMI que utilice Oracle Linux 7. Para resolver este problema, aplique en la instancia de base de datos un parche con la AMI más reciente mediante la aplicación de parches del sistema operativo. Para obtener más información, consulte Opciones de actualización de CEV.
- Antes de realizar operaciones de RDS, asegúrese de que su Cuenta de AWS dispone de una cuota suficiente de procesamiento y almacenamiento.
- Si la base de datos está en el estado de creación y usted inicia sesión activamente en la base de datos o en el host de Amazon EC2 y ejecuta comandos, es posible que la creación de la base de datos no se complete.
- Actualmente, no se admite la multiplexación de archivos de control, debido a un problema de lectura de réplicas. Antes de crear una réplica de lectura, asegúrese de especificar solo un nombre de archivo en el parámetro de inicialización `CONTROL_FILES` de la base de datos de origen.
- No puede cambiar el modo de la base de datos de `PHYSICAL STANDBY` (montada o de solo lectura) a `SNAPSHOT STANDBY` (conversión a lectura/escritura).
- Si una Cuenta de AWS forma parte de una organización de AWS con una política de control de servicio (SCP) y el SCP contiene una clave de condición, es posible que no se pueda crear una instancia de base de datos de RDS Custom para Oracle y se produzca el siguiente error:

```
You can't create the DB instance because of incompatible resources.
The IAM instance profile role [AWSRDSCustomInstanceRole1-us-east-1] is missing the
 following permissions:
```

```
EFFECT [Allow] on ACTION(S) [ssm:DescribeAssociation, ssm:DescribeDocument,
 ssm:GetConnectionStatus,
  ssm:GetDeployablePatchSnapshotForInstance, ssmmessages:OpenControlChannel,
 ssm:GetParameters,
  ssm:ListInstanceAssociations, ssm:PutConfigurePackageResult,
 ssmmessages:CreateControlChannel,
  ssm:GetParameter, ssm:UpdateAssociationStatus, ssm:GetManifest,
 ssmmessages:CreateDataChannel,
  ssm:PutInventory, ssm:UpdateInstanceInformation, ssm:DescribeInstanceInformation,
  ssmmessages:OpenDataChannel, ssm:GetDocument, ssm:ListAssociations,
 ssm:PutComplianceItems,
  ssm:UpdateInstanceAssociationStatus] for RESOURCE(S) [], EFFECT [Allow] on
 ACTION(S) [ec2messages:DeleteMessage,
  ec2messages:FailMessage, ec2messages:GetEndpoint, ec2messages:AcknowledgeMessage,
 ec2messages:GetMessages,
  ec2messages:SendReply] for RESOURCE(S) [], EFFECT [Allow] on ACTION(S)
 [logs:CreateLogStream,
  logs:DescribeLogStreams, logs:PutRetentionPolicy, logs:PutLogEvents]
```

Para resolver este problema, cree un ticket con Soporte.

Problemas conocidos con cuentas de usuario de bases de datos

Observe los problemas siguientes:

- No elimine las cuentas de usuario de la base de datos que comiencen por la cadena `RDS`, como `RDSADMIN` y `RDS_DATAGUARD`. RDS Custom for Oracle utiliza la cuenta de `RDS` para la automatización. Si elimina esta cuenta de usuario, RDS Custom mueve la instancia al estado de configuración no compatible.
- No puede modificar el nombre de usuario principal de una instancia de base de datos de RDS Custom for Oracle con la API `ModifyDBInstance`.
- RDS Custom for Oracle rota las credenciales de las cuentas de usuario en todas las instancias de base de datos. Para obtener más información, consulte Rotación de credenciales de RDS Custom para Oracle para programas de conformidad. Si utiliza una configuración principal o en espera en las instalaciones, la rotación de credenciales puede afectar a los siguientes recursos:
  - Instancias de RDS Custom for Oracle en espera creadas manualmente

    Para resolver este problema, elimine las bases de datos manuales en espera y, a continuación, cree una réplica de lectura de Oracle mediante una llamada a la API. Administre manualmente

los secretos de las bases de datos en espera manuales para que coincidan con la instancia de base de datos de origen.

- Réplicas de lectura entre regiones creadas manualmente

  Para resolver este problema, guarde los secretos manualmente para que coincidan con la instancia de base de datos principal.

Problemas conocidos con los archivos de parámetros y configuración

- Debe configurar el archivo `crontab` tras escalar la computación, las actualizaciones del sistema operativo y otras operaciones en las que RDS Custom sustituya al volumen raíz. Le recomendamos que mantenga una copia de seguridad de `crontab`.
- Tenga en cuenta las siguientes instrucciones al configurar el archivo `listener.ora`:
  - Asegúrese de que todas las entradas del archivo estén en una sola línea. Este enfoque evita problemas de sangría durante la creación de la instancia.
  - Asegúrese de que `GLOBAL_DBNAME` sea igual al valor de `SID_NAME`.
  - Asegúrese de que el valor de `LISTENER` sigue la convención de nomenclatura `L_`*`dbname`*`_001`.
  - Asegúrese de que el archivo `listener.ora` mantenga una conexión con el nombre de la base de datos. RDS Custom utiliza esta conexión para comprobar el inicio de la base de datos. Si modifica este archivo de forma incorrecta, es posible que se produzcan errores en operaciones como la escalabilidad, el cálculo o la aplicación de parches.

    En el siguiente ejemplo se muestra un `listener.ora` configurado correctamente.

```
ADR_BASE_L_ORCL_001=/rdsdbdata/log/
USE_SID_AS_SERVICE_L_ORCL_001=ON
SID_LIST_L_ORCL_001=(SID_LIST = (SID_DESC = (SID_NAME = ORCL)(GLOBAL_DBNAME = ORCL)
 (ORACLE_HOME = /rdsdbbin/oracle.19.custom.r1.EE.1)))
SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_ORCL_001=OFF
L_ORCL_001=(DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT =
 XXXX)(HOST = x.x.x.x))) (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = XXXX)
(HOST = 127.0.0.1))))
```

- No hay soporte para comentarios en un archivo de parámetros de servidor ni en un archivo de parámetros de inicialización.
- Debe declarar los siguientes parámetros de inicialización en el archivo de parámetros de servidor (`/rdsdbdata/config/oracle_pfile`):

- MEMORY_MAX_TARGET
- MEMORY_TARGET
- PGA_AGGREGATE_TARGET
- PROCESSES
- SGA_TARGET
- USE_LARGE_PAGES

Si los parámetros anteriores no se declaran en `/rdsdbdata/config/oracle_pfile`, es posible que haya un error en la creación de réplicas de lectura y en el escalado de la computación.

- No puede eliminar los enlaces simbólicos de los archivos de configuración, como el archivo de parámetros del servidor, los archivos de auditoría, `listener.ora`, `tnsnames.ora` o `sqlnet.ora`. Tampoco puede modificar la estructura de directorios de estos archivos. La automatización de RDS Custom espera que estos archivos estén en una estructura de directorios específica.

  Para crear un archivo de parámetros de servidor a partir de un archivo de parámetros de inicialización, utilice la siguiente sintaxis.

```
CREATE SPFILE='/rdsdbdata/admin/$ORACLE_SID/pfile/spfile$ORACLE_SID.ora'
    FROM PFILE='/rdsdbdata/config/oracle_pfile';
```

Trabajar con RDS Custom for SQL Server

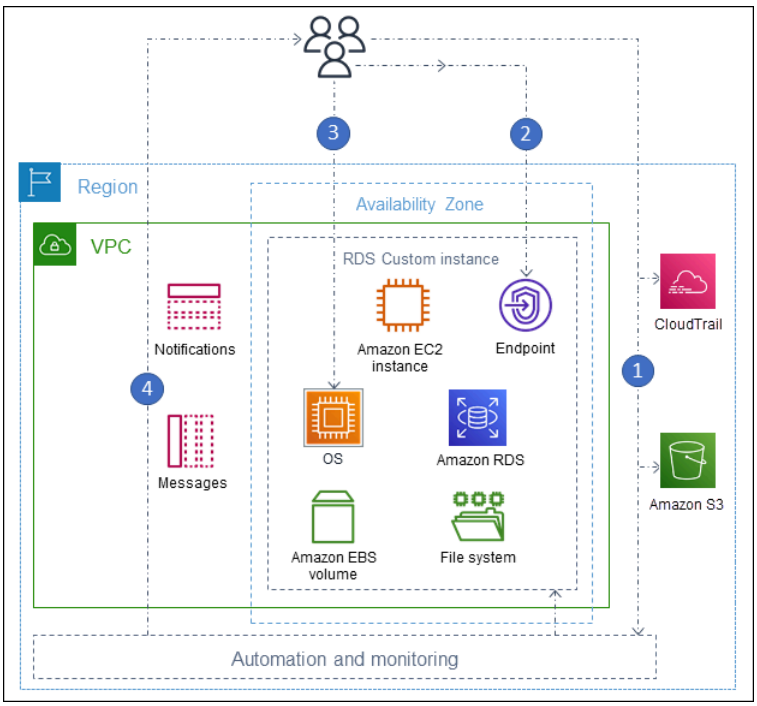
A continuación encontrará instrucciones para crear, administrar y mantener sus instancias de base de datos de RDS Custom for SQL Server.

Temas

- Flujo de trabajo de RDS Custom for SQL Server
- Requisitos y limitaciones de Amazon RDS Custom for SQL Server
- Configuración del entorno para Amazon RDS Custom for SQL Server
- Bring Your Own Media con RDS Custom para SQL Server
- Uso de versiones de motor personalizadas para RDS Custom para SQL Server
- Creación y conexión a una instancia de base de datos para Amazon RDS Custom for SQL Server
- Administración de una instancia de base de datos para Amazon RDS Custom for SQL Server
- Uso de Microsoft Active Directory con RDS Custom para SQL Server
- Administración de una implementación multi-AZ de RDS Custom para SQL Server
- Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS Custom for SQL Server
- Copia de una instantánea de base de datos de Amazon RDS Custom para SQL Server
- Migración de una base de datos en las instalaciones a Amazon RDS Custom for SQL Server
- Actualización de una instancia de base de datos de Amazon RDS Custom para SQL Server
- Solución de problemas de base de datos para Amazon RDS Custom para SQL Server

Flujo de trabajo de RDS Custom for SQL Server

En el siguiente diagrama se muestra el flujo de trabajo típico de RDS Custom for SQL Server.



Los pasos son los siguientes:

1. Cree una instancia de base de datos RDS Custom para SQL Server a partir de una versión de motor ofrecida por RDS Custom.

   Para obtener más información, consulte Creación de una instancia de base de datos de RDS Custom para SQL Server.
2. Conecte la aplicación al punto de conexión de instancia de base de datos de RDS Custom.

   Para obtener más información, consulte Conexión a la instancia de base de datos de RDS Custom DB mediante AWS Systems Manager y Conexión a la instancia de base de datos de RDS Custom mediante RDP.
3. (Opcional) Acceda al host para personalizar el software.
4. Supervise las notificaciones y los mensajes generados por la automatización de RDS Custom.

Creación de una instancia de base de datos para RDS Custom

Puede crear su instancia de base de datos de RDS Custom mediante el comando `create-db-instance`. El procedimiento es similar al que se debe seguir para crear una instancia de Amazon RDS. Sin embargo, algunos de los parámetros son diferentes. Para obtener más información,

consulte Creación y conexión a una instancia de base de datos para Amazon RDS Custom for SQL Server.

Conexión a la base de datos

Al igual que una instancia de base de datos de Amazon RDS, la instancia de base de datos de RDS Custom for SQL Server reside en una VPC. La aplicación se conecta a la instancia de RDS Custom mediante un cliente como SQL Server Management Suite (SSMS), al igual que en RDS for SQL Server.

Personalización de RDS Custom

Puede acceder al host de RDS Custom para instalar o personalizar el software. Para evitar conflictos entre los cambios y la automatización de RDS Custom, puede pausar la automatización durante un periodo determinado. Durante este periodo, RDS Custom no hace monitoreos ni recuperación de instancias. Al final del periodo, RDS Custom reanuda la automatización completa. Para obtener más información, consulte Pausa y reanudación de la automatización de RDS Custom.

Requisitos y limitaciones de Amazon RDS Custom for SQL Server

A continuación, puede encontrar un resumen de los requisitos y limitaciones de Amazon RDS Custom for SQL Server para una consulta rápida. Los requisitos y limitaciones también aparecen en las secciones correspondientes.

Temas

- Disponibilidad en regiones y versiones
- Requisitos generales de RDS Custom for SQL Server
- Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL
- Limitaciones de RDS Custom for SQL Server
- Configuración de conjuntos de caracteres e intercalaciones para instancias de base de datos de RDS Custom para SQL Server
- Zona horaria local para las instancias de base de datos de RDS Custom para SQL Server
- Uso de una clave maestra de servicio con RDS Custom para SQL Server
- Compatibilidad de captura de datos de cambios (CDC) con RDS Custom para SQL Server

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de Amazon RDS con Amazon RDS Custom para SQL Server, consulte Regiones y motores de base de datos admitidos para RDS Custom para SQL Server.

Requisitos generales de RDS Custom for SQL Server

Asegúrese de cumplir estos requisitos para Amazon RDS Custom for SQL Server:

- Utilice las clases de instancias que se muestran en Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL. Los únicos tipos de almacenamiento admitidos son las unidades de estado sólido (SSD) de los tipos gp2, gp3, io1 y io2 Block Express. El límite máximo de almacenamiento para io1, gp2 y gp3 es de 16 TiB, mientras que io2 admite 64 TiB.
- Asegúrese de que tiene una clave de cifrado AWS KMS simétrica para crear una instancia de base de datos de RDS Custom. Para obtener más información, consulte Asegúrese de que tiene una clave de cifrado simétrica AWS KMS.

- Asegúrese de crear un perfil de rol de AWS Identity and Access Management (IAM) e instancia. Para obtener más información, consulte Creación manual del Rol de IAM y el perfil de instancias y Creación automática de perfiles de instancias mediante la AWS Management Console.
- Asegúrese de proporcionar una configuración de redes que RDS Custom pueda utilizar para acceder a otros Servicios de AWS. Para conocer los requisitos específicos, consulte Paso 2: configuración de la red, perfil de instancia y cifrado.
- El número combinado de instancias de base de datos RDS Custom y Amazon RDS no puede superar el límite de cuota. Por ejemplo, si su cuota es de 40 instancias de base de datos, puede tener 20 instancias de base de datos de RDS Custom for SQL Server y 20 instancias de base de datos de Amazon RDS.
- RDS Custom crea automáticamente un rastro de AWS CloudTrail cuyo nombre empieza por `do-not-delete-rds-custom-`. El perímetro de soporte personalizado de RDS se basa en los eventos de CloudTrail para determinar si sus acciones afectan a la automatización de RDS Custom. RDS Custom creará el rastro cuando cree su primera instancia de base de datos. Para usar un CloudTrail ya existente, póngase en contacto con AWS Support. Para obtener más información, consulte AWS CloudTrail.

Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL

Compruebe si la clase de instancia de base de datos es compatible en su región mediante el comando describe-orderable-db-instance-options.

RDS Custom para SQL Server admite las clases de instancias de base de datos que se muestran en la siguiente tabla.

Edición de SQL Server	RDS Custom admite
Enterprise Edition	db.r5.xlarge–db.r5.24xlarge db.r5b.xlarge–db.r5b.24xlarge db.m5.xlarge–db.m5.24xlarge db.r6i.xlarge–db.r6i.32xlarge db.m6i.xlarge–db.m6i.32xlarge

Edición de SQL Server	RDS Custom admite
	db.x2iedn.xlarge–db.x2iedn.32xlarge
Standard Edition	db.r5.large–db.r5.24xlarge db.r5b.large–db.r5b.8xlarge db.m5.large–db.m5.24xlarge db.r6i.large–db.r6i.8xlarge db.m6i.large–db.m6i.8xlarge db.x2iedn.xlarge–db.x2iedn.8xlarge
Developer Edition	db.r5.xlarge–db.r5.24xlarge db.r5b.xlarge–db.r5b.24xlarge db.m5.xlarge–db.m5.24xlarge db.r6i.xlarge–db.r6i.32xlarge db.m6i.xlarge–db.m6i.32xlarge db.x2iedn.xlarge–db.x2iedn.32xlarge
Web Edition	db.r5.large–db.r5.4xlarge db.m5.large–db.m5.4xlarge db.r6i.large–db.r6i.4xlarge db.m6i.large–db.m6i.4xlarge db.r5b.large–db.r5b.4xlarge

Las siguientes recomendaciones se aplican a los tipos de clases db.x2iedn:

- En el momento de la creación, el almacenamiento local es un dispositivo sin formato y no asignado. Antes de utilizar una instancia de base de datos con esta clase de instancia, debe montar y formatear el almacenamiento local. Luego, configure `tempdb` en él para garantizar un rendimiento óptimo. Para obtener más información, consulte Optimize tempdb performance in Amazon RDS Custom for SQL Server using local instance storage.
- El almacenamiento local vuelve a su estado original y sin asignar cuando ejecuta operaciones de instancias de base de datos, como el cálculo de escala, el reemplazo de instancias, la restauración de instantáneas o la recuperación en un momento dado (PITR). En estas situaciones, debe volver a montar, formatear y configurar la unidad y `tempdb` para restablecer su funcionalidad.
- Para las instancias multi-AZ, se recomienda realizar la configuración en una instancia de base de datos en espera. De esta forma, si se produce una conmutación por error, el sistema sigue funcionando sin problemas porque la configuración ya está implementada en la instancia en espera.

Limitaciones de RDS Custom for SQL Server

Las siguientes limitaciones se aplican a RDS for SQL Server:

- No puede crear réplicas de lectura en Amazon RDS para RDS Custom for SQL Server. Sin embargo, puede configurar la alta disponibilidad automáticamente con una implementación multi-AZ. Para obtener más información, consulte Administración de una implementación multi-AZ de RDS Custom para SQL Server.
- No puede modificar el identificador de instancia de base de datos de una instancia de base de datos actual de RDS Custom para SQL Server.
- Cuando una instancia de base de datos de RDS Custom para SQL Server no se ha creado con una versión del motor personalizada (CEV), no se garantiza la persistencia de los cambios en el sistema operativo Microsoft Windows. Por ejemplo, perderá estos cambios cuando inicie una operación de restauración de instantáneas o de un momento dado. Si la instancia de base de datos de RDS Custom para SQL Server se ha creado con una CEV, esos cambios persisten.
- No todas las opciones son compatibles. Por ejemplo, al crear una instancia de base de datos de RDS Custom for SQL Server, no puede hacer lo siguiente:
  - Cambiar el número de núcleos de CPU y subprocesos por núcleo de la clase de instancia de base de datos.
  - Activar el escalado automático del almacenamiento.

  - Especificar su propio grupo de parámetros de base de datos, grupo de opciones o codificación de caracteres.
  - Activar la Información sobre rendimiento.
  - Activar las actualizaciones automáticas de versiones secundarias.
- El almacenamiento máximo de instancias de base de datos es de 64 TiB.
- No se puede utilizar RDS Proxy con RDS Custom para SQL Server.
- No puede usar la API `describe-reserved-db-instances` para las instancias de bases de datos de RDS Custom for SQL Server.

Configuración de conjuntos de caracteres e intercalaciones para instancias de base de datos de RDS Custom para SQL Server

Información general

Con las instancias de base de datos de RDS Custom para SQL Server, puede establecer la configuración de conjuntos de caracteres y de intercalaciones que determinan cómo se almacenan y clasifican los datos. Los conjuntos de caracteres definen los caracteres que se permiten, mientras que las intercalaciones especifican las reglas para clasificar y comparar los datos. Es importante establecer los conjuntos de caracteres y las intercalaciones adecuados para las aplicaciones que funcionan con datos multilingües o que tienen requisitos de clasificación específicos. Por ejemplo, es posible que necesite gestionar los caracteres acentuados y definir reglas de clasificación específicas para cada idioma, o bien mantener la integridad de los datos en distintas configuraciones regionales. En las siguientes secciones, se proporciona información sobre la compatibilidad de conjuntos de caracteres e intercalaciones para las instancias de base de datos de RDS Custom para SQL Server.

RDS Custom para SQL Server admite una amplia variedad de intercalaciones de servidores, tanto en codificación tradicional como en UTF-8, para las configuraciones regionales SQL_Latin, japonés, alemán y árabe. La intercalación de servidores predeterminada es `SQL_Latin1_General_CP1_CI_AS`; sin embargo, puede seleccionar otra intercalación compatible para utilizarla. Puede seleccionar una intercalación con el mismo procedimiento que utiliza RDS para SQL Server. Para obtener más información, consulte Administración de intercalaciones y conjuntos de caracteres de Amazon RDS para Microsoft SQL Server.

Consideraciones

Las intercalaciones de servidores en RDS Custom para SQL Server tienen los siguientes requisitos y limitaciones:

- Puede configurar la intercalación de servidores al crear una instancia de base de datos de RDS Custom para SQL Server. No puede modificar la intercalación a nivel de servidor una vez creada la instancia de base de datos.
- No puede modificar la intercalación a nivel de servidor cuando se restaura a partir de una instantánea de base de datos o durante una recuperación en un momento dado (PITR).
- Al crear una instancia de base de datos a partir de una CEV de RDS Custom para SQL Server, la instancia de base de datos no hereda la intercalación de servidores de la CEV. En su lugar, se utiliza la intercalación de servidores predeterminada de `SQL_Latin1_General_CP1_CI_AS`. Si ha configurado una intercalación de servidores no predeterminada en una CEV de RDS Custom para SQL Server y desea utilizar esa misma intercalación en una nueva instancia de base de datos, asegúrese de seleccionar la misma intercalación al crear la instancia de base de datos a partir de la CEV.

  > **Note**
  >
  > Si la intercalación que selecciona al crear la instancia de base de datos es diferente de la intercalación de la CEV, las bases de datos del sistema Microsoft SQL Server de la nueva instancia de base de datos de RDS Custom para SQL Server se volverán a crear para utilizar la intercalación actualizada. El proceso de nueva creación solo se realiza en la nueva instancia de base de datos de RDS Custom para SQL Server y no afecta a la CEV en sí. Las modificaciones anteriores que haya realizado en las bases de datos del sistema en la CEV no se conservarán en la nueva instancia de base de datos de RDS Custom para SQL Server una vez que se hayan vuelto a crear las bases de datos del sistema. Algunos ejemplos de algunas modificaciones son los objetos definidos por el usuario en la base de datos `master`, los trabajos programados en la base de datos `msdb` o los cambios en la configuración predeterminada de la base de datos `model` de la CEV. Puede volver a crear las modificaciones de forma manual una vez que se crea la nueva instancia de base de datos de RDS Custom para SQL Server.

- Al crear una instancia de base de datos a partir de una versión del motor personalizada (CEV) de RDS Custom para SQL Server y seleccionar una intercalación diferente de la CEV, asegúrese de que la imagen dorada (AMI) que se ha utilizado para crear la CEV cumpla los siguientes requisitos para que las bases de datos del sistema Microsoft SQL Server de la nueva instancia de base de datos puedan volver a crearse:

- En el caso de SQL Server 2022, asegúrese de que el archivo `setup.exe` esté ubicado en la siguiente ruta: `C:\Program Files\Microsoft SQL Server\160\Setup Bootstrap \SQL2022\setup.exe`
- En el caso de SQL Server 2019, asegúrese de que el archivo `setup.exe` esté ubicado en la siguiente ruta: `C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap \SQL2019\setup.exe`
- Las copias de las plantillas de datos y registro de las bases de datos `master`, `model` y `msdb` deben estar en sus ubicaciones predeterminadas. Para obtener más información, consulte Regeneración de las bases de datos del sistema en la documentación pública de Microsoft.
- Asegúrese de que su motor de base de datos de SQL Server utilice `NT Service \MSSQLSERVER` o `NT AUTHORITY\NETWORK SERVICE` como cuenta de servicio. Cualquier otra cuenta no tendrá los permisos necesarios en la unidad `C:\` al configurar una intercalación de servidores no predeterminada para la instancia de base de datos.

- Si la intercalación de servidores seleccionada para una nueva instancia de base de datos es la misma que la configurada en la CEV, las bases de datos del sistema Microsoft SQL Server de la nueva instancia de base de datos de RDS Custom para SQL Server no se someten al proceso de nueva creación. Cualquier modificación anterior que haya realizado en las bases de datos del sistema en la CEV se conservará automáticamente en la nueva instancia de base de datos de RDS Custom para SQL Server.

Intercalaciones admitidas

Puede definir su intercalación en uno de los valores que se muestran en la siguiente tabla.

Collation (Intercalación)	Descripción
Arabic_100_BIN	Arabic-100, clasificación binaria
Arabic_100_BIN2	Arabic-100, clasificación de comparación de punto de código binario
Arabic_100_CI_AI	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Arabic_100_CI_AI_KS	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_100_CI_AI_KS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Arabic_100_CI_AI_KS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CI_AI_KS_WS	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Arabic_100_CI_AI_KS_WS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CI_AI_KS_WS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_100_CI_AI_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Arabic_100_CI_AI_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CI_AI_WS	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Arabic_100_CI_AI_WS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CI_AI_WS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_100_CI_AS	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Arabic_100_CI_AS_KS	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_100_CI_AS_KS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Arabic_100_CI_AS_KS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Arabic_100_CI_AS_KS_WS	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Arabic_100_CI_AS_KS_WS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CI_AS_KS_WS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_100_CI_AS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Arabic_100_CI_AS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CI_AS_WS	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Arabic_100_CI_AS_WS_SC	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Arabic_100_CI_AS_WS_SC_UTF8	Arabic-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AI	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Arabic_100_CS_AI_KS	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_100_CS_AI_KS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Arabic_100_CS_AI_KS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AI_KS_WS	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Arabic_100_CS_AI_KS_WS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CS_AI_KS_WS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Arabic_100_CS_AI_SC	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Arabic_100_CS_AI_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AI_WS	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Arabic_100_CS_AI_WS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CS_AI_WS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AS	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Arabic_100_CS_AS_KS	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_100_CS_AS_KS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Arabic_100_CS_AS_KS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AS_KS_WS	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Arabic_100_CS_AS_KS_WS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CS_AS_KS_WS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Arabic_100_CS_AS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Arabic_100_CS_AS_WS	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura

Collation (Intercalación)	Descripción
Arabic_100_CS_AS_WS_SC	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Arabic_100_CS_AS_WS_SC_UTF8	Arabic-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Arabic_BIN	Árabe, clasificación binaria
Arabic_BIN2	Árabe, clasificación de comparación de punto de código binario
Arabic_CI_AI	Árabe, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Arabic_CI_AI_KS	Árabe, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_CI_AI_KS_WS	Árabe, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Arabic_CI_AI_WS	Árabe, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Arabic_CI_AS	Árabe, no distingue entre mayúsculas y minúsculas, no distingue acentos, tipos de kana ni anchura

Collation (Intercalación)	Descripción
Arabic_CI_AS_KS	Árabe, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_CI_AS_KS_WS	Árabe, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Arabic_CI_AS_WS	Árabe, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Arabic_CS_AI	Árabe, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Arabic_CS_AI_KS	Árabe, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Arabic_CS_AI_KS_WS	Árabe, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Arabic_CS_AI_WS	Árabe, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Arabic_CS_AS	Árabe, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Arabic_CS_AS_KS	Árabe, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Arabic_CS_AS_KS_WS	Árabe, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Arabic_CS_AS_WS	Árabe, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Chinese_PRC_BIN2	Chinese-PRC, clasificación de comparación de punto de código binario
Chinese_PRC_CI_AS	Chino de RPC, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Chinese_Taiwan_Stroke_CI_AS	Chino de Taiwán (trazos), distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Danish_Norwegian_CI_AS	Danés-noruego, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana ni anchura
Finnish_Swedish_CI_AS	Finés-sueco, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
French_CI_AS	Francés, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
German_PhoneBook_100_BIN	German-PhoneBook-100, clasificación binaria
German_PhoneBook_100_BIN2	German-PhoneBook-100, clasificación de comparación de punto de código binario

Collation (Intercalación)	Descripción
German_PhoneBook_100_CI_AI	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CI_AI_KS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CI_AI_KS_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AI_KS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CI_AI_KS_WS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_100_CI_AI_KS_WS_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AI_KS_WS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
German_PhoneBook_100_CI_AI_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AI_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CI_AI_WS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
German_PhoneBook_100_CI_AI_WS_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AI_WS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CI_AS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CI_AS_KS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
German_PhoneBook_100_CI_AS_KS_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AS_KS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CI_AS_KS_WS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_100_CI_AS_KS_WS_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AS_KS_WS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CI_AS_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
German_PhoneBook_100_CI_AS_WS	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
German_PhoneBook_100_CI_AS_WS_SC	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
German_PhoneBook_100_CI_AS_WS_SC_UTF8	German-PhoneBook-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CS_AI	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CS_AI_KS	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CS_AI_KS_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CS_AI_KS_SC_UTF8	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
German_PhoneBook_100_CS_AI_KS_WS	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_100_CS_AI_KS_WS_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
German_Phonebook_100_CS_AI_KS_WS_SC_UTF8	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CS_AI_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CS_AI_SC_UTF8	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CS_AI_WS	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_100_CS_AI_WS_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
German_PhoneBook_100_CS_AI_WS_SC_UTF8	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CS_AS	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CS_AS_KS	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_100_CS_AS_KS_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
German_PhoneBook_100_CS_AS_KS_SC_UTF8	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_100_CS_AS_KS_WS	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_100_CS_AS_KS_WS_SC	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
German_PhoneBook_100_CS_AS_KS_WS_SC_UTF8	German-PhoneBook-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
German_PhoneBook_BIN	German-PhoneBook, clasificación binaria
German_PhoneBook_BIN2	German-PhoneBook, clasificación de comparación de punto de código binario
German_PhoneBook_CI_AI	German-PhoneBook, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
German_PhoneBook_CI_AI_KS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_CI_AI_KS_WS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_CI_AI_WS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
German_PhoneBook_CI_AS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
German_PhoneBook_CI_AS_KS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_CI_AS_KS_WS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_CI_AS_WS	German-PhoneBook, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
German_PhoneBook_CS_AI	German-PhoneBook, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
German_PhoneBook_CS_AI_KS	German-PhoneBook, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_CS_AI_KS_WS	German-PhoneBook, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_CS_AI_WS	German-PhoneBook, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_CS_AS	German-PhoneBook, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
German_PhoneBook_CS_AS_KS	German-PhoneBook, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
German_PhoneBook_CS_AS_KS_WS	German-PhoneBook, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
German_PhoneBook_CS_AS_WS	German-PhoneBook, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Hebrew_BIN	Hebreo, orden binario
Hebrew_CI_AS	Hebreo, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Japanese_90_BIN	Japanese-90, clasificación binaria
Japanese_90_BIN2	Japanese-90, clasificación de comparación de punto de código binario
Japanese_90_CI_AI	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_90_CI_AI_KS	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_90_CI_AI_KS_SC	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Japanese_90_CI_AI_KS_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AI_KS_WS	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_90_CI_AI_KS_WS_SC	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CI_AI_KS_WS_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AI_SC	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CI_AI_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AI_WS	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura

Collation (Intercalación)	Descripción
Japanese_90_CI_AI_WS_SC	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CI_AI_WS_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AS	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_90_CI_AS_KS	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_90_CI_AS_KS_SC	Japanese-90, no distingue entre mayúscula s y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CI_AS_KS_SC_UTF8	Japanese-90, no distingue entre mayúscula s y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AS_KS_WS	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_90_CI_AS_KS_WS_SC	Japanese-90, no distingue entre mayúscula s y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Japanese_90_CI_AS_KS_WS_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AS_SC	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CI_AS_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CI_AS_WS	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_90_CI_AS_WS_SC	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CI_AS_WS_SC_UTF8	Japanese-90, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AI	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_90_CS_AI_KS	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_90_CS_AI_KS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CS_AI_KS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AI_KS_WS	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_90_CS_AI_KS_WS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CS_AI_KS_WS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AI_SC	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CS_AI_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Japanese_90_CS_AI_WS	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_90_CS_AI_WS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CS_AI_WS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AS	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_90_CS_AS_KS	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_90_CS_AS_KS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CS_AS_KS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AS_KS_WS	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura

Collation (Intercalación)	Descripción
Japanese_90_CS_AS_KS_WS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CS_AS_KS_WS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_90_CS_AS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_90_CS_AS_WS	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_90_CS_AS_WS_SC	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_90_CS_AS_WS_SC_UTF8	Japanese-90, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_BIN	Japonés, clasificación binaria

Collation (Intercalación)	Descripción
Japanese_BIN2	Japonés, clasificación de comparación de punto de código binario
Japanese_Bushu_Kakusu_100_BIN	Japanese-Bushu-Kakusu-100, clasificación binaria
Japanese_Bushu_Kakusu_100_BIN2	Japanese-Bushu-Kakusu-100, clasificación de comparación de punto de código binario
Japanese_Bushu_Kakusu_100_CI_AI	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CI_AI_KS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CI_AI_KS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AI_KS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CI_AI_KS_WS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CI_AI_KS_WS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AI_KS_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CI_AI_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AI_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CI_AI_WS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CI_AI_WS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AI_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CI_AS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CI_AS_KS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CI_AS_KS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AS_KS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CI_AS_KS_WS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CI_AS_KS_WS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AS_KS_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CI_AS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CI_AS_WS	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CI_AS_WS_SC	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CI_AS_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CS_AI	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CS_AI_KS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CS_AI_KS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AI_KS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CS_AI_KS_WS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CS_AI_KS_WS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AI_KS_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CS_AI_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AI_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CS_AI_WS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CS_AI_WS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AI_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CS_AS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CS_AS_KS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Bushu_Kakusu_100_CS_AS_KS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AS_KS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CS_AS_KS_WS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CS_AS_KS_WS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AS_KS_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CS_AS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_Bushu_Kakusu_100_CS_AS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_100_CS_AS_WS	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Bushu_Kakusu_100_CS_AS_WS_SC	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_100_CS_AS_WS_SC_UTF8	Japanese-Bushu-Kakusu-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_Bushu_Kakusu_140_BIN	Japanese-Bushu-Kakusu-140, clasificación binaria
Japanese_Bushu_Kakusu_140_BIN2	Japanese-Bushu-Kakusu-140, clasificación de comparación de punto de código binario
Japanese_Bushu_Kakusu_140_CI_AI	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_KS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_KS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AI_KS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CI_AI_KS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AI_KS_WS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_KS_WS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AI_KS_WS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_KS_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AI_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CI_AI_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AI_WS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_WS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AI_WS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AI_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CI_AS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_KS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_KS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japonés_Bushu_Kakusu_140_CI_AS_KS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_KS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AS_KS_WS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CI_AS_KS_WS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AS_KS_WS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_KS_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CI_AS_WS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_WS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CI_AS_WS_VSS	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CI_AS_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AI_KS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CS_AI_KS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI_KS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AI_KS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI_KS_WS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AI_KS_WS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI_KS_WS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CS_AI_KS_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AI_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AI_WS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AI_WS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CS_AI_WS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AI_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_KS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_KS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS_KS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CS_AS_KS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS_KS_WS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_KS_WS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS_KS_WS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_KS_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_Bushu_Kakusu_140_CS_AS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS_WS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_WS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_Bushu_Kakusu_140_CS_AS_WS_VSS	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_Bushu_Kakusu_140_CS_AS_WS_VSS_UTF8	Japanese-Bushu-Kakusu-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_CI_AI	Japonés, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_CI_AI_KS	Japonés, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_CI_AI_KS_WS	Japonés, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_CI_AI_WS	Japonés, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_CI_AS	Japonés, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Japanese_CI_AS_KS	Japonés, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_CI_AS_KS_WS	Japonés, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_CI_AS_WS	Japonés, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_CS_AI	Japonés, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_CS_AI_KS	Japonés, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_CS_AI_KS_WS	Japonés, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_CS_AI_WS	Japonés, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_CS_AS	Japonés, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Japanese_CS_AS_KS	Japonés, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_CS_AS_KS_WS	Japonés, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_CS_AS_WS	Japonés, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Unicode_BIN	Japanese-Unicode, clasificación binaria
Japanese_Unicode_BIN2	Japanese-Unicode, clasificación de comparación de punto de código binario
Japanese_Unicode_CI_AI	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_Unicode_CI_AI_KS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Unicode_CI_AI_KS_WS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Unicode_CI_AI_WS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Unicode_CI_AS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_Unicode_CI_AS_KS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Unicode_CI_AS_KS_WS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Unicode_CI_AS_WS	Japanese-Unicode, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Unicode_CS_AI	Japanese-Unicode, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_Unicode_CS_AI_KS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Unicode_CS_AI_KS_WS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Unicode_CS_AI_WS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_Unicode_CS_AS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_Unicode_CS_AS_KS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_Unicode_CS_AS_KS_WS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_Unicode_CS_AS_WS	Japanese-Unicode, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_XJIS_100_BIN	Japanese-XJIS-100, clasificación binaria
Japanese_XJIS_100_BIN2	Japanese-XJIS-100, clasificación de comparación de código binario
Japanese_XJIS_100_CI_AI	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CI_AI_KS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_XJIS_100_CI_AI_KS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_XJIS_100_CI_AI_KS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AI_KS_WS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_XJIS_100_CI_AI_KS_WS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_XJIS_100_CI_AI_KS_WS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AI_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CI_AI_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AI_WS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_XJIS_100_CI_AI_WS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_XJIS_100_CI_AI_WS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_XJIS_100_CI_AS_KS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_XJIS_100_CI_AS_KS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CI_AS_KS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AS_KS_WS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_XJIS_100_CI_AS_KS_WS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_XJIS_100_CI_AS_KS_WS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_XJIS_100_CI_AS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CI_AS_WS	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CI_AS_WS_SC	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_XJIS_100_CI_AS_WS_SC_UTF8	Japanese-XJIS-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AI	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_XJIS_100_CS_AI_KS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Japanese_XJIS_100_CS_AI_KS_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_XJIS_100_CS_AI_KS_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AI_KS_WS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura
Japanese_XJIS_100_CS_AI_KS_WS_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CS_AI_KS_WS_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AI_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_XJIS_100_CS_AI_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AI_WS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_XJIS_100_CS_AI_WS_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_XJIS_100_CS_AI_WS_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura
Japanese_XJIS_100_CS_AS_KS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CS_AS_KS_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_XJIS_100_CS_AS_KS_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AS_KS_WS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Japanese_XJIS_100_CS_AS_KS_WS_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales
Japanese_XJIS_100_CS_AS_KS_WS_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, UTF8
Japanese_XJIS_100_CS_AS_SC	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales
Japanese_XJIS_100_CS_AS_SC_UTF8	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8

Collation (Intercalación)	Descripción
Japanese_XJIS_100_CS_AS_WS	Japanese-XJIS-100, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Japanese_XJIS_140_BIN	Japanese-XJIS-140, clasificación binaria
Japanese_XJIS_140_BIN2	Japanese-XJIS-140, clasificación de comparación de código binario
Japanese_XJIS_140_CI_AI	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CI_AI_KS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CI_AI_KS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AI_KS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CI_AI_KS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CI_AI_KS_WS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CI_AI_KS_WS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AI_KS_WS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_XJIS_140_CI_AI_KS_WS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AI_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CI_AI_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CI_AI_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CI_AI_WS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CI_AI_WS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AI_WS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_XJIS_140_CI_AI_WS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CI_AS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres suplementarios, no distingue selectores de variación
Japanese_XJIS_140_CI_AS_KS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CI_AS_KS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AS_KS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres suplementarios, no distingue selectores de variaciones
Japanese_XJIS_140_CI_AS_KS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CI_AS_KS_WS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CI_AS_KS_WS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AS_KS_WS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CI_AS_KS_WS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CI_AS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres suplementarios, no distingue selectores de variaciones
Japanese_XJIS_140_CI_AS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CI_AS_WS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CI_AS_WS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CI_AS_WS_VSS	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CI_AS_WS_VSS_UTF8	Japanese-XJIS-140, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AI	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CS_AI_KS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CS_AI_KS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CS_AI_KS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CS_AI_KS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AI_KS_WS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CS_AI_KS_WS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CS_AI_KS_WS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CS_AI_KS_WS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_XJIS_140_CS_AI_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CS_AI_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CS_AI_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AI_WS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CS_AI_WS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CS_AI_WS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación
Japanese_XJIS_140_CS_AI_WS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variación, UTF8
Japanese_XJIS_140_CS_AS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CS_AS_KS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación
Japanese_XJIS_140_CS_AS_KS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8
Japanese_XJIS_140_CS_AS_KS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CS_AS_KS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AS_KS_WS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variaciones
Japanese_XJIS_140_CS_AS_KS_WS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AS_KS_WS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CS_AS_KS_WS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, no distingue selectores de variación, UTF8

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CS_AS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CS_AS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AS_WS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variaciones
Japanese_XJIS_140_CS_AS_WS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, no distingue selectores de variaciones, UTF8
Japanese_XJIS_140_CS_AS_WS_VSS	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones
Japanese_XJIS_140_CS_AS_WS_VSS_UTF8	Japanese-XJIS-140, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura, caracteres adicionales, distingue selectores de variaciones, UTF8

Collation (Intercalación)	Descripción
Korean_Wansung_CI_AS	Coreano (Wansung), distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_100_BIN	Latin1-General-100, orden binario
Latin1_General_100_BIN2	Latin1-General-100, orden de comparación de punto de código binario
Latin1_General_100_BIN2_UTF8	Latin1-General-100, clasificación de comparación de punto de código binario, UTF8
Latin1_General_100_CI_AS	Latin1 general 100, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_100_CI_AS_SC_UTF8	Latin1-General-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres adicionales, UTF8
Latin1_General_BIN	Latín 1 general, orden binario
Latin1_General_BIN2	Latin1-General, orden de comparación de punto de código binario
Latin1_General_CI_AI	Latín 1 general, no distingue entre mayúsculas y minúsculas, acentos, tipos de kana ni anchura
Latin1_General_CI_AS	Latín 1 general, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_CI_AS_KS	Latín1-General, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura

Collation (Intercalación)	Descripción
Latin1_General_CS_AS	Latín 1 general, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana ni anchura
Modern_Spanish_CI_AS	Español moderno, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
SQL_1xCompat_CP850_CI_AS	Latín1-General, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 49 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_CP1_CI_AI	Latín 1 general, no distingue entre mayúscula s y minúsculas, acentos, tipos de kana ni anchura para datos Unicode; orden de clasifica ción 54 de SQL Server en la página de códigos 1252 para datos que no son Unicode
SQL_Latin1_General_CP1_CI_AS	Latín 1 general, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 52 de SQL Server en la página de códigos 1252 para datos que no son Unicode
SQL_Latin1_General_CP1_CS_AS	Latín 1 general, distingue acentos y entre mayúsculas y minúsculas y no distingue tipos de kana ni anchura para datos Unicode; orden de clasificación 51 de SQL Server en la página de códigos 1252 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP1250_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 82 de SQL Server en la página de códigos 1250 para datos que no son Unicode
SQL_Latin1_General_CP1250_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 81 de SQL Server en la página de códigos 1250 para datos que no son Unicode
SQL_Latin1_General_CP1251_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 106 de SQL Server en la página de códigos 1251 para datos que no son Unicode
SQL_Latin1_General_CP1251_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 105 de SQL Server en la página de códigos 1251 para datos que no son Unicode
SQL_Latin1_General_CP1253_CI_AI	Latin1-General, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 124 de SQL Server en la página de códigos 1253 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP1253_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 114 de SQL Server en la página de códigos 1253 para datos que no son Unicode
SQL_Latin1_General_CP1253_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 113 de SQL Server en la página de códigos 1253 para datos que no son Unicode
SQL_Latin1_General_CP1254_CI_AS	Turco, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 130 de SQL Server en la página de códigos 1254 para datos que no son Unicode
SQL_Latin1_General_CP1254_CS_AS	Turco, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 129 de SQL Server en la página de códigos 1254 para datos que no son Unicode
SQL_Latin1_General_CP1255_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 138 de SQL Server en la página de códigos 1255 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP1255_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 137 de SQL Server en la página de códigos 1255 para datos que no son Unicode
SQL_Latin1_General_CP1256_CI_AS	Latín1-General, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 146 de SQL Server en la página de códigos 1256 para datos que no son Unicode
SQL_Latin1_General_CP1256_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 145 de SQL Server en la página de códigos 1256 para datos que no son Unicode
SQL_Latin1_General_CP1257_CI_AS	Latin1-General, no distingue entre mayúscula s y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 154 de SQL Server en la página de códigos 1257 para datos que no son Unicode
SQL_Latin1_General_CP1257_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 153 de SQL Server en la página de códigos 1257 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP437_BIN	Latin1-General, clasificación binaria para datos Unicode, orden de clasificación 30 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_CP437_BIN2	Latin1-General, clasificación de comparación de punto de código binario para datos Unicode, orden de clasificación 30 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_CP437_CI_AI	Latín 1 general, no distingue entre mayúscula s y minúsculas, acentos, tipos de kana ni anchura para datos Unicode; orden de clasifica ción 34 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_CP437_CI_AS	Latin1-General, no distingue entre mayúscula s y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 32 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_CP437_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 31 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_CP850_BIN	Latin1-General, clasificación binaria para datos Unicode, orden de clasificación 40 de SQL Server en la página de códigos 850 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP850_BIN2	Latín 1 general, clasificación de comparación de punto de código binario para datos Unicode, orden de clasificación 40 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_CP850_CI_AI	Latín 1 general, no distingue entre mayúsculas y minúsculas, acentos, tipos de kana ni anchura para datos Unicode; orden de clasificación 44 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_CP850_CI_AS	Latín 1 general, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 42 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_CP850_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 41 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_Pref_CP1_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 53 de SQL Server en la página de códigos 1252 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_Pref_CP437_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 33 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_Pref_CP850_CI_AS	Latin1-General, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 43 de SQL Server en la página de códigos 850 para datos que no son Unicode
Thai_CI_AS	Tailandés, no distingue entre mayúsculas y minúsculas, no distingue acentos, tipos de kana ni anchura

Zona horaria local para las instancias de base de datos de RDS Custom para SQL Server

La zona horaria de una instancia de base de datos de RDS Custom para SQL Server se define de forma predeterminada. El valor predeterminado actual es la Hora universal coordinada (UTC). Si lo prefiere, puede definir la zona horaria de su instancia de base de datos en una hora local para que coincida con la zona horaria de sus aplicaciones.

La zona horaria se define al crear inicialmente la instancia de base de datos. Puede crear su instancia de base de datos con la AWS Management Console, la acción CreateDBInstance de la API de Amazon RDS o con el comando de la AWS CLI create-db-instance.

Si su instancia de base de datos forma parte de una implementación Multi-AZ, al conmutar por error, la zona horaria seguirá siendo la zona horaria local que definió.

Cuando solicite una restauración a un momento dado, debe especificar la hora a la que desea restaurar. La hora se muestra en la zona horaria local. Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

A continuación se indican las limitaciones de la definición de la hora local en una instancia de base de datos:

- Puede configurar la zona horaria de una instancia de base de datos durante la creación de la instancia, pero no puede modificar la zona horaria de una instancia de base de datos de RDS Custom para SQL Server existente.
- Si se modifica la zona horaria de una instancia de base de datos de RDS Custom para SQL Server existente, RDS Custom cambia el estado de la instancia de base de datos a `unsupported-configuration` y envía notificaciones de eventos.
- No puede restaurar una instantánea a partir de una instancia de base de datos de una zona horaria en una instancia de base de datos de una zona horaria diferente.
- Es recomendable que no restaure un archivo de copia de seguridad de una zona horaria en una zona horaria diferente. Si restaura un archivo de copia de seguridad de una zona horaria en otra zona horaria distinta, debe auditar las consultas y las aplicaciones para comprobar los efectos del cambio de zona horaria. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Zonas horarias admitidas

Puede definir su zona horaria local en uno de los valores que se muestran en la siguiente tabla.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Afganistán	(UTC+04:30)	Kabul	Esta zona horaria no aplica el horario de verano.
Hora estándar de Alaska	(UTC–09:00)	Alaska	
Hora estándar de las Islas Aleutianas	(UTC–10:00)	Islas Aleutianas	
Hora estándar de Altai	(UTC+07:00)	Barnaul, Gorno-Altaisk	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar árabe	(UTC+03:00)	Kuwait, Riad	Esta zona horaria no aplica el horario de verano.
Hora estándar árabe	(UTC+04:00)	Abu Dabi, Muscat	
Hora estándar arábica	(UTC+03:00)	Bagdad	Esta zona horaria no aplica el horario de verano.
Hora estándar de Argentina	(UTC–03:00)	Ciudad de Buenos Aires	Esta zona horaria no aplica el horario de verano.
Hora estándar de Astracán	(UTC+04:00)	Astracán, Uliánovsk	
Hora estándar del Atlántico	(UTC–04:00)	Hora del Atlántico (Canadá)	
Hora estándar central de Australia	(UTC+09:30)	Darwin	Esta zona horaria no aplica el horario de verano.
Hora estándar del centro-oeste de Australia	(UTC+08:45)	Eucla	
Hora estándar de Australia oriental	(UTC+10:00)	Canberra, Melbourne, Sídney	
Hora estándar de Azerbaiyán	(UTC+04:00)	Bakú	
Hora estándar de las Azores	(UTC–01:00)	Azores	
Hora estándar de Bahía	(UTC–03:00)	Salvador	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Bangladesh	(UTC+06:00)	Dacca	Esta zona horaria no aplica el horario de verano.
Hora estándar de Bielorrusia	(UTC+03:00)	Minsk	Esta zona horaria no aplica el horario de verano.
Hora estándar de Bougainville	(UTC+11:00)	Isla Bougainville	
Hora estándar central de Canadá	(UTC–06:00)	Saskatchewan	Esta zona horaria no aplica el horario de verano.
Hora estándar de Cabo Verde	(UTC–01:00)	Archipiélago de Cabo Verde	Esta zona horaria no aplica el horario de verano.
Hora estándar del Cáucaso	(UTC+04:00)	Ereván	
Hora estándar de Australia central	(UTC+09:30)	Adelaida	
Hora estándar de América central	(UTC–06:00)	América Central	Esta zona horaria no aplica el horario de verano.
Hora estándar de Asia central	(UTC+06:00)	Astana	Esta zona horaria no aplica el horario de verano.
Hora estándar de Brasil central	(UTC–04:00)	Cuiaba	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Europa central	(UTC+01:00)	Belgrado, Bratislava, Budapest, Liubliana, Praga	
Hora estándar europea central	(UTC+01:00)	Sarajevo, Skopie, Varsovia, Zagreb	
Hora estándar del Pacífico central	(UTC+11:00)	Islas Salomón, Nueva Caledonia	Esta zona horaria no aplica el horario de verano.
Hora estándar central	(UTC–06:00)	Hora central (Estados Unidos y Canadá)	
Hora estándar central (México)	(UTC–06:00)	Guadalajara, Ciudad de México, Monterrey	
Hora estándar de las islas Chatham	(UTC+12:45)	Islas Chatham	
Hora estándar de China	(UTC+08:00)	Pekín, Chongqing, Hong Kong, Urumchi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Cuba	(UTC–05:00)	Habana	
Hora estándar de línea de fecha	(UTC–12:00)	Línea internacional de cambio de fecha del oeste	Esta zona horaria no aplica el horario de verano.
Hora estándar de África oriental	(UTC+03:00)	Nairobi	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Australia oriental	(UTC+10:00)	Brisbane	Esta zona horaria no aplica el horario de verano.
Hora estándar de Europa oriental	(UTC+02:00)	Chisinau	
Hora estándar de América del Sur oriental	(UTC–03:00)	Brasilia	
Hora estándar de la Isla de Pascua	(UTC–06:00)	Isla de Pascua	
Hora estándar oriental	(UTC–05:00)	Hora oriental (Estados Unidos y Canadá)	
Hora estándar oriental (México)	(UTC–05:00)	Chetumal	
Hora estándar de Egipto	(UTC+02:00)	El Cairo	
Hora estándar de Ekaterimburgo	(UTC+05:00)	Ekaterimburgo	
Hora estándar de Fiyi	(UTC+12:00)	Fiyi	
Hora estándar de FLE	(UTC+02:00)	Helsinki, Kiev, Riga, Sofía, Tallin, Vilna	
Hora estándar de Georgia	(UTC+04:00)	Tiflis	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar GMT	(UTC)	Dublín, Edimburgo, Lisboa, Londres	Esta zona horaria no es la misma que la hora media de Greenwich. Esta zona horaria aplica el horario de verano.
Hora estándar de Groenlandia	(UTC–03:00)	Groenlandia	
Hora estándar de Greenwich	(UTC)	Monrovia, Reikiavik	Esta zona horaria no aplica el horario de verano.
Hora estándar GTB	(UTC+02:00)	Atenas, Bucarest	
Hora estándar de Haití	(UTC–05:00)	Haití	
Hora estándar de Hawái	(UTC–10:00)	Hawái	
Hora estándar de India	(UTC+05:30)	Chennai, Calcuta, Mumbai, Nueva Delhi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Irán	(UTC+03:30)	Teherán	
Hora estándar de Israel	(UTC+02:00)	Jerusalén	
Hora estándar de Jordania	(UTC+02:00)	Amán	
Hora estándar de Kaliningrado	(UTC+02:00)	Kaliningrado	
Hora estándar de Kamchatka	(UTC+12:00)	Petropavlovsk-Kamchatsky – Antiguo	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Corea	(UTC+09:00)	Seúl	Esta zona horaria no aplica el horario de verano.
Hora estándar de Libia	(UTC+02:00)	Trípoli	
Hora estándar de las Islas de la Línea	(UTC+14:00)	Isla Kiritimati	
Hora estándar de Lord Howe	(UTC+10:30)	Isla Lord Howe	
Hora estándar de Magadán	(UTC+11:00)	Magadán	Esta zona horaria no aplica el horario de verano.
Hora estándar de Magallanes	(UTC–03:00)	Punta Arenas	
Hora estándar de Marquesas	(UTC–09:30)	Islas Marquesas	
Hora estándar de Mauricio	(UTC+04:00)	Port-Louis	Esta zona horaria no aplica el horario de verano.
Hora estándar de Oriente Medio	(UTC+02:00)	Beirut	
Hora estándar de Montevideo	(UTC–03:00)	Montevideo	
Hora estándar de Marruecos	(UTC+01:00)	Casablanca	
Hora estándar de las montañas	(UTC–07:00)	Hora de las montañas (Estados Unidos y Canadá)	
Hora estándar de las montañas (México)	(UTC–07:00)	Chihuahua, La Paz, Mazatlán	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Myanmar	(UTC+06:30)	Yangón (Rangún)	Esta zona horaria no aplica el horario de verano.
Hora estándar de Asia central norte	(UTC+07:00)	Novosibirsk	
Hora estándar de Namibia	(UTC+02:00)	Windhoek	
Hora estándar de Nepal	(UTC+05:45)	Katmandú	Esta zona horaria no aplica el horario de verano.
Hora estándar de Nueva Zelanda	(UTC+12:00)	Auckland, Wellington	
Hora estándar de Terranova	(UTC–03:30)	Terranova	
Hora estándar de Norfolk	(UTC+11:00)	Isla Norfolk	
Hora estándar del este de Asia del Norte	(UTC+08:00)	Irkutsk	
Hora estándar del norte de Asia	(UTC+07:00)	Krasnoyarsk	
Hora estándar de Corea del Norte	(UTC+09:00)	Pyongyang	
Hora estándar de Omsk	(UTC+06:00)	Omsk	
Hora estándar de Sudamérica del Pacífico	(UTC–03:00)	Santiago	
Hora estándar del Pacífico	(UTC–08:00)	Hora del Pacífico (Estados Unidos y Canadá)	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar del Pacífico (México)	(UTC–08:00)	Baja California	
Hora estándar de Pakistán	(UTC+05:00)	Islamabad, Karachi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Paraguay	(UTC–04:00)	Asunción	
Hora estándar romance	(UTC+01:00)	Bruselas, Copenhague, Madrid, París	
Zona horaria 10 de Rusia	(UTC+11:00)	Chokurdakh	
Zona horaria 11 de Rusia	(UTC+12:00)	Anadyr, Petropavlovsk-Kamchatsky	
Zona horaria 3 de Rusia	(UTC+04:00)	Izhevsk, Samara	
Hora estándar de Rusia	(UTC+03:00)	Moscú, San Petersburgo, Volgogrado	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudamérica oriental	(UTC–03:00)	Cayena, Fortaleza	Esta zona horaria no aplica el horario de verano.
Hora estándar del Pacífico de Sudamérica	(UTC–05:00)	Bogotá, Lima, Quito, Río Branco	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudamérica occidental	(UTC–04:00)	Georgetown, La Paz, Manaos, San Juan	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de San Pedro	(UTC–03:00)	San Pedro y Miquelón	
Hora estándar de Sajalín	(UTC+11:00)	Sajalín	
Hora estándar de Samoa	(UTC+13:00)	Samoa	
Hora estándar de Santo Tomé	(UTC+01:00)	Santo Tomé	
Hora estándar de Sarátov	(UTC+04:00)	Sarátov	
Hora estándar del sureste de Asia	(UTC+07:00)	Bangkok, Hanói, Yakarta	Esta zona horaria no aplica el horario de verano.
Hora estándar de Singapur	(UTC+08:00)	Kuala Lumpur, Singapur	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudáfrica	(UTC+02:00)	Harare (Pretoria)	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sri Lanka	(UTC+05:30)	Sri Jayawarde nepura	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudán	(UTC+02:00)	Jartum	
Hora estándar de Siria	(UTC+02:00)	Damasco	
Hora estándar de Taipéi	(UTC+08:00)	Taipéi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Tasmania	(UTC+10:00)	Hobart	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Tocantins	(UTC–03:00)	Araguaina	
Hora estándar de Tokio	(UTC+09:00)	Osaka, Sapporo, Tokio	Esta zona horaria no aplica el horario de verano.
Hora estándar de Tomsk	(UTC+07:00)	Tomsk	
Hora estándar de Tonga	(UTC+13:00)	Nuku'alofa	Esta zona horaria no aplica el horario de verano.
Hora estándar de Transbaikal	(UTC+09:00)	Chita	
Hora estándar de Turquía	(UTC+03:00)	Estambul	
Hora estándar de Islas Turcas y Caicos	(UTC–05:00)	Islas Turcas y Caicos	
Hora estándar de Ulán Bator	(UTC+08:00)	Ulán Bator	Esta zona horaria no aplica el horario de verano.
Hora estándar oriental de Estados Unidos	(UTC–05:00)	Indiana (Este)	
Hora estándar de las montañas (Estados Unidos)	(UTC–07:00)	Arizona	Esta zona horaria no aplica el horario de verano.
UTC	UTC	Horario universal coordinado	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
UTC–02	(UTC–02:00)	Horario universal coordinado–02	Esta zona horaria no aplica el horario de verano.
UTC–08	(UTC–08:00)	Horario universal coordinado–08	
UTC–09	(UTC–09:00)	Horario universal coordinado–09	
UTC–11	(UTC–11:00)	Horario universal coordinado–11	Esta zona horaria no aplica el horario de verano.
UTC+12	(UTC+12:00)	Horario universal coordinado+12	Esta zona horaria no aplica el horario de verano.
UTC+13	(UTC+13:00)	Horario universal coordinado+13	
Hora estándar de Venezuela	(UTC–04:00)	Caracas	Esta zona horaria no aplica el horario de verano.
Hora estándar de Vladivostok	(UTC+10:00)	Vladivostok	
Hora estándar de Volgogrado	(UTC+04:00)	Volgogrado	
Hora estándar de Australia occidental	(UTC+08:00)	Perth	Esta zona horaria no aplica el horario de verano.
Hora estándar de África central occidental	(UTC+01:00)	África central occidental	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Europa occidental	(UTC+01:00)	Ámsterdam, Berlín, Berna, Roma, Estocolmo, Viena	
Hora estándar de Mongolia occidental	(UTC+07:00)	Hovd	
Hora estándar de Asia occidental	(UTC+05:00)	Ashgabat, Tashkent	Esta zona horaria no aplica el horario de verano.
Hora estándar de Cisjordania	(UTC+02:00)	Gaza, Hebrón	
Hora estándar del Pacífico occidental	(UTC+10:00)	Guam, Port Moresby	Esta zona horaria no aplica el horario de verano.
Hora estándar de Yakutsk	(UTC+09:00)	Yakutsk	

Uso de una clave maestra de servicio con RDS Custom para SQL Server

RDS Custom para SQL Server admite el uso de una clave maestra de servicio (SMK). RDS Custom conserva la misma SMK durante toda la vida útil de su instancia de base de datos de RDS Custom para SQL Server. Al conservar la misma SMK, la instancia de base de datos puede utilizar objetos cifrados con la SMK, como contraseñas y credenciales de servidores vinculados. Si utiliza una Implementación multi-AZ, RDS Custom también sincroniza y mantiene la SMK entre la instancia de base de datos principal y la secundaria.

Temas

- Disponibilidad en regiones y versiones
- Características admitidas
- Uso de TDE
- Configuración de características
- Requisitos y limitaciones

Disponibilidad en regiones y versiones

El uso de una SMK se admite en todas las regiones en las que está disponible RDS Custom para SQL Server, para todas las versiones de SQL Server disponibles en RDS Custom. Para obtener más información sobre la disponibilidad en versiones y regiones de RDS con Amazon RDS Custom para SQL Server, consulte Regiones y motores de base de datos admitidos para RDS Custom para SQL Server.

Características admitidas

Cuando se utiliza una SMK con RDS Custom para SQL Server, se admiten las siguientes funciones:

- Cifrado de datos transparente (TDE)
- Cifrado en el nivel de columna
- Correo electrónico de base de datos
- Servidores vinculados
- SQL Server Integration Services (SSIS)

Uso de TDE

Una SMK permite configurar el Cifrado de Datos Transparente (TDE), que cifra los datos antes de que se escriban en el sistema de almacenamiento y los descifra automáticamente cuando se leen desde el almacenamiento. A diferencia de RDS para SQL Server, para configurar el TDE en una instancia de base de datos de RDS Custom para SQL Server no es necesario utilizar grupos de opciones. En su lugar, una vez que haya creado un certificado y una clave de cifrado de base de datos, puede ejecutar el siguiente comando para activar el TDE en el nivel de base de datos:

```
ALTER DATABASE [myDatabase] SET ENCRYPTION ON;
```

Para obtener más información sobre el uso de TDE con RDS para SQL Server, consulte Compatibilidad con el Cifrado de datos transparente en SQL Server.

Para obtener información detallada sobre el TDE en Microsoft SQL Server, consulte Cifrado de datos transparente en la documentación de Microsoft.

Configuración de características

Para ver los pasos detallados sobre la configuración de las características que utilizan una SMK con RDS Custom para SQL Server, puede utilizar las siguientes publicaciones del blog de bases de datos de Amazon RDS:

- Servidores vinculados: Configuración de servidores vinculados en RDS Custom para SQL Server.
- SSIS: Migración de paquetes de SSIS a RDS Custom para SQL Server.
- TDE: Protección de sus datos con TDE en RDS Custom para SQL Server.

Requisitos y limitaciones

Cuando utilice una SMK con una instancia de base de datos de RDS Custom para SQL Server, tenga en cuenta los siguientes requisitos y limitaciones:

- Si vuelve a generar la SMK en la instancia de base de datos, debe realizar inmediatamente una instantánea de base de datos manual. Si es posible, le recomendamos que evite volver a generar la SMK.
- Debe mantener copias de seguridad de los certificados del servidor y de las contraseñas de las claves maestras de la base de datos. Si no mantiene copias de seguridad de estas, puede provocar la pérdida de datos.
- Si configura SSIS, debe utilizar un documento SSM para unir la instancia de base de datos de RDS Custom para SQL Server al dominio en caso de una sustitución de computación a escala o el host.
- Cuando el TDE o el cifrado en el nivel de columna están activados, las copias de seguridad de las bases de datos se cifran automáticamente. Al realizar una restauración de instantáneas o una recuperación puntual, se restaura la SMK de la instancia de base de datos de origen para descifrar los datos de la restauración y se genera una nueva SMK para volver a cifrar los datos de la instancia restaurada.

Para obtener más información sobre las claves maestras de servicio en Microsoft SQL Server, consulte Claves de cifrado de SQL Server y bases de datos en la documentación de Microsoft.

Compatibilidad de captura de datos de cambios (CDC) con RDS Custom para SQL Server

Descripción general

RDS Custom para SQL Server ofrece compatibilidad nativa para la captura de datos de cambios (CDC), lo que le permite rastrear y capturar las modificaciones de los datos en las tablas de SQL Server. CDC almacena metadatos detallados sobre estos cambios para su posterior recuperación y análisis. Para obtener más información sobre la funcionalidad de CDC, consulte Captura de datos de cambios en la documentación de Microsoft.

El funcionamiento de CDC en SQL Server requiere que coincidan los valores entre el servidor local (que tiene `server_id` = 0) en `sys.servers` y los identificadores de `SERVERPROPERTY('ServerName')`. RDS Custom para SQL Server mantiene automáticamente esta sincronización durante todo el ciclo de vida de la instancia para garantizar el funcionamiento continuo de CDC, incluso si los hosts se sustituyen durante las operaciones de mantenimiento o recuperación.

> **Important**
>
> Tras una conmutación por error de una instancia multi-AZ, la función `SERVERPROPERTY('Servername')` refleja automáticamente los cambios en el nombre de la red o el equipo. Sin embargo, la función `@@SERVERNAME` retiene el nombre del servidor anterior hasta que se reinicie el servicio de `MSSQLSERVER`. La consulta de @@SERVERNAME devuelve el nombre del servidor anterior tras una conmutación por error. Para obtener el nombre de servidor preciso después de una conmutación por error, utilice la siguiente consulta SQL:
>
> ```
> SELECT name FROM sys.servers WHERE server_id=0
> ```
>
> Esta consulta proporciona la información de nombre de servidor más actualizada sin necesidad de reiniciar un servicio.

Disponibilidad en regiones y versiones

La funcionalidad CDC se admite en todas las Regiones de AWS en las que está disponible RDS Custom para SQL Server, para todas las versiones de SQL Server compatibles con RDS Custom.

Para obtener más información sobre la disponibilidad de versiones y regiones compatibles de RDS Custom para SQL Server, consulte Regiones y motores de base de datos admitidos para RDS Custom para SQL Server.

Requisitos y limitaciones

Cuando implemente CDC en RDS Custom para SQL Server, tenga en cuenta las siguientes consideraciones clave:

- Si configura manualmente `@@SERVERNAME` o el servidor local en `sys.servers` para utilizar características como replicación de MS, si el valor del servidor local (que tiene `server_id = 0`) en `sys.servers` está establecido en un formato que coincide con `*.rds.amazonaws.com` o `*.awsrds.*.com`, RDS Custom para SQL Server no intenta modificarlo para que coincida con `SERVERPROPERTY('ServerName')`.
- RDS no puede modificar el servidor local (que tiene `server_id = 0`) en `sys.servers` a un nuevo nombre de host mientras los inicios de sesión remotos o los servidores vinculados utilicen activamente el nombre de host anterior. Esta limitación se aplica en dos escenarios:
  - Cuando un servidor vinculado establece una conexión con el servidor local mediante un inicio de sesión remoto asociado al nombre de host anterior.
  - Cuando una instancia de RDS Custom para SQL Server actúa como publicadora o distribuidora y tiene inicios de sesión vinculados asociados al nombre de host anterior en sus instancias de suscriptor.

Solución de problemas

Para identificar los inicios de sesión remotos o los inicios de sesión vinculados asociados al nombre del servidor anterior, utilice las siguientes consultas. Valide los resultados y elimine estos inicios de sesión para garantizar el correcto funcionamiento de CDC.

```
SELECT * FROM sys.remote_logins WHERE server_id=0
```

o

```
select sss.srvname,ssp.name,srl.remote_name  from sys.server_principals ssp
inner join sys.remote_logins srl on srl.local_principal_id=ssp.principal_id
inner join sys.sysservers sss  on srl.server_id = sss.srvid
where sss.srvname = @@SERVERNAME
```

Configuración del entorno para Amazon RDS Custom for SQL Server

Antes de crear y administrar una instancia de base de datos para la instancia de base de datos de Amazon RDS Custom for SQL Server, asegúrese de realizar las siguientes tareas.

Contenido

- Requisitos previos para configurar RDS Custom for SQL Server
  - Creación automática de perfiles de instancias mediante la AWS Management Console
- Paseo 1: concesión de los permisos necesarios a la entidad principal de IAM
- Paso 2: configuración de la red, perfil de instancia y cifrado
  - Configuración con AWS CloudFormation
    - Parámetros requeridos por CloudFormation
    - Descarga del archivo de plantilla AWS CloudFormation
    - Configuración de recursos mediante CloudFormation
  - Configuración manual
    - Asegúrese de que tiene una clave de cifrado simétrica AWS KMS
    - Creación manual del Rol de IAM y el perfil de instancias
      - Creación del Rol de IAM de AWSRDSCustomSQLServerInstanceRole
      - Agregar una política de acceso a AWSRDSCustomSQLServerInstanceRole
      - Cree su perfil de instancias de RDS Custom for SQL Server
      - Agregue AWSRDSCustomSQLServerInstanceRole a su perfil de instancias de RDS Custom for SQL Server
    - Configuración manual de la VPC
      - Configure los grupos de seguridad de la VPC
      - Configuración de puntos de conexión para los Servicios de AWS dependientes
      - Configurar el servicio de metadatos de instancia
- Restricciones entre instancias

> **Note**
>
> Para ver un tutorial paso a paso sobre cómo configurar los requisitos previos e iniciar Amazon RDS Custom para SQL Server, consulte Get started with Amazon RDS Custom for

SQL Server using an CloudFormation template (Network setup) y Explore the prerequisites required to create an Amazon RDS Custom for SQL Server instance.

Requisitos previos para configurar RDS Custom for SQL Server

Antes de crear una instancia de base de datos de RDS Custom para SQL Server, asegúrese de que su entorno cumple los requisitos descritos en este tema. También puede usar la plantilla de CloudFormation para configurar los requisitos previos en su Cuenta de AWS. Para obtener más información, consulte Configuración con AWS CloudFormation

RDS Custom para SQL Server requiere que configure los siguientes requisitos previos:

- Configure los permisos de AWS Identity and Access Management (IAM) necesarios para la creación de instancias. Es el usuario o rol de AWS Identity and Access Management (IAM) necesario para realizar una solicitud `create-db-instance` a RDS.
- Configure los recursos de requisitos previos que requiere la instancia de base de datos de RDS Custom para SQL Server:
  - Configure la clave de AWS KMS necesaria para el cifrado de la instancia de RDS Custom. RDS Custom requiere una clave administrada por el cliente en el momento de la creación de la instancia para el cifrado. El ARN de la clave de KMS, el ID, el alias de ARN o el nombre de alias se transmiten como parámetro `kms-key-id` en la solicitud para crear la instancia de base de datos de RDS Custom.
  - Configure los permisos necesarios en la instancia de base de datos de RDS Custom para SQL Server. RDS Custom adjunta un perfil de instancia a la instancia de base de datos en el momento de la creación y lo utiliza para la automatización dentro de la instancia de base de datos. El nombre del perfil de la instancia se establece en `custom-iam-instance-profile` en la solicitud de creación de RDS Custom. Puede crear un perfil de instancia desde la AWS Management Console o crear su perfil de instancia de forma manual. Para obtener más información, consulte Creación automática de perfiles de instancias mediante la AWS Management Console y Creación manual del Rol de IAM y el perfil de instancias.
  - Configure los ajustes de red de acuerdo con los requisitos de RDS Custom para SQL Server. Las instancias de RDS Custom residen en las subredes (configuradas con el grupo de subredes de base de datos) que proporciona al crear la instancia. Estas subredes deben permitir que las instancias de RDS Custom se comuniquen con los servicios necesarios para la automatización de RDS.

> **Note**
>
> Para cumplir con los requisitos mencionados antes, asegúrese de que no haya políticas de control de servicios (SCP) que restrinjan los permisos en el nivel de cuenta.
> Si la cuenta que está utilizando forma parte de una organización de AWS, es posible que tenga políticas de control de servicio (SCP) que restrinjan los permisos en el nivel de cuenta. Asegúrese de que las SCP no restrinjan los permisos de los usuarios y los roles que cree mediante los siguientes procedimientos.
> Para obtener más información acerca de las SCP, consulte Políticas de control de servicios (SCP) en la Guía del usuario de AWS Organizations. Utilice el comando describe-organization de la AWS CLI para comprobar si su cuenta forma parte de una organización de AWS.
> Para obtener más información acerca de AWS Organizations, consulte ¿Qué es AWS Organizations? en la Guía del usuario de AWS Organizations.

Para obtener información sobre los requisitos generales aplicables a RDS Custom for SQL Server, consulte Requisitos generales de RDS Custom for SQL Server.

Creación automática de perfiles de instancias mediante la AWS Management Console

RDS Custom requiere que cree y configure un perfil de instancia para lanzar cualquier instancia de base de datos de RDS Custom para SQL Server. Use la AWS Management Console para crear y adjuntar un nuevo perfil de instancia en un solo paso. Esta opción está disponible en la sección de seguridad de RDS Custom, en las páginas de la consola Crear base de datos, Restaurar instantánea y Restaurar a un momento dado. Elija Crear un nuevo perfil de instancia y proporcione un sufijo de nombre de perfil de instancia. La AWS Management Console crea un nuevo perfil de instancia que tiene los permisos necesarios para las tareas de automatización de RDS Custom. Para crear automáticamente nuevos perfiles de instancia, el usuario que ha iniciado sesión en la AWS Management Console debe tener permisos `iam:CreateInstanceProfile`, `iam:AddRoleToInstanceProfile`, `iam:CreateRole` y `iam:AttachRolePolicy`.

> **Note**
>
> Esta opción solo está disponible en la AWS Management Console. Si utiliza la CLI o el SDK, utilice la plantilla de CloudFormation proporcionada por RDS Custom o cree un perfil de

instancia manualmente. Para obtener más información, consulte Creación manual del Rol de IAM y el perfil de instancias.

Paseo 1: concesión de los permisos necesarios a la entidad principal de IAM

Asegúrese de que tiene acceso suficiente para crear una instancia de RDS Custom. El rol de IAM o el usuario de IAM (denominado entidad principal de IAM) para crear una instancia de base de datos de RDS Custom para SQL Server mediante la consola o la CLI debe tener una de las siguientes políticas para crear correctamente una instancia de base de datos:

- La política `AdministratorAccess`
- La política `AmazonRDSFullAccess` con los siguientes permisos adicionales:

```
iam:SimulatePrincipalPolicy
cloudtrail:CreateTrail
cloudtrail:StartLogging
s3:CreateBucket
s3:PutBucketPolicy
s3:PutBucketObjectLockConfiguration
s3:PutBucketVersioning
kms:CreateGrant
kms:DescribeKey
kms:Decrypt
kms:ReEncryptFrom
kms:ReEncryptTo
kms:GenerateDataKeyWithoutPlaintext
kms:GenerateDataKey
ec2:DescribeImages
ec2:RunInstances
ec2:CreateTags
```

RDS Custom utiliza estos permisos durante la creación de la instancia. Estos permisos configuran los recursos de su cuenta que son necesarios para las operaciones de RDS Custom.

Para obtener más información acerca del permiso de `kms:CreateGrant`, consulte Administración de AWS KMS key.

La siguiente política de JSON de muestra otorga los permisos necesarios.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ValidateIamRole",
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
            "Resource": "*"
        },
        {
            "Sid": "CreateCloudTrail",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:StartLogging"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
        },
        {
            "Sid": "CreateS3Bucket",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::do-not-delete-rds-custom-*"
        },
        {
            "Sid": "CreateKmsGrant",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

La entidad principal de IAM requiere los siguientes permisos adicionales para funcionar con versiones de motor personalizadas (CEV):

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigureKmsKeyEncryptionPermission",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:Decrypt",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:region:account_id:key/key_id"
        },
        {
            "Sid": "CreateEc2Instance",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:RunInstances",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Sustituya *account_id* por el identificador de la cuenta que está utilizando para crear la instancia. Sustituya *region* por la Región de AWS en la que vaya a crear la instancia. Sustituya *key_id* por el identificador de clave administrada por el cliente. Puede agregar varias claves según sea necesario.

Para obtener más información sobre los permisos de recursos necesarios para lanzar una instancia de EC2, consulte Lanzar instancias (RunInstances).

Además, la entidad principal de IAM requiere el permiso `iam:PassRole` en el rol de IAM. Debe adjuntarse al perfil de instancia pasado en el parámetro `custom-iam-instance-profile` en la solicitud para crear la instancia de base de datos de RDS Custom. El perfil de instancia y su rol adjunto se crean más adelante en Paso 2: configuración de la red, perfil de instancia y cifrado.

> **Note**
>
> Asegúrese de que los permisos enumerados anteriormente no están restringidos por las políticas de control de servicio (SCP), los límites de los permisos o las políticas de sesión asociadas a la entidad principal de IAM.

Paso 2: configuración de la red, perfil de instancia y cifrado

Puede configurar el rol de perfil de instancia de IAM, la nube privada virtual (VPC) y la clave de cifrado simétrica de AWS KMS mediante cualquiera de los siguientes procesos:

- Configuración con AWS CloudFormation (recomendado)
- Configuración manual

> **Note**
>
> Si su cuenta forma parte de cualquier AWS Organizations, asegúrese de que los permisos requeridos por el rol de perfil de instancia no están restringidos por políticas de control de servicios (SCP).
>
> Las siguientes configuraciones de red en este tema funcionan mejor con instancias de base de datos que no son de acceso público. No puede conectarse directamente a la instancia de base de datos desde fuera de la VPC.

Configuración con AWS CloudFormation

Para simplificar la configuración, puede utilizar un archivo de plantilla AWS CloudFormation para crear pilas de CloudFormation. Una plantilla de CloudFormation crea todas las redes, los perfiles de instancia y los recursos de cifrado de acuerdo con los requisitos de RDS Custom.

Para aprender a crear pilas, consulte Creación de una pila en la consola de AWS CloudFormation en la Guía del usuario de AWS CloudFormation.

Para obtener un tutorial sobre cómo iniciar Amazon RDS Custom para SQL Server mediante una plantilla de AWS CloudFormation, consulte Get started with Amazon RDS Custom for SQL Server using an AWS CloudFormation template (Empiece a utilizar Amazon RDS Custom para SQL Server con una plantilla de AWS CloudFormation) en el blog de AWS Database.

Temas

- Parámetros requeridos por CloudFormation
- Descarga del archivo de plantilla AWS CloudFormation
- Configuración de recursos mediante CloudFormation

Parámetros requeridos por CloudFormation

Los siguientes parámetros son necesarios para configurar los recursos de requisitos previos de RDS Custom con CloudFormation:

Grupo de parámetros	Nombre del parámetro	Valor predeterminado	Descripción
Configuración de disponibilidad	Seleccione una configuración de disponibilidad para ajustar los requisitos previos	Multi-AZ	Especifique si desea configurar los requisitos previos en una configuración Single-AZ o Multi-AZ para instancias de RDS Custom. Debe utilizar la configura ción Multi-AZ si necesita al menos una instancia de base de datos Multi-AZ en esta configuración
Configuración de red	Bloque de CIDR de IPv4 para VPC	10.0.0.0/16	Especifique un bloque de CIDR de IPv4 (o un rango de direcciones IP) para la VPC. Esta VPC

Grupo de parámetros	Nombre del parámetro	Valor predeterminado	Descripción
			está configurada para crear y trabajar con una instancia de base de datos de RDS Custom.
	Bloque de CIDR de IPv4 para 1 de 2 subredes privadas	10.0.128.0/20	Especifique un bloque de CIDR de IPv4 (o un rango de direccion es IP) para su primera subred privada. Esta es una de las dos subredes en las que se puede crear la instancia de base de datos de RDS Custom. Se trata de una subred privada sin acceso a Internet.
	Bloque de CIDR de IPv4 para 2 de 2 subredes privadas	10.0.144.0/20	Especifique un bloque de CIDR de IPv4 (o un rango de direcciones IP) para su segunda subred privada. Esta es una de las dos subredes en las que se puede crear la instancia de base de datos de RDS Custom. Se trata de una subred privada sin acceso a Internet.

Grupo de parámetros	Nombre del parámetro	Valor predeterminado	Descripción
	Bloque de CIDR de IPv4para subred pública	10.0.0.0/20	Especifique un bloque de CIDR de IPv4 (o un rango de direcciones IP) para su subred pública. Esta es una de las subredes en las que se puede conectar la instancia de EC2 con la instancia de base de datos de RDS Custom que se puede crear. Se trata de una subred pública con acceso a Internet.
Configuración de acceso RDP	Bloque CIDR de IPv4 de su origen	-	Especifique un bloque de CIDR de IPv4 (o un rango de direccion es IP) para su origen. Este es el rango de IP desde el que se establece la conexión RDP a la instancia de EC2 en la subred pública. Si no se establece, la conexión RDP a la instancia de EC2 no está configura da.

Grupo de parámetros	Nombre del parámetro	Valor predeterminado	Descripción
	Configuración del acceso RDP a la instancia de RDS Custom para SQL Server	No	Especifique si desea habilitar la conexión RDP desde la instancia de EC2 a la instancia de RDS Custom para SQL Server. De forma predeterminada, la conexión RDP desede la instancia de EC2 a la instancia de base de datos no está configurada.

Recursos creados por CloudFormation

La creación correcta de la pila de CloudFormation con la configuración predeterminada crea los siguientes recursos en su Cuenta de AWS:

- Clave de KMS de cifrado simétrico para el cifrado de datos administrado por RDS Custom.
- El perfil de la instancia está asociado a un rol de IAM con `AmazonRDSCustomInstanceProfileRolePolicy` para proporcionar los permisos requeridos por RDS Custom. Para obtener más información, consulte AmazonRDSCustomServiceRolePolicy en la Guía de referencia de políticas administradas de AWS.
- VPC con el intervalo CIDR especificado como parámetro de CloudFormation. El valor predeterminado es `10.0.0.0/16`.
- Dos subredes privadas con el intervalo CIDR especificado en los parámetros, y dos zonas de disponibilidad diferentes en la Región de AWS. Los valores predeterminados de los CIDR de subred son `10.0.128.0/20` y `10.0.144.0/20`.
- Una subred pública con el intervalo CIDR especificado en los parámetros. El valor predeterminado de CIDR de subred es 10.0.0.0/20. La instancia de EC2 reside en esta subred y se puede utilizar para conectarse a la instancia de RDS Custom.

- Opción DHCP configurada para la VPC con resolución de nombres de dominio a un servidor de sistema de nombres de dominio (DNS) de Amazon.
- Tabla de enrutamiento para la asociación con dos subredes privadas y sin acceso a Internet.
- Tabla de enrutamiento para la asociación con la subred pública y con acceso a Internet.
- Puerta de enlace de Internet asociada a la VPC para permitir el acceso de Internet a la subred pública.
- Lista de control de acceso a la red (ACL) para la asociación con dos subredes privadas y acceso restringido a HTTPS y puerto de base de datos dentro de VPC.
- Grupo de seguridad de la VPC que se asociará a la instancia de RDS Custom. El acceso está restringido para HTTPS saliente a puntos de conexión de Servicio de AWS que requiere RDS Custom y al puerto de base de datos entrante desde el grupo de seguridad de instancias de EC2.
- Grupo de seguridad de que debe asociarse con la instancia de EC2 en la subred pública. El acceso está restringido para el puerto de base de datos saliente al grupo de seguridad de instancias de RDS Custom.
- Grupo de seguridad de VPC que se asociará a los puntos de conexión de VPC que se creen para los puntos de conexión de Servicio de AWS que requiera RDS Custom.
- Grupo de subredes de base de datos en el que se crean instancias de RDS Custom. Se añaden dos subredes privadas creadas por esta plantilla al grupo de subredes de base de datos.
- Puntos de conexión de VPC para cada uno de los puntos de conexión de Servicio de AWS que requiere RDS Custom.

Si se establece la configuración de disponibilidad en multi-az, se crearán los siguientes recursos además de la lista anterior:

- Reglas de ACL de red que permiten la comunicación entre subredes privadas.
- Acceso entrante y saliente al puerto Multi-AZ dentro del grupo de seguridad de VPC asociado a la instancia de RDS Custom.
- Puntos de conexión de VPC a los puntos de conexión de servicio de AWS que se requieren para la comunicación Multi-AZ.

Además, al establecer la configuración de acceso RDP, se crean los siguientes recursos:

- Configuración del acceso RDP a la subred pública desde la dirección IP de origen:
  - Reglas de ACL de red que permiten la conexión RDP desde la IP de origen a la subred pública.

  - Acceso de entrada al puerto RDP desde la IP de origen al grupo de seguridad de VPC asociado a la instancia de EC2.
- Configuración del acceso RDP desde una instancia de EC2 en una subred pública a una instancia de RDS Custom en subredes privadas:
  - Reglas de ACL de red que permiten la conexión RDP desde una subred pública a subredes privadas.
  - Acceso entrante al puerto RDP desde el grupo de seguridad de VPC asociado a la instancia de EC2 al grupo de seguridad de VPC asociado a la instancia de RDS Custom.

Utilice los procedimientos siguientes para crear la pila de CloudFormation para RDS Custom para SQL Server.

Descarga del archivo de plantilla AWS CloudFormation

Para descargar el archivo de plantilla

1. Abra el menú contextual (haga clic con el botón derecho del ratón) del enlace custom-sqlserver-onboard.zip y elija Save Link As (Guardar enlace como).
2. Guarde y extraiga el archivo en su equipo.

Configuración de recursos mediante CloudFormation

Para configurar recursos mediante CloudFormation

1. Abra la consola de CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Para iniciar el Asistente de creación de pila, elija Create Stack (Crear pila).

   Aparecerá la página Create stack (Crear pila).
3. En Requisito previo - Preparar plantilla, elija La plantilla está lista.
4. En Specify template (Especificar plantilla), haga lo siguiente:

   a. Para Origen de plantilla, elija Cargar un archivo de plantilla.

   b. En Elegir archivo, navegue hasta el archivo correcto y selecciónelo.
5. Elija Siguiente.

   Aparecerá la página Specify stack details (Especificar los detalles de la pila).

6. En Nombre de pila, escriba **`rds-custom-sqlserver`**.
7. En Parameters (Parámetros), haga lo siguiente:

   a. Para conservar las opciones predeterminadas, elija Next (Siguiente).

   b. Para cambiar las opciones, elija la configuración de disponibilidad, la configuración de red y la configuración de acceso RDP adecuadas; a continuación, elija Siguiente.

      Lea detenidamente la descripción de cada parámetro antes de cambiarlo.

> **Note**
>
> Si decide crear al menos una instancia Multi-AZ en esta pila de CloudFormation, asegúrese de que el parámetro de pila de CloudFormation Select an availability configuration for prerequisites setup esté establecido en `Multi-AZ`. Si crea la pila de CloudFormation como Single-AZ, actualice la pila de CloudFormation a la configuración Multi-AZ antes de crear la primera instancia Multi-AZ.

8. En la página Configurar opciones de pila, elija Siguiente.
9. En la página Review rds-custom-sqlserver (Revisar rds-custom-sqlserver), haga lo siguiente:

   a. Para Capabilities (Capacidades), seleccione la casilla de verificación I acknowledge that AWS CloudFormation might create IAM resources with custom names (Reconozco que podría crear recursos de IAM con nombres personalizados).

   b. Elija Create stack (Crear pila).

> **Note**
>
> No actualice los recursos creados a partir de esta pila de AWS CloudFormation directamente desde las páginas de recursos. Esto le impide aplicar futuras actualizaciones a estos recursos mediante una plantilla de AWS CloudFormation.

CloudFormation crea los recursos que requiere RDS Custom para SQL Server. Si se produce un error en la creación de la pila, lea la pestaña Events (Eventos) para ver qué error ha habido en la creación de recursos y el motivo de su estado.

La pestaña Outputs (Salidas) de esta pila de CloudFormation en la consola debe tener información sobre todos los recursos que se pasarán como parámetros para crear una instancia de base de datos de RDS Custom para SQL Server. Asegúrese de utilizar el grupo de seguridad de VPC y el grupo de subred de base de datos creado por CloudFormation para las instancias de base de datos de RDS Custom. De forma predeterminada, RDS intenta adjuntar el grupo de seguridad de VPC predeterminado, que podría no tener el acceso que necesita.

Si ha utilizado CloudFormation para crear recursos, puede omitir Configuración manual.

Actualización de la pila de CloudFormation

También puede actualizar parte de la configuración de la pila de CloudFormation después de la creación. Las configuraciones que se pueden actualizar son:

- Configuración de disponibilidad para RDS Custom para SQL Server
  - Select an availability configuration for prerequisites setup: actualice este parámetro para cambiar entre la configuración Single-AZ y Multi-AZ. Si utiliza esta pila de CloudFormation para al menos una instancia Multi-AZ, debe actualizar la pila para elegir la configuración Multi-AZ.
- Configuración de acceso RDP para RDS Custom para SQL Server
  - Bloque de CIDR de IPv4: puede actualizar el bloque de CIDR de IPv4 (o el intervalo de direcciones IP) de la fuente mediante la actualización de este parámetro. Si se deja este parámetro en blanco, se elimina la configuración de acceso RDP del bloque CIDR de origen a la subred pública.
  - Configure el acceso RDP a RDS Custom para SQL Server: habilite o deshabilite la conexión RDP desde la instancia de EC2 a la instancia de RDS Custom para SQL Server.

Eliminación de la pila de CloudFormation

Puede eliminar la pila de CloudFormation después de eliminar todas las instancias de RDS Custom que utilizan recursos de la pila. RDS Custom no realiza un seguimiento de la pila de CloudFormation, por lo que no bloquea la eliminación de la pila cuando hay instancias de base de datos que utilizan recursos de pila. Asegúrese de que no haya ninguna instancia de base de datos de RDS Custom que utilice los recursos de la pila al eliminar la pila.

> **Note**
>
> Al eliminar una pila de CloudFormation, se eliminan todos los recursos creados para la pila excepto la clave de KMS. La clave de KMS cambia al estado pendiente de eliminación y

se elimina después de 30 días. Para conservar la clave de KMS, realice una operación CancelKeyDeletion durante el periodo de gracia de 30 días.

Configuración manual

Si elige configurar los recursos manualmente, realice las siguientes tareas.

> **Note**
>
> Para simplificar la configuración, puede utilizar el archivo de plantilla de AWS CloudFormation para crear una pila de CloudFormation en lugar de realizar la configuración manualmente. Para obtener más información, consulte Configuración con AWS CloudFormation.
> También puede utilizar la AWS CLI para completar esta sección. Si lo hace, descargue e instale la última CLI.

Temas

- Asegúrese de que tiene una clave de cifrado simétrica AWS KMS
- Creación manual del Rol de IAM y el perfil de instancias
- Configuración manual de la VPC

Asegúrese de que tiene una clave de cifrado simétrica AWS KMS

Se requiere una AWS KMS key de cifrado simétrica para RDS Custom. Cuando crea una instancia de base de datos de RDS Custom para SQL Server, asegúrese de proporcionar el identificador de clave de KMS como parámetro `kms-key-id`. Para obtener más información, consulte Creación y conexión a una instancia de base de datos para Amazon RDS Custom for SQL Server.

Dispone de las opciones siguientes:

- Si ya dispone de una clave KMS administrada por el cliente en su Cuenta de AWS, puede utilizarla con RDS Custom. No hay que hacer nada más.
- Si ya ha creado una clave KMS de cifrado simétrica administrada por el cliente para un motor diferente de RDS Custom, puede reutilizar la misma clave. No hay que hacer nada más.

- Si no tiene una clave KMS de cifrado simétrica administrada por el cliente en su cuenta, cree una clave KMS mediante las instrucciones de Creating keys (Creación de claves) en la Guía para desarrolladores de AWS Key Management Service.
- Si va a crear una instancia de base de datos de CEV o RDS Custom y su clave de KMS está en una Cuenta de AWS diferente, asegúrese de utilizar la AWS CLI. No puede usar la consola de AWScon claves de KMS entre cuentas.

> **Important**
>
> RDS Custom no admite claves KMS administradas por AWS.

Asegúrese de que su clave de cifrado simétrica proporcione acceso a las operaciones `kms:Decrypt` y `kms:GenerateDataKey` al rol de IAM AWS Identity and Access Management en su perfil de instancia de IAM. Si tiene una nueva clave de cifrado simétrica en su cuenta, no se requieren cambios. De lo contrario, asegúrese de que la política de claves de cifrado simétricas proporcione acceso a estas operaciones.

Para obtener más información, consulte Paso 4: configurar IAM para RDS Custom for Oracle.

Creación manual del Rol de IAM y el perfil de instancias

Puede crear manualmente un perfil de instancia y utilizarlo para lanzar instancias de RDS Custom. Si tiene pensado crear la instancia en la AWS Management Console, omita esta sección. La AWS Management Console permite crear y asociar un perfil de instancia a sus instancias de base de datos de RDS Custom. Para obtener más información, consulte Creación automática de perfiles de instancias mediante la AWS Management Console.

Cuando cree manualmente un perfil de instancia, pase el nombre del perfil de instancia como parámetro `custom-iam-instance-profile` en su comando de CLI `create-db-instance`. RDS Custom usa el rol asociado a este perfil de instancia para ejecutar la automatización y administrar la instancia.

Para crear el perfil de instancia de IAM y los roles de IAM para RDS Custom para SQL Server

1. Creación del Rol de IAM denominado `AWSRDSCustomSQLServerInstanceRole` con una política de confianza que Amazon EC2 puede utilizar para asumir esta función.

2. Agregue la política administrada de AWS `AmazonRDSCustomInstanceProfileRolePolicy` a `AWSRDSCustomSQLServerInstanceRole`.
3. Cree un perfil de instancia de IAM para RDS Custom para SQL Server que se llame `AWSRDSCustomSQLServerInstanceProfile`.
4. Agregue `AWSRDSCustomSQLServerInstanceRole` al perfil de instancias.

Creación del Rol de IAM de AWSRDSCustomSQLServerInstanceRole

En el siguiente ejemplo se crea el rol `AWSRDSCustomSQLServerInstanceRole`. La política de confianza permite que Amazon EC2 asuma el rol.

```
aws iam create-role \
    --role-name AWSRDSCustomSQLServerInstanceRole \
    --assume-role-policy-document '{
        "Version": "2012-10-17",
          "Statement": [
            {
              "Action": "sts:AssumeRole",
              "Effect": "Allow",
              "Principal": {
                  "Service": "ec2.amazonaws.com"
              }
            }
          ]
        }'
```

Agregar una política de acceso a AWSRDSCustomSQLServerInstanceRole

Para proporcionar los permisos necesarios, asocie la política administrada de AWS `AmazonRDSCustomInstanceProfileRolePolicy` a`AWSRDSCustomSQLServerInstanceRole`. `AmazonRDSCustomInstanceProfileRolePolicy` permite a las instancias de RDS Custom enviar y recibir mensajes y realizar diversas acciones de automatización.

> **Note**
>
> Asegúrese de que los permisos de la política de acceso no estén restringidos por SCP ni límites de permisos asociados al rol de perfil de instancia.

En el siguiente ejemplo, se asocia una política administrada de AWS `AmazonRDSCustomInstanceProfileRolePolicy` al rol`AWSRDSCustomSQLServerInstanceRole`.

```
aws iam attach-role-policy \
    --role-name AWSRDSCustomSQLServerInstanceRole \
    --policy-arn arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy
```

Cree su perfil de instancias de RDS Custom for SQL Server

Un perfil de instancia es un contenedor que incluye un rol de IAM único. RDS Custom usa el perfil de instancia para pasar el rol a la instancia.

Si utiliza la AWS Management Console para crear un rol para Amazon EC2, la consola crea automáticamente un perfil de instancias y le da el mismo nombre que al rol cuando se creó. Cree su perfil de instancias de la siguiente manera, nombrándolo `AWSRDSCustomSQLServerInstanceProfile`.

```
aws iam create-instance-profile \
    --instance-profile-name AWSRDSCustomSQLServerInstanceProfile
```

Agregue AWSRDSCustomSQLServerInstanceRole a su perfil de instancias de RDS Custom for SQL Server

Añada el rol `AWSRDSCustomInstanceRoleForRdsCustomInstance` al perfil `AWSRDSCustomSQLServerInstanceProfile` creado anteriormente.

```
aws iam add-role-to-instance-profile \
    --instance-profile-name AWSRDSCustomSQLServerInstanceProfile \
    --role-name AWSRDSCustomSQLServerInstanceRole
```

Configuración manual de la VPC

La instancia de base de datos de RDS Custom se encuentra en una nube privada virtual (VPC) basada en el servicio Amazon VPC, tal como lo es una instancia de Amazon EC2 o una instancia de Amazon RDS. Proporcione y configure su propia VPC. Por lo tanto, tiene control total sobre la configuración de redes de instancias.

RDS Custom envía la comunicación desde la instancia de base de datos a otros Servicios de AWS. Asegúrese de que se pueda acceder a los siguientes servicios desde la subred en la que creó las instancias de base de datos de RDS Custom:

- Amazon CloudWatch (`com.amazonaws.region.monitoring`)
- Registros de Amazon CloudWatch (`com.amazonaws.region.logs`)
- Eventos de Amazon CloudWatch (`com.amazonaws.region.events`)
- Amazon EC2 (`com.amazonaws.region.ec2` y `com.amazonaws.region.ec2messages`)
- Amazon EventBridge (`com.amazonaws.region.events`)
- Amazon S3 (`com.amazonaws.region.s3`)
- AWS Secrets Manager (`com.amazonaws.region.secretsmanager`)
- AWS Systems Manager (`com.amazonaws.region.ssm` y `com.amazonaws.region.ssmmessages`)

Si se crean implementaciones multi-AZ

- Amazon Simple Queue Service (`com.amazonaws.region.sqs`)

Si RDS Custom no puede comunicarse con los servicios necesarios, publica los siguientes eventos:

```
Database instance in incompatible-network. SSM Agent connection not available. Amazon
 RDS can't connect to the dependent AWS services.
```

```
Database instance in incompatible-network. Amazon RDS can't connect to dependent AWS
 services. Make sure port 443 (HTTPS) allows outbound connections, and try again.
 "Failed to connect to the following services: s3 events"
```

Para evitar errores `incompatible-network`, asegúrese de que los componentes de la VPC que intervienen en la comunicación entre la instancia de base de datos de RDS Custom y Servicios de AWS cumplen los siguientes requisitos:

- La instancia de base de datos puede realizar conexiones salientes en el puerto 443 a otros Servicios de AWS.
- La VPC permite respuestas entrantes a solicitudes originadas en la instancia de base de datos de RDS Custom.

- RDS Custom puede resolver correctamente los nombres de dominio de los puntos de conexión de cada Servicio de AWS.

Si ya ha configurado una VPC para otro motor de base de datos de RDS Custom, puede reutilizar esa VPC y omitir este proceso.

Temas

- Configure los grupos de seguridad de la VPC
- Configuración de puntos de conexión para los Servicios de AWS dependientes
- Configurar el servicio de metadatos de instancia

Configure los grupos de seguridad de la VPC

Un security group (grupo de seguridad) actúa como un firewall virtual para una instancia de VPC, al controlar el tráfico entrante y saliente. Una instancia de base de datos de RDS Custom tiene un grupo de seguridad predeterminado asociado a su interfaz de red que protege la instancia. Asegúrese de que el grupo de seguridad permite el tráfico entre RDS Custom y otros Servicios de AWS a través de HTTPS. Debe pasar este grupo de seguridad como el parámetro `vpc-security-group-ids` en la solicitud de creación de la instancia.

Para configurar el grupo de seguridad para RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc.
2. Permita que RDS Custom utilice el grupo de seguridad predeterminado o cree su propio grupo de seguridad.

   Para obtener instrucciones detalladas, consulta Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.
3. Asegúrese de que el grupo de seguridad permita conexiones salientes en el puerto 443. RDS Custom necesita este puerto para comunicarse con los Servicios de AWS dependientes.
4. Si tiene una VPC privada y utiliza puntos de conexión de VPC, asegúrese de que el grupo de seguridad asociado a la instancia de base de datos permite las conexiones salientes en el puerto 443 a los puntos de conexión de VPC. Asegúrese también de que el grupo de seguridad asociado al punto de conexión de VPC permite las conexiones entrantes en el puerto 443 desde la instancia de base de datos.

Si no se permiten las conexiones entrantes, la instancia personalizada de RDS no podrá conectarse a los puntos de conexión de AWS Systems Manager y Amazon EC2. Para obtener más información, consulte Crear un punto de conexión de nube privada virtual en la Guía del usuario de AWS Systems Manager.

5. En el caso de instancias Multi-AZ de RDS Custom para SQL Server, asegúrese de que el grupo de seguridad asociado a la instancia de base de datos permite las conexiones entrantes y salientes en el puerto 1120 a este mismo grupo de seguridad. Esto es necesario para la conexión de host homólogo en una instancia de base de datos Multi-AZ de RDS Custom para SQL Server.

Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad de la VPC en la Guía para desarrolladores de Amazon VPC.

Configuración de puntos de conexión para los Servicios de AWS dependientes

Le recomendamos que agregue puntos de conexión para cada servicio a la VPC mediante las siguientes instrucciones. Sin embargo, puede utilizar cualquier solución que le permita a su VPC comunicarse con los puntos de conexión del servicio AWS. Por ejemplo, puede utilizar Network Address Translation (NAT) o AWS Direct Connect.

Para configurar los puntos de conexión de los Servicios de AWS con los que funciona RDS Custom

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En la barra de navegación, use el selector de Región para elegir la Región de AWS.
3. En el panel de navegación, elija Endpoints (Puntos de conexión). En el panel principal, elija Create Endpoint (Crear punto de conexión).
4. En Service category (Categoría de servicios), elija Servicios de AWS.
5. Para Service Name (Nombre del servicio), elija el punto de conexión que se muestra en la tabla.
6. En VPC, elija su VPC.
7. En Subnets (Subredes), elija una subred de cada zona de disponibilidad para su inclusión.

   El punto de conexión de VPC puede abarcar varias zonas de disponibilidad. AWS crea una interfaz de red elástica para el punto de conexión de VPC en cada una de las subredes que usted elija. Cada interfaz de red tiene un nombre de host del Sistema de nombres de dominio (DNS) y una dirección IP privada.
8. En Security group (Grupo de seguridad), elija o cree un grupo de seguridad.

Puede utilizar grupos de seguridad para controlar el acceso a su punto de conexión, de la misma forma que utiliza un firewall. Asegúrese también de que el grupo de seguridad permite las conexiones entrantes en el puerto 443 desde las instancias de base de datos. Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad de su VPC en la Guía de usuario de Amazon VPC.

9. Si lo desea, puede adjuntar una política al punto de conexión de VPC. Las políticas del punto de conexión pueden controlar el acceso al Servicio de AWS que se está conectando. La política predeterminada permite que todas las solicitudes pasen por el punto de conexión. Si utiliza una política personalizada, asegúrese de que las solicitudes de la instancia de base de datos están permitidas en la política.
10. Elija Create endpoint (Crear punto de conexión).

En la tabla siguiente se explica cómo encontrar la lista de puntos de conexión que necesita la VPC para las comunicaciones salientes.

Servicio	Formato de punto de conexión	Notas y enlaces
AWS Systems Manager	Use los siguientes formatos de punto de conexión: • `ssm.region.amazonaws.com` • `ssmmessages. region.amazonaws.com`	Para obtener una lista de todos los puntos de conexión de cada región, consulte AWS Systems Manager endpoints and quotas (Puntos de conexión y cuotas de AWS Systems Manager) en la Referencia general de Amazon Web Services.
AWS Secrets Manager	Use el formato de punto de conexión `secretsmanager. region.amazonaws.com .`	Para obtener una lista de todos los puntos de conexión de cada región, consulte AWS Secrets Manager endpoints and quotas (Puntos de conexión y cuotas de AWS Secrets Manager) en la Referencia general de Amazon Web Services.

Servicio	Formato de punto de conexión	Notas y enlaces
Amazon CloudWatch	Use los siguientes formatos de punto de conexión: • Para las métricas de CloudWatch, utilice `monitoring. region .amazonaws.com` • Para CloudWatch Events, utilice `events.region.amazonaws.com` • Para CloudWatch Logs, utilice `logs.region.amazonaws.com`	Para obtener la lista de puntos de conexión de cada Región, consulte: • Puntos de conexión y cuotas de Amazon CloudWatch en la Referencia general de Amazon Web Services • Puntos de conexión y cuotas de Registros de Amazon CloudWatch en la Referencia general de Amazon Web Services • Puntos de conexión y cuotas de Amazon CloudWatch Events en la Referencia general de Amazon Web Services
Amazon EC2	Use los siguientes formatos de punto de conexión: • `ec2.region.amazonaws.com` • `ec2messages. region .amazonaws.com`	Para obtener la lista de puntos de conexión en cada región, consulte Amazon Elastic Compute Cloud endpoints and quotas (Puntos de conexión y cuotas de Amazon Elastic Compute Cloud) en la Referencia general de Amazon Web Services.

Servicio	Formato de punto de conexión	Notas y enlaces
Amazon S3	Use el formato de punto de conexión `s3.region.amazonaws.com` .	Para obtener la lista de puntos de conexión en cada región, consulte Amazon Simple Storage Service endpoints and quotas (Puntos de conexión y cuotas de Amazon Simple Storage Service) en la Referencia general de Amazon Web Services. Para obtener más información sobre los puntos de conexión de puerta de enlace para Simple Storage Service (Amazon S3), consulte Endpoints for Amazon S3 (Puntos de conexión para Amazon S3) en la Guía para desarroll adores de Amazon VPC. Para obtener información sobre cómo crear un punto de acceso, consulte Creating access points (Creación de puntos de acceso) en la Guía para desarrolladores de Amazon VPC. Para obtener información acerca de cómo crear puntos de conexión de puerta de enlace para Amazon S3, consulte Puntos de enlace de la VPC de punto de enlace.
Amazon Simple Queue Service	Use el formato de punto de conexión `sqs.region.amazonaws.com`	Para obtener la lista de puntos de conexión en cada región, consulte Amazon Simple Storage Service endpoints and quotas.

Configurar el servicio de metadatos de instancia

Asegúrese de que la instancia pueda hacer lo siguiente:

- Acceda al servicio de metadatos de la instancia mediante la versión 2 del servicio de metadatos de la instancia (IMDSv2).
- Permitir comunicaciones salientes a través del puerto 80 (HTTP) a la dirección IP del enlace IMDS.
- Solicitar metadatos de instancia de `http://169.254.169.254`, el enlace IMDSv2.

Para obtener más información, consulte Utilizar IMDSv2 en la Guía del usuario de Amazon EC2.

Restricciones entre instancias

Al crear un perfil de instancia siguiendo los pasos anteriores, utiliza la política administrada de AWS `AmazonRDSCustomInstanceProfileRolePolicy` para proporcionar los permisos necesarios a RDS Custom, lo que permite la automatización de la administración y supervisión de las instancias. La política administrada garantiza que los permisos permitan el acceso únicamente a los recursos que RDS Custom necesita para ejecutar la automatización. Recomendamos utilizar la política administrada para admitir nuevas funciones y abordar requisitos de seguridad que se aplican automáticamente a los perfiles de instancia existentes sin intervención manual. Para obtener más información, consulte Política administrada de AWS: AmazonRDSCustomInstanceProfileRolePolicy.

La política administrada `AmazonRDSCustomInstanceProfileRolePolicy` restringe que el perfil de instancia tenga acceso entre cuentas, pero puede permitir el acceso a algunos recursos administrados de RDS Custom en las instancias de RDS Custom de la misma cuenta. Según sus requisitos, puede usar los límites de los permisos para restringir aún más el acceso entre instancias. Los límites de permisos definen los permisos máximos que las políticas basadas en identidad pueden conceder a una entidad, pero no conceden permisos por sí mismos. Para obtener más información, consulte Evaluación de los permisos efectivos cuando se usan límites.

Por ejemplo, la siguiente política de límite restringe el acceso del rol del perfil de instancia a una clave de AWS KMS específica y limita el acceso a los recursos administrados por RDS Custom en todas las instancias que utilizan claves de AWS KMS diferentes.

JSON

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "DenyOtherKmsKeyAccess",
            "Effect": "Deny",
            "Action": "kms:*",
            "NotResource": "arn:aws:kms:region:acct_id:key/KMS_key_ID"
        },
        {
            "Sid": "NoBoundarySetByDefault",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Asegúrese de que el límite de permisos no bloquee ningún permiso que `AmazonRDSCustomInstanceProfileRolePolicy` conceda a RDS Custom.

Bring Your Own Media con RDS Custom para SQL Server

RDS Custom para SQL Server admite dos modelos de licencia: licencia incluida (LI) y Bring Your Own Media (BYOM).

En BYOM, tiene las siguientes opciones:

1. Proporcione e instale sus propios archivos binarios de Microsoft SQL Server con actualizaciones acumulativas (CU, por sus siglas en inglés) compatibles en una AMI de AWS EC2 Windows.
2. Guarde la AMI como imagen dorada, que es una plantilla que puede utilizar para crear una versión de motor personalizada (CEV, por sus siglas en inglés).
3. Cree una CEV a partir de la imagen dorada.
4. Cree instancias de base de datos de RDS Custom para SQL Server nuevas con la CEV.

A continuación, Amazon RDS administra estas instancias de base de datos en su nombre.

> **Note**
>
> Si también tiene una instancia de base de datos de RDS Custom para SQL Server con licencia incluida (LI), no puede utilizar el software SQL Server de esta instancia de base de datos con BYOM. Debe traer sus propios archivos binarios de SQL Server a BYOM.

Requisitos de BYOM para RDS Custom para SQL Server

Al BYOM se aplican los mismos requisitos generales que para las versiones de motores personalizados para RDS Custom para SQL Server. Para obtener más información, consulte Requisitos de las CEV para RDS Custom para SQL Server.

Cuando utilice BYOM, asegúrese de que cumpla los siguientes requisitos adicionales:

- Utilice una de las siguientes ediciones compatibles: SQL Server 2022 o 2019 Enterprise, Standard o Developer Edition.
- Otorgue el privilegio de rol de servidor sysadmin (SA) de SQL Server a `NT AUTHORITY\SYSTEM`.
- Mantenga configurado el sistema operativo de EC2 para Windows Server con la zona horaria `UTC`.

  De forma predeterminada, las instancias subyacentes de Amazon EC2 Windows están establecidas en la zona horaria UTC. Para obtener más información sobre cómo ver y cambiar la

zona horaria de una instancia de Windows, consulte Sincronización precisa del reloj y la hora en su instancia EC2 en la Guía del usuario de Amazon EC2.

- Abra el puerto TCP 1433 y el puerto UDP 1434 para permitir las conexiones SSM.

Limitaciones de RDS Custom para SQL Server

Las mismas limitaciones generales de RDS Custom para SQL Server también se aplican a BYOM. Para obtener más información, consulte Requisitos y limitaciones de Amazon RDS Custom for SQL Server.

Con BYOM, se aplican las siguientes limitaciones adicionales:

- Solo se admite la instancia predeterminada de SQL Server (MSSQLSERVER). No se admiten las instancias designadas de SQL Server. RDS Custom para SQL Server detecta y monitorea solo la instancia de SQL Server predeterminada.
- Solo se admite una instalación de SQL Server en cada AMI. No se admiten varias instalaciones de diferentes versiones de SQL Server.
- La edición Web de SQL Server no es compatible con BYOM.
- Las versiones de evaluación de las ediciones de SQL Server no son compatibles con BYOM. Al instalar SQL Server, no active la casilla de verificación para usar una versión de evaluación.
- La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información, consulte Disponibilidad regional de las CEV de RDS Custom para SQL Server y Compatibilidad de versiones CEV para RDS Custom para SQL Server.

Creación de una instancia de base de datos de RDS Custom para SQL Server con BYOM

Para preparar y crear una instancia de base de datos de RDS Custom para SQL Server con BYOM, consulte Preparación de una CEV con Bring Your Own Media (BYOM).

Uso de versiones de motor personalizadas para RDS Custom para SQL Server

Una versión de motor personalizada (CEV) de RDS Custom para SQL Server es una imagen de máquina de Amazon (AMI) que incluye Microsoft SQL Server.

Los pasos básicos del flujo de trabajo de la CEV son los siguientes:

1. Elija una AMI de AWS EC2 Windows para usarla como imagen base para una CEV. Tiene la opción de utilizar Microsoft SQL Server preinstalado o de traer sus propios medios para instalar SQL Server usted mismo.
2. Instale otro software en el sistema operativo y personalice la configuración del sistema operativo y de SQL Server para satisfacer las necesidades de su empresa.
3. Guarde la AMI como imagen dorada.
4. Cree una versión de motor personalizada (CEV) a partir de la imagen dorada.
5. Cree instancias de base de datos de RDS Custom para SQL Server nuevas con la CEV.

A continuación, Amazon RDS administra estas instancias de base de datos por usted.

Una CEV le permite mantener la configuración básica preferida del sistema operativo y de la base de datos. Usar una CEV garantiza que la configuración del host, como la instalación de cualquier agente de terceros u otras personalizaciones del sistema operativo, se conserve en las instancias de base de datos de RDS Custom para SQL Server. Una CEV le permite implementar rápidamente flotas de instancias de base de datos de RDS Custom para SQL Server con la misma configuración.

Temas

- Preparación para crear una CEV para RDS Custom para SQL Server
- Creación de una CEV para RDS Custom para SQL Server
- Modificación de una CEV para RDS Custom para SQL Server
- Visualización de detalles de la CEV de Amazon RDS Custom para SQL Server
- Eliminación de una CEV para RDS Custom para SQL Server

Preparación para crear una CEV para RDS Custom para SQL Server

Puede crear una CEV mediante una imagen de máquina de Amazon (AMI) que contenga Microsoft SQL Server preinstalado y con licencia (LI), o con una AMI en la que instale sus propios medios de instalación de SQL Server (BYOM).

Preparación de una CEV

Utilice los siguientes procedimientos para crear una CEV con Bring Your Own Media (BYOM) o Microsoft SQL Server (LI) preinstalado.

Preparación de una CEV con Bring Your Own Media (BYOM)

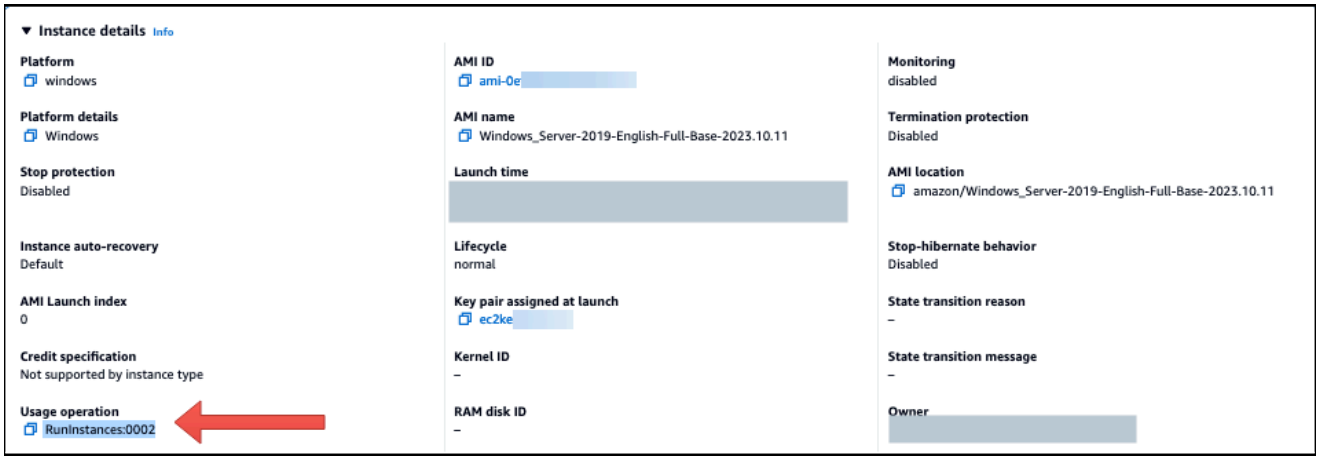
En los pasos siguientes se utiliza una AMI con Windows Server 2019 Base como ejemplo.

Creación de una CEV con BYOM

1. En el panel de la consola de Amazon EC2, seleccione Lanzar instancia.
2. En Nombre, ingrese el nombre de la instancia.
3. En Inicio rápido, selecciona Windows.
4. Seleccione Microsoft Windows Server 2019 Base.
5. Elija el tipo de instancia, el par de claves y la configuración de red y almacenamiento adecuados y lance la instancia.
6. Tras lanzar o crear la instancia EC2, asegúrese de seleccionar la AMI de Windows correcta en el paso 4:

    a. Seleccione la instancia EC2 en la consola de Amazon EC2.

    b. En la sección Detalles, compruebe la Operación de uso y asegúrese de que esté configurada en RunInstances:0002.



7. Inicie sesión en la instancia EC2 y copie el medio de instalación de SQL Server en ella.

   > **Note**
   >
   > Si está creando una CEV con la edición SQL Server Developer, es posible que necesite obtener los medios de instalación mediante su Suscripción a Microsoft Visual Studio.

8. Instale SQL Server. Asegúrese de hacer lo siguiente:

   a. Revise Requisitos de BYOM para RDS Custom para SQL Server y Compatibilidad de versiones CEV para RDS Custom para SQL Server.

   b. Establezca el directorio raíz de la instancia en el valor `C:\Program Files\Microsoft SQL Server\` predeterminado. No cambie este directorio.

   c. Defina el nombre de la cuenta del motor de base de datos de SQL Server en `NT Service\MSSQLSERVER` o `NT AUTHORITY\NETWORK SERVICE`.

   d. Defina el modo de inicio de SQL Server en Manual.

   e. Elija el modo de autenticación de SQL Server Mixto.

   f. Deje la configuración actual para los directorios de datos y las ubicaciones de TempDB predeterminados.

9. Otorgue el privilegio de rol de servidor sysadmin (SA) de SQL Server a `NT AUTHORITY\SYSTEM`:

```
USE [master]
GO
EXEC master..sp_addsrvrolemember @loginame = N'NT AUTHORITY\SYSTEM' , @rolename =
 N'sysadmin'
GO
```

10. Instale el software adicional o personalice la configuración del sistema operativo y la base de datos para que cumplan con sus requisitos.

11. Ejecute Sysprep en la instancia EC2. Para obtener más información, consulte Creación de una AMI de Amazon EC2 con Windows Sysprep.

12. Guarde la AMI que contiene la versión de SQL Server instalada, otro software y las personalizaciones. Esta será su imagen dorada.

13. Cree una CEV nueva con el ID de AMI de la imagen que ha creado. Para ver los pasos detallados, consulte Creación de una CEV para RDS Custom para SQL Server.

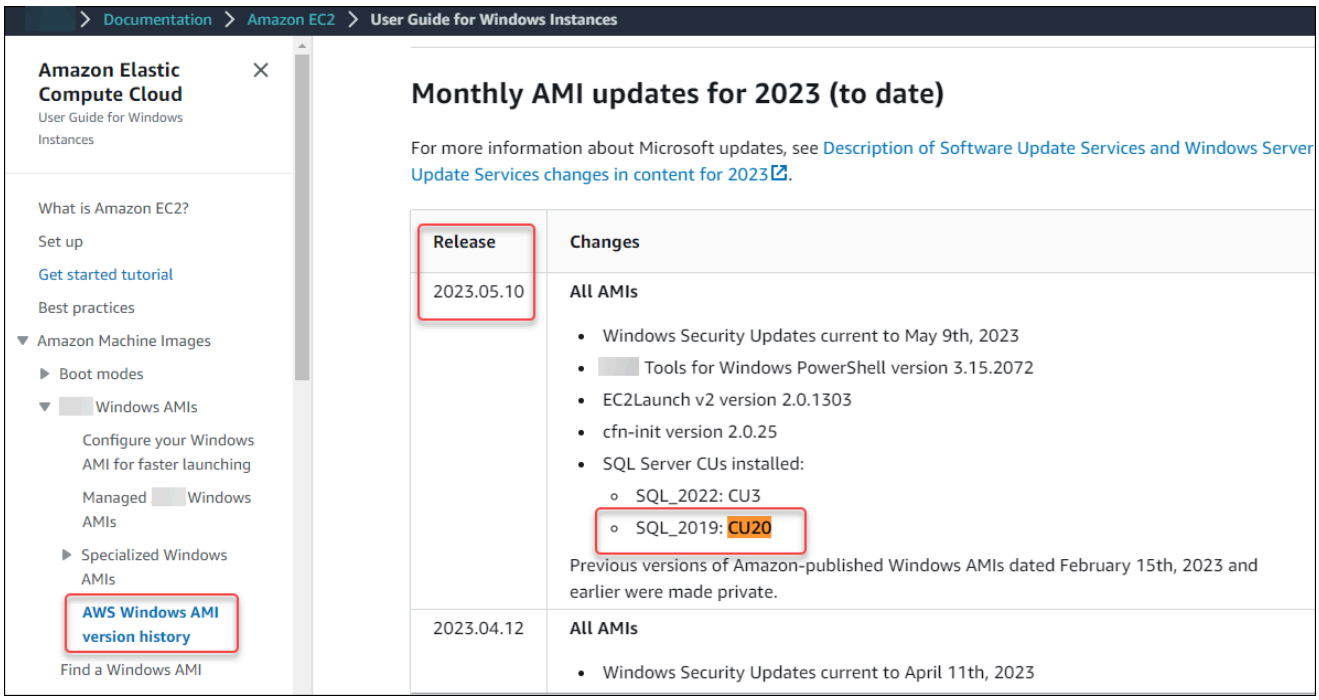
14. Cree una instancia de base de datos de RDS Custom para SQL Server nueva con la CEV. Para ver los pasos detallados, consulte Crear una instancia de base de datos de RDS Custom para SQL Server a partir de una CEV.

Preparación de una CEV con SQL Server (LI) preinstalado

En los siguientes pasos para crear una CEV con Microsoft SQL Server (LI) preinstalado se utiliza una AMI con el número de versión SQL Server CU20 `2023.05.10` como ejemplo. Al crear una CEV, elija una AMI con el número de versión más reciente. Esto garantiza que se utilice una versión compatible de Windows Server y SQL Server con la actualización acumulativa (CU) más reciente.

Para crear una CEV con Microsoft SQL Server (LI) preinstalado

1. Elija la imagen de máquina de Amazon (AMI) de AWS EC2 más reciente disponible con Microsoft Windows Server y SQL Server con licencia incluida (LI).
   a. Busque CU20 en el historial de versiones de AMI para Windows.
   b. Anote el número de versión. Para SQL Server 2019 CU20, el número de versión es `2023.05.10`.

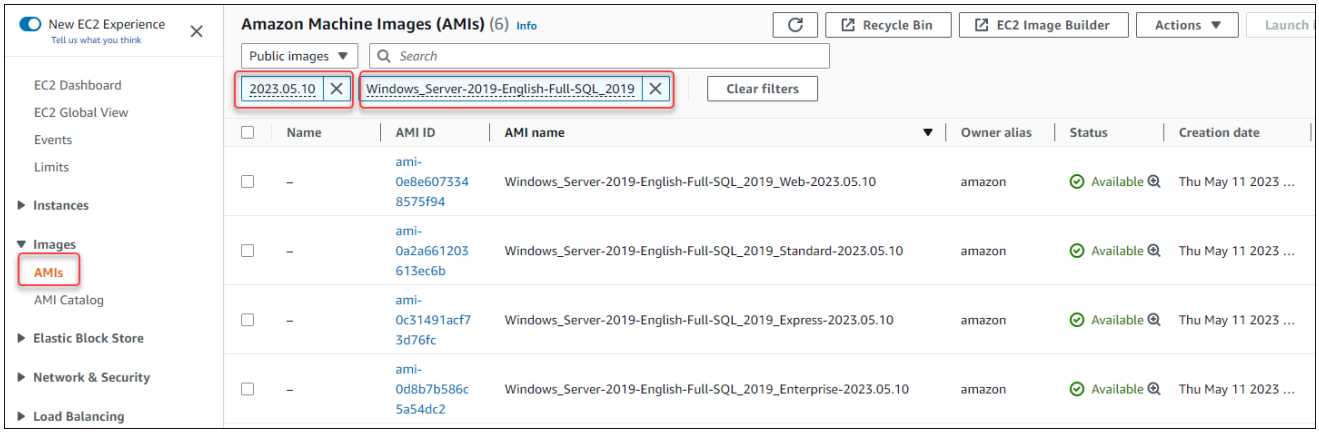


   c. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
   d. En el panel de navegación izquierdo de la consola de Amazon EC2, elija Images (Imágenes) y, luego, AMI.

e. Seleccione Imágenes públicas.

f. Introduzca `2023.05.10` en el cuadro de búsqueda. Aparece una lista de AMI.

g. Introduzca `Windows_Server-2019-English-Full-SQL_2019` en el cuadro de búsqueda para filtrar los resultados. Deberían aparecer los siguientes resultados.



h. Elija la AMI con la edición de SQL Server que desee usar.

2. Cree o lance una instancia EC2 desde la AMI que haya elegido.
3. Inicie sesión en la instancia EC2 e instale software adicional o personalice la configuración del sistema operativo y la base de datos para que cumplan con sus requisitos.
4. Ejecute Sysprep en la instancia EC2. Para obtener más información sobre cómo preparar la AMI con Sysprep, consulte Create a standardized Amazon Machine Image (AMI) using Sysprep (Crear una imagen de máquina de Amazon (AMI) estandarizada con Sysprep).
5. Guarde la AMI que contiene la versión de SQL Server instalada, otro software y las personalizaciones. Esta será su imagen dorada.
6. Cree una CEV nueva con el ID de AMI de la imagen que ha creado. Para ver los pasos detallados sobre la creación de una CEV, consulte Creación de una CEV para RDS Custom para SQL Server.
7. Cree una instancia de base de datos de RDS Custom para SQL Server nueva con la CEV. Para ver los pasos detallados, consulte Crear una instancia de base de datos de RDS Custom para SQL Server a partir de una CEV.

Disponibilidad regional de las CEV de RDS Custom para SQL Server

La compatibilidad con la versión de motor personalizada (CEV) de RDS Custom para SQL Server está disponible en las siguientes Regiones de AWS:

- Este de EE. UU. (Ohio)

- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Oregón)
- Oeste de EE. UU. (Norte de California)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- América del Sur (São Paulo)

Compatibilidad de versiones CEV para RDS Custom para SQL Server

La creación de CEV para RDS Custom para SQL Server es compatible con las siguientes AMI de AWS EC2 Windows:

- Para las CEV que usan medios presintalados, las AMI de AWS EC2 Windows con Microsoft Windows Server 2019 (OS) y SQL Server 2022 o 2019 con licencia incluida (LI)
- Para las CEV que utilizan sus propios medios (BYOM), las AMI de AWS EC2 Windows con Microsoft Windows Server 2019 (OS)

La creación de CEV para RDS Custom para SQL Server es compatible con las siguientes ediciones de sistemas operativos y bases de datos:

- Para las CEV que utilizan medios preinstalados:
  - SQL Server 2022 Enterprise, Standard o Web, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19.

  - SQL Server 2019 Enterprise, Standard o Web, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
- Para las CEV que utilizan sus propios medios (BYOM):
  - SQL Server 2022 Enterprise, Standard o Developer, con CU9, CU13, CU14-GDR, CU15-GDR, CU16, CU17, CU18 y CU19.
  - SQL Server 2019 Enterprise, Standard o Developer, con CU8, CU17, CU18, CU20, CU24, CU26, CU28-GDR, CU29-GDR, CU30 y CU32.
- Para las CEV que utilizan medios preinstalados o sus propios medios (BYOM), Windows Server 2019 es el único sistema operativo compatible.

Para obtener más información, consulte AWS Windows AMI version history.

Requisitos de las CEV para RDS Custom para SQL Server

Los siguientes requisitos se aplican a la creación de una CEV para RDS Custom para SQL Server:

- La AMI utilizada para crear una CEV se debe basar en una configuración de sistema operativo y de base de datos compatible con RDS Custom para SQL Server. Para obtener más información sobre las configuraciones admitidas, consulte Requisitos y limitaciones de Amazon RDS Custom for SQL Server.
- La CEV debe tener un nombre único. No puede crear una CEV con el mismo nombre que una CEV existente.
- El nombre de la CEV debe cumplir el patrón de nomenclatura versión principal + versión secundaria + cadena personalizada de SQL Server. La versión principal + versión secundaria deben coincidir con la versión de SQL Server proporcionada con la AMI. Por ejemplo, puede asignar el siguiente nombre a una AMI con SQL Server 2019 CU17: 15.00.4249.2.my_cevtest.
- Debe preparar una AMI con Sysprep. Para obtener más información sobre cómo preparar la AMI con Sysprep, consulte Create a standardized Amazon Machine Image (AMI) using Sysprep (Crear una imagen de máquina de Amazon (AMI) estandarizada con Sysprep).
- Usted es responsable de mantener el ciclo de vida de la AMI. Una instancia de base de datos de RDS Custom para SQL Server creada a partir de una CEV no almacena una copia de la AMI. Mantiene un puntero a la AMI que utilizó para crear la CEV. La AMI debe existir para que una instancia de base de datos de RDS Custom para SQL Server siga funcionando.

Limitaciones de las CEV para RDS Custom para SQL Server

Se aplican las siguientes limitaciones a las versiones de motor personalizadas con RDS Custom para SQL Server:

- No puede eliminar una CEV si tiene recursos asociados, como instancias de base de datos o instantáneas de base de datos.
- Para crear una instancia de base de datos de RDS Custom para SQL Server, una CEV debe tener el estado `pending-validation`, `available`, `failed` o `validating`. No se puede crear una instancia de base de datos de RDS Custom para SQL Server con una CEV si el estado de la CEV es `incompatible-image-configuration`.
- Para modificar una instancia de base de datos de RDS Custom para SQL Server para que utilice una nueva CEV, la CEV debe tener el estado `available`.
- No se admite la creación de una AMI o CEV a partir de una instancia de base de datos de RDS Custom para SQL Server existente.
- No se puede modificar una CEV existente para que use una AMI diferente. Sin embargo, puede modificar una instancia de base de datos de RDS Custom para SQL Server para que use una CEV distinta. Para obtener más información, consulte Modificación de una instancia de base de datos de RDS Custom for SQL Server.
- No se admite el cifrado de una AMI o CEV con una clave de KMS administrada por el cliente diferente de la clave de KMS proporcionada durante la creación de la instancia de base de datos.
- No se admite la copia de CEV entre regiones.
- No se admite la copia de CEV entre cuentas.
- No puede restaurar ni recuperar una CEV después de eliminarla. No obstante, puede crear una CEV nueva a partir de la misma AMI.
- Una instancia de base de datos de RDS Custom para SQL Server almacena los archivos de base de datos de SQL Server en la unidad D:\. La AMI asociada a una CEV debe almacenar los archivos de la base de datos del sistema Microsoft SQL Server en la unidad C:\.
- Una instancia de base de datos de RDS Custom para SQL Server conserva los cambios de configuración realizados en SQL Server. No se conservan los cambios de configuración del sistema operativo de una instancia de base de datos de RDS Custom para SQL Server en ejecución creada a partir de una CEV. Si necesita realizar un cambio de configuración permanente en el sistema operativo y conservarlo como su nueva configuración de referencia, cree una CEV nueva y modifique la instancia de base de datos para usar la CEV nueva.

> **Important**
>
> Modifique una instancia de base de datos de RDS Custom para SQL Server para usar una CEV nueva en una operación sin conexión. Puede realizar la modificación inmediatamente o programarla para que se produzca durante un período de mantenimiento semanal.

- Al modificar una CEV, Amazon RDS no envía esas modificaciones a ninguna instancia de base de datos de RDS Custom para SQL Server asociada. Debe modificar cada instancia de base de datos de RDS Custom para SQL Server para que use la CEV nueva o actualizada. Para obtener más información, consulte Modificación de una instancia de base de datos de RDS Custom for SQL Server.
-

> **Important**
>
> Si se elimina una AMI utilizada por una CEV, se producirá un error en cualquier modificación que pueda requerir el reemplazo del host, por ejemplo, la computación a escala. A continuación, la instancia de base de datos de RDS Custom para SQL Server se colocará fuera del perímetro de soporte de RDS Custom para SQL Server. Le recomendamos que evite eliminar cualquier AMI que esté asociada a una CEV.

Creación de una CEV para RDS Custom para SQL Server

Puede crear una versión de motor personalizada (CEV, por sus siglas en inglés) mediante laAWS CLI o la AWS Management Console. A continuación, puede utilizar la CEV para crear una instancia de base de datos de RDS Custom para SQL Server.

Asegúrese de que la imagen de máquina de Amazon (AMI) esté en la misma cuenta y región de AWS que su CEV. De lo contrario, el proceso para crear un CEV falla.

Para obtener más información, consulte Creación y conexión a una instancia de base de datos para Amazon RDS Custom for SQL Server.

> **Important**
>
> Los pasos para crear una CEV son los mismos para las AMI creadas con SQL Server preinstalado y para las creadas con Bring Your Own Media (BYOM).

Consola

Para crear una CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).

   La página de Custom engine versions (Versiones de motor personalizadas) muestra todos las CEV que existen actualmente. Si no ha creado ninguna CEV, la página estará vacía.
3. Elija Crear versión de motor personalizada.
4. En Engine type (Tipo de motor), elija Microsoft SQL Server.
5. En Edición, elija la edición del motor de base de datos que desee utilizar.
6. En Major version (Versión principal), elija la versión principal del motor que está instalada en su AMI.
7. En Version details (Detalles de la versión), ingrese un nombre válido en Custom engine version name (Nombre de versión del motor personalizada).

   El formato del nombre es *major-engine-version*.*minor-engine-version*.*customized_string*. Puede utilizar de 1 a 50 caracteres alfanuméricos, guiones bajos, guiones y puntos. Por ejemplo, puede ingresar el nombre **15.00.4249.2.my_cevtest**.

   De manera opcional, ingrese una descripción para su CEV.
8. Para Installation Media (Medios de instalación), busque o introduzca el ID de AMI desde el que desea crear la CEV.
9. En la sección Tags (Etiquetas), añada cualquier etiqueta para identificar la CEV.
10. Elija Crear versión de motor personalizada.

Aparece la página de Custom engine versions (Versiones de motor personalizadas). Su CEV se muestra con el estado pending-validation

AWS CLI

Para crear una CEV mediante la AWS CLI, ejecute el comando create-custom-db-engine-version.

Se requieren las siguientes opciones:

- `--engine`

- `--engine-version`
- `--image-id`

También puede especificar las siguientes opciones:

- `--description`
- `--region`
- `--tags`

El siguiente ejemplo crea una CEV denominado `15.00.4249.2.my_cevtest`. Asegúrese de que el nombre de la CEV comience con el número de versión principal del motor.

Example

Para Linux, macOS o:Unix

```
aws rds create-custom-db-engine-version \
    --engine custom-sqlserver-ee \
    --engine-version 15.00.4249.2.my_cevtest \
    --image-id ami-0r93cx31t5r596482 \
    --description "Custom SQL Server EE 15.00.4249.2 cev test"
```

En la siguiente salida parcial se muestra el motor, los grupos de parámetros y otra información.

```
"DBEngineVersions": [
    {
    "Engine": "custom-sqlserver-ee",
    "MajorEngineVersion": "15.00",
    "EngineVersion": "15.00.4249.2.my_cevtest",
    "DBEngineDescription": "Microsoft SQL Server Enterprise Edition for RDS Custom for
 SQL Server",
    "DBEngineVersionArn": "arn:aws:rds:us-east-1:<my-account-id>:cev:custom-sqlserver-
ee/15.00.4249.2.my_cevtest/a1234a1-123c-12rd-bre1-1234567890",
    "DBEngineVersionDescription": "Custom SQL Server EE 15.00.4249.2 cev test",

    "Image": [
        "ImageId": "ami-0r93cx31t5r596482",
        "Status": "pending-validation"
     ],
```

```
    "CreateTime": "2022-11-20T19:30:01.831000+00:00",
    "SupportsLogExportsToCloudwatchLogs": false,
    "SupportsReadReplica": false,
    "Status": "pending-validation",
    "SupportsParallelQuery": false,
    "SupportsGlobalDatabases": false,
    "TagList": []
    }
]
```

Si se produce un error en el proceso de creación de una CEV, RDS Custom para SQL Server emite `RDS-EVENT-0198` con el mensaje `Creation failed for custom engine version` *`major-engine-version.cev_name`*. El mensaje incluye detalles sobre el error, por ejemplo, el evento imprime los archivos que faltan. Para encontrar ideas para solucionar problemas de creación de CEV, consulte Solución de errores de CEV para RDS Custom para SQL Server.

Crear una instancia de base de datos de RDS Custom para SQL Server a partir de una CEV

Una vez que haya creado correctamente una CEV, se mostrará el CEV status (Estado de la CEV) `pending-validation`. A continuación, puede utilizar la CEV para crear una instancia de base de datos de RDS Custom para SQL Server nueva. Para crear una instancia de base de datos de RDS Custom para SQL Server a partir de una CEV, consulte Creación de una instancia de base de datos de RDS Custom para SQL Server.

Ciclo de vida de una CEV

El ciclo de vida de CEV incluye los siguientes estados.

Estado de CEV	Descripción	Sugerencias para la solución de problemas	
`pending-validation`	Se ha creado una CEV y está pendiente de la validación de la AMI asociada. Una CEV permanecerá activa en `pending-validation`	Si no existen tareas, crea una nueva instancia de base de datos de RDS Custom para SQL Server a partir de la CEV. Al crear la instancia de base de datos de RDS Custom para SQL Server, el sistema intenta validar la AMI asociada para una CEV.	

Estado de CEV	Descripción	Sugerencias para la solución de problemas	
	hasta que se cree una instancia de base de datos de RDS Custom para SQL Server a partir de ella.		
`validating`	Está en curso una tarea de creación de la instancia de base de datos de RDS Custom para SQL Server basada en una CEV nueva. Al crear la instancia de base datos de RDS Custom for SQL Server, el sistema intenta validar la AMI asociada de una CEV nueva.	Espere a que finalice la tarea de creación de la instancia de base de datos de RDS Custom para SQL Server. Puede utilizar la consola de RDS EVENTS para revisar los mensajes de eventos detallados a fin de solucionar problemas.	

Estado de CEV	Descripción	Sugerencias para la solución de problemas	
`available`	La CEV se ha validado correctamente. Una CEV pasará a tener el estado `available` cuando se cree correctamente una instancia de base de datos de RDS Custom para SQL Server a partir de ella.	La CEV no requiere ninguna validació n adicional. Puede usarse para crear instancias de base de datos de RDS Custom para SQL Server adicionales o para modificar las existentes.	
`inactive`	La CEV ha cambiado a un estado inactivo.	No se puede crear ni actualizar una instancia de base de datos de RDS Custom con esta CEV. Además, no puede restaurar una instantánea de base de datos para crear una nueva instancia de base de datos de RDS Custom con esta CEV. Para obtener información sobre cómo cambiar el estado a `ACTIVE`, consulte Modificación de una CEV para RDS Custom para SQL Server.	

Estado de CEV	Descripción	Sugerencias para la solución de problemas	
`failed`	No se ha podido realizar el paso de creación de la instancia de base de datos para esta CEV antes de validar la AMI. Alternativamente, la AMI subyacente utilizada por la CEV no estaba disponible.	Solucione la causa principal por la que el sistema no ha podido crear la instancia de base de datos. Consulte el mensaje de error detallado e intente crear una nueva instancia de base de datos. Asegúrese de que la AMI subyacente utilizada por la CEV esté disponible.	

Estado de CEV	Descripción	Sugerencias para la solución de problemas	
`incompatible-image-configuration`	Se ha producido un error al validar la AMI.	Consulte los detalles técnicos del error. No puede volver a intentar validar la AMI con esta CEV. Revise lo siguiente: recomendaciones: • Asegúrese de que su CEV se denomine con el patrón de nomenclatura requerido versión principal + versión secundaria + cadena personalizada de SQL Server. • Asegúrese de que la versión de SQL Server en el nombre de la CEV coincida con la versión proporcionada con la AMI. • Asegúrese de que la versión de compilación del sistema operativo cumpla con la versión de compilación mínima requerida. • Asegúrese de que la versión principal del sistema operativo cumpla con la versión de compilación principal requerida. Cree una nueva CEV con la información correcta. Si es necesario, cree una nueva instancia de EC2 con una AMI compatible y ejecute el proceso de Sysprep en ella.	

Modificación de una CEV para RDS Custom para SQL Server

Puede modificar una CEV mediante la AWS Management Console o la AWS CLI. Puede modificar la descripción de la CEV o su estado de disponibilidad. La CEV tiene uno de los siguientes valores de estado:

- `available` – Puede utilizar esta CEV para crear una nueva instancia de base de datos de RDS Custom o actualizar una instancia de base de datos. Este es el estado predeterminado de una CEV recién creada.
- `inactive` – No se puede crear ni actualizar una instancia de base de datos de RDS Custom con esta CEV. No puede restaurar una instantánea de base de datos para crear una nueva instancia de base de datos de RDS Custom con esta CEV.

Puede cambiar el estado de la CEV de `available` a `inactive` o de `inactive` a `available`. Puede cambiar el estado a `INACTIVE` para evitar el uso accidental de una CEV o hacer que una CEV interrumpida pueda utilizarse de nuevo.

Consola

Para modificar una CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).
3. Elija una CEV cuya descripción o estado desee modificar.
4. Para Actions (Acciones), elija Modify (Modificar).
5. Realice cualquiera de los siguientes cambios:
   - Para CEV status settings (Configuración del estado de CEV), elija un nuevo estado de disponibilidad.
   - Para Version description (Descripción de la versión), ingrese una nueva descripción.
6. Elija Modify CEV (Modificar CEV).

   Si la CEV está en uso, la consola muestra You can't modify the CEV status (No se puede modificar el estado de la CEV). Corrija los problemas e inténtelo de nuevo.

Aparece la página de Custom engine versions (Versiones de motor personalizadas).

AWS CLI

Para modificar una CEV mediante la AWS CLI, ejecute el comando modify-custom-db-engine-version. Puede encontrar las CEV para modificarlas al ejecutar el comando describe-db-engine-versions.

Se requieren las siguientes opciones:

- `--engine`
- `--engine-version` *`cev`*, donde *`cev`* es el nombre de la versión del motor personalizada que desea modificar
- `--status` *`status`*, donde *`status`* es el estado de disponibilidad que desea asignar a la CEV

En el siguiente ejemplo se cambia una CEV denominada `15.00.4249.2.my_cevtest` de su estado actual a `inactive`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-custom-db-engine-version \
    --engine custom-sqlserver-ee \
    --engine-version 15.00.4249.2.my_cevtest \
    --status inactive
```

En:Windows

```
aws rds modify-custom-db-engine-version ^
    --engine custom-sqlserver-ee ^
    --engine-version 15.00.4249.2.my_cevtest ^
    --status inactive
```

Para modificar una instancia de base de datos de RDS Custom para SQL Server para usar una CEV nueva, consulte Modificación de una instancia de base de datos de RDS Custom para SQL Server para usar una CEV nueva.

Modificación de una instancia de base de datos de RDS Custom para SQL Server para usar una CEV nueva

Puede modificar una instancia de base de datos de RDS Custom para SQL Server para usar una CEV distinta. Los cambios que puede realizar son los siguientes:

- Modificar la CEV
- Cambiar la clase de instancia de base de datos
- Cambiar el periodo de retención de copia de seguridad y la ventana de la copia de seguridad

- Cambio del periodo de mantenimiento

Consola

Para modificar una instancia de base de datos de RDS Custom for SQL Server

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea modificar.
4. Elija Modify.
5. Realice los siguientes cambios según sea necesario:
   a. Para DB engine version (Versión del motor de base de datos), elija una CEV diferente.
   b. Cambie el valor de DB instance class (Clase de instancia de base de datos). Para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL.
   c. Cambie el valor de Backup retention period (Periodo de retención de copia de seguridad).
   d. Para Backup window (Periodo de la copia de seguridad), establezca valores para la Start time (Hora de inicio) y la Duration (Duración).
   e. Para el DB instance maintenance window (Periodo de mantenimiento de la instancia de base de datos), establezca valores para el Start day (Día de inicio), la Start time (Hora de inicio) y la Duration (Duración).
6. Elija Continuar.
7. Elija Apply immediately (Aplicar inmediatamente) o Apply during the next scheduled maintenance window (Aplicar durante el próximo periodo de mantenimiento programado).
8. Elija Modify DB instance (Modificar la instancia de base de datos).

> **Note**
>
> Al modificar una instancia de base de datos de una CEV a otra CEV, por ejemplo, al actualizar una versión secundaria, las bases de datos del sistema SQL Server, incluidos sus datos y configuraciones, se conservan de la instancia de base de datos de RDS Custom para SQL Server actual.

AWS CLI

Para modificar una instancia de base de datos para que use una CEV distinta mediante la AWS CLI, ejecute el comando modify-db-instance.

Se requieren las siguientes opciones:

- `--db-instance-identifier`
- `--engine-version` *`cev`*, donde *`cev`* es el nombre de la versión del motor personalizada al que desea que cambie la instancia de base de datos.

En el siguiente ejemplo, se modifica una instancia de base de datos denominada `my-cev-db-instance` para que utilice una CEV denominada `15.00.4249.2.my_cevtest_new`. El cambio se aplica inmediatamente.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-cev-db-instance \
    --engine-version 15.00.4249.2.my_cevtest_new \
    --apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-cev-db-instance ^
    --engine-version 15.00.4249.2.my_cevtest_new ^
    --apply-immediately
```

Visualización de detalles de la CEV de Amazon RDS Custom para SQL Server

Puede ver los detalles de su CEV mediante la AWS Management Console o la AWS CLI.

Consola

Para ver los detalles de la CEV

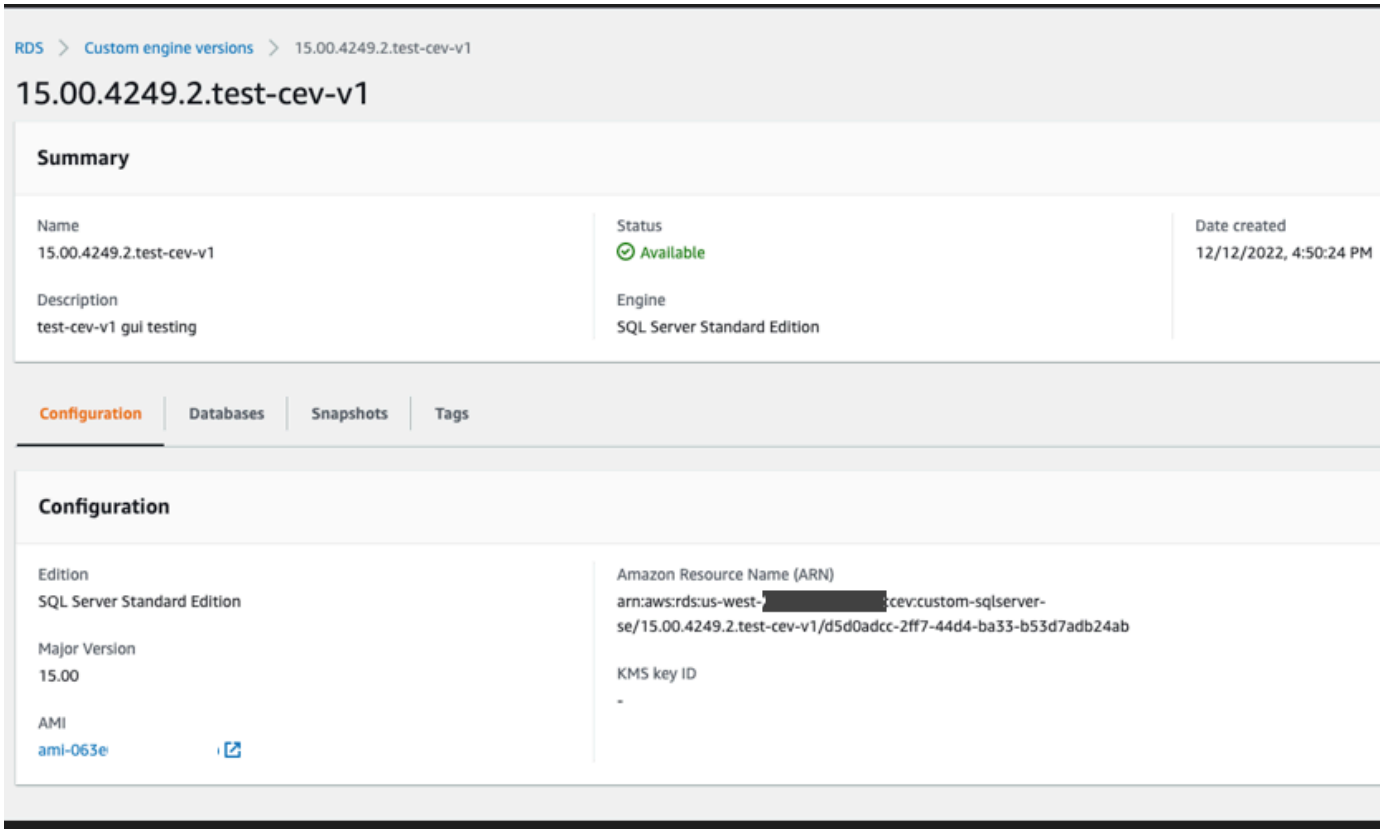
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).

   La página de Custom engine versions (Versiones de motor personalizadas) muestra todos las CEV que existen actualmente. Si no ha creado ninguna CEV, la página está vacía.

3. Elija el nombre de la CEV que desea ver.

4. Para ver los detalles, elija Configuration (Configuración).



AWS CLI

Para ver los detalles de una CEV mediante la AWS CLI, ejecute el comando describe-db-engine-versions.

También puede especificar las siguientes opciones:

- `--include-all`, para ver todas las CEV con cualquier estado de ciclo de vida. Sin la opción `--include-all`, solo se devolverán las CEV con el estado de ciclo de vida `available`.

```
aws rds describe-db-engine-versions --engine custom-sqlserver-ee --engine-version
 15.00.4249.2.my_cevtest --include-all
```

```
{
    "DBEngineVersions": [
        {
            "Engine": "custom-sqlserver-ee",
            "MajorEngineVersion": "15.00",
            "EngineVersion": "15.00.4249.2.my_cevtest",
            "DBParameterGroupFamily": "custom-sqlserver-ee-15.0",
            "DBEngineDescription": "Microsoft SQL Server Enterprise Edition for custom
 RDS",
            "DBEngineVersionArn": "arn:aws:rds:us-east-1:{my-account-id}:cev:custom-
sqlserver-ee/15.00.4249.2.my_cevtest/a1234a1-123c-12rd-bre1-1234567890",
            "DBEngineVersionDescription": "Custom SQL Server EE 15.00.4249.2 cev test",
            "Image": {
                "ImageId": "ami-0r93cx31t5r596482",
                "Status": "pending-validation"
            },
            "DBEngineMediaType": "AWS Provided",
            "CreateTime": "2022-11-20T19:30:01.831000+00:00",
            "ValidUpgradeTarget": [],
            "SupportsLogExportsToCloudwatchLogs": false,
            "SupportsReadReplica": false,
            "SupportedFeatureNames": [],
            "Status": "pending-validation",
            "SupportsParallelQuery": false,
            "SupportsGlobalDatabases": false,
            "TagList": [],
            "SupportsBabelfish": false
        }
    ]
}
```

Puede usar filtros para ver las CEV con un estado de ciclo de vida determinado. Por ejemplo, para ver las CEV que tienen un estado de ciclo de vida de `pending-validation`, `available` o `failed`:

```
aws rds describe-db-engine-versions engine custom-sqlserver-ee
                region us-west-2 include-all query 'DBEngineVersions[?Status ==
 pending-validation ||
                Status == available || Status == failed]'
```

Eliminación de una CEV para RDS Custom para SQL Server

Puede eliminar una CEV con la AWS Management Console o la AWS CLI. Esto normalmente dura unos minutos.

Antes de eliminar una CEV, asegúrese de no que no la esté usando ninguna de las siguientes opciones:

- Una instancia de base de datos de RDS Custom
- Instantánea de una instancia de base de datos de RDS Custom
- Una copia de seguridad automatizada de su instancia de base de datos de RDS Custom

Consola

Para eliminar una CEV

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Custom engine versions (Versiones de motor personalizadas).
3. Elija una CEV cuya descripción o estado desea eliminar.
4. En Actions (Acciones), seleccione Delete (Eliminar).

   Aparece el cuadro de diálogo Delete ***cev_name***? (¿Desea eliminar cev_name?).
5. Introduzca **`delete me`** y luego escriba Delete (Eliminar).

   En la página de Custom engine versions (Versiones de motor personalizadas), el banner muestra que se está eliminando su CEV.

AWS CLI

Para eliminar una CEV mediante la AWS CLI, ejecute el comando delete-custom-db-engine-version.

Se requieren las siguientes opciones:

- `--engine custom-sqlserver-ee`
- `--engine-version` *`cev`*, donde *`cev`* es el nombre de la versión del motor personalizada que se va a eliminar

El siguiente ejemplo elimina una CEV denominada `15.00.4249.2.my_cevtest`.

Example

Para Linux, macOS o:Unix

```
aws rds delete-custom-db-engine-version \
    --engine custom-sqlserver-ee \
    --engine-version 15.00.4249.2.my_cevtest
```

En:Windows

```
aws rds delete-custom-db-engine-version ^
    --engine custom-sqlserver-ee ^
    --engine-version 15.00.4249.2.my_cevtest
```

Creación y conexión a una instancia de base de datos para Amazon RDS Custom for SQL Server

Puede crear una instancia de base de datos de RDS Custom y, a continuación, conectarse a ella mediante AWS Systems Manager o Remote Desktop Protocol (RDP).

> **Important**
>
> Antes de que pueda crear o conectarse a una instancia de base de datos de RDS Custom for SQL Server, asegúrese de completar las tareas en Configuración del entorno para Amazon RDS Custom for SQL Server.
>
> Puede etiquetar instancias de base de datos de RDS Custom cuando las crea, pero no cree ni modifique la etiqueta `AWSRDSCustom` necesaria para la automatización de RDS Custom. Para obtener más información, consulte Etiquetado de los recursos de RDS Custom for SQL Server.
>
> La primera vez que crea una instancia de base de datos de RDS Custom for SQL Server, podría recibir el siguiente error: The service-linked role is in the process of being created (El rol vinculado al servicio se está creando). Inténtelo de nuevo más tarde. Si lo hace, espere unos minutos e intente crear la instancia de base de datos de nuevo.

Temas

- Creación de una instancia de base de datos de RDS Custom para SQL Server
- Rol vinculado al servicio de RDS Custom
- Conexión a la instancia de base de datos de RDS Custom DB mediante AWS Systems Manager
- Conexión a la instancia de base de datos de RDS Custom mediante RDP

Creación de una instancia de base de datos de RDS Custom para SQL Server

Cree una instancia de base de datos de Amazon RDS Custom for SQL Server mediante la AWS Management Console o la AWS CLI. El procedimiento es similar al que se debe seguir para crear una instancia de base de datos de Amazon RDS.

Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

Consola

Para crear una instancia de base de datos de RDS Custom for SQL Server

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija Create database (Crear base de datos).
4. Elija Standard Create (Creación estándar) para el método de creación de la base de datos.
5. Para Engine options (Opciones del motor), elija Microsoft SQL Server para el tipo de motor.
6. Para Database management type (Tipo de administración de base de datos), elija Amazon RDS Custom.
7. En la sección Edition (Edición), elija la edición del motor de base de datos que desea utilizar.
8. (Opcional) Si tiene la intención de crear la instancia de base de datos a partir de una CEV, active la casilla Use custom engine version (CEV) (Usar versión de motor personalizada [CEV]). En la lista desplegable, seleccione CEV.
9. Para Versión de la base de datos, mantenga el valor predeterminado de la versión.
10. Para Templates (Plantillas), elija Production (Producción).
11. En la sección Settings (Configuración), ingrese un nombre exclusivo para el DB instance identifier (Identificador de instancias de bases de datos).
12. Para ingresar la contraseña maestra, proceda del modo siguiente:

    a. En la sección Settings (Configuración), abra Credential Settings (Configuración de credenciales).

    b. Desmarque la casilla Auto generate a password (Generar automáticamente una contraseña).

    c. Cambie el valor del Master username (Nombre de usuario maestro) e ingrese la misma contraseña en Master password (Contraseña maestra) y Confirm password (Confirmar contraseña).

    De forma predeterminada, la nueva instancia de base de datos de RDS Custom utiliza una contraseña generada automáticamente para el usuario maestro.
13. En la sección DB instance size (Tamaño de la instancia de base de datos), elija un valor para la DB instance class Clase de instancia de base de datos.

Para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL.

14. Elija la configuración de Storage (Almacenamiento).
15. Para RDS Custom security (Seguridad de RDS Custom), realice una de las siguientes opciones:

    a. Para el perfil de instancia IAM tiene dos opciones para elegir el perfil de instancia para la instancia de base de datos de RDS Custom para SQL Server.

        1. Elija Crear un nuevo perfil de instancia y proporcione un sufijo de nombre de perfil de instancia. Para obtener más información, consulte Creación automática de perfiles de instancias mediante la AWS Management Console.
        2. Elija un perfil de instancia existente. En la lista desplegable, elige el perfil de instancia que comience por `AWSRDSCustom`.

    b. Para Encryption (Cifrado), elija Enter a key ARN (Ingresar una ARN de clave) para enumerar las claves de AWS KMS disponibles. A continuación, elija la clave de la lista.

        Se requiere una clave AWS KMS para RDS Custom. Para obtener más información, consulte Asegúrese de que tiene una clave de cifrado simétrica AWS KMS.

16. Para las secciones restantes, especifique la configuración de la instancia de base de datos de RDS Custom que prefiera. Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos. La siguiente configuración no aparece en la consola y no se admite:

    - Processor features (Características del procesador)
    - Storage autoscaling (Escalado automático de almacenamiento)
    - Disponibilidad y durabilidad
    - Opción de Password and Kerberos authentication (autenticación de Contraseña y Kerberos) en la Database authentication (Autenticación de base de datos) (solo se admite Password authentication [Autenticación de contraseña])
    - Grupo de Database options (Opciones de base de datos) en Additional configuration (Configuración adicional)
    - Performance Insights (Información sobre rendimiento)
    - Log exports (Exportaciones de registros)
    - Enable auto minor version upgrade (Habilitar la actualización automática de la versión secundaria)

- Deletion protection (Protección contra eliminación

Backup retention period (Periodo de retención de copia de seguridad) es compatible, pero no puedes elegir 0 días.

17. Elija Crear base de datos.

    El botón View credential details (Ver detalles de la credencial) aparece en la página Databases (Bases de datos).

    Para ver el nombre de usuario y la contraseña maestros para la instancia de base de datos de RDS Custom, elija View credential details (Ver detalles de credenciales).

    Para conectarse a la instancia de base de datos como usuario maestro, utilice el nombre de usuario y la contraseña que aparecen.

    > **Important**
    >
    > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla. Para cambiar la contraseña del usuario maestro después de que la instancia de base de datos de RDS Custom esté disponible, modifique la instancia de base de datos. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Administración de una instancia de base de datos para Amazon RDS Custom for SQL Server.

18. Elija Databases (Bases de datos) para ver la lista de instancias de base de datos de RDS Custom.
19. Elija la instancia de base de datos de RDS Custom que acaba de crear.

    En la consola de RDS, aparecen los detalles de la nueva instancia de base de datos de RDS Custom:

    - La instancia de base de datos tiene un estado de creating (creación) hasta que la instancia de base de datos de RDS Custom se crea y está lista para su uso. Cuando el estado cambie a available (disponible), podrá conectarse a la instancia de base de datos. En función de la clase de instancia y el almacenamiento asignado, la nueva instancia de base de datos puede tardar varios minutos en estar disponible.
    - El Role (Rol) tiene el valor Instance (RDS Custom) [Instancia (RDS Custom]).

- El RDS Custom automation mode (Modo de automatización de RDS Custom) tiene el valor Full automation (Automatización completa). Esta configuración significa que la instancia de base de datos proporciona monitoreo automático y recuperación de instancias.

AWS CLI

Puede crear una instancia de base de datos de RDS Custom mediante el comando AWS CLI create-db-instance.

Se requieren las siguientes opciones:

- `--db-instance-identifier`
- `--db-instance-class` (para obtener una lista de clases de instancias admitidas, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL)
- `--engine` (`custom-sqlserver-ee`, `custom-sqlserver-se` o `custom-sqlserver-web`)
- `--kms-key-id`
- `--custom-iam-instance-profile`

El siguiente ejemplo crea una instancia de base de datos de RDS Custom for SQL Server denominada `my-custom-instance`. El periodo de retención de copia de seguridad es de 3 días.

> **Note**
>
> Para crear una instancia de base de datos a partir de una versión de motor personalizada (CEV, por sus siglas en inglés), proporcione un nombre CEV existente al parámetro `--engine-version`. Por ejemplo, `--engine-version 15.00.4249.2.my_cevtest`

Example

Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --engine custom-sqlserver-ee \
    --engine-version 15.00.4073.23.v1 \
    --db-instance-identifier my-custom-instance \
    --db-instance-class db.m5.xlarge \
```

```
    --allocated-storage 20 \
    --db-subnet-group mydbsubnetgroup \
    --master-username myuser \
    --master-user-password mypassword \
    --backup-retention-period 3 \
    --no-multi-az \
    --port 8200 \
    --kms-key-id mykmskey \
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance
```

En:Windows

```
aws rds create-db-instance ^
    --engine custom-sqlserver-ee ^
    --engine-version 15.00.4073.23.v1 ^
    --db-instance-identifier my-custom-instance ^
    --db-instance-class db.m5.xlarge ^
    --allocated-storage 20 ^
    --db-subnet-group mydbsubnetgroup ^
    --master-username myuser ^
    --master-user-password mypassword ^
    --backup-retention-period 3 ^
    --no-multi-az ^
    --port 8200 ^
    --kms-key-id mykmskey ^
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Obtenga detalles sobre la instancia mediante el comando `describe-db-instances`.

```
aws rds describe-db-instances --db-instance-identifier my-custom-instance
```

En la siguiente salida parcial se muestra el motor, los grupos de parámetros y otra información.

```
{
    "DBInstances": [
```

```
        {
            "PendingModifiedValues": {},
            "Engine": "custom-sqlserver-ee",
            "MultiAZ": false,
            "DBSecurityGroups": [],
            "DBParameterGroups": [
                {
                    "DBParameterGroupName": "default.custom-sqlserver-ee-15",
                    "ParameterApplyStatus": "in-sync"
                }
            ],
            "AutomationMode": "full",
            "DBInstanceIdentifier": "my-custom-instance",
            "TagList": []
        }
    ]
}
```

Rol vinculado al servicio de RDS Custom

Un service-linked role (rol vinculado al servicio) le otorga a Amazon RDS Custom acceso a los recursos de su Cuenta de AWS. Facilita el uso de RDS Custom porque no tiene que agregar manualmente los permisos necesarios. RDS Custom define los permisos de sus roles vinculados al servicio y, a menos que se defina lo contrario, solo RDS Custom puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Cuando crea una instancia de base de datos de RDS Custom, se crean y utilizan los roles vinculados a servicios de Amazon RDS y RDS Custom (si aún no existen). Para obtener más información, consulte Uso de roles vinculados a servicios de Amazon RDS.

La primera vez que crea una instancia de base de datos de RDS Custom for SQL Server, podría recibir el siguiente error: The service-linked role is in the process of being created (El rol vinculado al servicio se está creando). Inténtelo de nuevo más tarde. Si lo hace, espere unos minutos e intente crear la instancia de base de datos de nuevo.

Conexión a la instancia de base de datos de RDS Custom DB mediante AWS Systems Manager

Una vez que haya creado la instancia de base de datos de RDS Custom, puede conectarse a ella mediante Session Manager AWS Systems Manager. Session Manager es una capacidad de

Systems Manager que puede utilizar para administrar instancias de Amazon EC2 a través de un shell basado en navegador o mediante la AWS CLI. Para obtener más información, consulte AWSSystems Manager Session Manager.

Consola

Para conectarse a su instancia de base de datos mediante Session Manager

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos de RDS Custom que desea detener.
3. Elija Configuration (Configuración).
4. Tenga en cuenta el valor de Resource ID (ID de recurso) para la instancia de base de datos. Por ejemplo, el ID del recurso puede ser `db-ABCDEFGHIJKLMNOPQRS0123456`.
5. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
6. En el panel de navegación, elija Instances (Instancias).
7. Busque el nombre de la instancia EC2 y, a continuación, elija el ID de instancia asociado a ella. Por ejemplo, el ID de instancia puede ser `i-abcdefghijklm01234`.
8. Elija Connect (Conectar).
9. Elija Session Manager.
10. Elija Conectar.

    Se abre una ventana para la sesión.

AWS CLI

Puede conectarse a la instancia de base de datos de RDS Custom mediante la AWS CLI. Esta técnica requiere el complemento Session Manager para la AWS CLI. Para obtener información sobre cómo instalar el complemento, consulte Install the Session Manager plugin for the AWS CLI (Instale el complemento Session Manager).

Para encontrar el ID de recurso de base de datos de la instancia de base de datos de RDS Custom, utilice `describe-db-instances`.

```
aws rds describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
```

```
    --output text
```

En el siguiente ejemplo de resultado se muestra el ID de recurso de la instancia de RDS Custom. El prefijo es `db-`.

```
db-ABCDEFGHIJKLMNOPQRS0123456
```

Para buscar el ID de instancia EC2 de la instancia de base de datos, utilice `aws ec2 describe-instances`. El siguiente ejemplo utiliza `db-ABCDEFGHIJKLMNOPQRS0123456` para el ID del recurso.

```
aws ec2 describe-instances \
    --filters "Name=tag:Name,Values=db-ABCDEFGHIJKLMNOPQRS0123456" \
    --output text \
    --query 'Reservations[*].Instances[*].InstanceId'
```

El siguiente ejemplo muestra el ID de instancia EC2.

```
i-abcdefghijklm01234
```

Use el comando `aws ssm start-session`, proporcionando el ID de instancia EC2 en el parámetro `--target`.

```
aws ssm start-session --target "i-abcdefghijklm01234"
```

Una conexión exitosa sería como la siguiente.

```
Starting session with SessionId: yourid-abcdefghijklm1234
[ssm-user@ip-123-45-67-89 bin]$
```

Conexión a la instancia de base de datos de RDS Custom mediante RDP

Después de crear su instancia de base de datos de RDS Custom, puede conectarse a esta instancia mediante un cliente RDP. El procedimiento es el mismo que para conectarse a una instancia de Amazon EC2. Para obtener más información, consulte Conexión con su instancia de Windows.

Para conectarse a la instancia de base de datos, necesita el par de claves asociado a la instancia. RDS Custom crea el par de claves por usted. El nombre del par utiliza el prefijo `do-not-delete-`

`rds-custom-DBInstanceIdentifier`. AWS Secrets Manager almacena la clave privada como secreto.

Complete la tarea en los siguientes pasos:

1. Configurar la instancia de base de datos para permitir conexiones RDP.
2. Recuperar la clave secreta.
3. Conéctese a la instancia EC2 mediante la utilidad RDP.

Configurar la instancia de base de datos para permitir conexiones RDP

Para permitir conexiones RDP, configure el grupo de seguridad de la VPC y establezca una regla de firewall en el host.

Configure los grupos de seguridad de la VPC

Asegúrese de que el grupo de seguridad de la VPC asociado a su instancia de base de datos permita conexiones entrantes en el puerto 3389 para Transmission Control Protocol (TCP). Para obtener información sobre cómo configurar el grupo de seguridad de la VPC, consulte Configure los grupos de seguridad de la VPC.

Establecer la regla de firewall en el host

Para permitir conexiones entrantes en el puerto 3389 para TCP, establezca una regla de firewall en el host. El siguiente ejemplo muestra cómo hacerlo.

Le recomendamos que use el valor específico `-Profile`: `Public`, `Private` o `Domain`. El uso de `Any` se refiere a los tres valores. También puede especificar una combinación de valores separados por una coma. Para obtener más información sobre la configuración de reglas de firewall, consulte Set-NetFirewallRule en la documentación de Microsoft.

Cómo usar el administrador de sesiones de Systems Manager para establecer una regla de firewall

1. Conéctese a Session Manager como se muestra en Conexión a la instancia de base de datos de RDS Custom DB mediante AWS Systems Manager.
2. Ejecute el siguiente comando de la .

```
Set-NetFirewallRule -DisplayName "Remote Desktop - User Mode (TCP-In)" -Direction
 Inbound -LocalAddress Any -Profile Any
```

Cómo usar los comandos de la CLI de Systems Manager para establecer una regla de firewall

1. Utilice el siguiente comando para abrir RDP en el host.

```
OPEN_RDP_COMMAND_ID=$(aws ssm send-command --region $AWS_REGION \
    --instance-ids $RDS_CUSTOM_INSTANCE_EC2_ID \
    --document-name "AWS-RunPowerShellScript" \
    --parameters '{"commands":["Set-NetFirewallRule -DisplayName \"Remote Desktop -
 User Mode (TCP-In)\" -Direction Inbound -LocalAddress Any -Profile Any"]}' \
    --comment "Open RDP port" | jq -r ".Command.CommandId")
```

2. Utilice el ID del comando devuelto en el resultado para obtener el estado del comando anterior. Para utilizar la siguiente consulta para devolver el ID del comando, asegúrese de tener el complemento jq instalado.

```
aws ssm list-commands \
    --region $AWS_REGION \
    --command-id $OPEN_RDP_COMMAND_ID
```

Recuperar la clave secreta

Recuperar la clave secreta mediante la AWS Management Console o la AWS CLI.

Consola

Para recuperar la clave secreta

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos de RDS Custom que desea detener.
3. Elija la pestaña Configuration (Configuración).
4. Tenga en cuenta el DB instance ID (ID de la instancia de base de datos) para su instancia de base de datos, por ejemplo *my-custom-instance*.
5. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
6. En el panel de navegación, elija Instances (Instancias).
7. Busque el nombre de la instancia EC2 y, a continuación, elija el ID de instancia asociado a ella.

   En este ejemplo, el ID de la instancia es `i-abcdefghijklm01234`.

8. En Details (Detalles), busque el Key pair name (Nombre del par de claves). El nombre del par incluye el identificador de base de datos. En este ejemplo, el nombre del par es `do-not-delete-rds-custom-`*`my-custom-instance`*`-`*`0d726c`*.
9. En el resumen de la instancia, busque Public IPv4 DNS (DNS IPv4 público). Por ejemplo, el DNS público podría ser `ec2-12-345-678-901.us-east-2.compute.amazonaws.com`.
10. Abra la consola de AWS Secrets Manager en https://console.aws.amazon.com/secretsmanager/.
11. Elija el secreto que tiene el mismo nombre que su par de claves.
12. Elija Retrieve secret value (Recuperar valor secreto).

AWS CLI

Para recuperar la clave privada

1. Obtenga la lista de instancias de base de datos de RDS Custom llamando al comando `aws rds describe-db-instances`.

```
aws rds describe-db-instances \
    --query 'DBInstances[*].[DBInstanceIdentifier,DbiResourceId]' \
    --output text
```

2. Elija el identificador de instancias de bases de datos de la salida de muestra, por ejemplo, `do-not-delete-rds-custom-`*`my-custom-instance`*.
3. Busque el ID de instancia EC2 de la instancia de base de datos llamando al comando `aws ec2 describe-instances`. En el siguiente ejemplo se utiliza el nombre de instancia EC2 para describir la instancia de base de datos.

```
aws ec2 describe-instances \
    --filters "Name=tag:Name,Values=do-not-delete-rds-custom-my-custom-instance" \
    --output text \
    --query 'Reservations[*].Instances[*].InstanceId'
```

   El siguiente ejemplo muestra el ID de instancia EC2.

```
i-abcdefghijklm01234
```

4. Para encontrar el nombre de la clave, especifique el ID de instancia EC2, como se muestra en el siguiente ejemplo.

```
aws ec2 describe-instances \
    --instance-ids i-abcdefghijklm01234 \
    --output text \
    --query 'Reservations[*].Instances[*].KeyName'
```

En el siguiente ejemplo de salida se muestra el nombre de la clave, que utiliza el prefijo do-not-delete-rds-custom-*DBInstanceIdentifier*.

```
do-not-delete-rds-custom-my-custom-instance-0d726c
```

Conéctese a la instancia EC2 mediante la utilidad RDP

Siga el procedimiento en Connect to your Windows instance using RDP en la Guía del usuario de Amazon EC2. Este procedimiento asume que creó un archivo .pem que contiene su clave privada.

Administración de una instancia de base de datos para Amazon RDS Custom for SQL Server

Amazon RDS Custom for SQL Server admite un subconjunto de las tareas de administración habituales para las instancias de base de datos de Amazon RDS. A continuación, encontrará instrucciones para las tareas de administración de RDS Custom for SQL Server compatibles con la AWS Management Console y la AWS CLI.

Temas

- Pausa y reanudación de la automatización de RDS Custom
- Modificación de una instancia de base de datos de RDS Custom for SQL Server
- Modificación del almacenamiento para una instancia de base de datos de RDS Custom para SQL Server
- Etiquetado de los recursos de RDS Custom for SQL Server
- Eliminación de una instancia de base de datos de RDS Custom for SQL Server
- Iniciar y detener una instancia de base de datos de RDS Custom para SQL Server

Pausa y reanudación de la automatización de RDS Custom

RDS Custom proporciona automáticamente monitoreo y recuperación de instancias para una instancia de base de datos de RDS Custom for SQL Server. Si necesita personalizar la instancia, siga este procedimiento:

1. Pause la automatización de RDS Custom durante un periodo determinado. La pausa garantiza que las personalizaciones no interfieran con la automatización de RDS Custom.
2. Personalice la instancia de base de datos de RDS Custom for SQL Server según sea necesario.
3. Haga una de estas dos operaciones:
   - Reanude la automatización manualmente.
   - Espere a que finalice el periodo de pausa. En este caso, RDS Custom reanuda el monitoreo y la recuperación de instancias automáticamente.

> **Important**
>
> La pausa y la reanudación de la automatización son las únicas tareas de automatización admitidas al modificar una instancia de base de datos de RDS Custom for SQL Server.

Consola

Para pausar o reanudar la automatización de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y luego elija la instancia de base de datos de RDS Custom que desea modificar.
3. Elija Modify (Modificar). Aparece la página Modify DB instance (Modificar instancia de base de datos).
4. Para RDS Custom automation mode (Modo de automatización de RDS Custom), elija una de las siguientes opciones:
   - Paused (En pausa) pausa el monitoreo y la recuperación de instancias de la instancia de base de datos de RDS Custom. Ingrese la duración de la pausa que desea (en minutos) para Automation mode duration (Duración del modo de automatización). El valor mínimo es 60 minutos (predeterminado). El valor máximo es 1440 minutos.
   - Full automation (Automatización completa) reanuda la automatización.
5. Elija Continue (Continuar) para ver el resumen de las modificaciones.

   Un mensaje indica que RDS Custom aplicará los cambios inmediatamente.
6. Si los cambios son correctos, elija Modify DB instance (Modificar instancia de base de datos). O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

   Los detalles de la modificación aparecen en la consola de RDS. Si ha puesto en pausa la automatización, el Status (Estado) de la instancia de base de datos de RDS Custom indica Automation paused (Automatización en pausa).
7. (Opcional) En el panel de navegación, elija Databases (Bases de datos) y luego la instancia de base de datos de RDS Custom.

En el panel Summary (Resumen), RDS Custom automation mode (Modo de automatización de RDS Custom) indica el estado de la automatización. Si se pausa la automatización, el valor es Paused (En pausa). La automatización se reanuda en ***num*** minutos.

AWS CLI

Para pausar o reanudar la automatización de RDS Custom, utilice el comando de la AWS CLI `modify-db-instance`. Identifique la instancia de base de datos mediante el parámetro requerido `--db-instance-identifier`. Controle el modo de automatización con los siguientes parámetros:

- `--automation-mode` especifica el estado de pausa de la instancia de base de datos. Los valores válidos son `all-paused`, que pausa la automatización, y `full`, que lo reanuda.
- `--resume-full-automation-mode-minutes` especifica la duración de la pausa. El valor predeterminado es 60 minutos.

> **Note**
>
> Independientemente de que especifique `--no-apply-immediately` o `--apply-immediately`, RDS Custom aplica las modificaciones de forma asíncrona tan pronto como sea posible.

En la respuesta de comando, `ResumeFullAutomationModeTime` indica la hora de reanudación como marca de hora UTC. Cuando el modo de automatización es `all-paused`, puede utilizar `modify-db-instance` para reanudar el modo de automatización o ampliar el periodo de pausa. No se admiten otras opciones de `modify-db-instance`.

En el siguiente ejemplo se pausa la automatización para `my-custom-instance` durante 90 minutos.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --automation-mode all-paused \
```

```
    --resume-full-automation-mode-minutes 90
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --automation-mode all-paused ^
    --resume-full-automation-mode-minutes 90
```

El siguiente ejemplo extiende la duración de la pausa durante 30 minutos adicionales. Los 30 minutos se añaden a la hora original que se muestra en `ResumeFullAutomationModeTime`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --automation-mode all-paused \
    --resume-full-automation-mode-minutes 30
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --automation-mode all-paused ^
    --resume-full-automation-mode-minutes 30
```

En el siguiente ejemplo se reanuda la automatización completa para `my-custom-instance`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --automation-mode full \
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --automation-mode full
```

En la siguiente salida de muestra parcial, el valor pendiente `AutomationMode` es `full`.


```
{
    "DBInstance": {
        "PubliclyAccessible": true,
        "MasterUsername": "admin",
        "MonitoringInterval": 0,
        "LicenseModel": "bring-your-own-license",
        "VpcSecurityGroups": [
            {
                "Status": "active",
                "VpcSecurityGroupId": "0123456789abcdefg"
            }
        ],
        "InstanceCreateTime": "2020-11-07T19:50:06.193Z",
        "CopyTagsToSnapshot": false,
        "OptionGroupMemberships": [
            {
                "Status": "in-sync",
                "OptionGroupName": "default:custom-oracle-ee-19"
            }
        ],
        "PendingModifiedValues": {
            "AutomationMode": "full"
        },
        "Engine": "custom-oracle-ee",
        "MultiAZ": false,
        "DBSecurityGroups": [],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.custom-oracle-ee-19",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        ...
        "ReadReplicaDBInstanceIdentifiers": [],
        "AllocatedStorage": 250,
        "DBInstanceArn": "arn:aws:rds:us-west-2:012345678912:db:my-custom-instance",
        "BackupRetentionPeriod": 3,
```

```
        "DBName": "ORCL",
        "PreferredMaintenanceWindow": "fri:10:56-fri:11:26",
        "Endpoint": {
            "HostedZoneId": "ABCDEFGHIJKLMNO",
            "Port": 8200,
            "Address": "my-custom-instance.abcdefghijk.us-west-2.rds.amazonaws.com"
        },
        "DBInstanceStatus": "automation-paused",
        "IAMDatabaseAuthenticationEnabled": false,
        "AutomationMode": "all-paused",
        "EngineVersion": "19.my_cev1",
        "DeletionProtection": false,
        "AvailabilityZone": "us-west-2a",
        "DomainMemberships": [],
        "StorageType": "gp2",
        "DbiResourceId": "db-ABCDEFGHIJKLMNOPQRSTUVW",
        "ResumeFullAutomationModeTime": "2020-11-07T20:56:50.565Z",
        "KmsKeyId": "arn:aws:kms:us-west-2:012345678912:key/
aa111a11-111a-11a1-1a11-1111a11a1a1a",
        "StorageEncrypted": false,
        "AssociatedRoles": [],
        "DBInstanceClass": "db.m5.xlarge",
        "DbInstancePort": 0,
        "DBInstanceIdentifier": "my-custom-instance",
        "TagList": []
    }
```


Modificación de una instancia de base de datos de RDS Custom for SQL Server

La modificación de una instancia de base de datos de RDS Custom for SQL Server es similar a hacerlo en Amazon RDS, pero los cambios que puede realizar se limitan a los siguientes:

- Cambiar la clase de instancia de base de datos
- Cambiar el periodo de retención de copia de seguridad y la ventana de la copia de seguridad
- Cambio del periodo de mantenimiento
- Actualización de la versión del motor de base de datos cuando hay una nueva versión disponible
- Cambio del almacenamiento asignado, las IOPS aprovisionadas y el tipo de almacenamiento
- Permitir y eliminar implementaciones multi-AZ

Las siguientes limitaciones se aplican a la modificación de una instancia de base de datos de RDS Custom for SQL Server:

- No se admiten grupos de parámetros y opciones de base de datos de Custom.
- Los volúmenes de almacenamiento que adjunte manualmente a la instancia de base de datos de RDS Custom están fuera del perímetro de soporte.

  Para obtener más información, consulte Perímetro de soporte de RDS Custom.

Consola

Para modificar una instancia de base de datos de RDS Custom for SQL Server

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea modificar.
4. Elija Modify.
5. Realice los siguientes cambios según sea necesario:
   a. Para DB engine version, elija la nueva versión.
   b. Cambie el valor de DB instance class (Clase de instancia de base de datos). Para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL.
   c. Cambie el valor de Backup retention period (Periodo de retención de copia de seguridad).
   d. Para Backup window (Periodo de la copia de seguridad), establezca valores para la Start time (Hora de inicio) y la Duration (Duración).
   e. Para el DB instance maintenance window (Periodo de mantenimiento de la instancia de base de datos), establezca valores para el Start day (Día de inicio), la Start time (Hora de inicio) y la Duration (Duración).
6. Elija Continuar.
7. Elija Apply immediately (Aplicar inmediatamente) o Apply during the next scheduled maintenance window (Aplicar durante el próximo periodo de mantenimiento programado).
8. Elija Modify DB instance (Modificar la instancia de base de datos).

AWS CLI

Para modificar una instancia de base de datos de RDS Custom for SQL Server, utilice el comando de la AWS CLI modify-db-instance. Configure los siguientes parámetros según sea necesario:

- `--db-instance-class`: para ver las clases compatibles, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom for SQL.
- `--engine-version` – El número de versión del motor de base de datos al que está actualizando.
- `--backup-retention-period`: ¿cuánto tiempo se retienen las copias de seguridad automatizadas? De 0 a 35 días.
- `--preferred-backup-window` – El intervalo de tiempo diario durante el que se crean las copias de seguridad automatizadas.
- `--preferred-maintenance-window` – El intervalo de tiempo semanal (en UTC) durante el cual puede llevarse a cabo el mantenimiento del sistema.
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente.

  También puede utilizar `--no-apply-immediately` (valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento.

Modificación del almacenamiento para una instancia de base de datos de RDS Custom para SQL Server

La modificación del almacenamiento para una instancia de base de datos de RDS Custom para SQL Server es similar a modificar el almacenamiento para una instancia de base de datos de Amazon RDS, pero solo puede hacer lo siguiente:

- Aumentar el tamaño de almacenamiento asignado.
- Cambiar el tipo de almacenamiento. Puede utilizar los tipos de almacenamiento disponibles, como el de uso general o el de IOPS aprovisionadas. Las IOPS aprovisionadas son compatibles con los tipos de almacenamiento gp3, io1 e io2 Block Express.
- Cambie las IOPS aprovisionadas, si utiliza los tipos de volumen que admiten las IOPS aprovisionadas.

Se aplican las siguientes limitaciones a la modificación de una instancia de base de datos de RDS Custom para SQL Server:

- El tamaño de almacenamiento mínimo asignado para RDS Custom para SQL Server es de 20 GiB. El límite máximo de almacenamiento para io1, gp2 y gp3 es de 16 TiB, mientras que io2 admite 64 TiB.
- Al igual que con Amazon RDS, no es posible reducir el almacenamiento asignado. Esta es una limitación de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Para obtener más información, consulte Uso de almacenamiento para instancias de base de datos de Amazon RDS
- El escalado automático de almacenamiento no es compatible con las instancias de base de datos de RDS Custom para SQL Server.
- Los volúmenes de almacenamiento que adjunte manualmente a la instancia de base de datos de RDS Custom no se tienen en cuenta para el escalado del almacenamiento. Para el escalado del almacenamiento solo se tienen en cuenta los volúmenes de datos predeterminados proporcionados por RDS, es decir, la unidad D.

  Para obtener más información, consulte Perímetro de soporte de RDS Custom.
- Por lo general, la escalabilidad del almacenamiento no causa ninguna interrupción o merma de rendimiento en la instancia de base de datos. Después de modificar el tamaño de almacenamiento para una instancia de base de datos, el estado de la instancia de base de datos es storage-optimization (optimización del almacenamiento).
- La optimización del almacenamiento puede tardar varias horas. No puede hacer modificaciones de almacenamiento adicionales hasta seis (6) horas o después de que se haya completado la optimización de almacenamiento en la instancia, lo que tarde más tiempo. Para obtener más información, consulte Uso de almacenamiento para instancias de base de datos de Amazon RDS

Para obtener más información acerca del almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

Para obtener información general sobre la modificación del almacenamiento de información, consulte Uso de almacenamiento para instancias de base de datos de Amazon RDS.

> **Important**
>
> No modifique el almacenamiento para la instancia de base de datos de RDS Custom para SQL Server mediante las consolas o las API de Amazon EC2 o Amazon EBS. Las modificaciones de almacenamiento directas fuera de la consola o de las API de Amazon RDS dan como resultado un estado de `unsupported-configuration` para la base de datos.

Cuando realiza cambios de almacenamiento directos mediante Amazon EC2 o Amazon EBS, Amazon RDS no puede rastrear ni administrar el estado de la instancia de la base de datos. Esto podría provocar que:

- Los mecanismos de conmutación por error de alta disponibilidad no funcionen correctamente
- Las configuraciones de replicación de bases de datos se rompan
- Las características de redundancia produzcan un error

Modifique el almacenamiento solo a través de la consola o las API de Amazon RDS para mantener la base de datos en un estado compatible. Consulte Corrección de configuraciones no compatibles en RDS Custom para SQL Server para obtener los pasos de recuperación.

Consola

Para modificar el almacenamiento para una instancia de base de datos de RDS Custom para SQL Server

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia de base de datos que desea modificar.
4. Elija Modify.
5. Realice los siguientes cambios según sea necesario:
    a. Ingrese un nuevo valor para Allocated Storage (Almacenamiento asignado). Debe ser mayor que el valor actual y de 20 GiB a 16 TiB.
    b. Cambie el valor de Storage type (Tipo de almacenamiento). Puede elegir entre los tipos de almacenamiento disponibles de uso general o de IOPS aprovisionadas. Las IOPS aprovisionadas son compatibles con los tipos de almacenamiento gp3, io1 e io2 Block Express.
    c. Si especifica un tipo de almacenamiento que admite IOPS aprovisionadas, puede definir el valor de IOPS aprovisionadas.
6. Elija Continuar.

7. Elija Apply immediately (Aplicar inmediatamente) o Apply during the next scheduled maintenance window (Aplicar durante el próximo periodo de mantenimiento programado).
8. Elija Modify DB instance (Modificar la instancia de base de datos).

AWS CLI

Para modificar el almacenamiento para una instancia de base de datos de RDS Custom para SQL Server, utilice el comando de la AWS CLI modify-db-instance. Configure los siguientes parámetros según sea necesario:

- `--allocated-storage`: cantidad de almacenamiento que se debe asignar a la instancia de base de datos, en gibibytes. Debe ser mayor que el valor actual y de 20 a 16 384 GiB.
- `--storage-type`: tipo de almacenamiento, por ejemplo, gp2, gp3, io1 o io2.
- `--iops`: IOPS aprovisionadas para la instancia de base de datos. Puede especificar esto solo para los tipos de almacenamiento que admiten las IOPS aprovisionadas (gp3, io1 e io2).
- `--apply-immediately`: utilice `--apply-immediately` para aplicar los cambios inmediatamente.

  También puede utilizar `--no-apply-immediately` (valor predeterminado) para aplicar los cambios en el siguiente período de mantenimiento.

En el siguiente ejemplo, se cambia el tamaño de almacenamiento de my-custom-instance a 200 GiB, el tipo de almacenamiento a io1 y las IOPS aprovisionadas a 3000.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --storage-type io1 \
    --iops 3000 \
    --allocated-storage 200 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
```

```
    --db-instance-identifier my-custom-instance ^
    --storage-type io1 ^
    --iops 3000 ^
    --allocated-storage 200 ^
    --apply-immediately
```

Etiquetado de los recursos de RDS Custom for SQL Server

Puede etiquetar recursos de RDS Custom como con los recursos de Amazon RDS, pero con algunas diferencias importantes:

- No cree ni modifique la etiqueta `AWSRDSCustom` necesaria para la automatización de RDS Custom. Si lo hace, podría interrumpir la automatización.
- La etiqueta `Name` se agrega a los recursos de RDS Custom con el prefijo `do-not-delete-rds-custom`. Se sobrescribe cualquier valor de la clave que el cliente haya pasado.
- Las etiquetas agregadas a las instancias de base de datos de RDS Custom durante la creación se propagan a todos los demás recursos de RDS Custom relacionados.
- Las etiquetas no se propagan cuando se agregan a los recursos de RDS Custom tras la creación de la instancia de base de datos.

Para obtener información general sobre el etiquetado de recursos, consulte Etiquetado de los recursos de y Amazon RDS.

Eliminación de una instancia de base de datos de RDS Custom for SQL Server

Para eliminar una instancia de base de datos de RDS Custom para SQL Server, haga lo siguiente:

- Proporcione el nombre de la instancia de base de datos.
- Elija o desactive la opción para tomar una instantánea de base de datos final de la instancia de base de datos.
- Elija o desactive la opción de retener copias de seguridad automatizadas.

Puede eliminar una instancia de base de datos de RDS Custom para SQL Server a través de la consola o la CLI. El tiempo necesario para eliminar una instancia de base de datos puede variar en función del periodo de retención de copia de seguridad (es decir, cuántas copias de seguridad se eliminarán), la cantidad de datos que se eliminen y si se toma una instantánea final.

> **Warning**
>
> Al eliminar una instancia de base de datos de RDS Custom para SQL Server, se eliminarán de forma permanente la instancia EC2 y los volúmenes de Amazon EBS asociados. No debe cancelar ni eliminar estos recursos en ningún momento; de lo contrario, la eliminación y la creación de la instantánea final podrían fallar.

> **Note**
>
> No puede crear una instantánea de base de datos final de la instancia de base de datos si tiene el estado `creating`, `failed`, `incompatible-create`, `incompatible-restore` o `incompatible-network`. Para obtener más información, consulte Visualización del estado de la instancia de base de datos de en un clúster de Aurora.

> **Important**
>
> Cuando decida tomar una instantánea final, le recomendamos que evite escribir datos en la instancia de base de datos mientras esta se está eliminando. Una vez iniciada la eliminación de la instancia de base de datos, no se garantiza que la instantánea final capture los cambios en los datos.

Consola

Para eliminar una instancia de base de datos de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y luego elija la instancia de base de datos de RDS Custom para SQL Server que desea eliminar. Las instancias de base de datos de RDS Custom para SQL Server muestran el rol Instance (RDS Custom for SQL Server) (Instancia [RDS Custom para SQL Server]).
3. En Actions (Acciones), seleccione Delete (Eliminar).
4. Para tomar una instantánea final, elija Create final snapshot (Crear instantánea final) y proporcione un nombre en Final snapshot name (Nombre de instantánea final).

5. Para conservar las copias de seguridad automatizadas, elija Retain automated backups (Conservar copias de seguridad automatizadas).
6. En el cuadro, escriba **`delete me`**.
7. Elija Eliminar (Delete).

AWS CLI

Elimine una instancia de base de datos de RDS Custom para SQL Server mediante el comando de la AWS CLI delete-db-instance. Identifique la instancia de base de datos mediante el parámetro requerido `--db-instance-identifier`. Los parámetros restantes son los mismos que para una instancia de base de datos de Amazon RDS.

En el siguiente ejemplo, se elimina la instancia de base de datos de RDS Custom para SQL Server denominada `my-custom-instance`, se toma una instantánea final y se retienen copias de seguridad automatizadas.

Example

Para Linux, macOS o:Unix

```
aws rds delete-db-instance \
    --db-instance-identifier my-custom-instance \
    --no-skip-final-snapshot \
    --final-db-snapshot-identifier my-custom-instance-final-snapshot \
    --no-delete-automated-backups
```

En:Windows

```
aws rds delete-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --no-skip-final-snapshot ^
    --final-db-snapshot-identifier my-custom-instance-final-snapshot ^
    --no-delete-automated-backups
```

Para tomar una instantánea final, la opción `--final-db-snapshot-identifier` es obligatoria y debe especificarse.

Para omitir la instantánea final, especifique la opción `--skip-final-snapshot` en lugar de las opciones `--no-skip-final-snapshot` y `--final-db-snapshot-identifier` en el comando.

Para eliminar las copias de seguridad automatizadas, especifique la opción `--delete-automated-backups` en lugar de la opción `--no-delete-automated-backups` en el comando.

Iniciar y detener una instancia de base de datos de RDS Custom para SQL Server

Puede iniciar y detener una instancia de base de datos de RDS Custom para SQL Server. Los mismos requisitos y limitaciones generales de las instancias de base de datos de RDS para SQL Server se aplican a la detención e inicio de las instancias de RDS Custom para SQL Server. Para obtener más información, consulte Parada de una instancia de base de datos de Amazon RDS temporalmente.

Las siguientes consideraciones también se aplican para iniciar y detener su instancia de base de datos de RDS Custom para SQL Server:

- No se admite la modificación de un atributo de instancia EC2 de una instancia de base de datos de RDS Custom para SQL Server si la instancia de base de datos no está `STOPPED`.
- Puede detener e iniciar una instancia de base de datos de RDS Custom para SQL Server solo si está configurada para una sola zona de disponibilidad. No puede detener una instancia de base de datos de Amazon RDS para SQL Server en una configuración Multi-AZ.
- Se creará una instantánea del `SYSTEM` cuando detenga una instancia de base de datos de RDS Custom para SQL Server. La instantánea se eliminará automáticamente cuando vuelva a iniciar la instancia de base de datos de RDS Custom para SQL Server.
- Si elimina la instancia EC2 mientras su instancia de base de datos de RDS Custom para SQL Server está detenida. la unidad `C:` se reemplazará cuando vuelva a iniciar la instancia de base de datos de RDS Custom para SQL Server.
- La unidad `C:\`, el nombre de host y sus configuraciones personalizadas se conservan al detener una instancia de base de datos de RDS Custom para SQL Server, siempre y cuando no modifique el tipo de instancia.
- Las siguientes acciones harán que RDS Custom coloque la instancia de base de datos fuera del perímetro de soporte y, además, se le cobrará la instancia de base de datos por horas:
  - Iniciar la instancia EC2 subyacente mientras Amazon RDS está detenido. Para resolver esta situación, puede llamar a la API `start-db-instance` de Amazon RDS o detener EC2 para que la instancia de RDS Custom vuelva al estado `STOPPED`.
  - Detener la instancia EC2 subyacente cuando la instancia de base de datos de RDS Custom para SQL Server está `ACTIVE`.

Para obtener más detalles sobre cómo detener e iniciar instancias de base de datos, consulte Parada de una instancia de base de datos de Amazon RDS temporalmente y Inicio de una instancia de base de datos de Amazon RDS parada previamente.

Uso de Microsoft Active Directory con RDS Custom para SQL Server

RDS Custom para SQL Server permite unir sus instancias a un Active Directory (AD) autoadministrado o AWS Managed Microsoft AD. Esto es independientemente de dónde esté alojado su AD, como un centro de datos en las instalaciones, Amazon EC2 o cualquier otro proveedor de servicios en la nube.

Para la autenticación de usuarios y servicios, puede usar la autenticación de NTML o Kerberos en su instancia de base de datos de RDS Custom para SQL Server sin utilizar dominios intermediarios ni relaciones de confianza entre bosques. Cuando un usuario intenta autenticarse en su instancia de base de datos RDS Custom para SQL Server con una instancia de Active Directory autounida, las solicitudes de autenticación se reenvían a un AD autoadministrado o AWS Managed Microsoft AD que usted especifique.

En las siguientes secciones, encontrará información sobre cómo utilizar Active Directory autoadministrado y AWS Managed Active Directory para RDS Custom para SQL Server.

Temas

- Disponibilidad en regiones y versiones
- Configurar AD autoadministrado o en las instalaciones
- Configuración de Microsoft Active Directory mediante AWS Directory Service
- Reglas de puertos de configuraciones de redes
- Validación de red
- Configuración de la autenticación de Windows para las instancias de RDS Custom para SQL Server
- Administración de una instancia de base de datos en un dominio
- Descripción de la pertenencia a los dominios
- Solución de problemas de Active Directory

Disponibilidad en regiones y versiones

RDS Custom para SQL Server admite AD autoadministrado y AWS Managed Microsoft AD usando NTLM o Kerberos en todas las regiones en las que se admite RDS Custom para SQL Server. Para obtener más información, consulte Regiones y motores de base de datos admitidos para RDS Custom.

Configurar AD autoadministrado o en las instalaciones

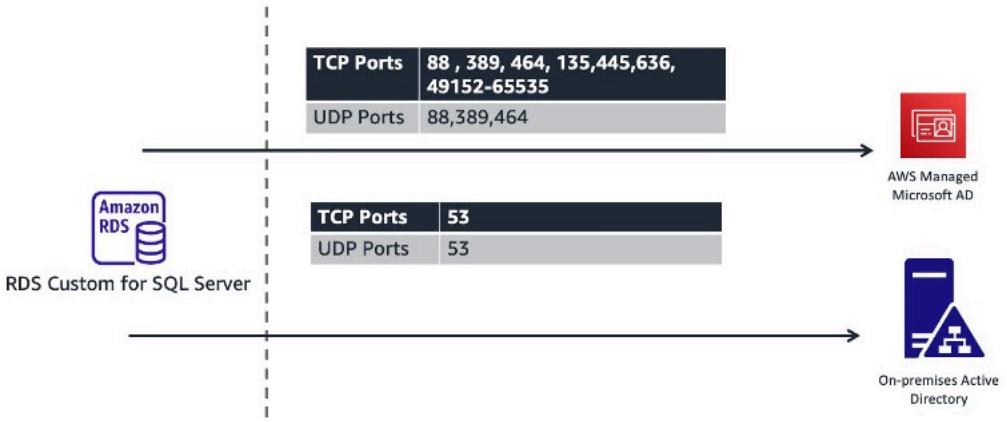
Para unir su Microsoft AD en las instalaciones o autoadministrado a su instancia de base de datos de RDS Custom para SQL Server, debe configurar su dominio activo de la siguiente manera:

- Defina las subredes de la VPC asociadas a su instancia de base de datos de RDS Custom para SQL Server en su AD autoadministrado o en las instalaciones. Confirme que no haya ningún conflicto entre las subredes de la VPC y las subredes de sus sitios de AD.
- El controlador de dominio de AD tiene un nivel funcional de dominio de Windows Server 2008 R2 o superior.
- El nombre de dominio de AD no puede estar en formato de dominio de etiqueta única (SLD). RDS Custom para SQL Server no admite dominios de SLD.
- El nombre de dominio completo (FQDN) y su AD no pueden superar los 47 caracteres.

Configure la conectividad de red

Configure la conectividad de red de AD en las instalaciones o autoadministradas de la siguiente manera:

- Configure la conectividad entre Amazon VPC en la que esté ejecutándose la instancia de RDS Custom para SQL Server y su AD. Utilice AWS Direct Connect, AWS VPN, AWS Transit Gateway y emparejamiento de VPC.
- Permita que el tráfico de los puertos de los grupos de seguridad y las ACL de su red de RDS Custom para SQL Server se dirija a su AD en las instalaciones o autoadministrado. Para obtener más información, consulte Reglas de puertos de configuraciones de redes.



Configuración de la resolución de DNS

Configure los siguientes requisitos para configurar la resolución de DNS con los AD autoadministrados o en las instalaciones:

- Configure la resolución de DNS en su VPC para resolver el nombre de dominio completo (FQDN) de Active Directory que está hospedado en el servidor. Un ejemplo de un FQDN es `corp.example.local`. Para configurar la resolución de DNS, configure la resolución de DNS de la VPC para que reenvíe las consultas de determinados dominios con una regla de resolución y punto de conexión de salida de Amazon Route 53. Para obtener más información, consulte Configure a Route 53 Resolver outbound endpoint to resolve DNS records.
- Para las cargas de trabajo que aprovechan tanto las VPC como los recursos locales, debe resolver los registros de DNS alojados en las instalaciones. Es posible que los recursos en las instalaciones deban resolver los nombres alojados en AWS.

  Para crear una configuración de nube híbrida, utilice puntos de conexión del solucionador y riles de reenvío condicional para resolver las consultas de DNS entre recursos ubicados en las instalaciones y VPC personalizadas. Para obtener más información, consulte Resolving DNS queries between VPCs and your network en la Guía para desarrolladores de Amazon Route 53.

> **Important**
>
> La modificación de la configuración del solucionador de DNS de la interfaz de red del servidor RDS Custom para SQL Server provoca que los puntos de conexión de VPC con DNS dejen de funcionar correctamente. Se requieren puntos de conexión de VPC habilitados para DNS para las instancias dentro de subredes privadas sin acceso a Internet.

Configuración de Microsoft Active Directory mediante AWS Directory Service

AWS Managed Microsoft AD crea una instancia de Microsoft Active Directory completamente administrada en AWS que está equipada con Windows Server 2019 y que opera en los niveles funcionales de bosque y dominio 2012 R2. AWS Directory Service crea los controladores de dominio en diferentes subredes de una Amazon VPC, lo que hace que su directorio esté altamente disponible incluso en caso de error.

Para crear un directorio con AWS Managed Microsoft AD, consulte Introducción a AWS Managed Microsoft AD en la Guía de administraciónAWS Directory Service.

Configure la conectividad de red

Cómo habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos

Para ubicar el directorio y la instancia de base de datos en la misma VPC, omita este paso y continúe con el siguiente paso en Reglas de puertos de configuraciones de redes.

Para ubicar el directorio y la instancia de base de datos en diferentes VPC, configure el tráfico entre VPC mediante el emparejamiento de VPC o AWS Transit Gateway. Para obtener más información sobre cómo usar el emparejamiento de VPC, consulte ¿Qué es una interconexión de VPC? en la Guía de interconexión de Amazon VPC y ¿Qué es AWS Transit Gateway? en Amazon VPC Transit Gateways.

Cómo habilitar el tráfico entre VPC mediante el emparejamiento de VPC

1. Configure las reglas de enrutamiento de VPC adecuadas para garantizar que el tráfico de red pueda fluir en ambos sentidos.
2. Permita que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico de entrada del grupo de seguridad del directorio. Para obtener más información, consulte Reglas de puertos de configuraciones de redes.
3. La lista de control de acceso (ACL) de red no debe bloquear el tráfico.

Si una Cuenta de AWS distinta es la propietaria del directorio, debe compartirlo. Para compartir el directorio con una Cuenta de AWS en la que se encuentra la instancia de RDS Custom para SQL Server, siga el Tutorial: uso compartido del directorio de AWS Managed Microsoft AD para una unión fluida al dominio de EC2 de la Guía de administración de AWS Directory Service.

Uso compartido de un directorio entre Cuentas de AWS

1. Inicie sesión en la consola de AWS Directory Service utilizando la cuenta para la instancia de base de datos y asegúrese de que el dominio tiene el estado `SHARED` antes de continuar.
2. Una vez iniciada sesión en la consola de AWS Directory Service utilizando la cuenta de la instancia de base de datos, anote el valor de ID de directorio. Utilice este identificador para unir la instancia de base de datos al dominio.

Configuración de la resolución de DNS

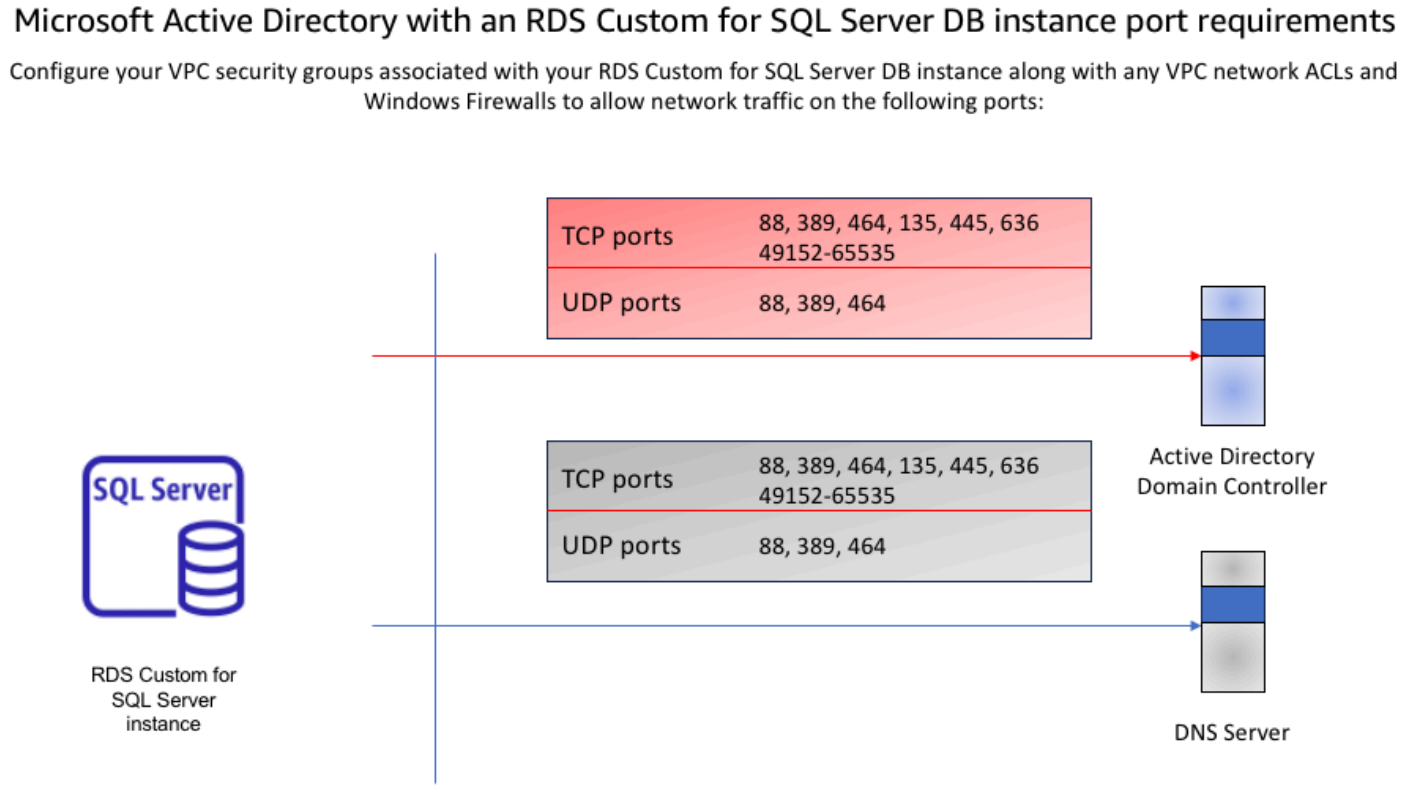
Al crear un directorio con AWS Managed Microsoft AD, AWS Directory Service crea dos controladores de dominio y añade el servicio DNS en su nombre.

Si ya tiene una instancia de AWS Managed Microsoft AD o planea lanzarla en una VPC distinta de su instancia de base de datos de RDS Custom para SQL Server, configure la instancia de resolución de DNS de la VPC para que reenvíe las consultas de determinados dominios con una regla de salida y resolución de Route 53, consulte ¿Cómo configuro un punto de conexión de salida de Route 53 Resolver para resolver los registros DNS alojados en una red remota a partir de los recursos de mi VPC?

Reglas de puertos de configuraciones de redes

Asegúrese de cumplir las siguientes configuraciones de red:

- Conectividad configurada entre la Amazon VPC donde desea crear la instancia de base de datos de RDS Custom para SQL Server en su Active Directory autoadministrado o AWS Managed Microsoft AD. En el caso de Active Directory autoadministrado, configure la conectividad mediante AWS Direct Connect, AWS VPN, emparejamiento de VPC o AWS Transit Gateway. Para AWS Managed Microsoft AD, configure la conectividad con el emparejamiento de VPC.
- Asegúrese de que el grupo de seguridad y las ACL de red de VPC de las subredes en las que va a crear su instancia de base de datos de RDS Custom para SQL Server permitan el tráfico en los puertos y en las direcciones que se muestran en el siguiente diagrama.



En la siguiente tabla se identifica la función de cada puerto.

Protocolo	Puertos	Rol
TCP/UDP	53	Sistema de nombres de dominio (DNS)
TCP/UDP	88	Autenticación de Kerberos
TCP/UDP	464	Cambiar/establecer contraseña
TCP/UDP	389	Protocolo ligero de acceso a directorios (LDAP)
TCP	135	Entorno de computación distribuido/asignador de puntos de conexión (DCE/EPMAP)

Protocolo	Puertos	Rol
TCP	445	Uso compartido de archivos SMB de Directory Services
TCP	636	Protocolo ligero de acceso a directorios sobre TLS/ SSL (LDAP)
TCP	49152 - 65535	Puertos efímeros para RPC

- Por lo general, los servidores DNS de dominio se encuentran en los controladores de dominio de AD. No es necesario configurar el conjunto de opciones de DHCP de VPC para utilizar esta característica. Para obtener más información, consulte Conjuntos de opciones de DHCP en la Guía del usuario de Amazon VPC.

> **Important**
>
> Si utiliza ACL de red de VPC, también debe permitir el tráfico saliente en los puertos dinámicos (49152-65535) desde su instancia de base de datos de RDS Custom para SQL Server. Asegúrese de que estas reglas de tráfico también se reflejen en los firewalls que se aplican a cada uno de los controladores de dominio de AD, los servidores DNS y las instancias de base de datos de RDS Custom para SQL Server.
> Si bien los grupos de seguridad de VPC requieren que los puertos se abran solo en la dirección en la que se inicia el tráfico de red, la mayoría de los firewalls de Windows y las ACL de red de VPC requieren que los puertos estén abiertos en ambas direcciones.

Validación de red

Antes de unir su instancia de RDS Custom a una instancia autoadministrada o AWS Managed Microsoft AD, compruebe lo siguiente desde una instancia de EC2 de la misma VPC en la que planea lanzar la instancia de RDS Custom para SQL Server.

- Compruebe si puede resolver el nombre de dominio completo (FQDN) en las IP del controlador de dominio.

```
nslookup corp.example.com
```

El comando debe devolver un resultado similar:

```
Server:  ip-10-0-0-2.us-west-2.compute.internal
Address:  25.0.0.2

Non-authoritative answer:
Name:    corp.example.com
Addresses:  40.0.9.25 (DC1 IP)
            40.0.50.123 (DC2 IP)
```

- Resuelva los servicios de AWS de una instancia de EC2 en la VPC en la que va a lanzar su instancia de RDS Custom:

```
$region='input-your-aws-region'
$domainFQDN='input-your-domainFQDN'

function Test-DomainPorts {
    param (
        [string]$Domain,
        [array]$Ports
    )

    foreach ($portInfo in $Ports) {
        try {
            $conn = New-Object System.Net.Sockets.TcpClient
            $connectionResult = $conn.BeginConnect($Domain, $portInfo.Port, $null,
 $null)
            $success = $connectionResult.AsyncWaitHandle.WaitOne(1000) # 1 second
 timeout
            if ($success) {
                $conn.EndConnect($connectionResult)
                $result = $true
            } else {
                $result = $false
            }
        }
        catch {
            $result = $false
        }
        finally {
            if ($null -ne $conn) {
                $conn.Close()
```

```
            }
        }
        Write-Host "$($portInfo.Description) port open: $result"
    }
}

# Check if ports can be reached
$ports = @(
    @{Port = 53;   Description = "DNS"},
    @{Port = 88;   Description = "Kerberos"},
    @{Port = 389;  Description = "LDAP"},
    @{Port = 445;  Description = "SMB"},
    @{Port = 5985; Description = "WinRM"},
    @{Port = 636;  Description = "LDAPS"},
    @{Port = 3268; Description = "Global Catalog"},
    @{Port = 3269; Description = "Global Catalog over SSL"},
    @{Port = 9389; Description = "AD DS"}
)

function Test-DomainReachability {
    param (
        [string]$DomainName
    )

    try {
        $dnsResults = Resolve-DnsName -Name $DomainName -ErrorAction Stop
        Write-Host "Domain $DomainName is successfully resolving to following IP
 addresses: $($dnsResults.IpAddress)"
        Write-Host ""
        return $true
    }
    catch {
        Write-Host ""
        Write-Host "Error Message: $($_.Exception.Message)"
        Write-Host "Domain $DomainName reachability check failed, please Configure
 DNS resolution"
        return $false
    }
}

$domain = (Get-WmiObject Win32_ComputerSystem).Domain
if ($domain -eq 'WORKGROUP') {
    Write-Host ""
```

```
    Write-Host "Host $env:computername is still part of WORKGROUP and not part of any
 domain"
    }
else {
    Write-Host ""
    Write-Host "Host $env:computername is joined to $domain domain"
    Write-Host ""
    }


$isReachable = Test-DomainReachability -DomainName $domainFQDN
if ($isReachable) {
    write-Host "Checking if domain $domainFQDN is reachable on required ports  "
    Test-DomainPorts -Domain $domainFQDN -Ports $ports
}
else {
    Write-Host "Port check skipped. Domain not reachable"
}



# Get network adapter configuration
$networkConfig = Get-WmiObject Win32_NetworkAdapterConfiguration |
                 Where-Object { $_.IPEnabled -eq $true } |
                 Select-Object -First 1

# Check DNS server settings
$dnsServers = $networkConfig.DNSServerSearchOrder

if ($dnsServers) {
    Write-Host "`nDNS Server settings:"
    foreach ($server in $dnsServers) {
        Write-Host "  - $server"
    }
} else {
    Write-Host "`nNo DNS servers configured or unable to retrieve DNS server
 information."
}

write-host ""

# Checks reachability to dependent services
$services = "s3", "ec2", "secretsmanager", "logs", "events", "monitoring", "ssm",
 "ec2messages", "ssmmessages"
```

```
function Get-TcpConnectionAsync {
    param (
        $ServicePrefix,
        $region
    )
    $endpoint = "${ServicePrefix}.${region}.amazonaws.com"
    $tcp = New-Object Net.Sockets.TcpClient
    $result = $false

    try {
        $connectTask = $tcp.ConnectAsync($endpoint, 443)
        $timedOut = $connectTask.Wait(3000)
        $result = $tcp.Connected
    }
    catch {
        $result = $false
    }
    return $result
}

foreach ($service in $services) {
    $validationResult = Get-TcpConnectionAsync -ServicePrefix $service -Region
 $region
    Write-Host "Reachability to $service is $validationResult"
}
```

El valor de `TcpTestSucceeded` debe devolver `True` para `s3`, `ec2`, `secretsmanager`, `logs`, `events`, `monitoring`, `ssm`, `ec2messages` y `ssmmessages`.

Configuración de la autenticación de Windows para las instancias de RDS Custom para SQL Server

Se recomienda crear credenciales de servicio y una OU dedicadas a esa unidad organizativa para todas las Cuenta de AWS que posean una instancia de base de datos de RDS Custom para SQL Server que se haya unido a su dominio de AD. Al crear credenciales de servicio u OU dedicadas, evita conflictos de permisos y seguir el principio de privilegio mínimo.

Las políticas de grupo de Active Directory pueden entrar en conflicto con las automatizaciones y los permisos de AWS. Se recomienda seleccionar GPO que se apliquen únicamente a la unidad organizativa que cree para RDS Custom para SQL Server.

- Para crear un usuario de dominio OU y AD en su AD en las instalaciones o autoadministrado, puede conectar el controlador de dominio como administrador de dominio.
- Para crear usuarios y grupos en un directorio de AWS Directory Service, debe estar conectado a una instancia de administración y haber iniciado sesión como usuario con privilegios para crear usuarios y grupos. Para obtener más información, consulte Administración de usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
- Para administrar su Active Directory desde una instancia de Amazon EC2 de Windows Server, es necesario instalar las herramientas de los servicios de dominio de Active Directory y los servicios de directorio de Active Directory Lightweight en la instancia de EC2. Para obtener más información, consulte Instalación de las herramientas de administración del Active Directory para AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
- Le recomendamos que instale estas herramientas en una instancia de EC2 independiente para la administración y no en su instancia de base de datos de RDS Custom para SQL Server para facilitar la administración.

Estos son los requisitos de la cuenta de servicio de dominio de AD:

- Debe tener una cuenta de servicio en su dominio de AD con permisos delegados para unir equipos al dominio. Una cuenta de servicio de dominio es una cuenta de usuario de su AD a la que se le ha delegado permiso para realizar determinadas tareas.
- Delegue los siguientes permisos a la cuenta de servicio de dominio de la unidad organizativa a la que va a unir su instancia de RDS Custom para SQL Server:
  - Capacidad validada para escribir en el nombre de host DNS
  - Capacidad validada para escribir en el nombre de entidad principal del servicio
  - Crear y eliminar objetos de equipo
- En el caso de AD en las instalaciones y autoadministrado, la cuenta de servicio de dominio debe ser miembro del grupo “Administradores delegados del sistema de nombres de dominio de AWS”.
- En el caso de AWS Managed Microsoft AD, la cuenta de servicio de dominio debe ser miembro del grupo “DnsAdmins”.

Estos son el conjunto mínimo de permisos que se requieren para unir objetos de equipo a su AD autoadministrado y AWS Managed Microsoft AD. Para obtener más información, consulte Error: Se deniega el acceso cuando los usuarios que no son administradores que han sido delegados intentan unir equipos a un dominio en la documentación de Microsoft Windows Server.

> **Important**
>
> No mueva los objetos de equipo que RDS Custom para SQL Server cree en la unidad organizativa (OU) después de crear la instancia de base de datos. Si mueve los objetos asociados, la instancia de base de datos de RDS Custom para SQL Server podría configurarse mal. Si necesita mover los objetos de equipo creados por Amazon RDS, utilice la acción ModifyDBInstance para modificar los parámetros del dominio con la ubicación deseada de los objetos del equipo.

Temas

- Paso 1: Crear una unidad organizativa (OU) en el AD
- Paso 2: Crear un usuario de dominio de AD
- Paso 3: Delegar el control al usuario de AD de forma autoadministrada o AWS Managed Microsoft AD
- Paso 4: Crear un secreto
- Paso 5: Crear o modificar una instancia de base de datos de RDS Custom para SQL Server
- Paso 6: Crear inicios de sesión de SQL Server de autenticación de Windows
- Paso 7: Uso de la autenticación Kerberos o NTLM

Paso 1: Crear una unidad organizativa (OU) en el AD

Efectúe los siguientes pasos para crear una unidad organizativa en su AD:

Creación de una OU en su AD

1. Conéctese a su AD de dominio como administrador de dominio.
2. Abra Usuarios y equipos de Active Directory y seleccione el dominio en el que desea crear la OU.
3. Haga clic con el botón derecho en el dominio y seleccione Nuevo y, a continuación, Unidad organizativa.
4. Escriba un nombre para la OU.

   Habilite Proteger el contenedor contra la eliminación accidental.
5. Seleccione Aceptar. La nueva OU aparece en su dominio.

Para AWS Managed Microsoft AD, el nombre de esta OU se basa en el nombre NetBIOS que escribió cuando creó el directorio. Esta OU es propiedad de AWS y contiene todos los objetos del directorio relacionados con AWS para los que a usted se le concede control total. De forma predeterminada, esta OU contiene dos OU secundarias Equipos y usuarios. Las nuevas OU que crea RDS Custom son secundarias de la unidad organizativa que se basa en NetBIOS.

Paso 2: Crear un usuario de dominio de AD

Las credenciales de usuario del dominio se utilizan para el secreto en Secrets Manager.

Creación de un usuario de dominio de AD en su AD

1. Abra Usuarios y equipos de Active Directory y seleccione el dominio y la OU en los que desea crear el usuario.
2. Haga clic con el botón derecho en el objeto Usuarios y seleccione Nuevo y, a continuación, Usuario.
3. Introduzca el nombre, los apellidos y el nombre de inicio de sesión del usuario. Haga clic en Next (Siguiente).
4. Introduzca una contraseña para el usuario. No seleccione El usuario debe cambiar la contraseña en el próximo inicio de sesión ni La cuenta está deshabilitada. Haga clic en Next (Siguiente).
5. Haga clic en OK (Aceptar). Su nuevo usuario aparece en su dominio.

Paso 3: Delegar el control al usuario de AD de forma autoadministrada o AWS Managed Microsoft AD

Para delegar el control al usuario del dominio AD de su dominio

1. Abra el complemento MMC Usuarios y equipos de Active Directory y seleccione su dominio.
2. Haga clic con el botón derecho en la OU que creó anteriormente y seleccione Delegar control.
3. En Asistente para delegación de control, haga clic en Siguiente.
4. En la sección Usuarios o grupos, haga clic en Agregar.
5. En Seleccionar usuarios, equipos o grupos, introduzca el usuario de AD que creó y haga clic en Verificar nombres. Si la comprobación de usuario de AD se ha realizado correctamente, haga clic en Aceptar.
6. En la sección Usuarios o grupos, confirme que ha agregado el usuario de AD y haga clic en Siguiente.

7. En la página Tareas que se delegarán, seleccione Crear una tarea personalizada para delegar y haga clic en Siguiente.
8. En la sección Tipo de objeto de Active Directory:

   Elija Solo los siguientes objetos de la carpeta.

   Seleccione Objetos computacionales.

   Seleccione Crear objetos seleccionados en esta carpeta.

   Seleccione Eliminar los objetos seleccionados en esta carpeta y haga clic en Siguiente.
9. En la sección Permisos:

   Mantenga seleccionada la opción General.

   Seleccione Escritura validada en el nombre de host DNS.

   Seleccione Escritura validada en el nombre de la entidad de servicio y haga clic en Siguiente.
10. Para Completar el asistente para delegación de control, confirme la configuración y haga clic en Finalizar.

Paso 4: Crear un secreto

Cree el secreto en la misma región y Cuenta de AWS que contiene la instancia de base de datos de RDS Custom para SQL Server que desea incluir en su directorio activo. Almacene las credenciales del usuario del dominio de AD creado en Paso 2: Crear un usuario de dominio de AD.

Console

- En AWS Secrets Manager, elija Almacenar un nuevo secreto.
- En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
- En Pares clave-valor, agregue sus dos claves:
  - La primera clave, `SELF_MANAGED_ACTIVE_DIRECTORY_USERNAME` e ingrese el nombre del usuario de AD (sin el prefijo de dominio) para el valor.
  - Para la segunda clave, introduzca `SELF_MANAGED_ACTIVE_DIRECTORY_PASSWORD` e introduzca la contraseña de su usuario de AD en su dominio.
- En Clave de cifrado, introduzca la misma clave de AWS KMS que utilizó para crear la instancia de RDS Custom para SQL Server.

- En Nombre secreto, elija el nombre secreto que empiece por `do-not-delete-rds-custom-` para permitir que el perfil de la instancia acceda a este secreto. Si quiere elegir un nombre diferente para el secreto, actualice `RDSCustomInstanceProfile` para acceder al Nombre secreto.
- (Opcional) En Descripción, escriba una descripción del nombre del secreto.
- Cómo agregar las etiquetas `Key="AWSRDSCustom",Value="custom-sqlserver"`
- Haga clic en Guardar y, a continuación, en Siguiente.
- En Configurar los ajustes de rotación, mantenga los valores predeterminados y seleccione Siguiente.
- Revise la configuración del secreto y haga clic en Guardar.
- Elija el nuevo secreto y copie el valor del ARN del secreto. Esto lo utilizaremos en el siguiente paso para configurar su Active Directory.

CLI

Ejecute el siguiente comando en su CLI para crear un secreto:

```
# Linux based
aws secretsmanager create-secret \
--name do-not-delete-rds-custom-DomainUserCredentails \
--description "Active directory user credentials for managing RDS Custom" \
--secret-string "{\"SELF_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"tester\",
\"SELF_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"xxxxxxxx\"}" \
--kms-key-id <RDSCustomKMSKey> \
--tags Key="AWSRDSCustom",Value="custom-sqlserver"

# Windows based
aws secretsmanager create-secret ^
--name do-not-delete-rds-custom-DomainUserCredentails ^
--description "Active directory user credentials for managing RDS Custom" ^
--secret-string "{\"SELF_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"tester\",
\"SELF_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"xxxxxxxx\"}" ^
--kms-key-id <RDSCustomKMSKey> ^
--tags Key="AWSRDSCustom",Value="custom-sqlserver"
```

Paso 5: Crear o modificar una instancia de base de datos de RDS Custom para SQL Server

Cree o modifique una instancia de base de datos de RDS Custom para SQL Server para usarla con su directorio. Puede utilizar la consola, CLI, o la API de RDS para asociar una instancia de base de datos con un directorio. Puede hacerlo de una de las siguientes formas:

- Cree una nueva instancia de base de datos de SQL Server mediante la consola, el comando de la CLI create-db-instance o la operación CreateDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de SQL Server existente mediante la consola, el comando de la CLI modify-db-instance o la operación ModifyDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Restaure una instancia de base de datos de SQL Server a partir de una instantánea de base de datos mediante la consola, el comando de la CLI restore-db-instance-from-db-snapshot o la operación RestoreDBInstanceFromDBSnapshot de la API de RDS.

  Para obtener instrucciones, consulte Restauración a una instancia de base de datos.
- Restaure una instancia de base de datos de SQL Server a un punto en el tiempo mediante la consola, el comando de la CLI restore-db-instance-to-point-in-time o la operación RestoreDBInstanceToPointInTime de la API de RDS.

  Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

> **Note**
>
> Si su instancia de RDS Custom para SQL Server ya está unida a un AD manualmente, compruebe la configuración de Reglas de puertos de configuraciones de redes, Validación de red y complete los pasos del 1 al 4. Actualice `--domain-fqdn`, `--domain-ou` y `--domain-auth-secret-arn` a su AD para que las credenciales y configuraciones de unión al dominio se registren en RDS Custom para supervisar, registrar el CNAME y tomar medidas de recuperación.

Cuando utilice la AWS CLI, se necesitan los siguientes parámetros para que la instancia de base de datos pueda usar el directorio que ha creado:

- Para el parámetro `--domain-fqdn`, utilice el nombre de dominio completo de su AD autoadministrado.
- Para el parámetro `--domain-ou`, utilice la OU que creó en su AD autoadministrado.
- Para el parámetro `--domain-auth-secret-arn`, utilice el valor del ARN del secreto que ha creado.

> **Important**
>
> Si modifica una instancia de base de datos para unirla a un dominio de AD autoadministrado o AWS Managed Microsoft AD, es necesario reiniciar la instancia de base de datos para que la modificación surta efecto. Puede optar por aplicar los cambios inmediatamente o esperar hasta el próximo período de mantenimiento. Si opta por Aplicar inmediatamente, se origina un tiempo de inactividad para las instancias de base de datos Single-AZ. El clúster de base de datos Multi-AZ realiza una conmutación por error antes de completar el reinicio. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

El siguiente comando de CLI crea una nueva instancia de base de datos de RDS Custom para SQL Server y la une a un dominio de AWS Managed Microsoft AD o autoadministrado.

Para Linux, macOS o Unix:

```
aws rds create-db-instance  \
--engine custom-sqlserver-se \
--engine-version 15.00.4312.2.v1 \
--db-instance-identifier my-custom-instance \
--db-instance-class db.m5.large \
--allocated-storage 100 --storage-type io1 --iops 1000 \
--master-username my-master-username \
--master-user-password my-master-password \
--kms-key-id  my-RDSCustom-key-id \
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance  \
--domain-fqdn "corp.example.com" \
--domain-ou "OU=RDSCustomOU,DC=corp,DC=example,DC=com" \
```

```
--domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:do-not-
delete-rds-custom-my-AD-test-secret-123456" \
--db-subnet-group-name my-DB-subnet-grp \
--vpc-security-group-ids  my-securitygroup-id \
--no-publicly-accessible \
--backup-retention-period 3 \
--port 8200 \
--region us-west-2 \
--no-multi-az
```

Para Windows:

```
aws rds create-db-instance  ^
--engine custom-sqlserver-se ^
--engine-version 15.00.4312.2.v1 ^
--db-instance-identifier my-custom-instance ^
--db-instance-class db.m5.large ^
--allocated-storage 100 --storage-type io1 --iops 1000 ^
--master-usernamemy-master-username ^
--master-user-password my-master-password ^
--kms-key-id  my-RDSCustom-key-id ^
--custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance  ^
--domain-fqdn "corp.example.com" ^
--domain-ou "OU=RDSCustomOU,DC=corp,DC=example,DC=com" ^
--domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:do-not-
delete-rds-custom-my-AD-test-secret-123456" ^
--db-subnet-group-name my-DB-subnet-grp ^
--vpc-security-group-ids  my-securitygroup-id ^
--no-publicly-accessible ^
--backup-retention-period 3 ^
--port 8200 ^
--region us-west-2 ^
--no-multi-az
```

Important

Si su NetBIOS para AWS Managed Microsoft AD es corpexample, entonces aparece como una OU en sí misma. Cualquier unidad organizativa nueva creada anteriormente aparecerá como una unidad organizativa

anidada. En AWS Managed Microsoft AD, establezca `--domain-ou` en `"OU=RDSCustomOU,OU=corpexample,DC=corp,DC=example,DC=com"`.

El siguiente comando modifica una instancia de base de datos de RDS Custom para SQL Server existente para que utilice un dominio de Active Directory.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --domain-fqdn "corp.example.com" \
    --domain-ou "OU=RDSCustomOU,DC=corp,DC=example,DC=com" \
    --domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:do-not-delete-rds-custom-my-AD-test-secret-123456" \
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --domain-fqdn "corp.example.com" ^
    --domain-ou "OU=RDSCustomOU,DC=corp,DC=example,DC=com" ^
    --domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:do-not-delete-rds-custom-my-AD-test-secret-123456" ^
```

El siguiente comando de CLI elimina una instancia de base de datos de RDS Custom para SQL Server de un dominio de Active Directory.

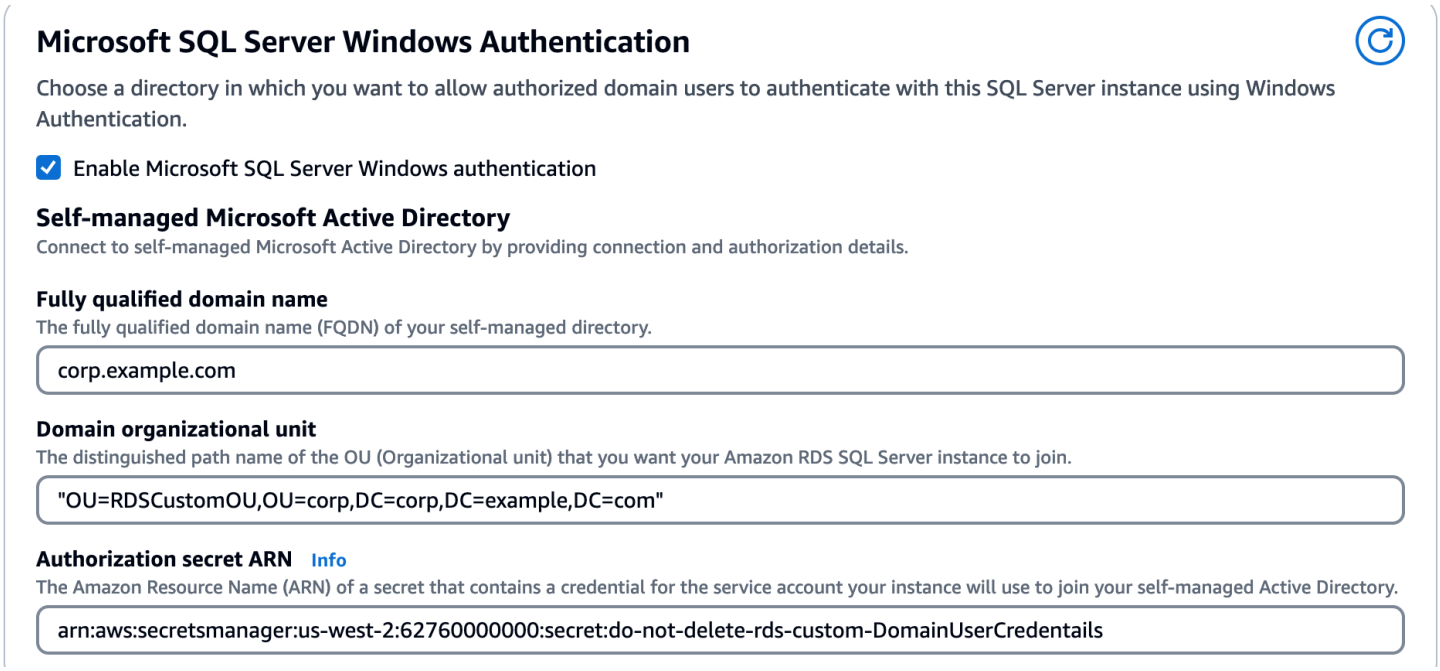
Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-custom-instance \
    --disable-domain
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-custom-instance ^
    --disable-domain
```

Cuando utilice la consola para crear o modificar su instancia, haga clic en Habilitar la autenticación de Microsoft SQL Server Windows para ver las siguientes opciones.



Usted es responsable de asegurarse de que el FQDN de su dominio se resuelva en las direcciones IP del controlador de dominio. Si las direcciones IP de los controladores de dominio no se resuelven, las operaciones de unión al dominio fallan, pero la creación de la instancia de RDS Custom for SQL Server se realiza correctamente. Para obtener información sobre la resolución de problemas, consulte Solución de problemas de Active Directory.

Paso 6: Crear inicios de sesión de SQL Server de autenticación de Windows

Use las credenciales del usuario maestro de Amazon RDS para conectarse a la instancia de base de datos de SQL Server como lo haría con cualquier otra instancia de base de datos. Como la instancia de base de datos está unida al dominio de AD, puede aprovisionar inicios de sesión y usuarios de SQL Server. Para ello, utilice la utilidad de usuarios y grupos de AD de su dominio de AD. Los permisos de bases de datos se administran a través de los permisos de SQL Server estándar otorgados y revocados para estos inicios de sesión de Windows.

Para que un usuario de AD se autentique con SQL Server, debe existir un inicio de sesión de Windows de SQL Server para el usuario de AD o para un grupo de Active Directory del que el usuario sea miembro. El control detallado del acceso se gestiona mediante la concesión y la revocación de permisos en estos inicios de sesión de SQL Server. Un usuario de AD que no tenga un inicio de sesión de SQL Server o no pertenezca a un grupo de AD con dicho inicio de sesión no puede tener acceso a la instancia de base de datos de SQL Server.

El permiso `ALTER ANY LOGIN` es necesario para crear un inicio de sesión de SQL Server de AD. Si todavía no ha creado ningún inicio de sesión con este permiso, conéctese como usuario maestro de la instancia de base de datos usando la autenticación de SQL Server y cree sus inicios de sesión de SQL Server de AD bajo el contexto del usuario maestro.

Puede ejecutar un comando de lenguaje de definición de datos (DDL), como el siguiente, para crear un inicio de sesión de SQL Server para un usuario o grupo de AD.

```
USE [master]
GO
CREATE LOGIN [mydomain\myuser] FROM WINDOWS WITH DEFAULT_DATABASE = [master],
 DEFAULT_LANGUAGE = [us_english];
GO
```

Los usuarios (tanto humanos como aplicaciones) del dominio pueden conectarse ahora a la instancia de RDS Custom para SQL Server desde un equipo cliente unido al dominio utilizando la autenticación de Windows.

Paso 7: Uso de la autenticación Kerberos o NTLM

Autenticación NTLM mediante un punto de conexión de RDS

Cada instancia de base de datos de Amazon RDS contiene un punto de conexión y cada punto de conexión contiene el nombre DNS y el número de puerto para la instancia de base de datos. Para conectarse a su instancia de base de datos mediante una aplicación cliente SQL, necesita el nombre DNS y el número de puerto para la instancia de base de datos. Para autenticarse mediante la autenticación NTLM, debe conectarse al punto de conexión de RDS.

Durante una interrupción del servicio no planificada o un mantenimiento planificado de la base de datos, Amazon RDS conmuta automáticamente a la base de datos secundaria actualizada para que las operaciones puedan reanudarse rápidamente sin intervención manual. Las instancias principal y secundaria usan el mismo punto de conexión, cuya dirección de red física cambia a la secundaria como parte del proceso de conmutación por error. No tiene que volver a configurar su aplicación cuando se produzca una conmutación por error.

Autenticación de Kerberos

La autenticación basada en Kerberos para RDS Custom para SQL Server requiere que las conexiones se realicen a un nombre principal de servicio (SPN) específico. Sin embargo, tras un evento de conmutación por error, es posible que la aplicación no conozca el nuevo SPN. Para

solucionar este problema, RDS Custom para SQL Server ofrece un punto de conexión basado en Kerberos.

El punto de conexión basado en Kerberos sigue un formato específico. Si su punto de conexión de RDS es *rds-instance-name*.*account-region-hash*.*aws-region*.rds.amazonaws.com, el punto de conexión correspondiente basado en Kerberos sería *rds-instance-name*.*account-region-hash*.*aws-region*.awsrds.*fully qualified domain name (FQDN)*.

Por ejemplo, si el punto de conexión de RDS es `ad-test.cocv6zwtircu.us-east-1.rds.amazonaws.com` y el nombre de dominio es `corp-ad.company.com`, el punto de conexión basado en Kerberos sería `ad-test.cocv6zwtircu.us-east-1.awsrds.corp-ad.company.com`.

Este punto de conexión basado en Kerberos se puede usar para autenticarse con la instancia de SQL Server mediante Kerberos, incluso después de un evento de conmutación por error, ya que el punto de conexión se actualiza automáticamente para que apunte al nuevo SPN de la instancia principal de SQL Server.

Cómo encontrar su CNAME

Para encontrar su CNAME, conéctese al controlador de dominio y abra Administrador de DNS. Navegue hasta Zonas de búsqueda avanzada y su FQDN.

Navegue por awsrds, aws-region y hash específicos de la cuenta y la región.

Si conecta la instancia de EC2 de RDS Custom e intenta conectarse a la base de datos de forma local mediante CNAME, la conexión utilizará la autenticación NTLM en lugar de Kerberos.

Si después de conectar CNAME desde un cliente remoto, se devuelve una conexión NTLM, compruebe si los puertos necesarios están en la lista de permitidos.

Para comprobar si su conexión usa Kerberos, ejecute la siguiente consulta:

```
SELECT net_transport, auth_scheme
    FROM sys.dm_exec_connections
    WHERE session_id = @@SSPID;
```

Administración de una instancia de base de datos en un dominio

Puede usar la consola, la AWS CLI o la API de Amazon RDS para administrar la instancia de base de datos y la relación con su dominio. Por ejemplo, puede mover la instancia de base de datos dentro, fuera o entre dominios.

Por ejemplo, con la API de Amazon RDS puede hacer lo siguiente:

- Para volver a intentar una unión de dominio para una suscripción que haya generado un error, use la operación ModifyDBInstance de la API y especifique el ID del directorio de suscripción actual.
- Para actualizar el nombre del rol de IAM para la suscripción, use la operación `ModifyDBInstance` de la API y especifique el ID del directorio de la suscripción actual y el nuevo rol de IAM.
- Para eliminar una instancia de base de datos de un dominio, use la operación `ModifyDBInstance` de la API y especifique `none` como parámetro del dominio.
- Para mover una instancia de base de datos de un dominio a otro, use la operación `ModifyDBInstance` de la API y especifique el identificador del nuevo dominio como parámetro del dominio.
- Para ver la suscripción de cada instancia de base de datos, use la operación DescribeDBInstances de la API.

Restauración de una instancia de base de datos de RDS Custom para SQL Server y adición de esta a un dominio de Active Directory

Puede restaurar una instantánea de base de datos o realizar una recuperación en un momento dado (PITR) para una instancia de base de datos de SQL Server y, a continuación, agregarla a un dominio de Active Directory. Una vez que la instancia de base de datos se haya restaurado, modifíquela usando el proceso que se explica en la sección Paso 5: Crear o modificar una instancia de base de datos de RDS Custom para SQL Server para agregar la instancia de base de datos a un dominio de AD.

Descripción de la pertenencia a los dominios

Una vez que haya creado o modificado una instancia de base de datos, esta se convierte en miembro del dominio. La consola AWS indica el estado de la pertenencia del dominio para la instancia de base de datos. El estado de la instancia de base de datos puede ser uno de los siguientes:

- joined: la instancia es miembro del dominio.
- joining: la instancia está en el proceso de convertirse en miembro del dominio.
- pending-join: la suscripción de la instancia está pendiente.
- pending-maintenance-join: AWS intentará convertir la instancia en miembro del dominio durante el próximo periodo de mantenimiento programado.

- pending-removal: la eliminación de la instancia del dominio está pendiente.
- pending-maintenance-removal: AWS intentará eliminar la instancia del dominio durante el próximo periodo de mantenimiento programado.
- error: un problema de configuración ha impedido que la instancia se una al dominio. Compruebe y corrija la configuración antes de volver a ejecutar el comando para modificar la instancia.
- removing: la instancia se está eliminando del dominio.

Una solicitud para convertirse en miembro de un dominio puede generar un error a causa de un problema de conectividad de la red o de un rol de IAM incorrecto. Por ejemplo, puede crear una instancia de base de datos o modificar una instancia existente y que se produzca un error al intentar que la instancia de base de datos se convierta en miembro de un dominio. En este caso, vuelva a emitir el comando para crear o modificar la instancia de base de datos o modificar la instancia recién creada para unirse al dominio.

Solución de problemas de Active Directory

Los siguientes son los problemas que pueden surgir al configurar o modificar un AD.

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
Error 2 / 0x2	El sistema no puede encontrar el archivo especificado.	El formato o la ubicación de la unidad organizativa (OU) especificados con el parámetro –`domain-ou` no es válido. La cuenta de servicio de dominio especificada mediante AWS Secrets Manager carece de los permisos necesarios para unirse a la OU.	Revise el parámetro –`domain-ou` . Asegúrese de que la cuenta de servicio de dominio tenga los permisos correctos para la OU.
Error 5 / 0x5	Se deniega el acceso.	Los permisos de la cuenta de servicio del dominio están mal configurados	Revise los permisos de la cuenta de servicio del dominio y compruebe que la cuenta del equipo de

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
		o la cuenta del equipo ya existe en el dominio.	RDS no esté duplicada en el dominio. Para comprobar el nombre de la cuenta del equipo de RDS, ejecute `SELECT @@SERVERNAME` en su instancia de base de datos de RDS Custom para SQL Server. Si utiliza Multi-AZ, intente reiniciar con conmutación por error y, a continuación, compruebe de nuevo la cuenta del equipo de RDS. Para obtener más información, consulte Reinicio de una instancia de base de datos.
Error 87 / 0x57	El parámetro es incorrecto.	La cuenta de servicio de dominio especificada mediante AWS Secrets Manager no tiene los permisos correctos. El perfil de usuario también podría estar dañado.	Revise los requisitos de la cuenta de servicio de dominio.
Error 234 / 0xEA	La unidad organizativa (OU) especificada no existe.	La OU especificada con el parámetro `–domain-ou` no existe en su AD.	Revise el parámetro `–domain-ou` y asegúrese de que la OU especificada exista en su AD.

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
Error 1326 / 0x52E	El nombre de usuario o la contraseña es incorrecto.	Las credenciales de la cuenta de servicio de dominio proporcionadas en AWS Secrets Manager contienen un nombre de usuario desconocido o una contraseña incorrecta. La cuenta de dominio también podría estar deshabilitada en su AD.	Asegúrese de que las credenciales proporcionadas en AWS Secrets Manager sean correctas y de que la cuenta de dominio esté habilitada en su Active Directory.
Error 1355 / 0x54B	El dominio especificado no existe o no se pudo contactar con él.	El dominio está inactivo, no se puede acceder al conjunto especificado de IP de DNS o no se puede acceder al FQDN especificado.	Revise los parámetros `–domain-dns-ips` y `–domain-fqdn` para asegurarse de que son correctos. Revise la configuración de red de su instancia de base de datos de RDS Custom para SQL Server y asegúrese de que sea posible acceder a su AD.
Error 1772/0x6BA	El servidor RPC no está disponible.	Se ha producido un problema al acceder al servicio de RPC de su dominio de AD. Puede deberse a un problema de red o de servicio.	Valide que el servicio de RPC se esté ejecutando en sus controladores de dominio y que se pueda acceder a los puertos de TCP `135` y `49152-65535` en su dominio desde su instancia de base de datos de RDS Custom para SQL Server.

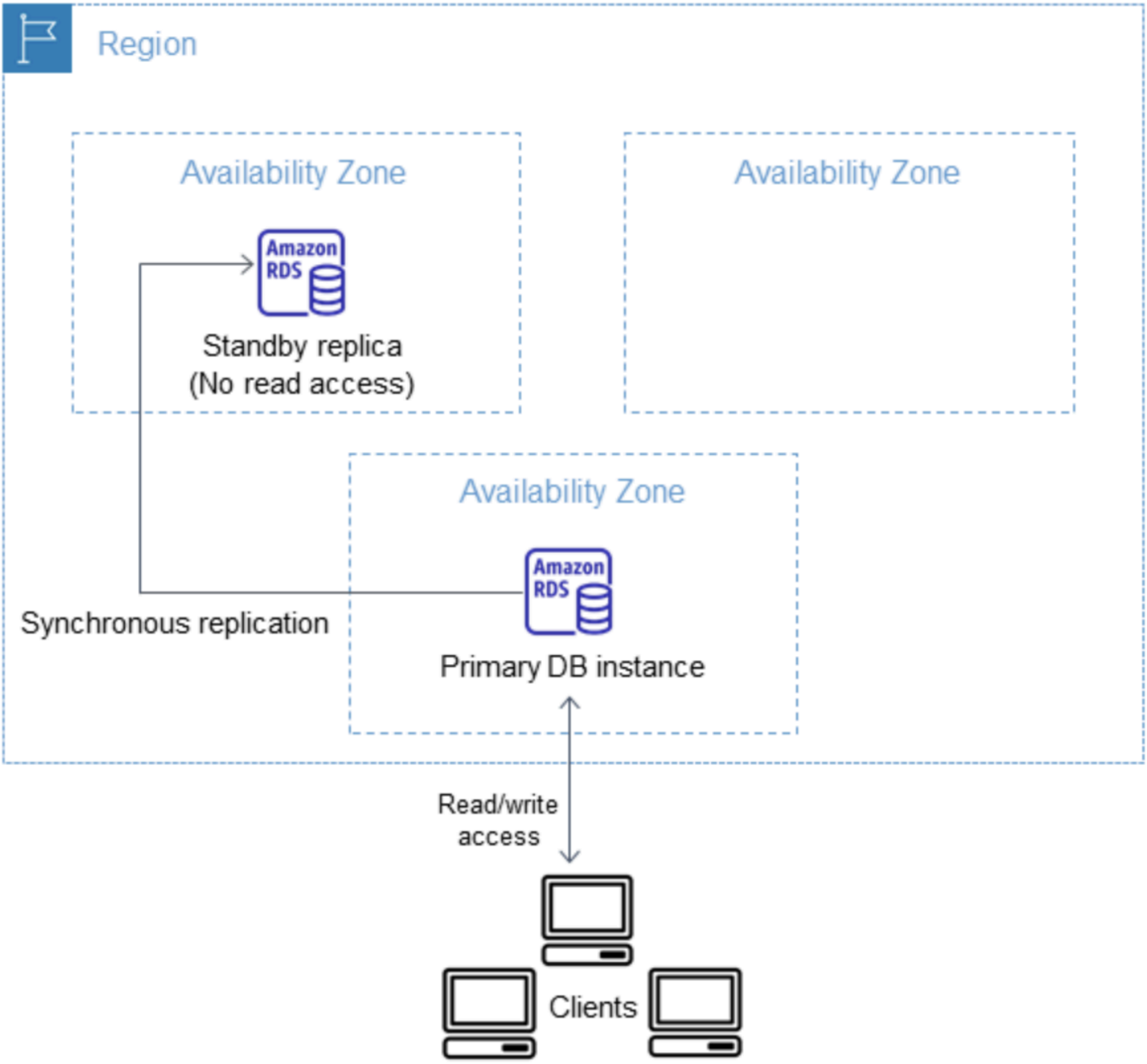
Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
Error 2224 / 0x8B0	La cuenta de usuario ya existe.	La cuenta de equipo que se intenta agregar al AD ya existe.	Para identificar la cuenta del equipo, ejecute `SELECT @@SERVERNAME` en su instancia de base de datos de RDS Custom para SQL Server y, a continuación, elimínela cuidadosamente de su AD.
Error 2242 / 0x8c2	La contraseña de este usuario ha caducado.	La contraseña de la cuenta de servicio de dominio especificada a través de AWS Secrets Manager ha caducado.	Actualice la contraseña de la cuenta de servicio de dominio utilizada para unir su instancia de base de datos de RDS Custom para SQL Server a su AD.

Administración de una implementación multi-AZ de RDS Custom para SQL Server

En una implementación de instancias de base de datos multi-AZ para RDS Custom para SQL Server, Amazon RDS aprovisiona y mantiene automáticamente una réplica síncrona en espera dentro de una zona de disponibilidad (AZ) diferente. La instancia de base de datos principal se replica de forma síncrona en las zonas de disponibilidad en una réplica en espera para proporcionar redundancia de datos.

> **Important**
>
> Una implementación multi-AZ para RDS Custom para SQL Server es diferente a una implementación multi-AZ para RDS para SQL Server. A diferencia de multi-AZ para RDS para SQL Server, debe cumplir los requisitos previos para RDS Custom para SQL Server antes de crear una instancia de base de datos multi-AZ, ya que RDS Custom se ejecuta dentro de su propia cuenta, lo que requiere permisos.
> Si no cumple los requisitos previos, es posible que su instancia de base de datos multi-AZ no se ejecute o que se revierta automáticamente a una instancia de base de datos Single-AZ. Para obtener más información acerca de los requisitos previos, consulte Requisitos previos de una implementación multi-AZ con RDS Custom para SQL Server.

La ejecución de una instancia de base de datos con alta disponibilidad puede mejorar la disponibilidad durante el mantenimiento de sistema planificado. Si se produce una interrupción del servicio no planificada o un mantenimiento planificado de la base de datos, Amazon RDS conmuta automáticamente a la instancia de base de datos secundaria. Esta funcionalidad permite que las operaciones de base de datos se reanuden rápidamente sin intervención manual. Las instancias principal y en espera usan el mismo punto de enlace, cuya dirección de red física cambia a la réplica secundaria como parte del proceso de conmutación por error. No tiene que volver a configurar su aplicación cuando se produzca una conmutación por error.



Para crear una implementación Multi-AZ de RDS Custom para SQL Server, especifique Multi-AZ al crear una instancia de base de datos de RDS Custom. Para usar la consola para convertir las instancias de base de datos de RDS Custom para SQL Server existentes en implementaciones multi-AZ, modifique la instancia de base de datos y especifique la opción Multi-AZ. También puede especificar una implementación de instancia de base de datos multi-AZ con la CLI de AWS o la API de Amazon RDS.

La consola de RDS muestra la zona de disponibilidad de la réplica en espera (AZ secundaria). También puede usar el comando de la CLI `describe-db-instances` o la operación de la API `DescribeDBInstances` para buscar la AZ secundaria.

Las instancias de base de datos de RDS Custom para SQL Server que usan implementaciones multi-AZ pueden tener una latencia de escritura y confirmación superior a la de una implementación single-AZ. Este aumento se puede producir debido a la replicación de datos síncrona entre las instancias de base de datos. Puede detectar un cambio en la latencia si la implementación conmuta a la réplica en espera, aunque AWS se ha diseñado con una conectividad de red de baja latencia entre zonas de disponibilidad.

> **Note**
>
> Para cargas de trabajo de producción, recomendamos que utilice una clase de instancia de base de datos con IOPS aprovisionadas (operaciones de entrada/salida por segundo) para conseguir un rendimiento rápido y uniforme. Para obtener más información sobre las clases de instancias de bases de datos, consulte Requisitos y limitaciones de Amazon RDS Custom for SQL Server.

Temas

- Disponibilidad en regiones y versiones
- Limitaciones de una implementación multi-AZ de RDS Custom para SQL Server
- Requisitos previos de una implementación multi-AZ con RDS Custom para SQL Server
- Creación de una implementación multi-AZ de RDS Custom para SQL Server
- Coversión de una implementación single-AZ de RDS Custom para SQL Server en una implementación multi-AZ
- Coversión de una implementación multi-AZ de RDS Custom para SQL Server en una implementación single-AZ
- Proceso de conmutación por error para una implementación multi-AZ de RDS Custom para SQL Server

Disponibilidad en regiones y versiones

Las implementaciones multi-AZ de RDS Custom para SQL Server son compatibles con las siguientes ediciones de SQL Server:

- Ediciones SQL Server 2022 y 2019, Enterprise, Standard, Web y Developer Edition.

> **Note**
>
> Las implementaciones multi-AZ para RDS Custom para SQL Server no son compatibles con SQL Server 2019 CU8 (15.00.4073.23) o versiones anteriores.

Las implementaciones multi-AZ de RDS Custom para SQL Server están disponibles en todas las regiones en las que está disponible RDS Custom para SQL Server. Para obtener más información sobre la disponibilidad en las regiones de las implementaciones multi-AZ de RDS Custom para SQL Server, consulte Regiones y motores de base de datos admitidos para RDS Custom para SQL Server.

Limitaciones de una implementación multi-AZ de RDS Custom para SQL Server

Las implementaciones multi-AZ de RDS Custom para SQL Server tienen las siguientes limitaciones:

- No se admiten implementaciones multi-AZ entre regiones.
- No puede configurar la instancia de base de datos secundaria de modo que acepte la actividad de lectura de bases de datos.
- Cuando utilice una versión de motor personalizada (CEV) con una implementación multi-AZ, la instancia de base de datos secundaria también utilizará la misma CEV. La instancia de base de datos secundaria no puede usar una CEV diferente.

Requisitos previos de una implementación multi-AZ con RDS Custom para SQL Server

Si ya tiene una implementación single-AZ de RDS Custom para SQL Server, se requieren los siguientes requisitos previos adicionales para convertirla en una implementación multi-AZ. Puede optar por completar los requisitos previos manualmente o con la plantilla de CloudFormation proporcionada. La plantilla de CloudFormation contiene los requisitos previos para las implementaciones single-AZ y multi-AZ.

> **Important**
>
> Para simplificar la configuración, le recomendamos que utilice el archivo de plantilla de AWS CloudFormation más reciente que se proporciona en las instrucciones de configuración

de red para completar los requisitos previos. Para obtener más información, consulte Configuración con AWS CloudFormation.

> **Note**
>
> Cuando modifique una implementación single-AZ de RDS Custom para SQL Server existente para convertirla en una implementación multi-AZ, debe completar estos requisitos previos. De lo contrario, se producirá un error en la configuración de multi-AZ. Para completar los requisitos previos, realice los pasos de Coversión de una implementación single-AZ de RDS Custom para SQL Server en una implementación multi-AZ.

- Actualice las reglas de entrada y salida del grupo de seguridad de RDS para permitir el puerto 1120.
- Añada una regla a la lista de control de acceso (ACL) de su red privada que permita los puertos TCP `0-65535` para la VPC de la instancia de base de datos.
- Cree nuevos puntos de conexión de VPC de Amazon SQS que permitan a la instancia de base de datos de RDS Custom para SQL Server comunicarse con SQS.
- Actualice los permisos de SQS en el rol del perfil de instancia.

Creación de una implementación multi-AZ de RDS Custom para SQL Server

Para crear una implementación multi-AZ de RDS Custom para SQL Server, siga los pasos que se indican en Creación y conexión a una instancia de base de datos para Amazon RDS Custom for SQL Server.

> **Important**
>
> Para simplificar la configuración, le recomendamos que utilice el archivo de plantilla de AWS CloudFormation más reciente que se proporciona en las instrucciones de configuración de red. Para obtener más información, consulte Configuración con AWS CloudFormation.

La creación de una implementación multi-AZ tarda unos cuantos minutos.

Coversión de una implementación single-AZ de RDS Custom para SQL Server en una implementación multi-AZ

Puede modificar una instancia de base de datos de RDS Custom para SQL Server existente para que pase de una implementación single-AZ a una implementación multi-AZ. Cuando modifica la instancia de base de datos, Amazon RDS realiza varias acciones:

- Realiza una instantánea de la instancia de base de datos principal.
- Crea nuevos volúmenes para la réplica en espera a partir de la instantánea. Estos volúmenes se inicializan en segundo plano y se alcanza el máximo rendimiento del volumen cuando los datos se han inicializado por completo.
- Activa la replicación síncrona a nivel de bloque entre las instancias de base de datos principal y secundaria.

> **Important**
>
> Le recomendamos que no modifique su instancia de base de datos de RDS Custom para SQL Server para convertir la implementación single-AZ en una implementación multi-AZ en una instancia de base de datos de producción durante los períodos de máxima actividad.

AWS usa una instantánea para crear la instancia en espera para evitar el tiempo de inactividad al convertir una implementación single-AZ en multi-AZ, pero el rendimiento podría verse afectado durante y después de la conversión a multi-AZ. Este impacto puede ser significativo para las cargas de trabajo sensibles a la latencia de escritura. Si bien esta capacidad permite restaurar rápidamente grandes volúmenes a partir de instantáneas, puede provocar un aumento considerable de la latencia de las operaciones de E/S debido a la replicación síncrona. Esta latencia puede afectar al rendimiento de la base de datos.

> **Note**
>
> Si creó la instancia de base de datos de RDS Custom para SQL Server antes del 29 de agosto de 2024, aplique el parche a la versión secundaria más reciente antes de modificarla.
>
> - Para las instancias de SQL Server 2019, actualice la versión del motor de base de datos a `15.00.4410.1.v1` o superior.

- Para las instancias de SQL Server 2022, actualice la versión del motor de base de datos a `16.00.4150.1.v1` o superior.

Temas

- Configuración de requisitos previos para convertir una implementación single-AZ en multi-AZ mediante CloudFormation
- Configuración de los requisitos previos para convertir manualmente una implementación single-AZ en multi-AZ
- Realice las modificaciones mediante la consola de RDS, la CLI de AWS o la API de RDS.

Configuración de requisitos previos para convertir una implementación single-AZ en multi-AZ mediante CloudFormation

Para utilizar una implementación multi-AZ, debe asegurarse de haber aplicado la plantilla de CloudFormation más reciente con los requisitos previos o de configurar manualmente los requisitos previos más recientes. Si ya ha aplicado la plantilla de requisitos previos de CloudFormation más reciente, puede omitir estos pasos.

Para configurar los requisitos previos de las implementaciones multi-AZ de RDS Custom para SQL Server mediante CloudFormation

1. Abra la consola de CloudFormation en https://console.aws.amazon.com/cloudformation.
2. Para iniciar el asistente Crear pila, seleccione la pila existente que utilizó para crear una implementación Single-AZ y elija Actualizar.

   Aparecerá la página Actualizar pila.
3. En Requisito previo: preparar la plantilla, elija Reemplazar la plantilla actual.
4. En Specify template (Especificar plantilla), haga lo siguiente:

   a. Descargue el archivo de plantilla de AWS CloudFormation más reciente. Abra el menú contextual (haga clic con el botón derecho del ratón) del enlace custom-sqlserver-onboard.zip y elija Save Link As (Guardar enlace como).

   b. Guarde y extraiga el archivo `custom-sqlserver-onboard.json` en su equipo.

   c. Para Origen de plantilla, elija Cargar un archivo de plantilla.

d. En Choose file (Elegir archivo), navegue hasta `custom-sqlserver-onboard.json` y elíjalo.

5. Elija Siguiente.

   Aparecerá la página Specify stack details (Especificar los detalles de la pila).

6. Para conservar las opciones predeterminadas, elija Next (Siguiente).

   Aparece la página Opciones avanzadas.

7. Para conservar las opciones predeterminadas, elija Next (Siguiente).
8. Para conservar las opciones predeterminadas, elija Next (Siguiente).
9. En la página Revisar los cambios, haga lo siguiente:

   a. Para Capabilities (Capacidades), seleccione la casilla de verificación I acknowledge that AWS CloudFormation might create IAM resources with custom names (Reconozco que podría crear recursos de IAM con nombres personalizados).

   b. Elija Enviar.

10. Compruebe que la actualización se ha realizado correctamente. Si la operación se ha realizado correctamente, aparece `UPDATE_COMPLETE`.

Si la actualización falla, se revertirá cualquier configuración nueva especificada en el proceso de actualización. El recurso existente seguirá pudiéndose utilizar. Por ejemplo, si añade reglas de ACL de red con los números 18 y 19, pero ya existían reglas con esos números, la actualización devolvería el siguiente error: `Resource handler returned message: "The network acl entry identified by 18 already exists.`. En este caso, puede modificar las reglas de ACL existentes para usar un número inferior a 18 y, a continuación, volver a intentar la actualización.

Configuración de los requisitos previos para convertir manualmente una implementación single-AZ en multi-AZ

> **Important**
>
> Para simplificar la configuración, le recomendamos que utilice el archivo de plantilla de AWS CloudFormation más reciente que se proporciona en las instrucciones de configuración de red. Para obtener más información, consulte Configuración de requisitos previos para convertir una implementación single-AZ en multi-AZ mediante CloudFormation.

Si decide configurar los requisitos previos manualmente, realice las siguientes tareas.

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija Punto de conexión. Aparecerá la página Create Endpoint (Creación de un punto de enlace).
3. En Categoría de servicio, elija Servicios de AWS.
4. En Servicios, busque *SQS*.
5. En VPC, elija la VPC en la que esté implementada la instancia de base de datos de RDS Custom para SQL Server.
6. En Subredes, elija las subredes en las que está implementada la instancia de base de datos de RDS Custom para SQL Server.
7. En Grupos de seguridad, elija el grupo *-vpc-endpoint-sg*.
8. En Política, elija Personalizada.
9. En su política personalizada, sustituya la *partición de AWS*, la *región*, el *identificador de cuenta* y el *rol de instancia de IAM* por sus propios valores.

   JSON

```
                {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Condition": {
                    "StringLike": {
                        "aws:ResourceTag/AWSRDSCustom": "custom-sqlserver"
                    }
                },
                "Action": [
                    "SQS:SendMessage",
                    "SQS:ReceiveMessage",
                    "SQS:DeleteMessage",
                    "SQS:GetQueueUrl"
                ],
                "Resource": "arn:${AWS::Partition}:sqs:${AWS::Region}:
${AWS::AccountId}:do-not-delete-rds-custom-*",
                "Effect": "Allow",
                "Principal": {
```

```
                    "AWS": "arn:${AWS::Partition}:iam::
${AWS::AccountId}:role/{IAM-Instance-role}"
                }
            }
        ]
    }
```

10. Actualice el perfil de instancia con permiso para acceder a Amazon SQS. Sustituya la *partición de AWS*, *la región* y el *identificador de cuenta* por sus propios valores.

```
                    {
    "Sid": "SendMessageToSQSQueue",
    "Effect": "Allow",
    "Action": [
      "SQS:SendMessage",
      "SQS:ReceiveMessage",
      "SQS:DeleteMessage",
      "SQS:GetQueueUrl"

    ],
    "Resource": [
      {
        "Fn::Sub": "arn:${AWS::Partition}:sqs:${AWS::Region}:${AWS::AccountId}:do-
not-delete-rds-custom-*"
      }
    ],
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/AWSRDSCustom": "custom-sqlserver"
      }
    }
  }
                    >
```

11. Actualice las reglas de entrada y salida del grupo de seguridad de Amazon RDS para permitir el puerto 1120.

    a. En Grupos de seguridad, elija el grupo *-rds-custom-instance-sg*.

    b. En Reglas de entrada, cree una regla TCP personalizada para permitir el puerto *1120* desde el grupo *-rds-custom-instance-sg* de origen.

c. En Reglas de salida, cree una regla TCP personalizada para permitir el puerto *1120* al grupo *-rds-custom-instance-sg* de destino.

12. Añada una regla a la lista de control de acceso (ACL) de su red privada que permita los puertos TCP `0-65535` para la subred de origen de la instancia de base de datos.

> **Note**
>
> Al crear una Regla de entrada y una Regla de salida, tome nota del Número de regla más alto. Las nuevas reglas que cree deben tener un Número de regla inferior a 100 y no coincidir con ningún Número de regla existente.

a. En ACL de red, elija el grupo *-private-network-acl*.

b. En Reglas de entrada, cree una regla para Todos los TCP para permitir los puertos TCP `0-65535` que se originan desde *privatesubnet1* y *privatesubnet2*.

c. En Reglas de salida, cree una regla para Todos los TCP para permitir los puertos TCP `0-65535` que van a *privatesubnet1* y *privatesubnet2*.

Realice las modificaciones mediante la consola de RDS, la CLI de AWS o la API de RDS.

Una vez completados los requisitos previos, puede modificar una instancia de base de datos de RDS Custom para SQL Server para convertir una implementación single-AZ en multi-AZ mediante la consola de RDS, la CLI de AWS o la API de RDS.

Consola

Para convertir una implementación single-AZ de RDS Custom para SQL Server en una implementación multi-AZ

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos).

   Aparece el panel Databases (Bases de datos).
3. Elija la instancia de base de datos de RDS Custom para SQL Server que desea restaurar.
4. En Acciones, elija Convertir a implementación multi-AZ.

5. Para aplicar los cambios de forma inmediata, seleccione la opción Aplicar inmediatamente en la página Confirmación. La elección de esta opción no provoca tiempo de inactividad, pero existe un posible impacto en el rendimiento. De forma alternativa, también puede aplicar la actualización durante la siguiente ventana de mantenimiento. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.
6. En la página Confirmación, seleccione Convertir a multi-AZ.

AWS CLI

Para convertirla en una implementación de instancia de base de datos multi-AZ mediante la AWS CLI, llame al comando modify-db-instance y defina la opción `--multi-az`. Especifique el identificador de instancias de base de datos y los valores de las otras opciones que desea modificar. Para obtener más información acerca de cada opción, consulte Configuración de instancias de base de datos.

Example

El código siguiente modifica `mycustomdbinstance` al incluir la opción `--multi-az`. Los cambios se aplican durante el siguiente periodo de mantenimiento si se utiliza el parámetro `--no-apply-immediately`. Utilice `--apply-immediately` para aplicar los cambios inmediatamente. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mycustomdbinstance \
    --multi-az \
    --no-apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mycustomdbinstance ^
    --multi-az  \ ^
    --no-apply-immediately
```

API de RDS

Para convertirla en una implementación de instancia de base de datos multi-AZ con la API de RDS, llame a la operación ModifyDBInstance y defina el parámetro `MultiAZ` en true.

Coversión de una implementación multi-AZ de RDS Custom para SQL Server en una implementación single-AZ

Puede modificar una instancia de base de datos de RDS Custom para SQL Server existente para convertirla de una implementación multi-AZ en una implementación single-AZ.

Consola

Para modificar una instancia de base de datos de RDS Custom para SQL Server para convertirla de una implementación multi-AZ en una implementación single-AZ.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos).

   Aparece el panel Databases (Bases de datos).
3. Elija la instancia de base de datos de RDS Custom para SQL Server que desea modificar.
4. En Implementación multi-AZ, elija No.
5. Para aplicar los cambios de forma inmediata, seleccione la opción Aplicar inmediatamente en la página Confirmación. La elección de esta opción no provoca tiempo de inactividad, pero existe un posible impacto en el rendimiento. De forma alternativa, también puede aplicar la actualización durante la siguiente ventana de mantenimiento. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.
6. En la página Confirmación, elija Modificar la instancia de base de datos.

AWS CLI

Para convertir una implementación multi-AZ en una implementación single-AZ mediante la AWS CLI, llame al comando modify-db-instance e incluya la opción `--no-multi-az`. Especifique el identificador de instancias de base de datos y los valores de las otras opciones que desea modificar. Para obtener más información acerca de cada opción, consulte Configuración de instancias de base de datos.

Example

El código siguiente modifica `mycustomdbinstance` al incluir la opción `--no-multi-az`. Los cambios se aplican durante el siguiente periodo de mantenimiento si se utiliza el parámetro

`--no-apply-immediately`. Utilice `--apply-immediately` para aplicar los cambios inmediatamente. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mycustomdbinstance \
    --no-multi-az  \
    --no-apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier mycustomdbinstance ^
    --no-multi-az \ ^
    --no-apply-immediately
```

API de RDS

Para convertir una implementación Multi-AZ en una implementación single-AZ mediante la API de RDS, ejecute la operación ModifyDBInstance y defina el parámetro `MultiAZ` en `false`.

Proceso de conmutación por error para una implementación multi-AZ de RDS Custom para SQL Server

Si se produce una interrupción planeada o no planeada de la instancia de base de datos a causa de un defecto de la infraestructura, Amazon RDS cambia automáticamente a una réplica en espera de otra zona de disponibilidad si se ha activado Multi-AZ. El tiempo requerido para completar la conmutación por error dependerá de la actividad de la base de datos y de otras condiciones existentes en el momento en que la instancia de base de datos principal deja de estar disponible. Los tiempos de conmutación por error suelen estar entre los 60 y 120 segundos. Sin embargo, las transacciones grandes o un proceso de recuperación largo pueden aumentar el tiempo de conmutación por error. Cuando la conmutación por error se haya completado, puede hacer falta más tiempo para que la consola de RDS muestre la nueva zona de disponibilidad.

> **Note**
>
> Puede forzar una conmutación por error manualmente cuando reinicie una instancia de base de datos con conmutación por error. Para obtener información sobre cómo reiniciar una instancia de base de datos, consulte Reinicio de una instancia de base de datos.

Amazon RDS gestiona las conmutaciones por error automáticamente para que sea posible reanudar las operaciones de la base de datos lo antes posible sin intervención administrativa. La instancia de base de datos principal conmuta automáticamente a la réplica en espera si se da cualquiera de las condiciones descritas en la siguiente tabla. Puede ver los motivos de la conmutación por error en el registro de eventos de RDS.

Motivo de la conmutación por error	Descripción
`The operating system for the RDS Custom for SQL Server Multi-AZ DB instance is being patched in an offline operation`	Se ha desencadenado una conmutación por error durante la ventana de mantenimiento para un parche del sistema operativo o una actualización de seguridad. Para obtener más información, consulte Mantenimiento de una instancia de base de datos.
`The primary host of the RDS Custom for SQL Server Multi-AZ DB instance is unhealthy.`	La implementación de una instancia de base de datos Multi-AZ detectó una instancia de base de datos principal deteriorada y se produjo una conmutación por error.
`The primary host of the RDS Custom for SQL Server Multi-AZ DB instance is unreachable due to loss of network connectivity.`	El monitoreo de RDS detectó un error de accesibilidad de la red a la instancia de base de datos principal y desencadenó una conmutación por error.

Motivo de la conmutación por error	Descripción
`The RDS Custom for SQL Server Multi-AZ DB instance was modified by the customer.`	Una modificación de la instancia de base de datos ha activado una conmutación por error. Para obtener más información, consulte Modificación de una instancia de base de datos de RDS Custom for SQL Server.
`The storage volume of the primary host of the RDS Custom for SQL Server Multi-AZ DB instance experienced a failure.`	La implementación de una instancia de base de datos Multi-AZ detectó un problema de almacenamiento en la instancia de base de datos principal y se produjo una conmutación por error.
`The user requested a failover of the RDS Custom for SQL Server Multi-AZ DB instance.`	La instancia de base de datos multi-AZ de RDS Custom para SQL Server se reinició con conmutación por error. Para obtener más información, consulte Reinicio de una instancia de base de datos.
`The RDS Custom for SQL Server Multi-AZ primary DB instance is busy or unresponsive.`	La instancia de base de datos principal no responde. Le recomendamos que pruebe los siguientes pasos: • Examine los registros de eventos y de CloudWatch en busca de uso excesivo de CPU, memoria o espacio de intercambio. Para obtener más información, consulte Uso de notificaciones de eventos de Amazon RDS. • Cree una regla que se active en función de un evento de Amazon RDS. Para obtener más información, consulte Creación de una regla que se desencadena en función de un evento Amazon RDS. • Evalúe su carga de trabajo para determinar si está utilizando la clase de instancia de base de datos adecuada. Para obtener más información, consulte Clases de instancia de base de datos de .

Para determinar si se produjo una conmutación por error en la instancia de base de datos Multi-AZ, puede hacer lo siguiente:

- Configure suscripciones de eventos de base de datos para notificar por correo electrónico o por SMS que se ha iniciado una conmutación por error. Para obtener más información sobre los eventos, consulte Uso de notificaciones de eventos de Amazon RDS.
- Visualice sus eventos de base de datos mediante la consola de RDS o las operaciones de la API.
- Puede ver el estado actual de la implementación de una instancia de base de datos multi-AZ de RDS Custom para SQL Server mediante la consola de RDS, la CLI o las operaciones de la API.

Configuración de Time to Live (TTL) con aplicaciones que utilizan una implementación multi-AZ de RDS Custom para SQL Server

El mecanismo de conmutación por error cambia automáticamente el registro del Sistema de nombres de dominio (DNS) de la instancia de base de datos para que apunte a la instancia de base de datos en espera. Como consecuencia, necesita restablecer las conexiones existentes a la instancia de base de datos. Asegúrese de que cualquier valor de configuración de tiempo de vida (TTL) de la memoria caché de DNS sea bajo y compruebe que la aplicación no almacene el DNS en caché durante un periodo prolongado. Un valor de TTL alto puede impedir que la aplicación se vuelva a conectar rápidamente a la instancia de base de datos tras la conmutación por error.

Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS Custom for SQL Server

Al igual que Amazon RDS, RDS Custom crea y guarda copias de seguridad automáticas de la instancia de base de datos de RDS Custom for SQL Server cuando la retención de copias de seguridad está activada. También puede realizar una copia de seguridad de su instancia de base de datos manualmente. Las copias de seguridad automatizadas se componen de copias de seguridad de instantáneas y copias de seguridad del registro de transacciones. Las copias de seguridad de instantáneas se realizan para todo el volumen de almacenamiento de la instancia de base de datos durante el período de copia de seguridad especificado. Las copias de seguridad de los registros de transacciones de las bases de datos aptas para el PITR se realizan a intervalos regulares. RDS Custom guarda las copias de seguridad automatizadas de la instancia de base de datos en función del periodo de retención de copia de seguridad especificado. Puede utilizar copias de seguridad automatizadas para recuperar la instancia de base de datos en un momento determinado dentro del periodo de retención de las copias de seguridad.

También puede realizar copias de seguridad de instantáneas de forma manual. Puede crear una nueva instancia de base de datos a partir de estas copias de seguridad de instantáneas en cualquier momento. Para obtener más información acerca de la creación de una instantánea de base de datos de forma manual, consulte Creación de una instantánea de RDS Custom for SQL Server.

Si bien las copias de seguridad de instantáneas funcionan desde el punto de vista operativo como copias de seguridad completas, solo se le facturará el uso incremental del almacenamiento. La primera instantánea de una instancia de base de datos de RDS Custom contiene los datos de la instancia de base de datos completa. Las instantáneas posteriores de la misma base de datos son incrementales, lo que significa que solo se guardan los datos que han cambiado después de la última instantánea.

Temas

- Creación de una instantánea de RDS Custom for SQL Server
- Restauración desde una instantánea de base de datos de RDS Custom for SQL Server
- Restauración de una instancia de RDS Custom for SQL Server a un momento dado
- Eliminación de una instantánea de RDS Custom for SQL Server
- Eliminación de copias de seguridad automatizadas de RDS Custom for SQL Server

Creación de una instantánea de RDS Custom for SQL Server

RDS Custom for SQL Server crea una instantánea del volumen de almacenamiento de la instancia de base de datos, al crear una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. Cuando cree una instantánea, especifique de qué instancia de base de datos de RDS Custom for SQL Server desea crear copia de seguridad. Asigne un nombre a la instantánea para poder restaurar desde esta más adelante.

Cuando crea una instantánea, RDS Custom for SQL Server crea una instantánea de Amazon EBS para el volumen `(D:)`, que es el volumen de base de datos asociado a la instancia de base de datos. Para que las instantáneas sean fáciles de asociar a una instancia de base de datos específica, se etiquetan con `DBSnapshotIdentifier`, `DbiResourceId` y `VolumeType`.

La creación de una instantánea de base de datos da como resultado una breve suspensión de E/S. Esta suspensión puede durar desde unos segundos hasta unos minutos, según el tamaño y la clase de la instancia de base de datos. El tiempo de creación de instantáneas varía según el número total y el tamaño de las base de datos. Para obtener más información sobre la cantidad de bases de datos aptas para una operación de restauración puntual (PITR), consulte Número de bases de datos aptas para el PITR por tipo de clase de instancia.

Debido a que la instantánea incluye todo el volumen de almacenamiento, el tamaño de los archivos (como los archivos temporales) también afecta el tiempo de creación de la instantánea. Para obtener más información acerca de la creación de segmentos, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Crear una instantánea de RDS Custom for SQL Server mediante la consola o la AWS CLI.

Consola

Para crear una instantánea de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. En la lista de instancias de base de datos de RDS Custom, seleccione la instancia para la que desea tomar una instantánea.
4. En Actions (Acciones), elija Take snapshot (Realizar instantánea).

   Aparece la ventana Take DB Snapshot (Realizar una instantánea de base de datos).

5. En Snapshot name (Nombre de la instantánea), ingrese el nombre de la instantánea.
6. Elija Take Snapshot (Realizar una instantánea).

AWS CLI

Puede crear una instantánea de una instancia de base de datos de RDS Custom mediante el comando AWS CLI create-db-snapshot.

Especifique las opciones siguientes:

- `--db-instance-identifier` – Identifica la instancia de base de datos de RDS Custom de la que va a realizar una copia de seguridad
- `--db-snapshot-identifier` – Nombra su instantánea de RDS Custom para que pueda restaurarla más tarde

En este ejemplo, crea una instantánea de base de datos llamada *`my-custom-snapshot`* para una instancia de base de datos de RDS Custom llamada *`my-custom-instance`*.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-snapshot \
    --db-instance-identifier my-custom-instance \
    --db-snapshot-identifier my-custom-snapshot
```

En:Windows

```
aws rds create-db-snapshot ^
    --db-instance-identifier my-custom-instance ^
    --db-snapshot-identifier my-custom-snapshot
```

Restauración desde una instantánea de base de datos de RDS Custom for SQL Server

Al restaurar una instancia de base de datos de RDS Custom for SQL Server, debe indicar el nombre de la instantánea de base de datos y un nombre para la nueva instancia. No es posible restaurar desde una instantánea a una instancia de base de datos RDS Custom existente. Al realizar la restauración se crea una nueva instancia de base de datos de RDS Custom for SQL Server

La restauración a partir de una instantánea restaurará el volumen de almacenamiento al momento en el que se tomó la instantánea. Esto incluirá todas las bases de datos y cualquier otro archivo que estuviera presente en el volumen `(D:)`.

Consola

Restaure una instancia de base de datos de RDS Custom a partir de una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de base de datos desde la que desea restaurar.
4. En Actions (Acciones), elija Restore snapshot (Restaurar instantánea).
5. En la página Restore DB instance (Restaurar instancia de base de datos), en DB instance identifier (Identificador de instancias de bases de datos), ingrese el nombre de su instancia de base de datos de RDS Custom restaurada.
6. Elija Restore DB Instance (Restaurar instancia de base de datos).

AWS CLI

Restaure una instantánea de base de datos de RDS Custom mediante el comando AWS CLI restore-db-instance-from-db-snapshot.

Si la instantánea desde la que va a restaurar es para una instancia de base de datos privada, asegúrese de especificar el `db-subnet-group-name` y el `no-publicly-accessible` correctos. De lo contrario, la instancia de base de datos pasa a ser de acceso público de manera predeterminada. Se requieren las siguientes opciones:

- `db-snapshot-identifier` – Identifica la instantánea desde la que se va a restaurar
- `db-instance-identifier` – Especifica el nombre de la instancia de base de datos de RDS Custom que se debe crear a partir de la instantánea de base de datos
- `custom-iam-instance-profile` – Especifica el perfil de instancia asociado a la instancia Amazon EC2 subyacente de una instancia de base de datos personalizada de RDS.

El siguiente código restaura la instantánea denominada `my-custom-snapshot` para `my-custom-instance`.

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-instance-from-db-snapshot \
  --db-snapshot-identifier my-custom-snapshot \
  --db-instance-identifier my-custom-instance \
  --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
  --no-publicly-accessible
```

En:Windows

```
aws rds restore-db-instance-from-db-snapshot ^
  --db-snapshot-identifier my-custom-snapshot ^
  --db-instance-identifier my-custom-instance ^
  --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
  --no-publicly-accessible
```

Restauración de una instancia de RDS Custom for SQL Server a un momento dado

Al crear una nueva instancia de base de datos puede restaurar una instancia de base de datos a un momento dado (PITR). Para admitir PITR, las instancias de base de datos deben tener una retención de copia de seguridad habilitada.

El último momento que se puede restaurar para una instancia de base de datos de RDS Custom for SQL Server depende de varios factores, pero normalmente se sitúa en los cinco minutos previos a la hora actual. Para ver el último momento que se puede restaurar para una instancia de base de datos, use el comando describe-db-instances de la AWS CLI y compruebe el valor que se devuelve en el campo `LatestRestorableTime` para la instancia de base de datos. Para consultar la hora restaurable más reciente para cada instancia de base de datos en la consola de Amazon RDS, elija Copias de seguridad automatizadas.

Puede restaurar a cualquier punto en el tiempo dentro del periodo de retención de copia de seguridad. Para consultar la hora restaurable más reciente para cada instancia de base de datos, elija Copias de seguridad automatizadas en la consola de Amazon RDS.

Para obtener información general sobre PITR, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Temas

- Consideraciones de PITR para RDS Custom for SQL Server
- Número de bases de datos aptas para el PITR por tipo de clase de instancia
- Hacer que las bases de datos no sean elegibles para PITR
- Registros de transacciones en Amazon S3
- Restauración de PITR mediante la AWS Management Console, la AWS CLI, o la API de RDS.

Consideraciones de PITR para RDS Custom for SQL Server

En RDS Custom for SQL Server, PITR difiere de las siguientes formas importantes de PITR en Amazon RDS:

- PITR solo restaura las bases de datos de la instancia de base de datos. No restaura el sistema operativo ni los archivos de la unidad C:.
- Para una instancia de base de datos de RDS Custom for SQL Server, una base de datos se respalda automáticamente y es elegible para PITR solo bajo las siguientes condiciones:
  - La base de datos está en línea.
  - El modelo de recuperación está configurado en FULL.
  - Se puede escribir.
  - Tiene sus archivos físicos en la unidad D:.
  - No se muestra en la tabla `rds_pitr_blocked_databases`. Para obtener más información, consulte Hacer que las bases de datos no sean elegibles para PITR.
- Las bases de datos aptas para PITR se determinan según el orden de su ID de base de datos. RDS Custom for SQL Server permite hasta 5000 bases de datos por instancia de base de datos. Sin embargo, el número máximo de bases de datos restauradas mediante una operación PITR para una instancia de base de datos de RDS Custom for SQL Server depende del tipo de clase de instancia. Para obtener más información, consulte Número de bases de datos aptas para el PITR por tipo de clase de instancia.

  Otras bases de datos que no forman parte de PITR se pueden restaurar a partir de instantáneas de base de datos, incluidas las copias de seguridad de instantáneas automatizadas utilizadas para PITR.
- Al agregar una nueva base de datos apta para PITR, cambiarle el nombre o restaurarla, se inicia una instantánea de la instancia de base de datos.
- La cantidad máxima de bases de datos aptas para el PITR cambia cuando la instancia de base de datos se somete a una operación de cálculo a escala, según el tipo de clase de instancia de

destino. Si la instancia se escala verticalmente, lo que permite que más bases de datos de la instancia sean aptas para la PITR, se toma una nueva instantánea.

- Las bases de datos restauradas tienen el mismo nombre que en la instancia de base de datos de origen. No puede especificar un nombre diferente.
- `AWSRDSCustomSQLServerIamRolePolicy` requiere acceso a otros servicios de AWS. Para obtener más información, consulte Agregar una política de acceso a AWSRDSCustomSQLServerInstanceRole.
- Los cambios de zona horaria no son compatibles con RDS Custom for SQL Server. Si cambia el sistema operativo o la zona horaria de la instancia de base de datos, PITR (y otra automatización) no funciona.

Número de bases de datos aptas para el PITR por tipo de clase de instancia

En la siguiente tabla se muestra el número máximo de bases de datos aptas para PITR en función del tipo de clase de instancia.

Tipo de clase de instancia	Número máximo de bases de datos aptas para PITR
db.*.large	100
db.*.xlarge a db.*.2xlarge	150
db.*.4xlarge a db.*.8xlarge	300
db.*.12xlarge a db.*.16xlarge	600
db.*.24xlarge, db.*32xlarge	1 000

* Representa los diferentes tipos de clase de instancia.

El número máximo de bases de datos aptas para PITR en una instancia de base de datos depende del tipo de clase de instancia. El número oscila entre 100 en los más pequeños y 1000 en los tipos de clase de instancia más grandes compatibles con RDS Custom for SQL Server. Las bases de datos de sistema de servidor SQL (`master, model, msdb, tempdb`) no se incluyen en este límite. Cuando una instancia de base de datos se escala o desescala verticalmente, según el tipo de clase de instancia de destino, RDS Custom actualizará automáticamente el número de bases de datos aptas para PITR. RDS Custom for SQL Server enviará `RDS-EVENT-0352` cuando cambie el número máximo de bases de datos aptas para PITR en una instancia de base de datos. Para obtener más información, consulte Eventos de versiones del motor personalizadas.

> **Note**
>
> La compatibilidad con PITR para más de 100 bases de datos solo está disponible en las instancias de base de datos creadas después del 26 de agosto de 2023. Para las instancias creadas antes del 26 de agosto de 2023, la cantidad máxima de bases de datos aptas para PITR es de 100, independientemente de la clase de instancia. Para habilitar la compatibilidad con PITR en más de 100 bases de datos en instancias de bases de datos creadas antes del 26 de agosto de 2023, puede realizar la siguiente acción:
>
> - Actualizar la versión del motor de base de datos a la 15.00.4322.2.v1 o posterior

Durante una operación de PITR, RDS Custom restaurará todas las bases de datos que formaban parte del PITR en la instancia de base de datos de origen en el momento de la restauración. Una vez que la instancia de base de datos de destino haya completado las operaciones de restauración, si la retención de copias de seguridad está habilitada, la instancia de base de datos empezará a realizar copias de seguridad en función del número máximo de bases de datos aptas para PITR en la instancia de base de datos de destino.

Por ejemplo, si su instancia de base de datos se ejecuta en una `db.*.xlarge` que tenga 200 bases de datos:

1. RDS Custom for SQL Server seleccionará las primeras 150 bases de datos, ordenadas por su ID de base de datos, para la copia de seguridad de PITR.
2. Modifique la instancia para escalarla verticalmente hasta db.*.4xlarge.

3. Una vez completada la operación de computación de escalado, RDS Custom for SQL Server seleccionará las primeras 300 bases de datos, ordenadas por su ID de base de datos, para la copia de seguridad de PITR. Cada una de las 200 bases de datos que cumpla los requisitos del PITR ahora podrá optar al PITR.
4. Ahora puede modificar la instancia para reducirla verticalmente a db.*.xlarge.
5. Una vez completada la operación de computación de escalado, RDS Custom for SQL Server seleccionará de nuevo las primeras 150 bases de datos, ordenadas por su ID de base de datos, para la copia de seguridad de PITR.

Hacer que las bases de datos no sean elegibles para PITR

Puede optar por excluir las bases de datos individuales del PITR. Para esto, ponga sus valores de `database_id` en una tabla de `rds_pitr_blocked_databases`. Utilice el siguiente script SQL para crear la tabla.

Para crear la tabla rds_pitr_blocked_databases

- Ejecute el siguiente script de SQL.

```
create table msdb..rds_pitr_blocked_databases
(
database_id INT NOT NULL,
database_name SYSNAME NOT NULL,
db_entry_updated_date datetime NOT NULL DEFAULT GETDATE(),
db_entry_updated_by SYSNAME NOT NULL DEFAULT CURRENT_USER,
PRIMARY KEY (database_id)
);
```

Para obtener la lista de bases de datos elegibles y no elegibles, consulte el archivo `RI.End` en el directorio `RDSCustomForSQLServer/Instances/`*`DB_instance_resource_ID`*`/TransactionLogMetadata` del bucket de Amazon S3 `do-not-delete-rds-custom-`*`$ACCOUNT_ID`*`-`*`$REGION`*`-`*`unique_identifier`*. Para obtener más información acerca del archivo `RI.End`, consulte Registros de transacciones en Amazon S3.

También puede determinar la lista de bases de datos aptas para PITR mediante el siguiente script SQL. Establezca la variable `@limit` en el número máximo de bases de datos aptas para PITR para la clase de instancia. Para obtener más información, consulte Número de bases de datos aptas para el PITR por tipo de clase de instancia.

Para determinar la lista de bases de datos aptas para PITR en una clase de instancia de base de datos

- Ejecute el siguiente script de SQL.

```
DECLARE @Limit INT;
SET @Limit = (insert-database-instance-limit-here);

USE msdb;
IF (EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA = 'dbo' AND
 TABLE_NAME = 'rds_pitr_blocked_databases'))
    WITH TABLE0 AS (
        SELECT hdrs.database_id as DatabaseId, sdb.name as DatabaseName,
 'ALWAYS_ON_NOT_WRITABLE_REPLICA' as Reason, NULL as DatabaseNameOnPitrTable
        FROM sys.dm_hadr_database_replica_states hdrs
        INNER JOIN sys.databases sdb ON sdb.database_id = hdrs.database_id
        WHERE (hdrs.is_local = 1 AND hdrs.is_primary_replica = 0)
        OR (sys.fn_hadr_is_primary_replica (sdb.name) = 1 AND DATABASEPROPERTYEX
 (sdb.name, 'Updateability') = 'READ_ONLY')
    ),
    TABLE1 as (
            SELECT dbs.database_id as DatabaseId, sysdbs.name as DatabaseName,
 'OPTOUT' as Reason,
            CASE WHEN dbs.database_name = sysdbs.name THEN NULL ELSE
 dbs.database_name END AS DatabaseNameOnPitrTable
            FROM msdb.dbo.rds_pitr_blocked_databases dbs
            INNER JOIN sys.databases sysdbs ON dbs.database_id = sysdbs.database_id
            WHERE sysdbs.database_id > 4
            ),
    TABLE2 as (
            SELECT
            db.name AS DatabaseName,
            db.create_date AS CreateDate,
            db.state_desc AS DatabaseState,
            db.database_id AS DatabaseId,
            rs.database_guid AS DatabaseGuid,
            rs.last_log_backup_lsn AS LastLogBackupLSN,
            rs.recovery_fork_guid RecoveryForkGuid,
            rs.first_recovery_fork_guid AS FirstRecoveryForkGuid,
            db.recovery_model_desc AS RecoveryModel,
            db.is_auto_close_on AS IsAutoClose,
            db.is_read_only as IsReadOnly,
            NEWID() as FileName,
```

```
            CASE WHEN(db.state_desc = 'ONLINE'
                    AND db.recovery_model_desc != 'SIMPLE'
                    AND((db.is_auto_close_on = 0 and db.collation_name IS NOT NULL)
 OR db.is_auto_close_on = 1))
                    AND db.is_read_only != 1
                    AND db.user_access = 0
                    AND db.source_database_id IS NULL
                    AND db.is_in_standby != 1
                    THEN 1 ELSE 0 END AS IsPartOfSnapshot,
            CASE WHEN db.source_database_id IS NULL THEN 0 ELSE 1 END AS
 IsDatabaseSnapshot
            FROM sys.databases db
            INNER JOIN sys.database_recovery_status rs
            ON db.database_id = rs.database_id
            WHERE DB_NAME(db.database_id) NOT IN('tempdb') AND
            db.database_id NOT IN (SELECT DISTINCT DatabaseId FROM TABLE1) AND
            db.database_id NOT IN (SELECT DISTINCT DatabaseId FROM TABLE0)
        ),
        TABLE3 as(
            Select @Limit+count(DatabaseName) as TotalNumberOfDatabases from TABLE2
 where TABLE2.IsPartOfSnapshot=1 and DatabaseName in ('master','model','msdb')
        )
        SELECT TOP(SELECT TotalNumberOfDatabases from TABLE3)
 DatabaseName,CreateDate,DatabaseState,DatabaseId from TABLE2 where
 TABLE2.IsPartOfSnapshot=1
        ORDER BY TABLE2.DatabaseID ASC
ELSE
    WITH TABLE0 AS (
        SELECT hdrs.database_id as DatabaseId, sdb.name as DatabaseName,
 'ALWAYS_ON_NOT_WRITABLE_REPLICA' as Reason, NULL as DatabaseNameOnPitrTable
        FROM sys.dm_hadr_database_replica_states hdrs
        INNER JOIN sys.databases sdb ON sdb.database_id = hdrs.database_id
        WHERE (hdrs.is_local = 1 AND hdrs.is_primary_replica = 0)
        OR (sys.fn_hadr_is_primary_replica (sdb.name) = 1 AND DATABASEPROPERTYEX
 (sdb.name, 'Updateability') = 'READ_ONLY')
    ),
    TABLE1 as (
            SELECT
            db.name AS DatabaseName,
            db.create_date AS CreateDate,
            db.state_desc AS DatabaseState,
            db.database_id AS DatabaseId,
            rs.database_guid AS DatabaseGuid,
            rs.last_log_backup_lsn AS LastLogBackupLSN,
```

```
            rs.recovery_fork_guid RecoveryForkGuid,
            rs.first_recovery_fork_guid AS FirstRecoveryForkGuid,
            db.recovery_model_desc AS RecoveryModel,
            db.is_auto_close_on AS IsAutoClose,
            db.is_read_only as IsReadOnly,
            NEWID() as FileName,
            CASE WHEN(db.state_desc = 'ONLINE'
                    AND db.recovery_model_desc != 'SIMPLE'
                    AND((db.is_auto_close_on = 0 and db.collation_name IS NOT NULL)
OR db.is_auto_close_on = 1))
                    AND db.is_read_only != 1
                    AND db.user_access = 0
                    AND db.source_database_id IS NULL
                    AND db.is_in_standby != 1
                    THEN 1 ELSE 0 END AS IsPartOfSnapshot,
            CASE WHEN db.source_database_id IS NULL THEN 0 ELSE 1 END AS
IsDatabaseSnapshot
            FROM sys.databases db
            INNER JOIN sys.database_recovery_status rs
            ON db.database_id = rs.database_id
            WHERE DB_NAME(db.database_id) NOT IN('tempdb') AND
            db.database_id NOT IN (SELECT DISTINCT DatabaseId FROM TABLE0)
        ),
        TABLE2 as(
            SELECT @Limit+count(DatabaseName) as TotalNumberOfDatabases from TABLE1
where TABLE1.IsPartOfSnapshot=1 and DatabaseName in ('master','model','msdb')
        )
        select top(select TotalNumberOfDatabases from TABLE2)
DatabaseName,CreateDate,DatabaseState,DatabaseId from TABLE1 where
TABLE1.IsPartOfSnapshot=1
        ORDER BY TABLE1.DatabaseID ASC
```

> **Note**
>
> Las bases de datos que son únicamente enlaces simbólicos también se excluyen de las bases de datos aptas para las operaciones de PITR. La consulta anterior no filtra en función de este criterio.

Registros de transacciones en Amazon S3

El periodo de retención de copia de seguridad determina si los registros de transacciones para las instancias de base de datos de RDS Custom for SQL Server se extraen y cargan automáticamente en Amazon S3. Un valor distinto de cero significa que se crean copias de seguridad automáticas y que el agente personalizado de RDS carga los registros de transacciones en S3 cada 5 minutos.

Los archivos de registro de transacciones en S3 se cifran en reposo mediante el AWS KMS key que proporcionó cuando creó su instancia de base de datos. Para obtener más información, consulte Protección de los datos con el cifrado del servidor en la Guía del usuario de Amazon Simple Storage Service.

Los registros de transacciones de cada base de datos se cargan en un bucket de S3 denominado `do-not-delete-rds-custom-`*`$ACCOUNT_ID`*`-`*`$REGION`*`-`*`unique_identifier`*. El directorio `RDSCustomForSQLServer/Instances/`*`DB_instance_resource_ID`* del bucket de S3 contiene dos subdirectorios:

- `TransactionLogs` – Contiene los registros de transacciones de cada base de datos y sus respectivos metadatos.

  El nombre del archivo de registro de transacciones sigue el patrón *`yyyyMMddHHmm`*`.`*`database_id`*`.`*`timestamp`*, por ejemplo:

  ```
  202110202230.11.1634769287
  ```

  El mismo nombre de archivo con el sufijo `_metadata` contiene información sobre el registro de transacciones, como números de secuencia de registros, nombre de base de datos y `RdsChunkCount`. `RdsChunkCount` determina cuántos archivos físicos representan un único archivo de registro de transacciones. Es posible que veas archivos con sufijos `_0001`, `_0002`, etc., lo que significa los fragmentos físicos de un archivo de registro de transacciones. Si quieres utilizar un archivo de registro de transacciones fragmentado, asegúrate de fusionar los fragmentos después de descargarlos.

  Considere un escenario en el que tenga los siguientes archivos:

  - `202110202230.11.1634769287`
  - `202110202230.11.1634769287_0001`
  - `202110202230.11.1634769287_0002`
  - `202110202230.11.1634769287_metadata`

El valor de `RdsChunkCount` es `3`. El orden de fusión de los archivos es el siguiente: `202110202230.11.1634769287`, `202110202230.11.1634769287_0001` y `202110202230.11.1634769287_0002`.

- `TransactionLogMetadata` – Contiene información de metadatos sobre cada iteración de la extracción del registro de transacciones.

  El archivo `RI.End` contiene información de todas las bases de datos de las que se extrajeron los registros de transacciones y de todas las bases de datos que existen, pero no se extrajeron los registros de transacciones. El nombre de archivo `RI.End` sigue el patrón *`yyyyMMddHHmm`*`.RI.End.`*`timestamp`*, por ejemplo:

  ```
  202110202230.RI.End.1634769281
  ```

Restauración de PITR mediante la AWS Management Console, la AWS CLI, o la API de RDS.

Puede restaurar una instancia de base de datos de RDS Custom for SQL Server a un momento dado mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para restaurar una instancia de base de datos de RDS Custom a un tiempo especificado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Copias de seguridad automáticas.
3. Elija la instancia de base de datos personalizada de RDS que desea restaurar.
4. Para Actions (Acciones), elija Restore to point in time (Restaurar a un momento dado).

   Aparecerá la ventana Restore to point in time (Restaurar a un momento dado).
5. Elija Latest restorable time (Última hora de restauración) para restaurar a la última hora posible o elija Custom (Personalizar) para elegir una hora.

   Si elige Personalizar, ingrese la fecha y la hora a la que desea restaurar la instancia.

   Las horas se muestran en su zona horaria local, que se indica mediante una diferencia de la hora universal coordinada (UTC). Por ejemplo, UTC-5 es la hora estándar del Este/horario de verano central.

6. Para el identificador de instancias de bases de datos, ingrese el nombre de la instancia de base de datos de RDS Custom restaurada de destino. El nombre debe ser único.
7. Elija otras opciones según sea necesario, como la clase de instancia de base de datos.
8. Elija Restore to point in time (Restaurar a un momento dado).

AWS CLI

Puede restaurar una instancia de base de datos a un momento dado mediante el comando restore-db-instance-to-point-in-time AWS CLI para crear una nueva instancia de base de datos de RDS Custom.

Utilice una de las siguientes opciones para especificar la copia de seguridad desde la que restaurar:

- `--source-db-instance-identifier` *`mysourcedbinstance`*
- `--source-dbi-resource-id` *`dbinstanceresourceID`*
- `--source-db-instance-automated-backups-arn` *`backupARN`*

La opción `custom-iam-instance-profile` es obligatoria.

En el siguiente ejemplo se restaura `my-custom-db-instance` a una nueva instancia de base de datos denominada `my-restored-custom-db-instance`, en la hora especificada.

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-instance-to-point-in-time \
    --source-db-instance-identifier my-custom-db-instance\
    --target-db-instance-identifier my-restored-custom-db-instance \
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance \
    --restore-time 2022-10-14T23:45:00.000Z
```

En:Windows

```
aws rds restore-db-instance-to-point-in-time ^
    --source-db-instance-identifier my-custom-db-instance ^
    --target-db-instance-identifier my-restored-custom-db-instance ^
    --custom-iam-instance-profile AWSRDSCustomInstanceProfileForRdsCustomInstance ^
    --restore-time 2022-10-14T23:45:00.000Z
```

Eliminación de una instantánea de RDS Custom for SQL Server

Puede eliminar instantáneas de base de datos administradas por RDS Custom for SQL Server cuando ya no las necesite. El procedimiento de eliminación es el mismo para las instancias de base de datos de Amazon RDS y RDS Custom.

Las instantáneas de Amazon EBS de los volúmenes binario y raíz permanecen en su cuenta durante más tiempo porque podrían estar vinculadas a algunas instancias que se ejecutan en su cuenta o a otras instantáneas de RDS Custom for SQL Server. Estas instantáneas de EBS se eliminan automáticamente después de que ya no están relacionadas con los recursos de RDS Custom for SQL Server existentes (instancias de base de datos o copias de seguridad).

Consola

Para eliminar una instantánea de una instancia de base de datos de RDS Custom

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de base de datos que desee eliminar.
4. En Actions (Acciones), elija Delete Snapshot (Eliminar instantánea).
5. En la página de confirmación, elija Delete (Eliminar).

AWS CLI

Para eliminar una instantánea de RDS Custom, utilice el comando AWS CLI delete-db-snapshot.

Se requiere la siguiente opción:

- `--db-snapshot-identifier` – La instantánea que se va a eliminar

El siguiente ejemplo elimina la instantánea de base de datos `my-custom-snapshot`.

Example

Para Linux, macOS o:Unix

```
aws rds delete-db-snapshot \
```

```
  --db-snapshot-identifier my-custom-snapshot
```

En:Windows

```
aws rds delete-db-snapshot ^
  --db-snapshot-identifier my-custom-snapshot
```

Eliminación de copias de seguridad automatizadas de RDS Custom for SQL Server

Puede eliminar las copias de seguridad automáticas retendas para RDS Custom for SQL Server cuando ya no sean necesarias. El procedimiento es el mismo que el procedimiento para eliminar las copias de seguridad de Amazon RDS.

Consola

Para eliminar una copia de seguridad automatizada retenida

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Automated backups (Copias de seguridad automatizadas).
3. Elija Retained (Retenidas).
4. Elija la copia de seguridad automatizada retenida que desea eliminar.
5. En Actions (Acciones), elija Delete (Eliminar).
6. En la página de confirmación, ingrese **`delete me`** y elija Delete (Eliminar).

AWS CLI

Puede eliminar una copia de seguridad automatizada retenida utilizando el comando de la AWS CLI delete-db-instance-automated-backup.

La siguiente opción se utiliza para eliminar una copia de seguridad automática retenida:

- `--dbi-resource-id` – El identificador de recurso para la instancia de base de datos de RDS Custom de origen.

  Puede encontrar el identificador de recursos para la instancia de base de datos de origen de una copia de seguridad automatizada retenida mediante el comando AWS CLI describe-db-instance-automated-backups.

El siguiente ejemplo elimina la copia de seguridad automatizada retenida con el identificador de recursos de la instancia de base de datos `custom-db-123ABCEXAMPLE`.

Example

Para Linux, macOS o:Unix

```
aws rds delete-db-instance-automated-backup \
    --dbi-resource-id custom-db-123ABCEXAMPLE
```

En:Windows

```
aws rds delete-db-instance-automated-backup ^
    --dbi-resource-id custom-db-123ABCEXAMPLE
```

Copia de una instantánea de base de datos de Amazon RDS Custom para SQL Server

Con RDS Custom para SQL Server, puede realizar copias de seguridad automatizadas e instantáneas de bases de datos manuales. Después de copiar una instantánea, la copia será una instantánea manual. Puede realizar varias copias de una copia de seguridad automatizada o instantánea manual, pero cada copia debe tener un identificador único.

Solo puede copiar una instantánea en la misma cuenta de AWS en Regiones de AWS en las que RDS Custom para SQL Server esté disponible. Actualmente, las siguientes operaciones no están disponibles:

- Copiar instantáneas de bases de datos dentro de la misma Región de AWS.
- Copiar instantáneas de bases de datos entre cuentas de AWS.

RDS Custom para SQL Server admite la copia incremental de instantáneas. Para obtener más información, consulte Aspectos a tener en cuenta sobre la copia de instantáneas incrementales.

Temas

- Limitaciones
- Tratamiento del cifrado
- Copias entre regiones
- Instantáneas de instancias de base de datos creadas con versiones de motor personalizadas (CEV)
- Concesión de los permisos necesarios a la entidad principal de IAM
- Copia de una instantánea de base de datos

Limitaciones

Las siguientes limitaciones se aplican a la copia de una instantánea de base de datos para RDS Custom para SQL Server:

- Si elimina una instantánea de origen antes de que la instantánea de destino esté disponible, la copia de la instantánea podría generar un error. Compruebe que la instantánea de destino tenga el estado `AVAILABLE` antes de eliminar la instantánea de origen.

- No puede especificar un nombre de grupo de opciones ni copiar un grupo de opciones en su solicitud de copia de instantánea de base de datos.
- Si elimina algún recurso de AWS dependiente de la instantánea de base de datos de origen antes del proceso de copia o durante este, la solicitud de copia de la instantánea podría fallar de forma asíncrona.
  - Si elimina el archivo de copia de seguridad de clave maestra de servicio (SMK) de la instancia de base de datos de origen almacenada en el bucket de S3 administrado por RDS Custom en su cuenta, la copia de la instantánea de base de datos se realizará correctamente de forma asíncrona. Sin embargo, las características de SQL Server que dependen de la SMK, como las bases de datos compatibles con TDE, tendrán problemas. Para obtener más información, consulte Resolución del problema PENDING_RECOVERY en bases de datos habilitadas para TDE en RDS Custom para SQL Server.
- Actualmente, no se admite la copia de instantáneas de bases de datos dentro de la misma Región de AWS.
- Actualmente, no se admite la copia de instantáneas de bases de datos entre cuentas de AWS.

Las limitaciones de copia de una instantánea de base de datos para Amazon RDS también se aplican a RDS Custom para SQL Server. Para obtener más información, consulte Limitaciones.

Tratamiento del cifrado

Todas las instancias de base de datos de RDS Custom para SQL Server se cifran con claves de KMS. Solo puede copiar una instantánea cifrada en una instantánea cifrada, por lo que debe especificar una clave de KMS valida en la Región de AWS de destino de la solicitud de copia de instantánea de base de datos.

La instantánea de origen permanece cifrada durante todo el proceso de copia. Amazon RDS utiliza el cifrado de sobre para proteger los datos durante la operación de copia con la clave de KMS de la Región de AWS de destino especificada. Para obtener más información, consulte Cifrado de sobre en la Guía para desarrolladores de AWS Key Management Service.

Copias entre regiones

Puede copiar instantáneas de base de datos en Regiones de AWS. Sin embargo, existen ciertas restricciones y consideraciones para la copia de instantáneas entre regiones.

Autorización de RDS para comunicarse entre Regiones de AWS para la copia de instantáneas

Cuando una solicitud de copia de instantánea de base de datos entre regiones se procesa correctamente, RDS inicia la copia. Se crea una solicitud de autorización para que RDS acceda a la instantánea de origen. Esta solicitud de autorización vincula la instantánea de base de datos de origen a la instantánea de base de datos de destino. Esto permite que RDS realice la copia solo en la instantánea de destino especificada.

RDS verifica la autorización mediante el permiso `rds:CrossRegionCommunication` en el rol de IAM vinculado al servicio. Si la copia está autorizada, RDS se comunica con la región de origen y completa la copia.

RDS no tiene acceso a instantáneas de base de datos que no estaban autorizadas previamente por una solicitud CopyDBSnapshot. La autorización se revoca cuando se completa la copia.

RDS utiliza el rol vinculado a servicios para verificar la autorización en la región de origen. La copia falla si elimina el rol vinculado al servicio durante el proceso de copia.

Para obtener más información, consulte Creación de un rol vinculado al servicio en la Guía del usuario de AWS Identity and Access Management.

Uso de credenciales de AWS Security Token Service

Los tokens de sesión del punto de conexión global de AWS Security Token Service (AWS STS) son válidos únicamente en Regiones de AWS que están habilitadas de forma predeterminada (regiones comerciales). Si utiliza credenciales de la operación de la API `assumeRole` en AWS STS, utilice el punto de conexión regional si la región de origen es una región registrada. De lo contrario, la solicitud devuelve un error. Las credenciales deben ser válidas en ambas regiones, pero, en el caso de las regiones registradas, solo cuando utiliza el punto de conexión regional de AWS STS.

Para utilizar el punto de conexión global, asegúrese de que está habilitado para operaciones en ambas regiones. Establezca el punto de conexión global en `Valid` en todas las Regiones de AWS en la configuración de la cuenta de AWS STS.

Para obtener más información, consulte Administración de AWS STS en una Región de AWS en la Guía del usuario de AWS Identity and Access Management.

Instantáneas de instancias de base de datos creadas con versiones de motor personalizadas (CEV)

En el caso de una instantánea de base de datos de una instancia de base de datos que utilice una versión de motor personalizada (CEV), RDS asocia la CEV a la instantánea de base de datos. Para copiar una instantánea de base de datos de origen asociada a una CEV entre Regiones de AWS, RDS copia la CEV junto con la instantánea de base de datos de origen en la región de destino.

Si va a copiar varias instantáneas de base de datos asociadas a la misma CEV en la misma región de destino, la primera solicitud de copia realiza la copia de la CEV asociada. El proceso de copia de las siguientes solicitudes busca la CEV copiada inicialmente y la asocia a las siguientes copias de instantáneas de base de datos. La copia de la CEV existente debe tener el estado `AVAILABLE` para que se pueda asociar a las copias de instantáneas de base de datos.

Para copiar una instantánea de base de datos asociada a una CEV, la política de IAM del solicitante debe tener los permisos necesarios para autorizar tanto la copia de la instantánea de base de datos como la copia de la CEV asociada. La política de IAM del solicitante requiere los siguientes permisos para permitir la copia de la CEV asociada:

- `rds:CopyCustomDBEngineVersion`: la entidad principal de IAM del solicitante debe tener permiso para copiar la CEV de origen en la región de destino junto con la instantánea de base de datos de origen. Si la entidad principal de IAM del solicitante no está autorizada a copiar la CEV de origen, la solicitud de copia de la instantánea fallará debido a errores de autorización.
- `ec2:CreateTags`: la AMI de EC2 subyacente de la CEV de origen se copia en la región de destino como parte de la copia de la CEV. RDS Custom intenta etiquetar la AMI con la etiqueta `AWSRDSCustom` antes de copiarla. Asegúrese de que la entidad principal de IAM del solicitante tenga el permiso necesario para crear la etiqueta con respecto a la AMI subyacente a la CEV de origen en la región de origen.

Para obtener más información sobre los permisos de copia de CEV, consulte Concesión de los permisos necesarios a la entidad principal de IAM.

Concesión de los permisos necesarios a la entidad principal de IAM

Debe tener el acceso necesario para copiar una instantánea de base de datos de RDS Custom para SQL Server. El usuario o rol de IAM (denominado entidad principal de IAM) para copiar una instantánea de base de datos mediante la consola o la CLI debe tener una de las siguientes políticas para crear correctamente la instancia de base de datos:

- La política `AdministratorAccess` o
- La política `AmazonRDSFullAccess` con los siguientes permisos adicionales:

```
s3:CreateBucket
s3:GetBucketPolicy
s3:PutBucketPolicy
kms:CreateGrant
kms:DescribeKey
ec2:CreateTags
```

RDS Custom utiliza estos permisos durante la copia de instantáneas entre Regiones de AWS. Estos permisos configuran los recursos de su cuenta que son necesarios para las operaciones de RDS Custom. Para obtener más información acerca del permiso de `kms:CreateGrant`, consulte Administración de AWS KMS key.

La siguiente política de JSON de muestra otorga los permisos necesarios además de la política `AmazonRDSFullAccess`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateS3BucketAndReadWriteBucketPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::do-not-delete-rds-custom-*"
        },
        {
            "Sid": "CreateKmsGrant",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "CreateEc2Tags",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Asegúrese de que los permisos enumerados no están restringidos por las políticas de control de servicio (SCP), los límites de los permisos o las políticas de sesión asociadas a la entidad principal de IAM.

Si utiliza condiciones con claves de contexto en la política de IAM del solicitante, ciertas condiciones pueden provocar un error en la solicitud. Para obtener más información sobre los errores más comunes debidos a las condiciones de la política de IAM, consulte Solicitudes de copia de instantáneas de base de datos entre regiones.

Copia de una instantánea de base de datos

Utilice el siguiente procedimiento para copiar una instantánea de base de datos. Para cada cuenta AWS, puede copiar hasta 20 instantáneas de base de datos a la vez de una Región de AWS a otra. Si copia una instantánea de base de datos en otra Región de AWS, crea una instantánea de base de datos manual que se conserva en esa Región de AWS. Al copiar una instantánea de base de datos fuera de la Región de AWS origen, se producen cargos por transferencia de datos de Amazon RDS. Para obtener más información acerca de los precios de las transferencias de datos, consulte Precios de Amazon RDS.

Una vez que la copia de la instantánea de base de datos se ha creado en la nueva Región de AWS, la copia de la instantánea de base de datos se comporta como las demás instantáneas de base de datos de esa Región de AWS.

Puede copiar una instantánea de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS.

Console

El siguiente procedimiento copia una instantánea de base de datos de RDS Custom para SQL Server con la AWS Management Console.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Seleccione la instantánea de base de datos de RDS Custom para SQL Server que desea copiar.
4. En el menú desplegable Acciones, seleccione Copiar instantánea.

RDS > Snapshots > Copy snapshot

Copy snapshot

Settings

Source DB snapshot
DB snapshot identifier for the snapshot being copied.
db1-snapshot

New DB snapshot identifier
DB snapshot identifier for the new snapshot.
copied-db1-snapshot
Must start with a letter and only contain letters, digits, or hyphens.

Destination Region Info
Choose a Region

Resource tags Info
Copy tags from the source DB snapshot

Depending on the amount of data to be copied and the Region you choose, this operation can take several hours to complete. The display on the progress bar might be delayed until setup is complete.

Encryption

Encryption Info
Enable Encryption
Choose to encrypt the copy of the source DB snapshot. Master key IDs and aliases appear in the list after they have been created using KMS. You cannot remove encryption from an encrypted DB snapshot.

AWS KMS key Info
Enter a key ARN

Amazon Resource Name (ARN)
Example: arn:aws:kms:<region>:<accountID>:key/<key-id>

Account

KMS key ID

5. Para copiar la instantánea de base de datos en una Región de AWS diferente, establezca Región de destino en el valor necesario.

   > **Note**
   >
   > La Región de AWS de destino debe tener la misma versión del motor de base de datos disponible que la Región de AWS de origen.

6. En Nuevo identificador de instantánea de base de datos, introduzca un nombre único para la instantánea de base de datos. Puede realizar varias copias de una copia de seguridad automatizada o instantánea manual, pero cada copia debe tener un identificador único.
7. (Opcional) Seleccione Copy Tags (Copiar etiquetqas) para copiar las etiquetas y los valores de la instantánea en la copia de la instantánea.
8. En Cifrado, especifique el identificador de la clave de KMS que se debe utilizar para cifrar la copia de la instantánea de base de datos.

   > **Note**
   >
   > RDS Custom para SQL Server cifra todas las instantáneas de base de datos. No puede crear una instantánea de base de datos sin cifrar.

9. Elija Copy Snapshot (Copiar instantánea).

RDS Custom para SQL Server crea una copia de instantánea de base de datos de la instancia de base de datos en la Región de AWS que seleccione.

AWS CLI

Puede copiar una instantánea de base de datos de RDS Custom para SQL Server usando el comando AWS CLI de la copy-db-snapshot. Si desea copiar la instantánea en una nueva Región de AWS, ejecute el comando en la nueva Región de AWS. Las siguientes opciones se usan para copiar una instantánea de base de datos. No todas las opciones son necesarias para todos los escenarios.

- `--source-db-snapshot-identifier`: identificador de la instantánea de base de datos de origen.

  - Si la instantánea de origen está en una Región de AWS distinta de la de la copia, especifique un ARN de instantánea de base de datos válido. Por ejemplo, `arn:aws:rds:us-west-2:123456789012:snapshot:instance1-snapshot-12345678`.
- `--target-db-snapshot-identifier`: identificador de la nueva copia de la instantánea de base de datos.
- `--kms-key-id`: identificador de la clave de KMS de una instantánea de base de datos cifrada. El identificador de la clave de KMS es el nombre de recurso de Amazon (ARN), el identificador de la clave o el alias de clave de la clave de KMS.
  - Si copia una instantánea cifrada en otra Región de AWS, debe especificar una clave de KMS para la región de Región de AWS de destino. Las claves de KMS son específicas de la Región de AWS en la que se han creado; no se pueden utilizar las claves de cifrado de una Región de AWS en otra Región de AWS a no ser que se utilice una clave multirregión. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en AWS KMS.
- `--copy-tags`: incluya las etiquetas y los valores de la instantánea de origen en la copia de la instantánea.

Las siguientes opciones no son compatibles en la copia de una instantánea de base de datos de RDS Custom para SQL Server:

- `--copy-option-group`
- `--option-group-name`
- `--pre-signed-url`
- `--target-custom-availability-zone`

El siguiente ejemplo de código copia una instantánea de base de datos cifrada de la región Oeste de EE. UU. (Oregón) a la región Este de EE. UU. (Norte de Virginia). Ejecute el comando en la región de destino (us-east-1).

Para Linux, macOS o Unix:

```
aws rds copy-db-snapshot \
     --region us-east-1 \
    --source-db-snapshot-identifier arn:aws:rds:us-
west-2:123456789012:snapshot:instance1-snapshot-12345678 \
    --target-db-snapshot-identifier mydbsnapshotcopy \
```

```
    --kms-key-id a1b2c3d4-1234-5678-wxyz-a1b2c3d4d5e6
```

Para Windows:

```
aws rds copy-db-snapshot ^
     --region us-east-1 ^
    --source-db-snapshot-identifier arn:aws:rds:us-
west-2:123456789012:snapshot:instance1-snapshot-12345678 ^
    --target-db-snapshot-identifier mydbsnapshotcopy ^
    --kms-key-id a1b2c3d4-1234-5678-wxyz-a1b2c3d4d5e6
```

RDS API

Puede copiar una instantánea de base de datos de RDS Custom para SQL Server usando la operación CopyDBSnapshot de la API de Amazon RDS. Si desea copiar la instantánea en una nueva Región de AWS, realice la acción en la nueva Región de AWS. Los siguientes parámetros se usan para copiar una instantánea de base de datos. No todos los parámetros son obligatorios:

- `SourceDBSnapshotIdentifier`: identificador de la instantánea de base de datos de origen.
  - Si la instantánea de origen está en una Región de AWS distinta de la de la copia, especifique un ARN de instantánea de base de datos válido. Por ejemplo, `arn:aws:rds:us-west-2:123456789012:snapshot:instance1-snapshot-12345678`.
- `TargetDBSnapshotIdentifier`: identificador de la nueva copia de la instantánea de base de datos.
- `KmsKeyId`: identificador de la clave de KMS de una instantánea de base de datos cifrada. El identificador de la clave de KMS es el nombre de recurso de Amazon (ARN), el identificador de la clave o el alias de clave de la clave de KMS.
  - Si copia una instantánea cifrada en otra Región de AWS, debe especificar una clave de KMS para la región de Región de AWS de destino. Las claves de KMS son específicas de la Región de AWS en la que se han creado; no se pueden utilizar las claves de cifrado de una Región de AWS en otra Región de AWS a no ser que se utilice una clave multirregión. Para obtener más información sobre las claves de varias regiones, consulte Uso de claves de varias regiones en AWS KMS.
- `CopyTags`: defina este parámetro como `true` para copiar las etiquetas y los valores de la instantánea de origen en la copia de la instantánea. El valor predeterminado es `false`.

Las siguientes opciones no son compatibles en la copia de una instantánea de base de datos de RDS Custom para SQL Server:

- `CopyOptionGroup`
- `OptionGroupName`
- `PreSignedUrl`
- `TargetCustomAvailabilityZone`

El siguiente código crea una copia de una instantánea, con el nuevo nombre `mydbsnapshotcopy`, en la región US East (N. Virginia).

```
https://rds.us-east-1.amazonaws.com/
    ?Action=CopyDBSnapshot
    &KmsKeyId=a1b2c3d4-1234-5678-wxyz-a1b2c3d4d5e6
    &SourceDBSnapshotIdentifier=arn%3Aaws%3Ards%3Aus-
west-2%3A123456789012%3Asnapshot%3Ainstance1-snapshot-12345678
    &TargetDBSnapshotIdentifier=mydbsnapshotcopy
    &Version=2014-10-31
    &X-Amz-Algorithm=AWS4-HMAC-SHA256
    &X-Amz-Credential=AKIADQKE4SARGYLE/20161117/us-east-1/rds/aws4_request
    &X-Amz-Date=20161117T221704Z
    &X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-
date
    &X-Amz-
Signature=da4f2da66739d2e722c85fcfd225dc27bba7e2b8dbea8d8612434378e52adccf
```

Migración de una base de datos en las instalaciones a Amazon RDS Custom for SQL Server

Puede utilizar el siguiente proceso para migrar una base de datos en las instalaciones de Microsoft SQL Server a Amazon RDS Custom for SQL Server mediante una copia de seguridad y una restauración nativas:

1. Realice una copia de seguridad completa de la base de datos en la instancia de base de datos en las instalaciones.
2. Cargue el archivo de copia de seguridad en Amazon S3.
3. Descargue el archivo de copia de seguridad de S3 en la instancia de base de datos de RDS Custom for SQL Server.
4. Restaurar una base de datos mediante el archivo de copia de seguridad descargado en la instancia de base de datos de RDS Custom for SQL Server.

En este proceso se explica la migración de una base de datos de las instalaciones a RDS Custom for SQL Server, mediante copias de seguridad y restauración completas nativas. Para reducir el tiempo de transición durante el proceso de migración, también podría considerar utilizar copias de seguridad diferenciales o de registros.

Para obtener información general sobre la copia de seguridad y restauración nativas de RDS para SQL Server, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Temas

- Requisitos previos
- Copia de seguridad de la base de datos en las instalaciones
- Cargar el archivo de copia de seguridad en Amazon S3
- Descargar el archivo de copia de seguridad de Amazon S3
- Restauración del archivo de copia de seguridad en la instancia de base de datos de RDS Custom for SQL Server

Requisitos previos

Realice las siguientes tareas antes de migrar la base de datos:

1. Configure Remote Desktop Connection (RDP) para la instancia de base de datos de RDS Custom for SQL Server. Para obtener más información, consulte Conexión a la instancia de base de datos de RDS Custom mediante RDP.
2. Configure el acceso a Amazon S3 para que pueda cargar y descargar el archivo de copia de seguridad de la base de datos.

Copia de seguridad de la base de datos en las instalaciones

Utilice la copia de seguridad nativa de SQL Server para realizar una copia de seguridad completa de la base de datos en la instancia de base de datos en las instalaciones.

En el siguiente ejemplo se muestra una copia de seguridad de una base de datos denominada `mydatabase`, con la opción `COMPRESSION` especificada para reducir el tamaño del archivo de copia de seguridad.

Para realizar una copia de seguridad de la base de datos en las instalaciones

1. Mediante SQL Server Management Studio (SSMS), conecte con la instancia de SQL Server en las instalaciones.
2. Ejecute el siguiente comando T-SQL.

```
backup database mydatabase to
disk ='C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Backup\mydb-full-compressed.bak'
with compression;
```

Cargar el archivo de copia de seguridad en Amazon S3

Utilice el AWS Management Console para cargar el archivo de copia de seguridad `mydb-full-compressed.bak` en Amazon S3.

Para cargar el archivo de copia de seguridad en S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Para Buckets, elija el nombre del bucket al que desea cargar su archivo de copia de seguridad.
3. Seleccione Cargar.

4. En la ventana Cargar, realice una de las siguientes acciones:

   - Arrastre y suelte `mydb-full-compressed.bak` en la ventana Upload (Cargar).
   - Elija Add file (Agregar archivo), `mydb-full-compressed.bak` y luego Open (Abrir).

   Amazon S3 carga el archivo de copia de seguridad como un objeto de S3. Cuando finalice la carga, puede ver un mensaje de éxito en la página Cargar: estado.

Descargar el archivo de copia de seguridad de Amazon S3

Utilice la consola para descargar el archivo de copia de seguridad de S3 a la instancia de base de datos de RDS Custom for SQL Server.

Para descargar el archivo de copia de seguridad de S3

1. Con RDP, conéctese a su instancia de base de datos de RDS Custom for SQL Server.
2. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
3. En la lista Buckets, elija el nombre del bucket que contiene su archivo de copia de seguridad.
4. Elija el archivo de copia de seguridad `mydb-full-compressed.bak`.
5. En Actions (Acciones), elija Download as (Descargar como).
6. Abra el menú contextual (haga clic con el botón derecho) del enlace que se proporciona, después elija Save As (Guardar como).
7. Guarde `mydb-full-compressed.bak` en el directorio `D:\rdsdbdata\BACKUP`.

Restauración del archivo de copia de seguridad en la instancia de base de datos de RDS Custom for SQL Server

Utilice la restauración nativa de SQL Server para restaurar el archivo de copia de seguridad en la instancia de base de datos de RDS Custom for SQL Server.

En este ejemplo, se especifica la opción `MOVE` porque los directorios de archivos de registro y datos son diferentes de la instancia de base de datos en las instalaciones.

Para restaurar el archivo de copia de seguridad

1. Con SSMS, conéctese a la instancia de base de datos de RDS Custom for SQL Server.

2. Ejecute el siguiente comando T-SQL.

```
restore database mydatabase from disk='D:\rdsdbdata\BACKUP\mydb-full-
compressed.bak'
with move 'mydatabase' to 'D:\rdsdbdata\DATA\mydatabase.mdf',
move 'mydatabase_log' to 'D:\rdsdbdata\DATA\mydatabase_log.ldf';
```

Actualización de una instancia de base de datos de Amazon RDS Custom para SQL Server

Puede actualizar una instancia de base de datos de Amazon RDS Custom para SQL Server al modificarla para utilizar una nueva versión del motor de base de datos. Para obtener información general sobre la actualización de instancias de base de datos, consulte Actualización de una versión del motor de una instancia de base de datos.

Temas

- Información general sobre las actualizaciones en RDS Custom para SQL Server
- Actualización de la versión principal y secundaria del motor
- Nivel de compatibilidad de la base de datos

Información general sobre las actualizaciones en RDS Custom para SQL Server

Amazon RDS Custom para SQL Server admite las actualizaciones de versiones principales y secundarias. Las actualizaciones de versiones secundarias pueden incluir parches de seguridad, correcciones de errores y mejoras del motor. Microsoft publica estas actualizaciones como actualizaciones acumulativas (CU). Las actualizaciones de versión principal ingresan nuevas características y cambios de motor entre versiones, como la actualización de SQL Server 2019 a 2022. Puede aplicar ambas actualizaciones de forma inmediata o durante las ventanas de mantenimiento programadas. Para evitar posibles problemas de compatibilidad con versiones anteriores, recomendamos probar las aplicaciones en un entorno que no sea de producción antes de la actualización.

RDS Custom para SQL Server le permite actualizar una versión de motor proporcionada por RDS (RPEV) o una versión de motor personalizada (CEV).

- Las versiones del motor proporcionadas por RDS (RPEV) contienen parches actualizados del sistema operativo (SO) y actualizaciones acumulativas (CU) de SQL Server.
- Para una versión de motor personalizada (CEV), debe seguir un proceso de dos pasos. En primer lugar, cree un nuevo CEV con la versión de SQL Server de destino, consulte Preparación para crear una CEV para RDS Custom para SQL Server. Esta versión de destino debe ser igual o más reciente que la versión actual. Una vez creado el nuevo CEV, modifique la instancia de la base de datos para usar esta nueva versión. Para obtener más información, consulte Realización de una actualización de versión secundaria para Amazon RDS Custom para SQL Server CEV con Multi-AZ.

No aplique actualizaciones acumulativas de SQL Server locales a la instancia de RDS Custom en ejecución. Una vez que cree una CEV con una versión específica de SQL Server (por ejemplo, SQL Server 2022 CU16), aplicar una actualización acumulativa más reciente directamente a la instancia la saca del perímetro de soporte y genera un error `SP-S3006`. Para aplicar un parche a una instancia de SQL Server existente mediante una CEV, cree una nueva CEV que incluya la actualización acumulativa deseada y, a continuación, modifique la instancia existente para cambiar a la nueva CEV.

Si actualiza una instancia de base de datos de RDS Custom para SQL Server en una implementación multi-AZ, RDS Custom para SQL Server realizará actualizaciones sucesivas para la instancia. Este enfoque minimiza el tiempo de inactividad mediante la actualización de una instancia a la vez. RDS realiza las siguientes acciones para llevar a cabo actualizaciones sucesivas:

1. Actualice la instancia de base de datos de reserva.
2. Conmutación por error a la instancia de base de datos en espera actualizada, convirtiéndola en la nueva instancia de base de datos principal.
3. Actualice la nueva instancia de base de datos de reserva.

El tiempo de inactividad de la instancia de base de datos para las implementaciones multi-AZ es el tiempo que tarda la conmutación por error.

Las siguientes limitaciones se aplican al actualizar una instancia de base de datos de RDS Custom para SQL Server:

- No se admiten grupos de parámetros y opciones de base de datos de Custom.
- Los volúmenes de almacenamiento adicionales que adjunte a la instancia de base de datos de RDS Custom para SQL Server no se adjuntarán después de la actualización.
- En el caso de las CEV, la aplicación local de las actualizaciones acumulativas de SQL Server no es compatible y resulta en que la instancia quede fuera del perímetro de soporte.

Actualización de la versión principal y secundaria del motor

Las actualizaciones de las versiones principal y secundaria del motor son irreversibles y siempre deben realizarse a una versión más reciente. Para identificar las versiones de destino disponibles, utilice AWS Management Console y elija entre las versiones disponibles al modificar la instancia de

base de datos. Como alternativa, utilice el comando `describe-db-engine-versions` de la CLI o el comando DescribeDBEngineVersions de la API de RDS.

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
    --engine custom-sqlserver-se \
    --engine-version 15.00.4322.2.v1 \
    --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" \
    --output table
```

Para Windows:

```
aws rds describe-db-engine-versions ^
    --engine custom-sqlserver-se ^
    --engine-version 15.00.4322.2.v1 ^
    --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" ^
    --output table
```

El resultado muestra las versiones del motor de destino disponibles:

```
--------------------------
|DescribeDBEngineVersions|
+------------------------+
|      EngineVersion     |
+------------------------+
|  15.00.4410.1.v1       |
|  15.00.4415.2.v1       |
|  15.00.4430.1.v1       |
|  16.00.4165.4.v1       |
|  16.00.4175.1.v1       |
|  16.00.4185.3.v1       |
+------------------------+
```

Tras identificar la versión de destino, utilice AWS Management Console y siga las instrucciones que se indican en Modificación de una instancia de base de datos de RDS Custom for SQL Server. Como alternativa, utilice el comando `modify-db-instance` de la CLI o el comando ModifyDBInstance de la API de RDS.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier DB_INSTANCE_IDENTIFIER \
    --engine-version ENGINE_VERSION \
    --allow-major-version-upgrade \
    --region Region \
    --no-apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier DB_INSTANCE_IDENTIFIER ^
    --engine-version ENGINE_VERSION ^
    --allow-major-version-upgrade ^
    --region Region ^
    --no-apply-immediately
```

> **Note**
>
> Debe incluir el parámetro `--allow-major-version-upgrade` para realizar actualizaciones de versiones principales.

Nivel de compatibilidad de la base de datos

Puede utilizar los niveles de compatibilidad de la base de datos de Microsoft SQL Server para ajustar algunos comportamientos de la base de datos con objeto de imitar versiones anteriores de SQL Server. Para obtener más información, consulte Niveles de compatibilidad en la documentación de Microsoft.

Al actualizar la instancia de base de datos, todas las bases de datos existentes conservan su nivel de compatibilidad original. Por ejemplo, si se actualiza desde SQL Server 2019 a SQL Server 2022, todas las bases de datos existentes tienen el nivel de compatibilidad de 150. Cualquier base de datos nueva creada después de la actualización tiene el nivel de compatibilidad 160.

Puede cambiar el nivel de compatibilidad de una base de datos mediante el comando ALTER DATABASE. Por ejemplo, para cambiar la base de datos `customeracct` de modo que sea compatible con SQL Server 2022, utilice el siguiente comando:

```
ALTER DATABASE customeracct SET COMPATIBILITY_LEVEL = 160
```

Solución de problemas de base de datos para Amazon RDS Custom para SQL Server

El modelo de responsabilidad compartida de RDS Custom proporciona acceso al shell del sistema operativo y acceso como administrador de bases de datos. RDS Custom ejecuta recursos en su cuenta, a diferencia de Amazon RDS, que ejecuta recursos en una cuenta del sistema. Un mayor acceso conlleva una mayor responsabilidad. En las siguientes secciones, puede obtener información sobre cómo solucionar problemas con las instancias de base de datos de Amazon RDS Custom para SQL Server.

> **Note**
>
> En esta sección, se explica cómo solucionar los problemas de RDS Custom para SQL Server. Para la solución de problemas de RDS Custom para Oracle, consulte Solución de problemas de base de datos de Amazon RDS Custom para Oracle.

Temas

- Visualización de eventos de RDS Custom
- Suscripción a eventos de RDS Custom
- Solución de errores de CEV para RDS Custom para SQL Server
- Corrección de configuraciones no compatibles en RDS Custom para SQL Server
- Solución de problemas Storage-Full en RDS Custom para SQL Server
- Resolución del problema PENDING_RECOVERY en bases de datos habilitadas para TDE en RDS Custom para SQL Server

Visualización de eventos de RDS Custom

El procedimiento para ver eventos es el mismo para las instancias de base de datos de RDS Custom y Amazon RDS. Para obtener más información, consulte Consulta de eventos de Amazon RDS.

Para ver la notificación de eventos de RDS Custom mediante la AWS CLI, utilice el comando `describe-events`. RDS Custom presenta varios eventos nuevos. Las categorías de eventos son las mismas que para Amazon RDS. Para ver la lista de eventos, consulte Categorías y mensajes de eventos de Amazon RDS.

En el siguiente ejemplo se recuperan los detalles de los eventos que se han producido para la instancia de base de datos de RDS Custom especificada.

```
aws rds describe-events \
    --source-identifier my-custom-instance \
    --source-type db-instance
```

Suscripción a eventos de RDS Custom

El procedimiento para suscribirse a eventos es el mismo para las instancias de base de datos de RDS Custom y Amazon RDS. Para obtener más información, consulte Suscripción a notificaciones de eventos de Amazon RDS.

Para suscribirse a las notificaciones de eventos de RDS Custom con la CLI, utilice el comando `create-event-subscription`. Incluya los siguientes parámetros obligatorios:

- `--subscription-name`
- `--sns-topic-arn`

En el siguiente ejemplo se crea una suscripción para eventos de copia de seguridad y recuperación de una instancia de base de datos de RDS Custom en la cuenta de AWS actual. Las notificaciones se envían a un tema de Amazon Simple Notification Service (Amazon SNS), especificado por `--sns-topic-arn`.

```
aws rds create-event-subscription \
    --subscription-name my-instance-events \
    --source-type db-instance \
    --event-categories '["backup","recovery"]' \
    --sns-topic-arn arn:aws:sns:us-east-1:123456789012:interesting-events
```

Solución de errores de CEV para RDS Custom para SQL Server

Cuando intenta crear una CEV, puede fallar. En este caso, RDS Custom emite el mensaje de evento `RDS-EVENT-0198`. Para obtener más información acerca de la visualización de eventos de RDS, consulte Categorías y mensajes de eventos de Amazon RDS.

Utilice la siguiente información para ayudarle a abordar las posibles causas.

Mensaje	Sugerencias para la solución de problemas		
`Custom Engine Version creation expected a Sysprep'd AMI. Retry creation using a Sysprep'd AMI.`	Ejecute Sysprep en la instancia EC2 que ha creado a partir de la AMI. Para obtener más informaci ón sobre cómo preparar la AMI con Sysprep, consulte Create a standardized Amazon Machine Image (AMI) using Sysprep (Crear una imagen de máquina de Amazon (AMI) estandarizada con Sysprep).		
`EC2 Image permissio ns for image (AMI_ID) weren't found for customer (Customer_ID). Verify customer (Customer_ID) has valid permissions on the EC2 Image.`	Compruebe que la cuenta y el perfil utilizados para la creación tengan los permisos necesarios en `create EC2 Instance` y `Describe Images` para la AMI seleccionada.		
`Failed to rebuild databases with server collation (collation name) due to missing setup.exe file for SQL Server.`	Compruebe que el archivo `setup` esté disponible en `C:\Progra m Files\Microsoft SQL Server\nnn\Setup Bootstrap \SQLnnnn\setup.exe` .		
`Image (AMI_ID) doesn't exist in your account (ACCOUNT_ID). Verify (ACCOUNT_ID) is the owner of the EC2 image.`	Asegúrese de que la AMI exista en la misma cuenta de cliente.		
`Image id (AMI_ID) isn't valid. Specify a valid image id, and try again.`	El nombre de la AMI es incorrecto. Asegúrese de proporcionar el ID de AMI correcto.		

Mensaje	Sugerencias para la solución de problemas		
`Image (AMI_ID) operating system platform isn't supported. Specify a valid image, and try again.`	Elija una AMI compatible que tenga Windows Server con las ediciones SQL Server Enterprise, Standard o Web. Elija una AMI con uno de los siguientes códigos de operación de uso del EC2 Marketplace: • RunInstances:0102 - Windows con SQL Server Enterprise • RunInstances:0006 - Windows con SQL Server Standard • RunInstances:0202 - Windows con SQL Server Web		
`SQL Server Web Edition isn't supported for creating a Custom Engine Version using Bring Your Own Media. Specify a valid image, and try again.`	Utilice una AMI que contenga una edición compatible de SQL Server. Para obtener más informaci ón, consulte Compatibilidad de versiones CEV para RDS Custom para SQL Server.		
`The custom engine version can't be the same as the OEV engine version. Specify a valid CEV, and try again.`	Las versiones del motor Classic RDS Custom para SQL Server no son compatibles. Por ejemplo, la versión 15.00.4073.23.v1. Utilice un número de versión compatible.		
`The custom engine version isn't in an active state. Specify a valid CEV, and try again.`	La CEV debe tener el estado `AVAILABLE` para que se pueda completar la operación. Modifique la CEV de `INACTIVE` a `AVAILABLE` .		

Mensaje	Sugerencias para la solución de problemas		
`The custom engine version isn't valid for an upgrade. Specify a valid CEV with an engine version greater or equal to (X), and try again.`	La CEV de destino no es válida. Compruebe los requisitos de una ruta de actualización válida.		
`The custom engine version isn't valid. Names can include only lowercase letters (a-z), dashes (-), underscores (_), and periods (.). Specify a valid CEV, and try again.`	Siga la convención de nomenclatura de CEV requerida. Para obtener más información, consulte Requisitos de las CEV para RDS Custom para SQL Server.		
`The custom engine version isn't valid. Specify valid database engine version, and try again. Example: 15.00.4073.23-cev123.`	Se ha proporcionado una versión de motor de base de datos no compatible. Use las versiones de motor de base de datos compatibles.		
`The expected architecture is (X) for image (AMI_ID), but architecture (Y) was found.`	Use una AMI basada en la arquitectura x86_64.		
`The expected owner of image (AMI_ID) is customer account ID (ACCOUNT_ID), but owner (ACCOUNT_ID) was found.`	Cree la instancia EC2 a partir de la AMI para la que tiene permiso. Ejecute Sysprep en la instancia EC2 para crear y guardar una imagen base.		

Mensaje	Sugerencias para la solución de problemas		
`The expected platform is (X) for image (AMI_ID), but platform (Y) was found.`	Utilice una AMI creada con la plataforma Windows.		
`The expected root device type is (X) for image %s, but root device type (Y) was found.`	Cree la AMI con el tipo de dispositivo EBS.		
`The expected SQL Server edition is (X), but (Y) was found.`	Elija una AMI compatible que tenga Windows Server con las ediciones SQL Server Enterprise, Standard o Web. Elija una AMI con uno de los siguientes códigos de operación de uso del EC2 Marketplace: • RunInstances:0102 - Windows con SQL Server Enterprise • RunInstances:0006 - Windows con SQL Server Standard • RunInstances:0202 - Windows con SQL Server Web		
`The expected state is (X) for image (AMI_ID), but the following state was found: (Y).`	Asegúrese de que la AMI tenga el estado `AVAILABLE` .		
`The provided Windows OS name (X) isn’t valid. Make sure the OS is one of the following: (Y).`	Utilice un sistema operativo Windows compatible.		

Mensaje	Sugerencias para la solución de problemas
`Unable to find bootstrap log file in path.`	Compruebe que el archivo de registro esté disponible en `C:\Program Files\Microsoft SQL Server\nnn\Setup Bootstrap\Log\Summary.txt` .
`RDS expected a Windows build version greater than or equal to (X), but found version (Y)..`	Utilice una AMI con una versión mínima de compilación del sistema operativo de 14393.
`RDS expected a Windows major version greater than or equal to (X), but found version (Y)..`	Utilice una AMI con una versión principal del sistema operativo 10.0 o superior.

Corrección de configuraciones no compatibles en RDS Custom para SQL Server

Como es un modelo de responsabilidad compartida, es su responsabilidad corregir los problemas de configuración que colocan la instancia de base de datos de RDS Custom para SQL Server en el estado `unsupported-configuration`. Si el problema está relacionado con la infraestructura de AWS, puede utilizar la consola o la AWS CLI para solucionarlo. Si el problema está relacionado con el sistema operativo o la configuración de la base de datos, puede iniciar sesión en el host para solucionarlo.

> **Note**
>
> Esta sección explica cómo corregir configuraciones no compatibles en RDS Custom para SQL Server. Para obtener información sobre RDS Custom para Oracle, consulte Corrección de configuraciones no compatibles en RDS Custom para Oracle.

En la siguiente tabla, encontrará descripciones de las notificaciones y eventos que envía el perímetro de soporte y cómo solucionarlos. Estas notificaciones y el perímetro de soporte están sujetos a cambios. Para obtener información sobre el perímetro de soporte, consulte Perímetro de soporte de RDS Custom. Para ver las descripciones de los eventos, consulte Categorías y mensajes de eventos de Amazon RDS.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
`SP-S0000`	Configuración manual no compatible	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a: X.	Para resolver este problema, cree un caso de soporte.

Recurso de AWS (infraestructura)

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
`SP-S1001`	Estado de la instancia EC2	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que la instancia EC2 subyacente %s se detuvo sin detener la instancia de RDS. Para resolver este problema,	Para comprobar el estado de una instancia de base de datos, utilice la consola o ejecute el siguiente comando de la AWS CLI: `aws rds describe-db-instances \ --db-instance-identifier db-instance-name |grep DBInstanceStatus`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
		inicie la instancia EC2 subyacente y asegúrese de que los volúmenes binarios y de datos estén conectados. Si su intención es detener la instancia de RDS, asegúrese primero de que la instancia EC2 subyacente esté en el estado DISPONIBLE y, a continuación, utilice la consola de RDS o la CLI para detener la instancia de RDS.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S1002	Estado de la instancia EC2	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que el estado de la instancia de base de datos está configurada como STOPPED pero la instancia EC2 subyacente %s se ha iniciado. Puede resolver este problema deteniendo la instancia EC2 subyacente. Si su intención es iniciar la instancia de RDS, utilice la consola o la CLI.	Utilice el siguiente comando de la AWS CLI para comprobar el estado de una instancia de base de datos.
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep DBInstanceStatus`
			También puede comprobar el estado de la instancia EC2 en la consola de EC2.
			Para iniciar una instancia de base de datos, utilice la consola o ejecute el siguiente comando de la AWS CLI:
			`aws rds start-db-instance \ --db-instance-identifier db-instance-name`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1003	Clase de instancia EC2	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que hay una discrepancia entre la clase de instancia de base de datos esperada y la configurada del host EC2. Puede resolver este problema modificando la clase de instancia de base de datos a su tipo de clase original.	Utilice el siguiente comando de la CLI con el fin de comprobar la clase de instancia de base de datos esperada: `aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep DBInstanceClass`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1004	No se puede acceder al volumen de almacenamiento de EBS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que actualmente no se puede acceder al volumen de almacenamiento de EBS original %s que estaba asociado a la instancia EC2.	
SP-S1005	Volumen de almacenamiento de EBS desconectado	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que el volume-id del volumen de almacenamiento de EBS original no está asociado. Puede resolver este problema asociando el volumen de EBS asociado a la instancia EC2.	Tras volver a asociar el volumen de EBS, utilice los siguientes comandos de la CLI para comprobar si el volumen de EBS “volume-id” está correctamente asociado a la instancia de RDS: `aws ec2 describe-volumes \ --volume-ids volume-id | grep InstanceId`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S1006	Tamaño del volumen de almacenamiento de EBS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que hay una discrepancia entre los ajustes esperados y configurados del volumen de almacenamiento de EBS volume-id. El tamaño del volumen se ha cambiado manualmente en el nivel de EC2 con respecto a sus valores originales de [%s]. Para resolver este problema, cree un caso de soporte.	Utilice el siguiente comando de la CLI para comparar el tamaño de los detalles del volumen de EBS “volume-id” y los detalles de la instancia de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep AllocatedStorage`
			Utilice el siguiente comando de la CLI para ver el tamaño real del volumen asignado:
			`aws ec2 describe-volumes \ --volume-ids |grep Size`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S1007	Configuración del volumen de almacenamiento de EBS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que hay una discrepancia entre los ajustes esperados y configurados del volumen de almacenamiento de EBS volume-id. Puede resolver este problema modificando la configuración del volumen de almacenamiento de EBS [IOPS, rendimiento, tipo de volumen] a sus valores originales de [IOPS: %s, rendimiento: %s, tipo de volumen: %s] al nivel de EC2. Para futuras modificaciones del almacenamiento, utilice la consola de RDS o la CLI.	Utilice el siguiente comando de la CLI para comparar el tipo de los detalles del volumen de EBS “volume-id” y los detalles de la instancia de RDS: Asegúrese de que los valores del nivel de EBS coincidan con los valores del nivel de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep StorageType`
			Para obtener el valor esperado del rendimiento de almacenamiento a nivel de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep StorageThroughput`
			Para obtener el valor esperado de IOPS de volumen a nivel de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep Iops`
			Para obtener el tipo de almacenamiento actual en el nivel de EC2:

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

		El tamaño del volumen también se ha cambiado manualmente en el nivel de EC2 con respecto a sus valores originales de [%s]. Para resolver este problema, cree un caso de soporte.	`aws ec2 describe-volumes \ --volume-ids |grep VolumeType`
			
			Para obtener el valor actual del rendimiento del almacenamiento en el nivel de EC2:
			
			`aws ec2 describe-volumes \ --volume-ids |grep Throughput`
			
			Para obtener el valor actual de IOPS de volumen a nivel de EC2:
			
			`aws ec2 describe-volumes \ --volume-ids |grep Iops`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S1008	Tamaño y configuración del volumen de almacenamiento de EBS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que hay una discrepancia entre los ajustes esperados y configurados del volumen de almacenamiento de EBS volume-id. Puede resolver este problema modificando la configuración del volumen de almacenamiento de EBS [IOPS, rendimiento, tipo de volumen] a sus valores originales de [IOPS: %s, rendimiento: %s, tipo de volumen: %s] al nivel de EC2. Para futuras modificaciones del almacenamiento, utilice la consola de RDS o la CLI.	Utilice el siguiente comando de la CLI para comparar el tipo de los detalles del volumen de EBS “volume-id” y los detalles de la instancia de RDS: Asegúrese de que los valores del nivel de EBS coincidan con los valores del nivel de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep StorageType`
			Para obtener el valor esperado del rendimiento de almacenamiento a nivel de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep StorageThroughput`
			Para obtener el valor esperado de IOPS de volumen a nivel de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep Iops`
			Para obtener el tipo de almacenamiento actual en el nivel de EC2:

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

		El tamaño del volumen también se ha cambiado manualmente en el nivel de EC2 con respecto a sus valores originales de [%s]. Para resolver este problema, cree un caso de soporte.	`aws ec2 describe-volumes \ --volume-ids |grep VolumeType`
			
			Para obtener el valor actual del rendimiento del almacenamiento en el nivel de EC2:
			
			`aws ec2 describe-volumes \ --volume-ids |grep Throughput`
			
			Para obtener el valor actual de IOPS de volumen a nivel de EC2:
			
			`aws ec2 describe-volumes \ --volume-ids |grep Iops`
			
			Para obtener el tamaño de volumen asignado esperado:
			
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name | grep AllocatedStorage`
			
			Para obtener el tamaño de volumen asignado real:
			
			`aws ec2 describe-volumes \ --volume-ids |grep Size`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1009	Permisos de SQS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que faltan los permisos de Amazon Simple Queue Service (SQS) para el perfil de instancia de IAM. Puede resolver este problema asegurándose de que el perfil de IAM asociado al host tenga los siguientes permisos: ["SQS:SendMessage","SQS:ReceiveMessage","SQS:DeleteMessage","SQS:GetQueueUrl"].	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1010	Puntos de conexión de VPC de SQS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que una política de punto de conexión de VPC bloquea las operaciones de Amazon Simple Queue Service (SQS). Puede resolver este problema modificando la política de puntos de conexión de VPC para permitir las acciones de SQS necesarias.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1011	Política de bus de eventos	The RDS Custom DB instance status is set to [Unsupported configuration] because of: The resource-based policy for your event bus arn:aws:events:region-1:123456789012:event-bus/default denies Amazon CloudWatch events:PutEvents actions. Resolve this by modifying your resource-based policy to allow events:PutEvents actions for EventBus %s.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1012	Permisos de VPC de CloudWatch	The RDS Custom DB instance status is set to [Unsupported configuration] because of: A VPC endpoint policy is missing permissions to access Amazon CloudWatch events. Resolve this by modifying your VPC endpoint policy to allow events:PutEvents on EventBus arn:aws:events:region-1:123456789012:event-bus/default.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1013	Política de control de servicios	The RDS Custom DB instance status is set to [Unsupported configuration] because of: A service control policy in your AWS Organizations is missing permissions to access Amazon CloudWatch events. Resolve this by modifying your service control policy to allow events:PutEvents on EventBus arn:aws:events:region-1:123456789012:event-bus/default.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1014	Perfil de instancia IAM	The RDS Custom DB instance status is set to [Unsupported configuration] because of: Your IAM instance profile %s permissions deny Amazon CloudWatch events. Resolve this by setting [“events:PutEvents”] to “Allow” and allowing events:PutEvents on EventBus arn:aws:events:region-1:123456789012:event-bus/default in your IAM profile associated with the instance.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1015	Perfil de instancia IAM	The RDS Custom DB instance status is set to [Unsupported configuration] because of: Your IAM instance profile %s is missing Amazon CloudWatch event permissions. Resolve this by including the [“events:PutEvents”] permissions and allowing events:PutEvents on EventBus arn:aws:events:region-1:123456789012:event-bus/default in your IAM profile associated with the instance.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S1016	Límite de permisos de IAM	The RDS Custom DB instance status is set to [Unsupported configuration] because of: Your IAM instance profile %s has permissions boundary that deny Amazon CloudWatch events. Resolve this by setting [“events:PutEvents”] to “Allow” for the EventBus arn:aws:events:region-1:123456789012:event-bus/default in your IAM instance profile permissions boundary.	

Sistema operativo

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S2001	Estado de los servicios de SQS	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
		a que el servicio de SQL Server no se ha iniciado. Puede resolver este problema reiniciando el servicio de SQL Server en el host. Si esta instancia de base de datos es una instancia de base de datos multi-AZ y se produce un error al reiniciarla, detenga e inicie el host para iniciar una conmutación por error.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S2002	Estado del agente de RDS Custom	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que el servicio del agente de RDS Custom no está instalado o no se ha podido iniciar. Puede resolver este problema consultando el registro de eventos de Windows para determinar por qué no se inicia el servicio y tomar las medidas adecuadas para solucionar el problema. Para obtener asistencia adicional, cree un caso de soporte.	Inicie sesión en el host y asegúrese de que el agente de RDS Custom está en ejecución.
			
			Puede utilizar los siguientes comandos para ver el estado del agente.
			
			`$name = "RDSCustomAgent"`
			`$service = Get-Service $name`
			`Write-Host $service.Status`
			
			Si el estado no es `Running`, puede iniciar el servicio con el comando siguiente:
			
			`Start-Service $name`
			
			Si el agente no puede iniciarse, consulte los eventos de Windows para ver por qué no se puede iniciar. El agente requiere que un usuario de Windows inicie el servicio. Asegúrese de que exista un usuario de Windows y de que tenga privilegios para ejecutar el servicio.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
`SP-S2003`	Estado del agente de SSM	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que no se puede llegar al servicio del agente de Amazon SSM. Para solucionar este problema, compruebe el estado del servicio con el comando de PowerShell `Get-Service AmazonSSMAgent` o inicie el servicio con `Start-Service AmazonSSMAgent` . Asegúrese de que se permita el tráfico saliente HTTPS (puerto 443) hacia los puntos de conexión regionales ssm, ssmmessages y ec2messages.	Para obtener información, consulte Solución de problemas de SSM Agent. Para solucionar problemas de puntos de conexión de SSM, consulte No es posible conectarse a los puntos de conexión de SSM y Use ssm-cli to troubleshoot managed node availability.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S2004	Inicio de sesión de agente de RDS Custom	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que se ha producido un problema inesperado con el inicio de sesión SQL "$HOSTNAME/RDSAgent" . Para resolver este problema, cree un caso de soporte.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S2005	Zona horaria	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que se ha cambiado la zona horaria de la instancia de Amazon EC2 [%s]. Puede resolver este problema modificando la zona horaria de nuevo a la configuración especificada durante la creación de la instancia . Si desea crear una instancia con una zona horaria específica, consulte la documentación de RDS Custom.	Ejecute el comando de PowerShell `Get-Timezone` para confirmar la zona horaria. Para obtener más información, consulte Zona horaria local para las instancias de base de datos de RDS Custom para SQL Server.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S2006	Versión de la solución de software de alta disponibilidad	El estado de la instancia de base de datos personalizada de RDS está establecido en [Configuración no compatible] debido a que la solución de software de alta disponibilidad de la instancia actual es diferente de la versión esperada. Para resolver este problema, cree un caso de soporte.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S2007	Configuración de la solución de software de alta disponibilidad	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que los ajustes de configuración de la solución de software de alta disponibilidad se han modificado a valores inesperados en la instancia %s. Para resolver este problema, reinicie la instancia EC2. Al reiniciar la instancia EC2, la configuración se actualiza automáticamente a la configuración requerida para la solución de software de alta disponibilidad.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S2008	Servicio SQL Server	La instancia de base de datos de RDS Custom está establecida en [Configuración no compatible]: el servicio SQL Server (MSSQLServer) no existe en el host. Para resolver esto, cree un caso de soporte.	Puede utilizar los siguientes comandos para ver el estado del agente.
			`$name = "MSSQLServer"`
			`$service = Get-Service $name`
			`Write-Host $service.Status`

SP-2009	SSL Certificate	La instancia de base de datos personalizada de RDS está establecida en [Configuración no admitida] debido a: Certificados SSL no autofirmados que causan interrupciones en RDS. Para resolver este problema, elimine los certificados que no estén autofirmados del almacén de certificados raíz de confianza.	Ejecute el siguiente comando de PowerShell para revisar los certificados que no estén autofirmados. `Get-ChildItem cert:\LocalMachine\root -Recurse | Where-Object {$_.Issuer -ne $_.Subject -and $_.Issuer -notlike "*RDSCustomAgentCA*"}` Para obtener más información, consulte Error HTTP 403.16 al intentar acceder a un sitio web alojado en IIS.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-2010	Estado de almacenamiento del volumen raíz	La instancia de base de datos de RDS Custom está establecida en [Configuración no compatible] debido a: el almacenamiento del volumen raíz está lleno. Para resolver este problema, libere al menos 500 MiB de espacio de almacenamiento en el volumen raíz de EBS "volume-id" o aumente el tamaño del volumen y cambie el tamaño de la unidad C de la instancia EC2 "instance-id". Los cambios en el tamaño del volumen raíz no persisten al reemplazar la instancia de EC2.	Utilice el siguiente comando para ver el almacenamiento disponible en el volumen raíz (C:). `(Get-PSDrive -Name C).Free / 1MB` Para obtener más información sobre cómo modificar el volumen raíz de EBS, consulte Cómo

Base de datos

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S3001	Protocolo de memoria compartida de SQL Server	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que el protocolo de memoria compartida de SQL Server está deshabilitado. Puede resolver este problema habilitando el protocolo de memoria compartida en el administrador de configuración de SQL Server.	Puede validarlo consultando: Administrador de configuración de SQL Server > Configuración de red de SQL Server > Protocolos para MSSQLSERVER > Memoria compartida como habilitada. Tras habilitar el protocolo, reinicie el proceso de SQL Server.
SP-S3002	Clave maestra de servicio	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que Automatización de RDS no puede realizar la copia de seguridad de la clave maestra de servicio (SMK) como parte de la nueva	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
		generación de SMK. Para resolver este problema, cree un caso de soporte.	
SP-S3003	Clave maestra de servicio	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que faltan los metadatos relacionados con la clave maestra de servicio (SMK) o están incompletos. Para resolver este problema, cree un caso de soporte.	

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S3004	Versión y edición del motor de base de datos	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que la versión y la edición esperadas de SQL Server no coinciden con la edición y la versión esperadas de SQL Server. Además, no se admite el cambio manual de la versión de SQL Server en la instancia de EC2 de RDS Custom. Para resolver este problema, cree un caso de soporte.	Ejecute la siguiente consulta para obtener la versión de SQL:
			`select @@version`
			Ejecute el siguiente comando AWS CLI para obtener la versión y la edición del motor SQL de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name |grep EngineVersion`
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name |grep Engine`
			Para obtener más información, consulte Modificación de una instancia de base de datos de RDS Custom for SQL Server y Actualización de una versión del motor de una instancia de base de datos.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S3005	Edición del motor de base de datos	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que la edición actual de SQL Server no coincide con la edición esperada de SQL Server [%s]: no se admite la modificación de la edición de SQL Server en RDS Custom for SQL Server. Para resolver este problema, cree un caso de soporte.	Ejecute la siguiente consulta para obtener la edición de SQL:
			Example
			`select @@version`
			Ejecute el siguiente comando AWS CLI para obtener la edición del motor SQL de RDS:
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name |grep Engine`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S3006	Versión del motor de la base de datos	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que la versión actual de SQL Server no coinciden con la versión esperada de SQL Server [%s]: no puede cambiar la versión de SQL Server manualmente en la instancia EC2 de RDS Custom. Para resolver este problema, cree un caso de soporte. Para cualquier modificación futura de la versión de SQL Server, puede modificar la instancia desde la consola de AWS RDS o mediante el comando de CLI modify-db-instance.	Ejecute la siguiente consulta para obtener la versión de SQL:
			
			Example
			
			`select @@version`
			
			Ejecute el siguiente comando AWS CLI para obtener la versión del motor SQL de RDS:
			
			`aws rds describe-db-instances \ --db-instance-identifier db-instance-name |grep EngineVersion`
			
			Para obtener más información, consulte Modificación de una instancia de base de datos de RDS Custom for SQL Server y Actualización de una versión del motor de una instancia de base de datos.

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación

SP-S3007	Ubicación de archivo de base de datos	El estado de la instancia de base de datos de RDS Custom está establecido en [Configuración no compatible] debido a que los archivos de base de datos se configuran fuera de la unidad D:\. Para resolver este problema, asegúrese de que todos los archivos de la base de datos, incluidos ROW, LOG, FILESTREAM, etc., estén almacenados en la unidad D:\.	Ejecute la siguiente consulta para ver la ubicación de los archivos de base de datos que no estén en la ruta predeterminada:
			`USE master;`
			`SELECT physical_name as files_not_in_default_path`
			`FROM sys.master_files`
			`WHERE SUBSTRING(physical_name,1,3)!='D:\';`

Código de evento	Área de configuración	Mensaje de evento de RDS	Proceso de validación
SP-S3008	Se ha superado el límite de bases de datos	The RDS Custom DB instance status is set to [Unsupported configuration] because of: The total number of databases on the DB instance exceeds the maximum limit of 5000. To resolve this, reduce the number of databases below the maximum supported limit.	Utilice el siguiente comando para ver el recuento total de bases de datos: `SELECT COUNT(name) as databaseCount FROM sys.databases WHERE name not in ('tempdb','master','model','msdb','DWDiagnostics','DWConfiguration','DWQueue');`

Solución de problemas **`Storage-Full`** en RDS Custom para SQL Server

RDS Custom también supervisa el volumen raíz (C:). La instancia de base de datos de RDS Custom para SQL Server se mueve al estado `unsupported-configuration` cuando el volumen raíz tiene menos de 500 MiB de espacio en disco disponible. Consulte `Event SP-S2010` en Corrección de configuraciones no compatibles en RDS Custom para SQL Server.

Resolución del problema PENDING_RECOVERY en bases de datos habilitadas para TDE en RDS Custom para SQL Server

Las bases de datos de SQL Server con el cifrado de datos transparente (TDE) activado pueden permanecer en el estado `PENDING_RECOVERY` si hay algún problema con el descifrado automático. Esto suele ocurrir después de la restauración de una instancia de base de datos si el archivo de copia de seguridad de la clave maestra de servicio (SMK) de la instancia de base de datos de origen almacenado en el bucket de S3 administrado por RDS Custom de su cuenta se ha eliminado antes de que se complete la restauración.

Para habilitar el descifrado automático y poner en línea las bases de datos compatibles con TDE, debe abrir la clave maestra de base de datos (DMK) con su contraseña y cifrar la DMK mediante la SMK.

Utilice los siguientes comandos de SQL Server como referencia:

```
-- Identify PENDING_RECOVERY TDE databases
USE MASTER;
GO
SELECT name, is_encrypted, state_desc FROM sys.databases;
GO

-- Open DMK using password
OPEN MASTER KEY DECRYPTION BY PASSWORD = '<password>';
GO

-- Encrypt DMK using SMK
ALTER MASTER KEY ADD ENCRYPTION BY SERVICE MASTER KEY;
GO

-- Close SMK
CLOSE MASTER KEY;
GO

-- Bring the TDE databases online
ALTER DATABASE <database_name> SET ONLINE;
GO

-- Verify TDE databases are now in ONLINE state
SELECT name, is_encrypted, state_desc FROM sys.databases;
GO
```

Amazon RDS en AWS Outposts

Amazon RDS en AWS Outposts amplía RDS para las bases de datos de SQL Server, RDS para MySQL y RDS para PostgreSQL a entornos de Gen1 y Gen2 de bastidor de AWS Outposts. AWS Outposts utiliza el mismo hardware que en las Regiones de AWS públicas para ofrecer servicios, infraestructuras y modelos de operación de AWS en las instalaciones. Con RDS en Outposts, puede aprovisionar instancias de base de datos administradas cercanas a las aplicaciones empresariales que deben ejecutarse en las instalaciones. Para obtener más información acerca de AWS Outposts, consulte la documentación de AWS Outposts y la página del producto AWS Outposts.

Utilice la misma AWS Management Console, la AWS CLI y la API de RDS para aprovisionar y administrar instancias de base de datos de RDS en Outposts en las instalaciones como para instancias de base de datos de RDS que se ejecutan en Nube de AWS. RDS on Outposts automatiza tareas, como el aprovisionamiento de base de datos, la aplicación de parches de sistema operativo y base de datos, la copia de seguridad y el archivado a largo plazo en Amazon S3.

RDS en Outposts admite copias de seguridad automatizadas de instancias de base de datos. Es obligatoria la conectividad de red entre su Outpost y su Región de AWS para realizar copias de seguridad y restaurar instancias de bases de datos. Todas las instantáneas de bases de datos y los registros de transacciones de un Outpost se almacenan en la Región de AWS. Desde la región de AWS, puede restaurar una instancia de base de datos desde una instantánea de base de datos a un Outpost diferente. Para obtener más información, consulte Introducción a las copias de seguridad.

RDS en Outposts admite el mantenimiento automatizado y las actualizaciones de las instancias de bases de datos. Para obtener más información, consulte Mantenimiento de una instancia de base de datos.

RDS on Outposts utiliza cifrado en reposo para las instancias de base de datos y las instantáneas de base de datos mediante su AWS KMS key. Para obtener más información sobre el cifrado en reposo, consulte Cifrado de recursos de Amazon RDS.

De forma predeterminada, las instancias EC2 de las subredes Outposts pueden utilizar el servicio Amazon Route 53 DNS para resolver nombres de dominio en direcciones IP. Es posible que encuentre tiempos de resolución de DNS más largos con Route 53, según la latencia de ruta entre Outpost y la Región de AWS. En tales casos, puede utilizar los servidores DNS instalados localmente en su entorno en las instalaciones. Para obtener más información, consulte DNS en la Guía del usuario de AWS Outposts.

Cuando la conectividad de red con la Región de AWS no está disponible, la instancia de base de datos continúa ejecutándose localmente. Puede acceder a instancias de base de datos mediante la resolución de nombres DNS al configurar un servidor DNS local como servidor secundario. Sin embargo, no puede crear nuevas instancias de base de datos ni modificar instancias de base de datos existentes. Las copias de seguridad automáticas no se producen cuando no hay conectividad. Si hay un error de instancia de base de datos, la instancia de base de datos no se reemplaza automáticamente hasta que se restablece la conectividad. Recomendamos restaurar la conectividad de red lo antes posible.

Temas

- Requisitos previos de Amazon RDS on AWS Outposts
- Compatibilidad de Amazon RDS on AWS Outposts para características de Amazon RDS
- Clases de instancia de base de datos compatibles con Amazon RDS on AWS Outposts
- Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts
- Trabajo con implementaciones Multi-AZ para Amazon RDS on AWS Outposts
- Creación de instancias de base de datos para Amazon RDS on AWS Outposts
- Creación de réplicas de lectura para Amazon RDS en AWS Outposts
- Consideraciones para restaurar instancias de base de datos en Amazon RDS en AWS Outposts

Requisitos previos de Amazon RDS on AWS Outposts

A continuación, se indican los requisitos previos para utilizar Amazon RDS on AWS Outposts:

- Instale AWS Outposts en su centro de datos en las instalaciones. Para obtener más información, consulte Installing an AWS Outposts server en la Guía de instalación del servidor de AWS Outposts.
- Asegúrese de que tiene al menos una subred disponible para RDS en Outposts. Puede utilizar la misma subred para otras cargas de trabajo.
- Asegúrese de que tiene una conexión de red de confianza entre su Outpost y una región de AWS.

Compatibilidad de Amazon RDS on AWS Outposts para características de Amazon RDS

La siguiente tabla describe las funciones de Amazon RDS admitidas por Amazon RDS en AWS Outposts.

Característica	Soportado	Notas	Más información

Aprovisionamiento de instancias de base de datos	Sí	Solo puede crear instancias de base de datos para motores de RDS for PostgreSQL base de datos RDS for SQL ServerRDS for MySQL,, y. Las siguientes versiones son compatibles:
		• Microsoft SQL Server:
		  • Versiones 15.00.4043.16.v1 y posteriores a la 2019
		  • Versiones 14.00.3294.2.v1 y posteriores a la 2017
		  • Versiones 13.00.5820.21.v1 y posteriores a la 2016
		• Todas las versiones de MySQL 8.0 y 8.4
		• Todas las versiones de PostgreSQL 16, 15, 14 y 13, y las versiones de PostgreSQL 12.5 y versiones posteriores de PostgreSQL 12
			Creación de instancias de base de datos para Amazon RDS on AWS Outposts

Característica	Soportado	Notas	Más información
Conectar una instancia de base de datos de Microsoft SQL Server con Microsoft SQL Server Management Studio	Sí	Es posible que algunas versiones TLS y cifrados de cifrado no sean seguras. Para desactiva rlos, siga las instrucciones en???.	Conexión a la instancia de base de datos de Microsoft SQL Server
Modificación de la contraseña del usuario principal	Sí	Ninguno	Modificación de una instancia de base de datos de Amazon RDS
Cambio del nombre de una instancia de base de datos	Sí	Ninguno	Modificación de una instancia de base de datos de Amazon RDS
Reinicio de una instancia de base de datos	Sí	Ninguno	Reinicio de una instancia de base de datos
Parar una instancia de base de datos	Sí	Ninguno	Parada de una instancia de base de datos de Amazon RDS temporalmente
Comienzo de una instancia de base de datos	Sí	Ninguno	Inicio de una instancia de base de datos de Amazon RDS parada previamente

Característica	Soportado	Notas	Más información
Implementaciones Multi-AZ	Sí	Las implementaciones Multi-AZ se admiten en instancias de base de datos de MySQL y PostgreSQL. Las implementaciones Multi-AZ no admiten el enrutamiento directo de VPC (DVR).	Creación de instancias de base de datos para Amazon RDS on AWS Outposts Configuración y administración de una implementación multi-AZ para Amazon RDS
Grupos de parámetros de base de datos	Sí	Ninguno	Grupos de parámetros para Amazon RDS
Réplicas de lectura	Sí	Las réplicas de lectura se admiten en instancias de base de datos de MySQL y PostgreSQL. Las réplicas de lectura no admiten el enrutamiento directo de VPC (DVR).	Creación de réplicas de lectura para Amazon RDS en AWS Outposts
Cifrado en reposo	Sí	RDS en Outposts no admite instancias de base de datos no cifradas.	Cifrado de recursos de Amazon RDS
AWS Identity and Access Managemen tAutenticación de base de datos de (IAM)	No	Ninguno	Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL

Característica	Soportado	Notas	Más información
Asociación de un rol de IAM con una instancia de base de datos	No	Ninguno	Comando de la AWS CLI add-role-to-db-instance Operación de la API de RDS AddRoleToDBInstance
Autenticación de Kerberos	No	Ninguno	Autenticación Kerberos
Etiquetado de recursos de Amazon RDS	Sí	Ninguno	Etiquetado de los recursos de y Amazon RDS
Grupos de opciones	Sí	Ninguno	Trabajo con grupos de opciones
Modificación del periodo de mantenimiento	Sí	Ninguno	Mantenimiento de una instancia de base de datos
Actualización de versiones secundarias automáticas	Sí	Ninguno	Actualización automática de la versión secundaria del motor
Modificación del periodo de copia de seguridad	Sí	Ninguno	Introducción a las copias de seguridad Modificación de una instancia de base de datos de Amazon RDS
Cambiar la clase de instancia de base de datos	Sí	Ninguno	Modificación de una instancia de base de datos de Amazon RDS

Característica	Soportado	Notas	Más información
Cambio del almacenamiento asignado	Sí	Ninguno	Modificación de una instancia de base de datos de Amazon RDS
Storage autoscaling (Escalado automático de almacenamiento)	Sí	Ninguno	Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS
Instantáneas de instancias de base de datos manuales y automáticas	Sí	Puede almacenar copias de seguridad automatizadas e instantáneas manuales en su Región de AWS. O puede almacenarlos de forma local en su Outpost. Las copias de seguridad locales se admiten en instancias de base de datos de MySQL y PostgreSQL. Para almacenar copias de seguridad en el Outpost, asegúrese de tener configurado Amazon S3 en Outposts. No se admiten las copias de seguridad locales de las implementaciones de instancias Multi-AZ.	Creación de instancias de base de datos para Amazon RDS on AWS Outposts Amazon S3 en Outposts Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS

Característica	Soportado	Notas	Más información
Restauración desde una instantánea de base de datos	Sí	Puede almacenar copias de seguridad automatizadas e instantáneas manuales para la instancia de base de datos restaurada en la Región de AWS principal o de manera local en su Outpost.	Consideraciones para restaurar instancias de base de datos en Amazon RDS en AWS Outposts Restauración a una instancia de base de datos
Restauración de una instancia de base de datos desde Amazon S3	No	Ninguno	Restauración de una copia de seguridad en una instancia de base de datos MySQL.
Exportación de datos de instantáneas a Amazon S3	No	Ninguno	Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS
Recuperación a un momento dado	Sí	Puede almacenar copias de seguridad automatizadas e instantáneas manuales para la instancia de base de datos restaurada en la Región de AWS principal o de manera local en su Outpost, con una excepción.	Consideraciones para restaurar instancias de base de datos en Amazon RDS en AWS Outposts Restauración de una instancia de base de datos a un momento especificado para Amazon RDS
Enhanced monitoring (Supervisión mejorada)	No	Ninguno	Supervisión de las métricas del sistema operativo con Supervisión mejorada

Característica	Soportado	Notas	Más información
Monitoreo de Amazon CloudWatch	Sí	Puede ver el mismo conjunto de métricas que están disponibles para las bases de datos de la Región de AWS.	Supervisión de métricas de Amazon RDS con Amazon CloudWatch
Publicación de registros del motor de base de datos en CloudWatch Logs	Sí	Ninguno	Publicación de registros de base de datos en registros de Amazon Cloudwatch
Notificación de eventos	Sí	Ninguno	Uso de notificaciones de eventos de Amazon RDS
Información de rendimiento de Amazon RDS	No	Ninguno	Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS

Característica	Soportado	Notas	Más información
Visualización o descarga de registros de bases de datos	No	RDS en Outposts no admite la visualización de los registros de la base de datos mediante la consola ni la descripción de los registros de la base de datos mediante AWS CLI o la API de RDS. RDS en Outposts no admite la descarga de registros de base de datos mediante la consola ni la descarga de registros de base de datos mediante AWS CLI o la API de RDS.	Supervisión de archivos de registro de Amazon RDS
Amazon RDS Proxy	No	Ninguno	Amazon RDS Proxy
Procedimientos almacenados para Amazon RDS for MySQL	Sí	Ninguno	Referencia de procedimientos almacenados de RDS para MySQL
Replicación con bases de datos externas para RDS for MySQL	No	Ninguno	Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Característica	Soportado	Notas	Más información
Copia de seguridad y restauración nativas para Amazon RDS for Microsoft SQL Server	Sí	Ninguno	Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas

Clases de instancia de base de datos compatibles con Amazon RDS on AWS Outposts

Amazon RDS on AWS Outposts admite las siguientes clases de instancia de base de datos:

- Clases de instancia de base de datos de uso general
  - db.m7i.48xlarge
  - db.m7i.24xlarge
  - db.m7i.16xlarge
  - db.m7i.12xlarge
  - db.m7i.8xlarge
  - db.m7i.4xlarge
  - db.m7i.2xlarge
  - db.m7i.xlarge
  - db.m7i.large
  - db.m5.24xlarge
  - db.m5.16xlarge
  - db.m5.12xlarge
  - db.m5.8xlarge
  - db.m5.4xlarge
  - db.m5.2xlarge
  - db.m5.xlarge

  - db.m5.large
- Clases de instancia de base de datos optimizadas para memoria
  - db.r7i.48xlarge
  - db.r7i.24xlarge
  - db.r7i.16xlarge
  - db.r7i.12xlarge
  - db.r7i.8xlarge
  - db.r7i.4xlarge
  - db.r7i.2xlarge
  - db.r7i.xlarge
  - db.r7i.large
  - db.r5.24xlarge
  - db.r5.16xlarge
  - db.r5.12xlarge
  - db.r5.8xlarge
  - db.r5.4xlarge
  - db.r5.2xlarge
  - db.r5.xlarge
  - db.r5.large

Según cómo haya configurado su Outpost, es posible que no tenga todas estas clases disponibles. Por ejemplo, si no ha comprado las clases db.r5 para su Outpost, no puede usarlas con RDS en Outposts.

Solo el almacenamiento de SSD de uso general es compatible con las instancias de base de datos de RDS en Outposts. Para obtener más información acerca de las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

Amazon RDS administra el mantenimiento y la recuperación de las instancias de base de datos y requiere capacidad activa en el Outpost para hacerlo. Se recomienda configurar instancias N+1 EC2 destinadas a cada clase de instancia de base de datos en los entornos de producción. RDS on Outposts puede utilizar la capacidad adicional de estas instancias EC2 para operaciones de mantenimiento y reparación. Por ejemplo, si los entornos de producción tienen 3 clases de instancia

de base de datos db.m5.large y 5 db.r5.xlarge, se recomienda que tengan al menos 4 instancias de EC2 m5.large y 6 instancias de EC2 r5.xlarge. Para obtener más información, consulte Resiliencia en AWS Outposts en la Guía del usuario de AWS Outposts.

Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts

Amazon RDS en AWS Outposts utiliza la información que proporciona acerca de la red en las instalaciones para crear un grupo de direcciones. Este grupo se conoce como grupo de direcciones IP propiedad del cliente (grupo CoIP). Las direcciones IP propiedad del cliente (CoIP) proporcionan conectividad local o externa a los recursos de sus subredes Outpost a través de su red local. Para obtener más información sobre los CoIP, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts.

Cada instancia de base de datos RDS en Outposts tiene una dirección IP privada para el tráfico dentro de su nube privada virtual (VPC). Esta dirección IP privada no es accesible públicamente. Puede utilizar la opción Público para definir si la instancia de base de datos también tiene una dirección IP pública además de la dirección IP privada. El uso de la dirección IP pública para las conexiones las dirige a través de Internet y puede dar lugar a altas latencias en algunos casos.

En lugar de utilizar estas direcciones IP privadas y públicas, RDS en Outposts admite el uso de CoIP para instancias de base de datos a través de sus subredes. Cuando usa un CoIP para una instancia de base de datos de RDS en Outposts, se conecta a la instancia de base de datos con el punto de enlace de la instancia de base de datos. RDS on Outposts utiliza después automáticamente el CoIP para todas las conexiones desde dentro y fuera de la VPC.

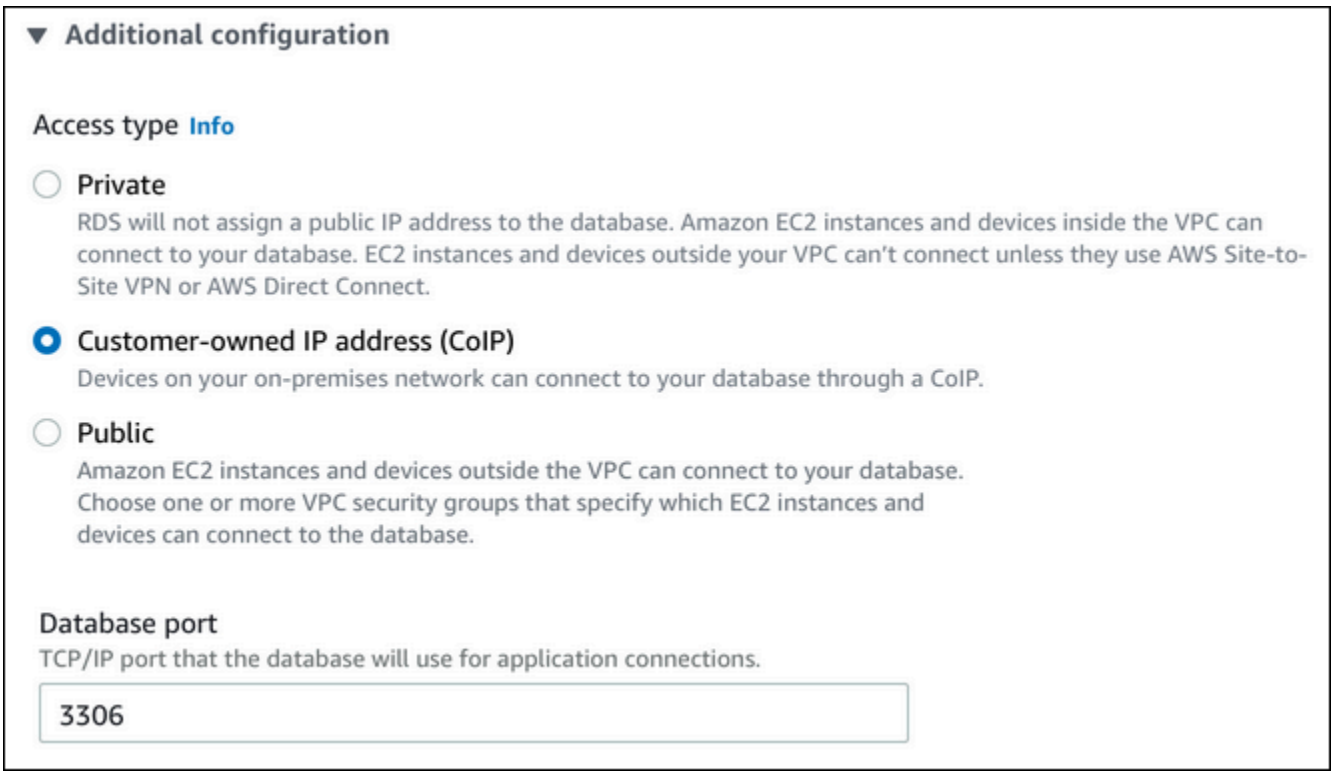
Las CoIP pueden proporcionar los siguientes beneficios para las instancias de base de datos de RDS en Outposts:

- Baja latencia de conexión
- Más seguridad

Uso de CoIP

Puede activar una CoIP para una instancia de base de datos de RDS on Outposts mediante la AWS Management Console, la AWS CLI, o la API de RDS:

- Con la AWS Management Console, elija la Dirección IP propiedad del cliente (CoIP) en Tipo de acceso para usar una CoIP. Elige uno de los otros ajustes para desactivarlas.



- Con la AWS CLI, utilice la opción `--enable-customer-owned-ip | --no-enable-customer-owned-ip`.
- Con la API de RDS, utilice el parámetro `EnableCustomerOwnedIp`.

Puede activar o desactivar una CoIP cuando realice cualquiera de las siguientes acciones:

- Crear una instancia de base de datos

  Para obtener más información, consulte Creación de instancias de base de datos para Amazon RDS on AWS Outposts.
- Modificar una instancia de base de datos

  Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Crear una réplica de lectura

  Para obtener más información, consulte Creación de réplicas de lectura para Amazon RDS en AWS Outposts.
- Restaurar una instancia de base de datos a partir de una instantánea

Para obtener más información, consulte Restauración a una instancia de base de datos.

- Restaurar una instancia de base de datos a un momento especificado

  Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

> **Note**
>
> En algunos casos, puede activar los CoIP para una instancia de base de datos, pero Amazon RDS no puede asignar un CoIP para la instancia de base de datos. En esos casos, el estado de la instancia de base de datos cambia a red incompatible. Para obtener más información acerca del estado de la instancia de base de datos, consulte Visualización del estado de la instancia de base de datos de en un clúster de Aurora.

Limitaciones

Las siguientes limitaciones se aplican a la compatibilidad con CoIP para instancias de base de datos de RDS en Outposts:

- Cuando se usa una CoIP para una instancia de base de datos, asegúrese de que la accesibilidad pública esté desactivada para la instancia de base de datos.
- Asegúrese de que las reglas de entrada de los grupos de seguridad de VPC incluyan el rango de direcciones CoIP (bloque CIDR). Para obtener más información acerca de la configuración de grupos de seguridad, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.
- No puede asignar una CoIP desde un grupo CoIP a una instancia de base de datos. Cuando usa una CoIP para una instancia de base de datos, Amazon RDS asigna automáticamente una CoIP de un grupo CoIP a la instancia de base de datos.
- Debe utilizar la Cuenta de AWS propietaria de los recursos de Outpost (propietario) o compartir los siguientes recursos con otras Cuentas de AWS (consumidores) de la misma organización.
  - El Outpost
  - La tabla de rutas de la puerta de enlace local (LGW) para la VPC de la instancia de base de datos
  - El grupo o grupos CoIP para la tabla de rutas de la LGW

Para obtener más información, consulte Trabajo con recursos compartidos de AWS Outposts en la Guía del usuario de AWS Outposts.

Trabajo con implementaciones Multi-AZ para Amazon RDS on AWS Outposts

Para implementaciones Multi-AZ, Amazon RDS crea una instancia de base de datos principal en un Outpost de AWS. RDS replica sincrónicamente los datos en una instancia de base de datos en espera en un Outpost diferente.

Las implementaciones Multi-AZ en AWS Outposts operan como implementaciones Multi-AZ en Regiones de AWS, pero con las siguientes diferencias:

- Requieren una conexión local entre dos o más Outposts.
- Requieren grupos IP propiedad del cliente (CoIP). Para obtener más información, consulte Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts.
- La replicación se ejecuta en la red local.

Multi-AZ on AWS Outposts está disponible para todas las versiones compatibles de MySQL y PostgreSQL en RDS on Outposts. No se admiten las copias de seguridad locales de las implementaciones Multi-AZ. Para obtener más información, consulte Creación de instancias de base de datos para Amazon RDS on AWS Outposts.

Trabajo con el modelo de responsabilidad compartida

Aunque AWS hace los esfuerzos comercialmente razonables para proporcionar instancias de base de datos configuradas para una alta disponibilidad, la disponibilidad utiliza un modelo de responsabilidad compartida. La capacidad de RDS on Outposts de conmutación por error y reparación de instancias de base de datos requiere que cada uno de los Outposts esté conectado a su Región de AWS.

RDS on Outposts también requiere conectividad entre el Outpost que aloja la instancia de base de datos principal y el Outpost que aloja la instancia de base de datos en espera para la replicación sincrónica. Cualquier impacto en esta conexión puede impedir que RDS on Outposts realice una conmutación por error.

Pueden producirse latencias elevadas para una implementación de instancia de base de datos estándar como resultado de la replicación de datos sincrónica. El ancho de banda y la latencia de la conexión entre Outpost que aloja la instancia de base de datos principal y el Outpost que aloja la instancia de base de datos en espera afectan directamente a las latencias. Para obtener más información, consulte Requisitos previos.

Mejora de la disponibilidad

Le recomendamos que utilice las siguientes acciones para mejorar la disponibilidad:

- Asigne suficiente capacidad adicional para sus aplicaciones de misión crítica para permitir la recuperación y la conmutación por error si se produce un problema de host subyacente. Esto se aplica a todos los Outposts avanzados que contienen subredes de su grupo de subredes de base de datos. Para obtener más información, consulte Resiliencia en AWS Outposts.
- Proporcione conectividad de red redundante para sus Outpost.
- Utilice más de dos Outposts. Tener más de dos Outposts permite a Amazon RDS recuperar una instancia de base de datos. RDS realiza esta recuperación trasladando la instancia de base de datos a otro Outpost si el Outpost actual tiene un error.
- Proporcione fuentes de alimentación duales y conectividad de red redundante para su Outpost.

Le recomendamos lo siguiente para las redes locales:

- La latencia del tiempo de ida y vuelta (RTT) entre Outpost que aloja su instancia de base de datos principal y la Outpost que aloja su instancia de base de datos en espera afecta directamente a la latencia de escritura. Mantenga la latencia de RTT entre el Outposts de AWS en milisegundos bajos de un solo dígito. Recomendamos no más de 5 milisegundos, pero sus requisitos pueden variar.

  Puede encontrar el impacto neto en la latencia de red en las métricas de Amazon CloudWatch para `WriteLatency`. Para obtener más información, consulte Métricas de Amazon CloudWatch para Amazon RDS.
- La disponibilidad de la conexión entre los Outposts afecta a la disponibilidad general de las instancias de base de datos. Tenga conectividad de red redundante entre los Outposts.

Requisitos previos

Las implementaciones Multi-AZ en RDS on Outposts tienen los siguientes requisitos previos:

- Tener al menos dos Outposts, conectados a través de conexiones locales y conectados a diferentes zonas de disponibilidad en una Región de AWS.
- Asegúrese de que los grupos de subredes de base de datos contengan lo siguiente:
  - Al menos dos subredes y en al menos dos zonas de disponibilidad en una Región de AWS dada.

  - Subredes solo en Outposts.
  - Al menos dos subredes en al menos dos Outposts dentro de la misma nube privada virtual (VPC).
- Asocie la VPC de su instancia de base de datos a todas las tablas de enrutamiento de la puerta de enlace local. Esta asociación es necesaria porque la replicación se ejecuta a través de la red local mediante las puertas de enlace locales de Outposts.

  Por ejemplo, supongamos que la VPC contiene la subred A en la salida A y la subred B en Outpost-B. Outpost A utiliza LocalGateway-A (LGW-A) y Outpost-B utiliza LocalGateway-B (LGW-B). LGW-A tiene la tabla de enrutamiento A y LGW-B tiene la tabla de enrutamiento B. Utilice RouteTable-A y RouteTable-B para el tráfico de replicación. Para ello, asocie su VPC con RouteTable-A y RouteTable-B.

  Para obtener más información sobre cómo crear una asociación, consulte el comando de la AWS CLI de Amazon EC2 create-local-gateway-ruta-table-vpc-association.
- Asegúrese de que los Outposts utilicen enrutamiento IP propiedad del cliente (CoIP). Cada tabla de rutas también debe tener al menos un grupo de direcciones. Amazon RDS asigna una dirección IP adicional para las instancias de base de datos principal y en espera para la sincronización de datos.
- Asegúrese deCuenta de AWS que la propietaria de las instancias de base de datos de RDS es propietaria de las tablas de enrutamiento de la puerta de enlace local y los grupos CoIP. O forma parte de un recurso compartido de Resource Access Manager con acceso a las tablas de enrutamiento de la puerta de enlace local y a los grupos CoIP.
- Asegúrese de que las direcciones IP de sus grupos CoIP se puedan enrutar desde una puerta de enlace local Outpost a las demás.
- Asegúrese de que los bloques CIDR de la VPC (por ejemplo, 10.0.0.0/4) y los bloques CIDR del grupo CoIP no contengan direcciones IP de la clase E (240.0.0.0/4). RDS utiliza estas direcciones IP internamente.
- Asegúrese de configurar correctamente el tráfico entrante y saliente relacionado.

  RDS on Outposts establece una conexión de red privada virtual (VPN) entre las instancias de base de datos principal y en espera. Para que esto funcione correctamente, la red local debe permitir el tráfico entrante y saliente relacionado para Internet Security Association and Key Management Protocol (ISAKMP). Lo hace en el puerto 500 del Protocolo de datagrama de usuario (UDP) y la transferencia de traducción de direcciones de red (NAT-T) de seguridad IP (IPSec) en el puerto UDP 4500.

Para obtener más información sobre los CoIP, consulte Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts en esta guía y Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts.

Trabajo con operaciones de la API para permisos de Amazon EC2

Independientemente de si utiliza COIP para su instancia de base de datos en AWS Outposts, RDS requiere acceso a los recursos del grupo CoIP. RDS puede llamar a las siguientes operaciones de API de permisos de EC2 para COIP en implementaciones Multi-AZ:

- `CreateCoipPoolPermission`: cuando crea una instancia de base de datos Multi-AZ en RDS on Outposts
- `DeleteCoipPoolPermission`: cuando elimina una instancia de base de datos Multi-AZ en RDS on Outposts

Estas operaciones de API otorgan el permiso (o lo eliminan) a las cuentas RDS internas para asignar direcciones IP elásticas del grupo CoIP especificado por el permiso. Puede ver estas direcciones IP mediante la operación de API `DescribeCoipPoolUsage`. Para obtener más información sobre los CoIP, consulte Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts y Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts.

RDS también puede llamar a las siguientes operaciones de API de permisos de EC2 para tablas de enrutamiento de puerta de enlace local en implementaciones Multi-AZ:

- `CreateLocalGatewayRouteTablePermission`: cuando crea una instancia de base de datos Multi-AZ en RDS on Outposts
- `DeleteLocalGatewayRouteTablePermission`: cuando elimina una instancia de base de datos Multi-AZ en RDS on Outposts

Estas operaciones de API otorgan (o eliminan) a las cuentas de RDS internas el permiso para asociar VPC RDS internas a las tablas de enrutamiento de la puerta de enlace local. Puede ver estas asociaciones de VPC de tablas de enrutamiento con las operaciones de la API `DescribeLocalGatewayRouteTableVpcAssociations`

Creación de instancias de base de datos para Amazon RDS on AWS Outposts

La creación de una instancia de base de datos de Amazon RDS on AWS Outposts es similar a la creación de una instancia de base de datos de Amazon RDS en la nube de AWS. Sin embargo, debe asegurarse de especificar un grupo de subredes de base de datos asociada a su Outpost.

Una nube virtual privada (VPC) basada en el servicio de Amazon VPC puede abarcar todas las zonas de disponibilidad en una Región de AWS. Puede ampliar cualquier VPC de la Región de AWS al Outpost al agregar una subred de Outpost. Para agregar una subred de Outpost a una VPC, especifique el nombre de recurso de Amazon (ARN) del Outpost al crear la subred.

Antes de crear una instancia de base de datos de RDS en Outposts, puede crear un grupo de subredes de base de datos que incluya una subred asociada a su Outpost. Al crear una instancia de base de datos de RDS en Outposts, debe especificar este grupo de subredes de base de datos. También puede elegir crear un nuevo grupo de subred de base de datos al crear la instancia de base de datos.

Para obtener información acerca de la configuración de AWS Outposts, consulte la Guía del usuario de AWS Outposts.

Consola

Creación de un grupo de subredes de base de datos

Cree un grupo de subredes de base de datos con una subred asociada a su Outpost.

También puede crear un nuevo grupo de subred de base de datos al crear la instancia de base de datos. Si desea hacerlo, omita este procedimiento.

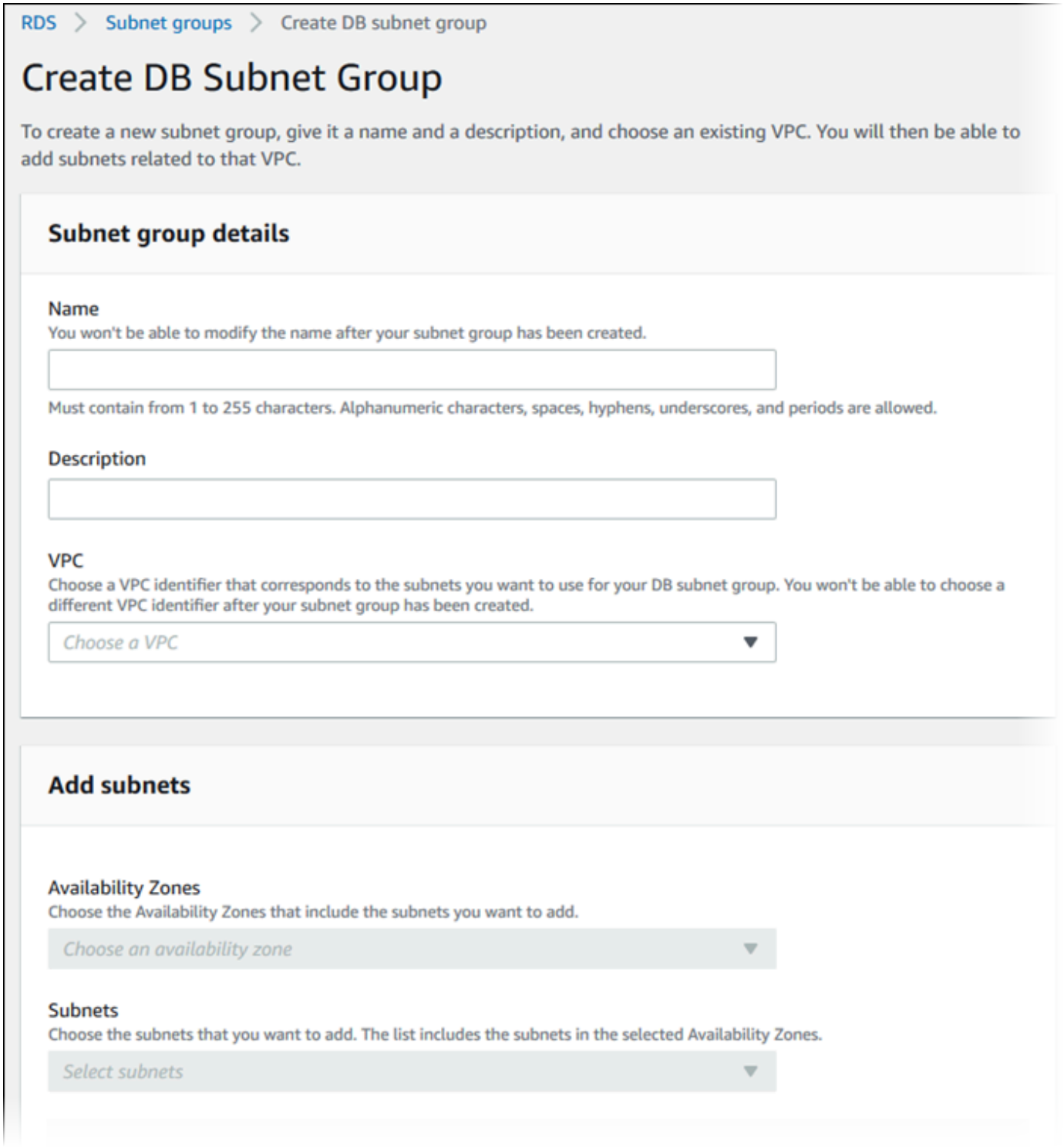
> **Note**
>
> Para crear un grupo de subredes de base de datos para Nube de AWS, debe especificar al menos dos subredes.

Para crear un grupo de subredes de base de datos para el Outpost

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear el grupo de subred de base de datos.
3. Elija Subnet Groups (Grupos de subredes) y, a continuación, elija Create DB Subnet Group (Crear grupo de subredes de base de datos).

   Aparece la página Create DB subnet group (Crear grupo de subredes de base de datos).



4. Para Name (Nombre), elija el nombre del grupo de subredes de base de datos.
5. Para Description (Descripción), elija una descripción del grupo de subredes de base de datos.
6. Para VPC, elija la VPC para la que está creando el grupo de subredes de base de datos.
7. En Availability Zones (Zonas de disponibilidad), elija la zona de disponibilidad de su Outpost.

8. En Subnets (Subredes), elija la subred que va a utilizar RDS en Outposts.
9. Elija Create (Crear) para crear el grupo de subredes de base de datos.

Creación de una instancia de base de datos de RDS en Outposts

Cree la instancia de base de datos y elija Outpost para su instancia de base de datos.

Para crear una instancia de base de datos de RDS en Outposts mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Elija Create database (Crear base de datos).

   La AWS Management Console detecta Outposts disponibles que ha configurado y presenta la opción Local en la sección Database location (Ubicación de la base de datos).

   > **Note**
   >
   > Si no ha configurado ningún Outpost, la sección Database location (Ubicación de la base de datos) no aparece ni la opción RDS on Outposts (RDS en Outposts) está disponible en la sección Choose an on-premises creation method (Elección de un método de creación en las instalaciones).

5. Para Database location (Ubicación de la base de datos), elija On-premise (En las instalaciones).
6. Para On-premises creation method (Método de creación en las instalaciones), elija RDS en Outposts.
7. Especifique la configuración de Outposts Connectivity (Conectividad de Outposts). Esta configuración es para el Outpost que utiliza la VPC que tiene el grupo de subredes de base de datos para la instancia de base de datos. Su VPC tiene que basarse en el servicio de Amazon VPC.

   a. Para Virtual Private Cloud (VPC) (Nube virtual privada [VPC]), elija la VPC que contiene el grupo de subredes de base de datos para la instancia de base de datos.

b. Para VPC security group (Grupo de seguridad de VPC), elija el grupo de seguridad de Amazon VPC para la instancia de base de datos.

c. Para DB subnet group (Grupo de subredes de base de datos), elija el grupo de subredes de base de datos para la instancia de base de datos.

   Puede seleccionar un grupo de subredes de base de datos existente que esté asociado al Outpost; por ejemplo, si ha realizado el procedimiento en Creación de un grupo de subredes de base de datos.

   También puede crear un nuevo grupo de subred de base de datos para el Outpost.

8. Para Multi-AZ deployment (Implementación Multi-AZ), elija Create a standby instance (recommended for production usage) (Creación de una instancia en espera (recomendada para uso de producción) para crear una instancia de base de datos en espera en otro Outpost.

> **Note**
>
> Esta opción no está disponible para Microsoft SQL Server.
> Si elige crear una implementación Multi-AZ, no puede almacenar copias de seguridad en Outpost.

9. En Backup (Copia de seguridad), haga lo siguiente:

   a. Para Backup target (Valor de destino), elija una de las siguientes opciones:

      - Nube de AWS para almacenar copias de seguridad automatizadas e instantáneas manuales en la Región de AWS principal.
      - Outposts (on-premises) (Outposts en las instalaciones) para crear copias de seguridad locales.

> **Note**
>
> Para almacenar copias de seguridad en el Outpost, el Outpost debe tener capacidad de Amazon S3. Para obtener más información, consulte Uso de Amazon S3 en Outposts.
> No se admiten las copias de seguridad locales de las implementaciones Multi-AZ o las réplicas de lectura.

b. Elija Enable automated backups (Habilitar las copias de seguridad) para crear instantáneas de un momento dado de la instancia de base de datos.

   Si habilita las copias de seguridad automatizadas, puede elegir la opción Backup retention period (Periodo de retención de copia de seguridad) y Backup window (Margen de copia de seguridad) o deje los valores predeterminados.

10. Especifique otra configuración de instancia de base de datos como considere necesario.

    Para obtener información acerca de cada configuración a la hora de crear una instancia de base de datos, consulte Configuración de instancias de base de datos.

11. Elija Create database (Crear base de datos).

    Aparece la página Databases (Bases de datos). Un banner indica que se está creando la instancia de base de datos y muestra View credential details (Ver detalles de las credenciales).

Visualización de detalles de la instancia de base de datos

Una vez que haya creado la instancia de base de datos, puede ver las credenciales y otros detalles para la instancia de base de datos.

Para ver los detalles de la instancia de base de datos

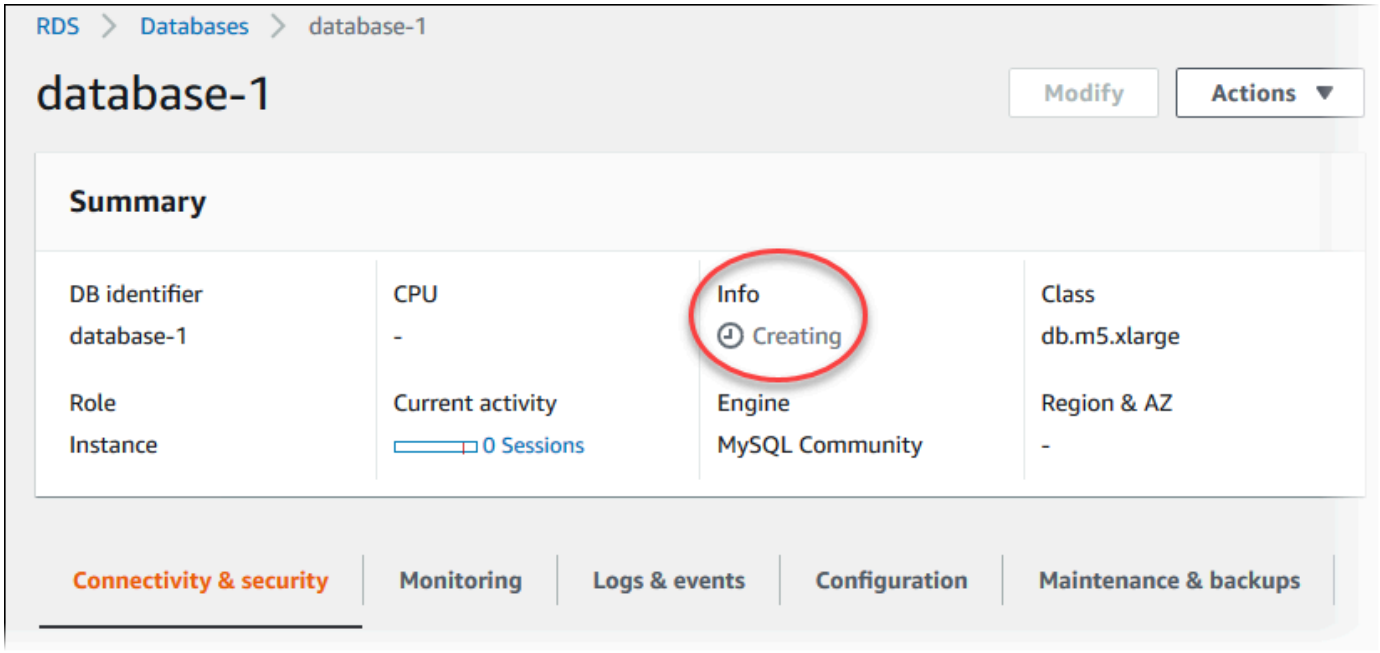
1. Para consultar la contraseña y el nombre de usuario maestros de la instancia de base de datos, seleccione View credential details (Ver detalles de credenciales) en la página Databases (Bases de datos).

   Puede conectarse a la instancia de base de datos como usuario maestro mediante estas credenciales.

   > **Important**
   >
   > No puede ver la contraseña de usuario maestro de nuevo. Si no la registra, es posible que tenga que cambiarla. Para cambiar la contraseña de usuario principal después de que la instancia de base de datos esté disponible, modifique la instancia de base de datos. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

2. En la página Databases (Bases de datos), elija el nombre de la nueva instancia de base de datos.

   Los detalles de la nueva instancia de base de datos aparecen en la consola de RDS. La instancia de base de datos tiene el estado Creating (Creándose) hasta que la instancia de base de datos se cree y esté lista para su uso. Cuando el estado cambie a Available, podrá conectarse a la instancia de base de datos. En función de la clase de instancia de base de datos y del almacenamiento asignado, es posible que la nueva instancia de base de datos tarde varios minutos en estar disponible.



   Cuando la instancia de base de datos esté disponible, puede administrarla de la misma forma que administra las instancias de base de datos de RDS en Nube de AWS.

AWS CLI

Antes de crear una nueva instancia de base de datos en un Outpost con AWS CLI, cree un grupo de subredes de base de datos para el uso de RDS en Outposts.

Para crear un grupo de subredes de base de datos para el Outpost

- Use el comando create-db-subnet-group. Para `--subnet-ids`, especifique el grupo de subredes en el Outpost para que lo utilice RDS en Outposts.

  Para Linux, macOS o:Unix

```
aws rds create-db-subnet-group \
    --db-subnet-group-name myoutpostdbsubnetgr \
    --db-subnet-group-description "DB subnet group for RDS on Outposts" \
    --subnet-ids subnet-abc123
```

En:Windows

```
aws rds create-db-subnet-group ^
    --db-subnet-group-name myoutpostdbsubnetgr ^
    --db-subnet-group-description "DB subnet group for RDS on Outposts" ^
    --subnet-ids subnet-abc123
```

Para crear una instancia de base de datos de RDS en Outposts mediante AWS CLI

- Para crear una instancia de base de datos, utilice el comando create-db-instance. Especifique una zona de disponibilidad para el Outpost, un grupo de seguridad de Amazon VPC asociado con el Outpost y el grupo de subredes de base de datos creado para el Outpost. Puede incluir las siguientes opciones:
  - `--db-instance-identifier`
  - `--db-instance-class`
  - `--engine`: el motor de base de datos. Utilice uno de los siguientes valores:
    - MySQL: especifique `mysql`.
    - PostgreSQL: especifique`postgres`.
    - Microsoft SQL Server: especifique `sqlserver-ee`, `sqlserver-se` o `sqlserver-web`.
  - `--availability-zone`
  - `--vpc-security-group-ids`
  - `--db-subnet-group-name`
  - `--allocated-storage`
  - `--max-allocated-storage`
  - `--master-username`
  - `--master-user-password`

- `--multi-az | --no-multi-az`: (opcional) si desea crear una instancia de base de datos en espera en una zona de disponibilidad diferente. El valor predeterminado es `--no-multi-az`.

  La opción `--multi-az` no está disponible para SQL Server.
- `--backup-retention-period`
- `--backup-target`: (opcional) dónde almacenar copias de seguridad automatizadas e instantáneas manuales. Utilice uno de los siguientes valores:
  - `outposts`: almacénelos de forma local en Outpost.
  - `region`: almacénelos en la región de Región de AWS principal. Este es el valor predeterminado.

  Si utiliza la opción `--multi-az`, no puedes usar `outposts` para `--backup-target`. Además, la instancia de base de datos no puede tener réplicas de lectura si las usa `outposts` para `--backup-target`.
- `--storage-encrypted`
- `--kms-key-id`

Example

En el siguiente ejemplo se crea una instancia de base de datos MySQL llamada `myoutpostdbinstance` con copias de seguridad almacenadas en el Outpost.

Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --db-instance-identifier myoutpostdbinstance \
    --engine-version 8.0.17 \
    --db-instance-class db.m5.large \
    --engine mysql \
    --availability-zone us-east-1d \
    --vpc-security-group-ids outpost-sg \
    --db-subnet-group-name myoutpostdbsubnetgr \
    --allocated-storage 100 \
    --max-allocated-storage 1000 \
    --master-username masterawsuser \
    --manage-master-user-password \
    --backup-retention-period 3 \
    --backup-target outposts \
```

```
    --storage-encrypted \
    --kms-key-id mykey
```

En:Windows

```
aws rds create-db-instance ^
    --db-instance-identifier myoutpostdbinstance ^
    --engine-version 8.0.17 ^
    --db-instance-class db.m5.large ^
    --engine mysql ^
    --availability-zone us-east-1d ^
    --vpc-security-group-ids outpost-sg ^
    --db-subnet-group-name myoutpostdbsubnetgr ^
    --allocated-storage 100 ^
    --max-allocated-storage 1000 ^
    --master-username masterawsuser ^
    --manage-master-user-password ^
    --backup-retention-period 3 ^
    --backup-target outposts ^
    --storage-encrypted ^
    --kms-key-id mykey
```

Para obtener información acerca de cada configuración a la hora de crear una instancia de base de datos, consulte Configuración de instancias de base de datos.

API de RDS

Para crear una nueva instancia de base de datos en un Outpost con la API de RDS, primero cree un grupo de subredes de base de datos para que lo utilice RDS en Outposts llamando a la operación CreateDBSubnetGroup. Para `SubnetIds`, especifique el grupo de subredes en el Outpost para que lo utilice RDS en Outposts.

A continuación, llame a la operación CreateDBInstance con los parámetros siguientes. Especifique una zona de disponibilidad para el Outpost, un grupo de seguridad de Amazon VPC asociado con el Outpost y el grupo de subredes de base de datos creado para el Outpost.

- `AllocatedStorage`
- `AvailabilityZone`
- `BackupRetentionPeriod`
- `BackupTarget`

Si está creando una implementación de instancia de base de datos Multi-AZ, no puede usar`outposts` para `BackupTarget`. Además, la instancia de base de datos no puede tener réplicas de lectura si las usa `outposts` para `BackupTarget`.

- `DBInstanceClass`
- `DBInstanceIdentifier`
- `VpcSecurityGroupIds`
- `DBSubnetGroupName`
- `Engine`
- `EngineVersion`
- `MasterUsername`
- `MasterUserPassword`
- `MaxAllocatedStorage` (opcional)
- `MultiAZ` (opcional)
- `StorageEncrypted`
- `KmsKeyID`

Para obtener información acerca de cada configuración a la hora de crear una instancia de base de datos, consulte Configuración de instancias de base de datos.

Creación de réplicas de lectura para Amazon RDS en AWS Outposts

Amazon RDS en AWS Outposts usa la funcionalidad de replicación integrada de los motores de base de datos de MySQL y PostgreSQL para crear una réplica de lectura a partir de una instancia de base de datos de origen. La instancia de base de datos de origen se convierte en la instancia de base de datos principal. Las actualizaciones realizadas en la instancia de base de datos principal se copian de forma asíncrona en la réplica de lectura. Puede reducir la carga de la instancia de la base de datos principal enrutando las consultas de lectura de sus aplicaciones a la réplica de lectura. Las réplicas de lectura le permiten ajustar la escala de manera elástica por encima de las restricciones de capacidad de una instancia de base de datos para las cargas de trabajo de las bases de datos con operaciones intensivas de lectura.

Al crear una réplica de lectura a partir de una instancia de base de datos de RDS en Outposts, la réplica de lectura utiliza una dirección IP propiedad del cliente (CoIP). Para obtener más información, consulte Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts.

Las réplicas de lectura en RDS en Outposts tienen las siguientes limitaciones:

- No puede crear réplicas de lectura en RDS para SQL Server en instancias de bases de datos de RDS en Outposts.
- Las réplicas de lectura entre regiones no se admiten en RDS en Outposts.
- Las réplicas de lectura en cascada no se admiten en RDS en Outposts.
- La instancia de base de datos de origen de RDS en Outposts no puede tener copias de seguridad locales. El destino de la copia de seguridad para la instancia de base de datos de origen debe ser su Región de AWS.
- Las réplicas de lectura requieren grupos de IP propiedad del cliente (CoIP). Para obtener más información, consulte Direcciones IP propiedad del cliente para Amazon RDS en AWS Outposts.
- Las réplicas de lectura en RDS en Outposts solo se pueden crear en la misma nube privada virtual (VPC) que la instancia de base de datos de origen.
- Las réplicas de lectura de RDS en Outposts pueden estar ubicadas en el mismo Outpost o en otro de la misma VPC que la instancia de base de datos de origen.
- No puede crear réplicas de lectura para instancias de bases de datos cifradas con AWS KMS External Key Store (XKS).

Puede crear una réplica de lectura a partir de una instancia de base de datos de RDS en Outposts, utilizando AWS Management Console, AWS CLI o la API de RDS. Para obtener más información acerca de las réplicas de lectura, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Consola

Para crear una réplica de lectura a partir de una instancia de base de datos de origen

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione la instancia de base de datos que desea usar como origen de una réplica de lectura
4. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).
5. En DB instance identifier (Identificador de instancias de bases de datos), escriba un nombre para la réplica de lectura.
6. Especifique la configuración de Outposts Connectivity (Conectividad de Outposts). Esta configuración es para el Outpost que utiliza la nube privada virtual (VPC) que tiene el grupo de subredes de base de datos para la instancia de base de datos. Su VPC tiene que basarse en el servicio de Amazon VPC.
7. Seleccione su clase de instancia de base de datos. Es recomendable usar la misma clase de instancia de base de datos y el mismo tipo de almacenamiento o mayores que la instancia de base de datos de origen para la réplica de lectura.
8. Para Multi-AZ deployment (Implementación Multi-AZ), elija Create a standby instance (recommended for production usage) (Crear una instancia en espera (recomendada para uso de producción) para crear una instancia de base de datos en espera en otra zona de disponibilidad.

   La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.
9. (Opcional) En Connectivity (Conectividad), defina los valores de Subnet Group (Grupo de subredes) y de Availability Zone (Zona de disponibilidad).

   Si especifica valores tanto para Subnet Group (Grupo de subredes) como para Availability Zone (Zona de disponibilidad), la réplica de lectura se crea en un Outpost asociado a la zona de disponibilidad del grupo de subredes de base de datos.

Si especifica un valor para Subnet Group (Grupo de subredes) y No preference (Sin preferencias) para Availability Zone (Zona de disponibilidad), la réplica de lectura se crea en un Outpost aleatorio de un grupo de subredes de base de datos.

10. Para AWS KMS key, elija el identificador AWS KMS key de la clave de KMS.

    La réplica de lectura debe estar cifrada.
11. Elija otras opciones según sea necesario.
12. Elija Create read replica (Crear réplica de lectura).

Después de crear la réplica de lectura, puede verla en la página Bases de datos de la consola de RDS. Muestra Réplica en la columna Rol .

AWS CLI

Para crear una réplica de lectura a partir de una instancia de base de datos de MySQL o PostgreSQL de origen, utilice el comando create-db-instance-read-replica de la AWS CLI.

Puede controlar dónde se crea la réplica de lectura especificando las opciones `--db-subnet-group-name` y `--availability-zone`:

- Si especifica valores tanto para las opciones `--db-subnet-group-name` y `--availability-zone`, la réplica de lectura se crea en un Outpost asociado a la zona de disponibilidad del grupo de subredes de base de datos.
- Si especifica la opción `--db-subnet-group-name` y no especifica la opción `--availability-zone`, la réplica de lectura se crea en un Outpost aleatorio del grupo de subredes de base de datos.
- Si no especifica ninguna opción, la réplica de lectura se crea en la misma Outpost que la instancia de base de datos de RDS en Outposts de origen.

El siguiente ejemplo crea una réplica y especifica la ubicación de la réplica de lectura mediante la inclusión de las opciones `--db-subnet-group-name` y `--availability-zone`.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-instance-read-replica \
```

```
    --db-instance-identifier myreadreplica \
    --source-db-instance-identifier mydbinstance \
    --availability-zone us-west-2a
```

En:Windows

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --source-db-instance-identifier mydbinstance ^
    --availability-zone us-west-2a
```

API de RDS

Para crear una réplica de lectura a partir de una instancia de base de datos de origen de MySQL o PostgreSQL, llame a la operación CreateDBInstanceReadReplica de la API de Amazon RDS con los siguientes parámetros requeridos:

- `DBInstanceIdentifier`
- `SourceDBInstanceIdentifier`

Puede controlar dónde se crea la réplica de lectura especificando los parámetros `DBSubnetGroupName` y `AvailabilityZone`:

- Si especifica valores tanto para los parámetros `DBSubnetGroupName` y `AvailabilityZone`, la réplica de lectura se crea en un Outpost asociado a la zona de disponibilidad del grupo de subredes de base de datos.
- Si especifica el parámetro `DBSubnetGroupName` y no especifica el parámetro `AvailabilityZone`, la réplica de lectura se crea en un Outpost aleatorio del grupo de subredes de base de datos.
- Si no especifica ningún parámetro, la réplica de lectura se crea en el mismo Outpost que la instancia de base de datos de RDS en Outposts de origen.

Consideraciones para restaurar instancias de base de datos en Amazon RDS en AWS Outposts

Al restaurar una instancia de base de datos en Amazon RDS en AWS Outposts, normalmente puede elegir la ubicación de almacenamiento para las copias de seguridad automatizadas y las instantáneas manuales de la instancia de base de datos restaurada.

- Al restaurar desde una instantánea de base de datos manual, puede almacenar copias de seguridad en la Región de AWS principal o de forma local en su Outpost.
- Al restaurar desde una copia de seguridad automatizada (recuperación a un momento dado), tiene menos opciones:
  - Si se restaura desde la Región de AWS principal, puede almacenar copias de seguridad en la Región de AWS o en el Outpost.
  - Si se restaura desde el Outpost, solo puede almacenar copias de seguridad en el Outpost.

Amazon RDS Proxy

Con Amazon RDS Proxy puede permitir a las aplicaciones agrupar y compartir conexiones de base de datos para mejorar su capacidad de escala. RDS Proxy hace que las aplicaciones sean más resistentes a los errores de base de datos al conectarse automáticamente a una instancia de base de datos en espera mientras se preservan las conexiones de las aplicaciones. RDS Proxy también le permite aplicar autenticación de AWS Identity and Access Management (IAM) para bases de datos y almacenar las credenciales de forma segura en AWS Secrets Manager.

Con RDS Proxy puede gestionar aumentos imprevistos en el tráfico de base de datos. De lo contrario, estas sobrecargas podrían causar problemas debido a la suscripción excesiva de conexiones o a la creación de nuevas conexiones a un ritmo rápido. RDS Proxy establece un grupo de conexiones de base de datos y reutiliza las conexiones de este grupo. Este enfoque evita la sobrecarga de memoria y de CPU que supone abrir una nueva conexión de base de datos cada vez. Para proteger una base de datos frente a un exceso de suscripciones, puede controlar el número de conexiones de base de datos que se crean.

RDS Proxy pone en cola o limita las conexiones de aplicaciones que no se pueden atender de inmediato desde el grupo de conexiones. Aunque las latencias pueden aumentar, la aplicación puede seguir ajustando la escala sin fallar bruscamente ni sobrecargar la base de datos. Si las solicitudes de conexión superan los límites especificados, RDS Proxy rechaza las conexiones de aplicación (es decir, se desprende de la carga). Al mismo tiempo, mantiene un rendimiento predecible para la carga que RDS puede servir con la capacidad disponible.

Puede reducir la sobrecarga para procesar credenciales y establecer una conexión segura para cada nueva conexión. RDS Proxy puede gestionar parte de ese trabajo en nombre de la base de datos.

RDS Proxy es totalmente compatible con las versiones de motor admitidas. Puede habilitar RDS Proxy para la mayoría de las aplicaciones sin cambios de código.

Temas

- Disponibilidad en regiones y versiones
- Cuotas y limitaciones de RDS Proxy
- Planificación del lugar de uso de RDS Proxy
- Conceptos y terminología de RDS Proxy
- Introducción al proxy de RDS
- Administración de un RDS Proxy

- Trabajo con puntos de enlace del proxy de Amazon RDS
- Supervisión de las métricas de RDS Proxy con Amazon CloudWatch
- Trabajo con eventos de RDS Proxy
- Solución de problemas de RDS Proxy
- Uso del proxy de RDS con AWS CloudFormation

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de Amazon RDS con RDS Proxy, consulte Regiones y motores de base de datos para Amazon RDS Proxy.

Cuotas y limitaciones de RDS Proxy

Las siguientes cuotas y limitaciones se aplican a RDS Proxy:

- Cada ID de Cuenta de AWS está limitado a 20 proxies. Si su aplicación requiere más proxies, solicite un aumento a través de la página Service Quotas dentro de la AWS Management Console. En la página Service Quotas, seleccione Amazon Relational Database Service (Amazon RDS) y busque Proxies para solicitar un aumento de cuota. AWS puede aumentar automáticamente su cuota o, en espera de la revisión de su solicitud, mediante Soporte.
- Cada proxy puede tener hasta 200 secretos de Secrets Manager asociados. Por lo tanto, cada proxy puede conectarse con hasta 200 cuentas de usuario distintas en un momento dado.
- Cada proxy tiene un punto de conexión predeterminado. También puede agregar hasta 20 puntos de conexión de proxy para cada proxy. Puede crear, ver, modificar y eliminar estos puntos de conexión.
- Para las instancias de base de datos de RDS en configuraciones de reproducción, solo puede asociar un proxy con la instancia de base de datos de escritura, no con una réplica de lectura.
- Su RDS Proxy debe estar en la misma nube privada virtual (VPC) que la base de datos. Aunque se puede acceder públicamente a la base de datos, no sucede lo mismo con el proxy. Por ejemplo, si va a crear prototipos de base de datos en un host local, no puede conectarse a su proxy, a menos que configure los requisitos de red necesarios para permitir la conexión al proxy. Esto es porque el host local está fuera de la VPC del proxy.
- No se puede utilizar RDS Proxy con una VPC que tenga su tenencia establecida en `dedicated`.

- Si utiliza RDS Proxy con una instancia de base de datos de RDS que tenga habilitada la autenticación de IAM, compruebe la autenticación del usuario. Los usuarios que se conecten a través de un proxy deben autenticarse con credenciales de inicio de sesión. Para obtener más información sobre la compatibilidad de Secrets Manager y IAM en RDS Proxy, consulte Configuración de credenciales de base de datos en AWS Secrets Manager para RDS Proxy y Configuración de políticas de AWS Identity and Access Management (IAM) para RDS Proxy.
- No se puede usar el proxy de RDS con DNS personalizados cuando se utiliza la validación de nombres de host SSL.
- Cada proxy se puede asociar con una única instancia de base de datos de destino. Sin embargo, puede asociar varios proxies con la misma instancia de base de datos.
- Cualquier instrucción con un tamaño de texto superior a 16 KB hace que el proxy fije la sesión a la conexión actual.
- Algunas regiones tienen restricciones de zona de disponibilidad (AZ) que debe tener en cuenta al crear el proxy. La región Este de EE. UU. (Norte de Virginia) no admite RDS Proxy en la zona de disponibilidad `use1-az3`. La región Oeste de EE. UU. (Norte de California) no admite RDS Proxy en la zona de disponibilidad `usw1-az2`. Al seleccionar subredes al crear el proxy, asegúrese de no seleccionar subredes en las zonas de disponibilidad mencionadas anteriormente.
- Actualmente, RDS Proxy no admite claves de contexto de condición globales.

  Para obtener más información sobre las claves de condición globales, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.
- No se puede utilizar RDS Proxy con RDS Custom para SQL Server.
- Para reflejar cualquier modificación del grupo de parámetros de la base de datos en el proxy, es necesario reiniciar la instancia aunque decida aplicar los cambios inmediatamente. Es necesario reiniciar todo el clúster para los parámetros de clúster.
- Su proxy crea automáticamente el usuario de base de datos `rdsproxyadmin` cuando registra un destino de proxy. Este es un usuario protegido que es esencial para la funcionalidad del proxy. Debe evitar cualquier alteración del usuario de `rdsproxyadmin` de cualquier forma. Eliminar o modificar el usuario de `rdsproxyadmin` o sus permisos puede provocar la total falta de disponibilidad del proxy en la aplicación.

Para conocer las limitaciones adicionales de cada motor de base de datos, consulte las secciones siguientes:

- Limitaciones adicionales para RDS para MariaDB

- Limitaciones adicionales para RDS para Microsoft SQL Server
- Limitaciones adicionales para RDS para MySQL
- Limitaciones adicionales para RDS para PostgreSQL

Limitaciones adicionales para RDS para MariaDB

Las siguientes limitaciones adicionales se aplican a RDS Proxy con RDS para MariaDB:

- Actualmente, todos los proxies escuchan en el puerto 3306 para MariaDB. Los proxies todavía se conectan a la base de datos mediante el puerto especificado en la configuración de la base de datos.
- No se puede usar RDS Proxy con bases de datos MariaDB autoadministradas en instancias Amazon EC2.
- No se puede usar RDS Proxy con una instancia de base de datos de RDS para MariaDB que tenga el parámetro `read_only` en su grupo de parámetros de base de datos establecido en `1`.
- RDS Proxy no admite el modo comprimido de MariaDB. Por ejemplo, no admite la compresión utilizada por las opciones `--compress` o `-C` del comando `mysql`.
- Algunas instrucciones y funciones SQL pueden cambiar el estado de conexión sin causar fijación. Para conocer el comportamiento de fijación más actual, consulte Cómo evitar la fijación de RDS Proxy.
- MariaDB no admite el complemento `auth_ed25519` de MariaDB.
- El proxy RDS no admite la versión 1.3 de seguridad de la capa de transporte (TLS) para las bases de datos de MariaDB.
- Las conexiones a bases de datos que procesan un comando `GET DIAGNOSTIC` pueden devolver información inexacta cuando RDS Proxy vuelve a utilizar la misma conexión de base de datos para ejecutar otra consulta. Esto puede ocurrir cuando RDS Proxy multiplexa las conexiones de bases de datos. Para obtener más información, consulte Información general de los conceptos de RDS Proxy.
- Actualmente, RDS Proxy no admite la opción `caching_sha2_password` para `ClientPasswordAuthType` para MariaDB.

> **Important**
>
> Para proxies asociados con bases de datos de MariaDB, no establezca el parámetro de configuración `sql_auto_is_null` en `true` o un valor distinto de cero en la consulta de inicialización. Si lo hace, es posible que la aplicación se comporte incorrectamente.

Limitaciones adicionales para RDS para Microsoft SQL Server

Las siguientes limitaciones adicionales se aplican a RDS Proxy con RDS para Microsoft SQL Server:

- El número de secretos de Secrets Manager que necesita crear para un proxy depende de la intercalación que utilice la instancia de base de datos. Por ejemplo, supongamos que la instancia de base de datos utiliza una intercalación que distingue mayúsculas Si su aplicación acepta tanto «Admin» como «admin», su proxy necesita dos secretos distintos. Para obtener más información sobre colación en SQL Server, consulte la documentación de Microsoft SQL Server.
- RDS Proxy no admite conexiones que utilizan Active Directory.
- No puede usar la autenticación de IAM con clientes que no admitan propiedades de token. Para obtener más información, consulte Consideraciones para conectarse a un proxy con Microsoft SQL Server.
- Los resultados de `@@IDENTITY`, `@@ROWCOUNT` y `SCOPE_IDENTITY` no siempre son precisos. Como solución alternativa, recupere sus valores en la misma sentencia de sesión para asegurarse de que devuelven la información correcta.
- Si la conexión usa varios conjuntos de resultados activos (MARS), RDS Proxy no ejecuta las consultas de inicialización. Para obtener más información sobre MARS, consulte la documentación de Microsoft SQL Server.
- Actualmente, RDS Proxy no admite instancias de base de datos de RDS para SQL Server que se ejecuten en la versión principal de SQL Server 2022.
- RDS Proxy no admite instancias de base de datos de RDS para SQL Server que se ejecuten en la versión principal de SQL Server 2014.
- RDS Proxy no admite aplicaciones cliente que no puedan gestionar varios mensajes de respuesta en un registro TLS.

Limitaciones adicionales para RDS para MySQL

Las siguientes limitaciones adicionales se aplican a RDS Proxy con bases de datos RDS para MySQL:

- La compatibilidad con RDS Proxy para la autenticación de `caching_sha2_password` requiere una conexión segura (TLS).
- Se sabe que `caching_sha2_password` presenta problemas de compatibilidad con RDS Proxy si se usan determinadas versiones del controlador go-sql.
- Cuando se utiliza el controlador C de MySQL 8.4, la API `mysql_stmt_bind_named_param` puede formar paquetes con un formato incorrecto si el recuento de parámetros supera el recuento de marcadores de posición en una instrucción preparada. Esto da como resultado respuestas incorrectas. Para obtener más información, consulte MySQL bug report.
- Actualmente, todos los proxies escuchan en el puerto 3306 para MySQL. Los proxies todavía se conectan a la base de datos mediante el puerto especificado en la configuración de la base de datos.
- No puede usar RDS Proxy con bases de datos MySQL autoadministradas en instancias EC2.
- No se puede usar RDS Proxy con una instancia de base de datos RDS para MySQL que tenga el parámetro `read_only` en su grupo de parámetros de base de datos establecido en `1`.
- RDS Proxy no admite el modo comprimido de MySQL. Por ejemplo, no admite la compresión utilizada por las opciones `--compress` o `-C` del comando `mysql`.
- Las conexiones a bases de datos que procesan un comando `GET DIAGNOSTIC` pueden devolver información inexacta cuando RDS Proxy vuelve a utilizar la misma conexión de base de datos para ejecutar otra consulta. Esto puede ocurrir cuando RDS Proxy multiplexa las conexiones de bases de datos.
- Algunas instrucciones y funciones SQL, como `SET LOCAL`, pueden cambiar el estado de conexión sin producir una fijación. Para conocer el comportamiento de fijación más actual, consulte Cómo evitar la fijación de RDS Proxy.
- No se admite el uso de la función `ROW_COUNT()` en una consulta de varias instrucciones.
- RDS Proxy no admite aplicaciones cliente que no puedan gestionar varios mensajes de respuesta en un registro TLS.
- RDS Proxy no admite las contraseñas duales de MySQL.

> **Important**
>
> Para proxies asociados con bases de datos de MySQL, no establezca el parámetro de configuración `sql_auto_is_null` en `true` o un valor distinto de cero en la consulta de inicialización. Si lo hace, es posible que la aplicación se comporte incorrectamente.

Limitaciones adicionales para RDS para PostgreSQL

Las siguientes limitaciones adicionales se aplican a RDS Proxy con bases de datos de RDS para PostgreSQL:

- RDS Proxy no admite los filtros de fijación de sesión para PostgreSQL.
- Actualmente, todos los proxies escuchan en el puerto 5432 para PostgreSQL.
- Para PostgreSQL, RDS Proxy no admite actualmente la cancelación de una consulta por parte de un cliente mediante la emisión de `CancelRequest`. Este es el caso, por ejemplo, cuando se cancela una consulta de larga duración en una sesión psql interactiva con Ctrl + C.
- Los resultados de la función de PostgreSQL lastval no siempre son precisos. Como alternativa, utilice la instrucción INSERT con la cláusula `RETURNING`.
- Actualmente, RDS Proxy no admite el modo de replicación en streaming.
- Con RDS para PostgreSQL 16, las modificaciones del valor `scram_iterations` afectan exclusivamente al proceso de autenticación entre el proxy y la base de datos. En concreto, si configura `ClientPasswordAuthType` como `scram-sha-256`, las personalizaciones que se realicen en el valor `scram_iterations` no influirán en la autenticación mediante contraseña de cliente a proxy. En su lugar, el valor de iteración para la autenticación de contraseña de cliente a proxy se fija en 4096.
- La base de datos `default` debe existir.
- Si usa `ALTER ROLE` para cambiar el rol de usuario con `SET ROLE`, es posible que las conexiones posteriores con ese usuario al proxy no usen esta configuración de rol si esas conexiones se encuentran con alguna fijación. Para evitarlo, cuando utilice un proxy, emplee `SET ROLE` en la consulta de inicialización del proxy. Para obtener más información, consulte Consulta de inicialización en Creación de un proxy para Amazon RDS.

Important

En el caso de los proxies existentes con bases de datos de PostgreSQL, si modifica la autenticación de la base de datos para utilizar únicamente `SCRAM`, el proxy dejará de estar disponible durante un máximo de 60 segundos. Para evitar este problema, lleve a cabo alguna de las siguientes operaciones:

- Asegúrese de que la base de datos permita la autenticación `SCRAM` y `MD5`.
- Para utilizar únicamente la autenticación `SCRAM`, cree un nuevo proxy, migre el tráfico de la aplicación al nuevo proxy y, a continuación, elimine el proxy previamente asociado a la base de datos.

Planificación del lugar de uso de RDS Proxy

Puede determinar cuáles de sus instancias de base de datos, clústeres y aplicaciones podrían beneficiarse más del uso de RDS Proxy. Para ello, tenga en cuenta estos factores:

- Cualquier instancia de base de datos que encuentre errores de "demasiadas conexiones" es un buen candidato para asociarse con un proxy. Esto suele caracterizarse por un valor alto de la métrica `ConnectionAttempts` de CloudWatch. El proxy permite a las aplicaciones abrir muchas conexiones de cliente, mientras que el proxy administra un número menor de conexiones de larga duración a la instancia de base de datos.
- Para instancias de base de datos que utilizan clases de instancias de AWS más pequeñas, como T2 o T3, el uso de un proxy puede ayudar a evitar condiciones de falta de memoria. También puede ayudar a reducir la sobrecarga de CPU para establecer conexiones. Estas condiciones pueden producirse cuando se trata de un gran número de conexiones.
- Puede monitorear ciertas métricas de Amazon CloudWatch para determinar si una instancia de base de datos se acerca a ciertos tipos de límite. Estos límites son para el número de conexiones y la memoria asociados a la administración de conexiones. También puede monitorear ciertas métricas de CloudWatch para determinar si una instancia de base de datos está controlando muchas conexiones de corta duración. Abrir y cerrar tales conexiones puede imponer una sobrecarga de rendimiento en su base de datos. Para obtener información sobre las métricas que se van a monitorizar, consulte Supervisión de las métricas de RDS Proxy con Amazon CloudWatch.

- AWS LambdaLas funciones de también pueden ser buenas candidatas para usar un proxy. Estas funciones hacen frecuentes conexiones cortas a la base de datos que aprovechan el grupo de conexiones que ofrece RDS Proxy. Puede aprovechar cualquier autenticación de IAM que ya tenga para funciones de Lambda, en lugar de administrar las credenciales de la base de datos en el código de la aplicación de Lambda.
- Las aplicaciones que suelen abrir y cerrar un gran número de conexiones de base de datos y no tienen mecanismos integrados de agrupación de conexiones son buenas candidatas para usar un proxy.
- Las aplicaciones que mantienen un gran número de conexiones abiertas durante largos períodos suelen ser buenas candidatas para usar un proxy. Las aplicaciones en sectores como el software como servicio (SaaS) o el comercio electrónico a menudo minimizan la latencia de las solicitudes de base de datos al dejar las conexiones abiertas. Con RDS Proxy, una aplicación puede mantener más conexiones abiertas que cuando se conecta directamente a la instancia de base de datos.
- Es posible que no haya adoptado la autenticación de IAM y Secrets Manager debido a la complejidad de configurar dicha autenticación para todas las instancias de base de datos. Si es así, puede dejar los métodos de autenticación existentes en su lugar y delegar la autenticación en un proxy. El proxy puede aplicar las directivas de autenticación para conexiones de cliente para aplicaciones concretas. Puede aprovechar cualquier autenticación de IAM que ya tenga para funciones de Lambda, en lugar de administrar las credenciales de la base de datos en el código de la aplicación de Lambda.
- RDS Proxy puede ayudar a que las aplicaciones sean más resilientes y transparentes ante los errores de base de datos. RDS Proxy evita las cachés del Sistema de nombres de dominio (DNS) a fin de reducir los tiempos de conmutación por error hasta en un 66 % para las instancias de base de datos de Amazon RDS Multi-AZ. RDS Proxy también dirige automáticamente el tráfico a una nueva instancia de base de datos y conserva las conexiones de la aplicación. Esto hace que la conmutación por error sea más transparente para las aplicaciones.

Conceptos y terminología de RDS Proxy

Puede simplificar la administración de conexiones de las instancias de base de datos de Amazon RDS usando RDS Proxy.

RDS Proxy controla el tráfico de red entre la aplicación cliente y la base de datos. Lo hace de una manera activa, comprendiendo primero el protocolo de base de datos. A continuación, ajusta su

comportamiento en función de las operaciones SQL de la aplicación y los conjuntos de resultados de la base de datos.

RDS Proxy reduce la sobrecarga de memoria y CPU para la administración de conexiones en la base de datos. La base de datos necesita menos memoria y recursos de CPU cuando las aplicaciones abren muchas conexiones simultáneas. Tampoco requiere lógica en las aplicaciones para cerrar y volver a abrir conexiones que permanecen inactivas durante mucho tiempo. Del mismo modo, requiere menos lógica de aplicación para restablecer conexiones en caso de un problema de base de datos.

La infraestructura para RDS Proxy está altamente disponible e implementada en varias zonas de disponibilidad (AZ). El cálculo, la memoria y el almacenamiento de RDS Proxy son independientes de las instancias de base de datos de RDS. Esta separación ayuda a reducir la sobrecarga en los servidores de bases de datos, de modo que puedan dedicar sus recursos a servir cargas de trabajo de base de datos. Los recursos informáticos de RDS Proxy no tienen servidor y se escalan automáticamente en función de la carga de trabajo de la base de datos.

Temas

- Información general de los conceptos de RDS Proxy
- Grupo de conexiones
- Seguridad de RDS Proxy
- Conmutación por error
- Transacciones

Información general de los conceptos de RDS Proxy

RDS Proxy gestiona la infraestructura para llevar a cabo la agrupación de conexiones y las demás características descritas en las siguientes secciones. Puede ver los proxies representados en la consola de RDS en la página Proxies.

Cada proxy gestiona las conexiones a una única instancia de base de datos de RDS. El proxy determina automáticamente la instancia de escritor actual para la instancia o clúster de base de datos de RDS Multi-AZ.

Las conexiones que un proxy mantiene abiertas y disponibles para que las aplicaciones de base de datos puedan utilizar el grupo de conexiones.

De forma predeterminada, RDS Proxy puede reutilizar una conexión después de cada transacción en la sesión. Esta reutilización en el nivel de transacción se denomina multiplexación. Cuando RDS Proxy elimina temporalmente una conexión del grupo de conexiones para reutilizarla, esa operación se denomina préstamo de la conexión. Cuando sea seguro hacerlo, RDS Proxy devuelve esa conexión al grupo de conexiones.

En algunos casos, RDS Proxy no puede estar seguro de que sea seguro volver a utilizar una conexión de base de datos fuera de la sesión actual. En estos casos, mantiene la sesión en la misma conexión hasta que finalice la sesión. Este comportamiento de reserva se denomina fijación.

Un proxy tiene un punto de conexión predeterminado. Se conecta a este punto de conexión cuando trabaja con una instancia de base de datos de Amazon RDS. Lo hace en lugar de conectarse al punto de conexión de lectura y escritura que se conecta directamente a la instancia. Para los clústeres de bases de datos de RDS, también puede crear puntos de conexión de lectura o escritura y de solo lectura adicionales. Para obtener más información, consulte Información general de los puntos de enlace de proxy.

Por ejemplo, aún puede conectarse al punto de enlace del clúster para conexiones de lectura y escritura sin agrupación de conexiones. Aún puede conectarse al punto de conexión del lector para conexiones de solo lectura con equilibrio de carga. Aún puede conectarse a los puntos de conexión de instancia para el diagnóstico y la resolución de problemas de instancias de base de datos específicas dentro de un clúster. Si utiliza otros servicios de AWS como AWS Lambda para conectarse a bases de datos de RDS, cambie la configuración de conexión para utilizar el punto de conexión del proxy. Por ejemplo, especifique el punto de conexión del proxy para permitir que las funciones de Lambda accedan a la base de datos mientras aprovechan la funcionalidad del RDS Proxy.

Cada proxy contiene un grupo de destino. Este grupo de destino abarca la instancia de base de datos de RDS que se puede conectar con el proxy. La instancia de base de datos de RDS asociada con un proxy se denomina destino de ese proxy. Para mayor comodidad, al crear un proxy a través de la consola, RDS Proxy también crea el grupo de destino correspondiente y registra los destinos asociados automáticamente.

Una familia de motores es un conjunto relacionado de motores de base de datos que utilizan el mismo protocolo de base de datos. Elija la familia de motores para cada proxy que cree.

Grupo de conexiones

Cada proxy realiza la agrupación de conexiones por separado para la instancia de escritor y de lector de la base de datos de RDS asociada. La agrupación de conexiones es una optimización que reduce la sobrecarga asociada a la apertura y el cierre de conexiones y al mantenimiento de muchas conexiones abiertas simultáneamente. Esta sobrecarga incluye la memoria necesaria para gestionar cada nueva conexión. También implica una sobrecarga de la CPU para cerrar cada conexión y abrir una nueva. Los ejemplos incluyen el protocolo de enlace Transport Layer Security/Secure Sockets Layer (TLS/SSL), autenticación, capacidades de negociación, etc. La agrupación de conexiones simplifica la lógica de la aplicación. No es necesario escribir código de aplicación para minimizar el número de conexiones abiertas simultáneas.

Además, todos los proxies hacen multiplexación de conexión, algo conocido también como reutilización de la conexión. Con la multiplexación, el proxy de RDS realiza todas las operaciones de una transacción mediante una conexión de base de datos subyacente. A continuación, RDS puede usar una conexión diferente para la siguiente transacción. Puede abrir muchas conexiones simultáneas al proxy y el proxy mantiene un número menor de conexiones abiertas a la instancia de base de datos o al clúster. Al hacerlo, se minimiza aún más la sobrecarga de memoria para las conexiones en el servidor de base de datos. Esta técnica también reduce la posibilidad de errores de «demasiadas conexiones».

Seguridad de RDS Proxy

El proxy de RDS utiliza los mecanismos de seguridad de RDS existentes, como TLS/SSL e AWS Identity and Access Management (IAM). Para obtener información general acerca de esas características de seguridad, consulte Seguridad en Amazon RDS. Además, asegúrese de familiarizarse con la forma en la que RDS trabaja con autenticación, autorización y otras áreas de seguridad.

RDS Proxy puede actuar como una capa adicional de seguridad entre las aplicaciones cliente y la base de datos subyacente. Por ejemplo, puede conectarse al proxy mediante TLS 1.3, incluso si la instancia de base de datos subyacente admite una versión más antigua de TLS. Puede conectarse al proxy mediante un rol de IAM. Esto es así incluso si el proxy se conecta a la base de datos mediante el método nativo de autenticación de usuario y contraseña. Mediante esta técnica, puede imponer requisitos de autenticación sólidos para las aplicaciones de base de datos sin un esfuerzo de migración costoso para las propias instancias de base de datos.

Almacene las credenciales de base de datos utilizadas por el proxy de RDS en AWS Secrets Manager. Cada usuario de base de datos para la instancia de base de datos de RDS a la que

accede un proxy debe tener un secreto correspondiente en Secrets Manager. También puede configurar la autenticación de IAM para los usuarios de RDS Proxy. Al hacerlo, puede aplicar la autenticación de IAM para el acceso a la base de datos incluso si las bases de datos utilizan la autenticación de contraseña nativa. Recomendamos utilizar estas características de seguridad en lugar de incorporar credenciales de base de datos en el código de la aplicación.

Uso de TLS/SSL con RDS Proxy

Puede conectarse a RDS Proxy con el protocolo TLS/SSL.

> **Note**
>
> El proxy de RDS utiliza certificados de AWS Certificate Manager (ACM). Si está utilizando RDS Proxy, no es necesario descargar certificados de Amazon RDS ni actualizar aplicaciones que usen conexiones RDS Proxy.

Para aplicar TLS a todas las conexiones entre el proxy y la base de datos, puede especificar la configuración Exigir Transport Layer Security al crear o modificar un proxy en la AWS Management Console.

RDS Proxy puede también garantizar que la sesión utiliza TLS/SSL entre el cliente y el punto de enlace de RDS Proxy. Para que RDS Proxy lo haga, especifique el requisito en el lado del cliente. Las variables de sesión SSL no están establecidas para las conexiones SSL a una base de datos usando RDS Proxy.

- En el caso de RDS para MySQL, especifique el requisito en el lado del cliente con el parámetro `--ssl-mode` cuando ejecute el comando `mysql`.
- En el caso de Amazon RDS PostgreSQL, especifique `sslmode=require` como parte de la cadena `conninfo` cuando ejecute el comando `psql`.

RDS Proxy admite las versiones 1.0, 1.1, 1.2 y 1.3 del protocolo TLS. Puede conectarse al proxy mediante una versión de TLS posterior a la que utiliza en la base de datos subyacente.

De forma predeterminada, los programas del cliente establecen una conexión cifrada con RDS Proxy, con un mayor control disponible gracias a la opción `--ssl-mode`. Desde el lado del cliente, RDS Proxy es compatible con todos los modos de SSL.

Para el cliente, los modos SSL son los siguientes:

PREFERRED

SSL es la primera opción, pero no es necesaria.

DISABLED

No se permite SSL.

REQUIRED

Obliga a usar SSL.

VERIFY_CA

Implemente SSL y verifique la entidad de certificación (CA).

VERIFY_IDENTITY

Obliga a usar SSL y comprueba CA y el nombre de host de CA.

Cuando se utiliza un cliente con `--ssl-mode VERIFY_CA` o `VERIFY_IDENTITY`, especifique la opción de `--ssl-ca` apuntando a una autoridad certificadora en formato `.pem`. Para usar el archivo `.pem`, descargue todos los PEM de CA raíz desde Amazon Trust Services y colóquelos en un solo archivo `.pem`.

RDS Proxy utiliza certificados comodín, que se aplican tanto a un dominio como a sus subdominios. Si utiliza el cliente `mysql` para conectarse con el modo SSL `VERIFY_IDENTITY`, actualmente deberá usar el comando `mysql` compatible con MySQL 8.0.

Conmutación por error

La conmutación por error es una característica de alta disponibilidad que reemplaza una instancia de base de datos por otra cuando la instancia original deja de estar disponible. Puede producirse una conmutación por error debido a un problema con una instancia de base de datos. También es posible que sea parte de los procedimientos normales de mantenimiento, como durante la actualización de una base de datos. La conmutación por error se aplica a las instancias de base de datos de RDS en una configuración Multi-AZ.

La conexión a través de un proxy hace que las aplicaciones sean más resistentes a las conmutaciones por error de la base de datos. Cuando la instancia de base de datos original deja de estar disponible, RDS Proxy se conecta a la base de datos en espera sin perder las conexiones de

aplicaciones inactivas. Esto le ayuda a acelerar y simplificar el proceso de conmutación por error. Esto es menos disruptivo para la aplicación que un problema típico de reinicio o base de datos.

Sin RDS Proxy, una conmutación por error implica una breve interrupción. Durante la interrupción, no puede realizar operaciones de escritura en esa base de datos en conmutación por error. Las conexiones de base de datos existentes se interrumpen y la aplicación debe volver a abrirlas. La base de datos está disponible para nuevas conexiones y operaciones de escritura cuando se promociona una instancia de base de datos de solo lectura para que tome el lugar de la que no está disponible.

Durante las conmutaciones por error de la base de datos, RDS Proxy continúa aceptando conexiones en la misma dirección IP y dirige automáticamente las conexiones a la nueva instancia de base de datos primaria. Los clientes que se conectan a través de RDS Proxy no son susceptibles a lo siguiente:

- Retrasos de propagación del sistema de nombres de dominio (DNS) en la conmutación por error.
- Almacenamiento en caché de DNS local.
- Tiempos de espera de conexión.
- Incertidumbre sobre qué instancia de base de datos es el escritor actual.
- Espera a la respuesta de una consulta de un escritor anterior que dejó de estar disponible sin cerrar las conexiones.

En el caso de las aplicaciones que mantienen su propio grupo de conexiones, pasar por RDS Proxy significa que la mayoría de las conexiones permanecen activas durante las conmutaciones por error u otras interrupciones. Solo se cancelan las conexiones que están en medio de una transacción o sentencia SQL. El proxy de RDS acepta inmediatamente nuevas conexiones. Cuando el escritor de la base de datos no está disponible, RDS Proxy pone en cola las solicitudes entrantes.

Para aplicaciones que no mantienen sus propios grupos de conexiones, RDS Proxy ofrece velocidades de conexión más rápidas y conexiones más abiertas. Descarga la costosa sobrecarga de reconexiones frecuentes de la base de datos. Lo hace reutilizando las conexiones de base de datos que se mantienen en el grupo de conexiones de RDS Proxy. Este enfoque es especialmente importante para las conexiones TLS, en las que los costos de instalación son importantes.

Transacciones

Todas las instrucciones dentro de una sola transacción siempre utilizan la misma conexión de base de datos subyacente. La conexión está disponible para su uso por parte de una sesión diferente

cuando finaliza la transacción. El uso de la transacción como unidad de granularidad tiene las siguientes consecuencias:

- La reutilización de la conexión puede ocurrir después de cada instrucción individual cuando se ha activado la configuración `autocommit` de RDS para MySQL.
- Por el contrario, cuando el parámetro `autocommit` está desactivado, la primera instrucción que emita en una sesión comienza una nueva transacción. Por ejemplo, suponga que introduce una secuencia de `SELECT`, `INSERT`, `UPDATE` y otras instrucciones de lenguaje de manipulación de datos (DML). En este caso, la reutilización de la conexión no se producirá hasta que emita un`COMMIT`, `ROLLBACK` o finalice la transacción.
- La introducción de una instrucción de lenguaje de definición de datos (DDL) hace que la transacción finalice después de que se complete esa instrucción.

RDS Proxy detecta cuándo finaliza una transacción a través del protocolo de red utilizado por la aplicación cliente de base de datos. La detección de transacciones no se basa en palabras clave como `COMMIT` o `ROLLBACK` que aparecen en el texto de la instrucción SQL.

En algunos casos, RDS Proxy podría detectar una solicitud de base de datos que hace que sea poco práctico trasladar la sesión a una conexión diferente. En estos casos, desactiva la multiplexación para esa conexión el resto de la sesión. La misma regla se aplica si RDS Proxy no puede estar seguro de que la multiplexación sea práctica para la sesión. Esta operación se denomina fijación. Para obtener información sobre formas de detectar y minimizar la fijación, consulte Cómo evitar la fijación de RDS Proxy.

Introducción al proxy de RDS

Utilice la información de las siguientes páginas para configurar y administrar Amazon RDS Proxy , así como para definir las opciones de seguridad relacionadas. Estas opciones de seguridad controlan quién puede acceder a cada proxy y cómo se conecta cada proxy a instancias de base de datos.

Si es la primera vez que utiliza RDS Proxy, le recomendamos que siga las páginas en el orden en que las presentamos.

Temas

- Configuración de requisitos previos de red para RDS Proxy
- Configuración de credenciales de base de datos en AWS Secrets Manager para RDS Proxy
- Configuración de políticas de AWS Identity and Access Management (IAM) para RDS Proxy

- Creación de un proxy para Amazon RDS
- Visualización de un proxy
- Conexión a una base de datos mediante RDS Proxy

Configuración de requisitos previos de red para RDS Proxy

El uso de RDS Proxy requiere que tenga una nube privada virtual (VPC) común entre su instancia de base de datos de RDS y RDS Proxy. Esta VPC debe tener un mínimo de dos subredes que se encuentren en diferentes zonas de disponibilidad. Tu cuenta puede poseer estas subredes o compartirlas con otras cuentas. Para obtener más información acerca del uso compartido de VPC, consulte Trabajar con VPC compartidas.

Los recursos de aplicaciones cliente, como Amazon EC2, Lambda o Amazon ECS, pueden estar en la misma VPC como el proxy. O pueden estar en una VPC independiente del proxy. Si se ha conectado correctamente a instancias de base de datos de RDS, ya dispone de los recursos de red necesarios.

Temas

- Obtención de información sobre subredes.
- Planificación de la capacidad de direcciones IP

Obtención de información sobre subredes.

Para crear un proxy, debe proporcionar las subredes y la VPC en las que opera el proxy. En el siguiente ejemplo de Linux se muestran comandos de la AWS CLI con los que se examinan las VPC y las subredes que son propiedad de su Cuenta de AWS. En particular, se pasan los ID de subred como parámetros si crea un proxy utilizando la CLI.

```
aws ec2 describe-vpcs
aws ec2 describe-internet-gateways
aws ec2 describe-subnets --query '*[].[VpcId,SubnetId]' --output text | sort
```

En el siguiente ejemplo de Linux, se muestran comandos de la AWS CLI que sirven para determinar los ID de subred correspondientes a una instancia de base de datos de RDS. Busque el ID de la VPC para la instancia de base de datos. Examine la VPC para encontrar sus subredes. En el siguiente ejemplo de Linux se muestra cómo.

```
$ #From the DB instance, trace through the DBSubnetGroup and Subnets to find the subnet
 IDs.
$ aws rds describe-db-instances --db-instance-identifier my_instance_id --query '*[].
[DBSubnetGroup]|[0]|[0]|[Subnets]|[0]|[*].SubnetIdentifier' --output text
```

```
subnet_id_1
subnet_id_2
subnet_id_3
...
```

```
$ #From the DB instance, find the VPC.
$ aws rds describe-db-instances --db-instance-identifier my_instance_id --query '*[].
[DBSubnetGroup]|[0]|[0].VpcId' --output text
```

```
my_vpc_id
```

```
$ aws ec2 describe-subnets --filters Name=vpc-id,Values=my_vpc_id --query '*[].
[SubnetId]' --output text
```

```
subnet_id_1
subnet_id_2
subnet_id_3
subnet_id_4
subnet_id_5
subnet_id_6
```

Planificación de la capacidad de direcciones IP

Un RDS Proxy ajusta automáticamente su capacidad según sea necesario en función del tamaño y la cantidad de instancias de base de datos registradas en él. Algunas operaciones también pueden requerir una capacidad de proxy adicional, como el aumento del tamaño de una base de datos registrada u operaciones de mantenimiento internas de RDS Proxy. Durante estas operaciones, es posible que el proxy necesite más direcciones IP para aprovisionar la capacidad adicional. Estas direcciones adicionales permiten que su proxy escale sin afectar a su carga de trabajo. La falta de direcciones IP gratuitas en las subredes impide que un proxy se amplíe. Esto puede provocar latencias de consulta más altas o errores en la conexión del cliente. RDS le notifica mediante un evento `RDS-EVENT-0243` cuando no hay suficientes direcciones IP libres en sus subredes. Para obtener información acerca de este evento, consulte Trabajo con eventos de RDS Proxy.

Reserve el número mínimo siguiente de direcciones IP libres en las subredes para el proxy, en función de los tamaños de las clases de instancias de bases de datos.

Clase de instancia de base de datos	Direcciones IP gratuitas mínimas
db.*.xlarge o menor	10
db.*.24xlarge	15
db.*.24xlarge	25
db.*.24xlarge	45
db.*.24xlarge	60
db.*.24xlarge	75
db.*.24xlarge	110

Estos números de direcciones IP recomendados son estimaciones para un proxy con solo el punto de conexión predeterminado. Un proxy con puntos de conexión adicionales o réplicas de lectura puede necesitar más direcciones IP gratuitas. Para cada punto de conexión adicional, le recomendamos que reserve tres direcciones IP más. Para cada réplica de lectura, le recomendamos que reserve direcciones IP adicionales tal como se especifica en la tabla en función del tamaño de dicha réplica de lectura.

> **Note**
>
> RDS Proxy no consume más de 215 direcciones IP en una VPC.

Configuración de credenciales de base de datos en AWS Secrets Manager para RDS Proxy

Proxy de RDS en Amazon RDS utiliza AWS Secrets Manager para almacenar y administrar las credenciales de la base de datos de forma segura. En lugar de incrustar credenciales en la aplicación, se asocia un proxy con un secreto de Secrets Manager que contiene los detalles de

autenticación necesarios. Cree un secreto independiente de Secrets Manager para cada cuenta de usuario de base de datos a la que se conecta el proxy en la instancia de base de datos de RDS.

Temas

- Creación de secretos para utilizar con Proxy de RDS

Creación de secretos para utilizar con Proxy de RDS

Antes de crear un proxy, debe crear al menos un secreto que almacene las credenciales de la base de datos.

Consola

Creación de un secreto

1. Abra la consola de Secrets Manager enhttps://console.aws.amazon.com/secretsmanager/.
2. Elija Almacenar un secreto nuevo.
3. Elija Credenciales para base de datos de Amazon RDS.
4. Introduzca un nombre de usuario y una contraseña. Las credenciales que introduzca deben coincidir con las credenciales de un usuario de base de datos que exista en la base de datos de RDS asociada. Proxy de RDS utiliza estas credenciales para autenticar y establecer conexiones con la base de datos en nombre de las aplicaciones.

   Si no hay coincidencia, puede actualizar el secreto para que coincida con la contraseña de la base de datos. Hasta que no actualice el secreto, los intentos de conexión a través del proxy mediante ese secreto no se realizarán correctamente, pero las conexiones que utilicen otros secretos válidos seguirán funcionando.

   > **Note**
   >
   > En el caso de RDS para SQL Server, Proxy de RDS requiere un secreto que distinga entre mayúsculas y minúsculas en Secrets Manager, independientemente de la configuración de intercalación de la instancia de base de datos. Si la aplicación permite nombres de usuario con distintas mayúsculas, como “Admin” y “admin”, deberá crear secretos distintos para cada uno. Proxy de RDS no admite la autenticación de nombre de usuario sin distinción entre mayúsculas y minúsculas entre el cliente y el proxy.

Para obtener más información sobre colación en SQL Server, consulte la documentación de Microsoft SQL Server.

5. En Base de datos, seleccione la base de datos de Amazon RDS a la que accederá el secreto.
6. Rellene otras configuraciones para el secreto y elija Guardar. Para obtener instrucciones completas, consulte Creación de un secreto de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

AWS CLI

Cuando cree un proxy a través de la AWS CLI, especifique los nombres de recursos de Amazon (ARN) de los secretos correspondientes. Lo hace para todas las cuentas de usuario de base de datos a las que puede acceder el proxy. En la AWS Management Console, elija los secretos por sus nombres descriptivos.

- Para crear un secreto de Secrets Manager para utilizarlo con Proxy de RDS, utilice el comando create-secret:

```
aws secretsmanager create-secret \
  --name "secret_name" \
  --description "secret_description" \
  --region region_name \
  --secret-string '{"username":"db_user","password":"db_user_password"}'
```

- También puede crear una clave personalizada para cifrar su secreto de Secrets Manager. El siguiente comando crea una clave de ejemplo.

```
aws kms create-key --description "test-key" --policy '{
  "Id":"kms-policy",
  "Version":"2012-10-17",
  "Statement":
    [
      {
        "Sid":"Enable IAM User Permissions",
        "Effect":"Allow",
        "Principal":{"AWS":"arn:aws:iam::account_id:root"},
        "Action":"kms:*","Resource":"*"
      },
      {
        "Sid":"Allow access for Key Administrators",
```

```
        "Effect":"Allow",
        "Principal":
          {
            "AWS":
              ["$USER_ARN","arn:aws:iam:account_id::role/Admin"]
          },
        "Action":
          [
            "kms:Create*",
            "kms:Describe*",
            "kms:Enable*",
            "kms:List*",
            "kms:Put*",
            "kms:Update*",
            "kms:Revoke*",
            "kms:Disable*",
            "kms:Get*",
            "kms:Delete*",
            "kms:TagResource",
            "kms:UntagResource",
            "kms:ScheduleKeyDeletion",
            "kms:CancelKeyDeletion"
          ],
        "Resource":"*"
      },
      {
        "Sid":"Allow use of the key",
        "Effect":"Allow",
        "Principal":{"AWS":"$ROLE_ARN"},
        "Action":["kms:Decrypt","kms:DescribeKey"],
        "Resource":"*"
      }
    ]
}'
```

Por ejemplo, los siguientes comandos crean secretos de Secrets Manager para dos usuarios de bases de datos:

```
aws secretsmanager create-secret \
  --name secret_name_1 --description "db admin user" \
  --secret-string '{"username":"admin","password":"choose_your_own_password"}'
```

```
aws secretsmanager create-secret \
  --name secret_name_2 --description "application user" \
  --secret-string '{"username":"app-user","password":"choose_your_own_password"}'
```

Para crear estos secretos cifrados con su clave de AWS KMS personalizada, use los siguientes comandos:

```
aws secretsmanager create-secret \
  --name secret_name_1 --description "db admin user" \
  --secret-string '{"username":"admin","password":"choose_your_own_password"}' \
  --kms-key-id arn:aws:kms:us-east-2:account_id:key/key_id

aws secretsmanager create-secret \
  --name secret_name_2 --description "application user" \
  --secret-string '{"username":"app-user","password":"choose_your_own_password"}' \
  --kms-key-id arn:aws:kms:us-east-2:account_id:key/key_id
```

Para ver los secretos que posee la cuenta de AWS, utilice el comando list-secrets:

```
aws secretsmanager list-secrets
```

Si crea un proxy mediante la CLI, se pasan los nombres de recursos de Amazon (ARN) de uno o más secretos al parámetro `--auth`. En el siguiente ejemplo se muestra cómo preparar un informe si solo se tiene el nombre y el ARN de cada secreto que es propiedad de la cuenta de AWS. En este ejemplo se utiliza el parámetro `--output table`, disponible en la versión 2 de la AWS CLI. Si está utilizando la versión 1 de la AWS CLI, use `--output text`.

```
aws secretsmanager list-secrets --query '*[].[Name,ARN]' --output table
```

Para confirmar que el secreto contiene las credenciales correctas en el formato adecuado, utilice el comando get-secret-value. Reemplace *your_secret_name* por el nombre corto o ARN del secreto.

```
aws secretsmanager get-secret-value --secret-id your_secret_name
```

La salida contiene una línea con un valor codificado en JSON similar al siguiente:

```
...
"SecretString": "{\"username\":\"your_username\",\"password\":\"your_password\"}",
...
```

Configuración de políticas de AWS Identity and Access Management (IAM) para RDS Proxy

Después de crear los secretos en Secrets Manager, se crea una política de IAM que puede acceder a esos secretos. Para obtener más información acerca del uso de la IAM, consulte Administración de la identidad y el acceso en Amazon RDS.

> **Tip**
>
> El procedimiento siguiente se aplica si utiliza la consola de IAM. Si utiliza la AWS Management Console para RDS, RDS puede crear automáticamente la política de IAM. En ese caso, puede omitir el siguiente procedimiento.

Para crear una política de IAM que acceda a sus secretos de Secrets Manager para su uso con su proxy

1. Inicie sesión en la consola de IAM. Siga el proceso de Crear rol, tal como se describe en Creación de roles de IAM, y elija Crear un rol para delegar permisos a un servicio de AWS.

   Elija Servicio de AWS en Tipo de entidad de confianza. En Caso de uso, seleccione RDS en el menú desplegable Casos de uso para otros servicios de AWS. Elija RDS: Añadir rol a la base de datos.

2. Para el nuevo rol, realice el paso Add inline policy (Añadir política en línea). Utilice los mismos procedimientos generales que en Edición de políticas de IAM. Pegue el siguiente JSON en el cuadro de texto de JSON. Sustituya su propio ID de cuenta. Sustituya su región de AWS por `us-east-2`. Sustituya los nombres de recurso de Amazon (ARN) por los secretos que ha creado. Consulte Especificación de claves KMS en declaraciones de políticas de IAM. Para la acción `kms:Decrypt`, sustituya el ARN de la clave de KMS predeterminada AWS KMS key o su propia clave de KMS. El que utilice depende del que haya utilizado para cifrar los secretos de Secrets Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": "secretsmanager:GetSecretValue",
            "Resource": [
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_1",
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_2"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-2:account_id:key/key_id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
                }
            }
        }
    ]
}
```

3. Modifique la política de confianza para este rol de IAM. Pegue el siguiente JSON en el cuadro de texto de JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Los comandos siguientes realizan la misma operación a través de la AWS CLI.

```
PREFIX=my_identifier
USER_ARN=$(aws sts get-caller-identity --query "Arn" --output text)
```

```
aws iam create-role --role-name my_role_name \
  --assume-role-policy-document '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"Service":
["rds.amazonaws.com"]},"Action":"sts:AssumeRole"}]}'

ROLE_ARN=arn:aws:iam::account_id:role/my_role_name

aws iam put-role-policy --role-name my_role_name \
  --policy-name $PREFIX-secret-reader-policy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Resource": [
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_1",
                "arn:aws:secretsmanager:us-east-2:account_id:secret:secret_name_2"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "kms:Decrypt",
            "Resource": "arn:aws:kms:us-east-2:account_id:key/key_id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Creación de un proxy para Amazon RDS

Puede asociar un proxy con una instancia de base de datos de RDS para MariaDB, RDS para Microsoft SQL Server, RDS para MySQL o RDS para PostgreSQL.

Consola

Para crear un proxy

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Proxies.
3. Elija Create proxy (Crear proxy).
4. Configure los siguientes ajustes para el proxy.

Opción	Descripción
Familia de motores	El protocolo de red de base de datos reconoce el proxy cuando interpreta el tráfico de red hacia y desde la base de datos. **Note** Para usar RDS para PostgreSQL, asegúrese de retener la base de datos de `postgres` en la instancia. Consulte Se ha eliminado la solución de problemas de una base de datos de `postgres`.
Identificador de proxy	Un nombre que sea único dentro del ID de cuenta de AWS y de la región de AWS actual.
Tiempo de espera de inactividad de conexión de cliente	El proxy cierra la conexión de un cliente si permanece inactiva durante un periodo determinado. De forma predeterminada, esto es 1800 segundos (30 minutos). Una conexión se considera inactiva cuando la aplicación no envía una nueva solicitud dentro del plazo especificado después de completar la solicitud anterior. El proxy mantiene abierta la conexión de base de datos subyacente y la devuelve al grupo de conexiones, de modo que esté disponible para nuevas conexiones de clientes. Para eliminar de forma proactiva las conexiones obsoletas, reduzca el tiempo de espera de conexión de cliente inactivo.

Opción	Descripción
	Para minimizar los costos de conexión durante los picos de carga de trabajo, aumente el tiempo de espera.
Base de datos	Instancia de base de datos de RDS para acceder a través de este proxy. La lista solo incluye instancias de base de datos y clústeres con motores de base de datos compatibles, versiones de motor y otras configuraciones. Si la lista está vacía, cree una nueva instancia de base de datos o clúster que sea compatible con RDS Proxy. Para ello, siga el procedimiento en Creación de una instancia de base de datos de Amazon RDS. A continuación, intente volver a crear el proxy.
Conexiones máximas de grupo de conexión	Un valor entre 1 y 100 para definir el porcentaje del límite de `max_connections` que RDS Proxy puede utilizar. Si solo tiene la intención de utilizar un proxy con esta instancia de base de datos o clúster, establezca este valor en 100. Para obtener más información sobre cómo RDS Proxy usa esta configuración, consulte the section called “MaxConnectionsPercent”.

Opción	Descripción
Filtros de fijación de sesión	Impide que RDS Proxy fije determinados estados de sesión detectados, lo que evita las medidas de seguridad predeterm inadas para las conexiones de multiplexación. Actualmente, PostgreSQL no admite esta configuración y la única opción disponible es `EXCLUDE_VARIABLE_SETS` . Si se habilita, es posible que las variables de sesión de una conexión afecten a otras, lo que puede provocar errores o problemas de correcció n si las consultas dependen de variables de sesión establecidas fuera de la transacción actual. Utilice esta opción solo después de confirmar que las aplicaciones pueden compartir conexiones de bases de datos de forma segura. Los siguientes patrones se consideran seguros: • Instrucciones `SET` donde no hay ningún cambio en el valor efectivo de la variable de sesión. En otras palabras, no hay ningún cambio en la variable de sesión. • Cambia el valor de la variable de sesión y ejecuta una instrucción en la misma transacción. Para obtener más información, consulte Cómo evitar la fijación de RDS Proxy.
Tiempo de espera de préstamo de conexión	Si espera que el proxy utilice todas las conexiones de base de datos disponibles, establezca el tiempo de espera antes de que devuelva un error de tiempo de espera. Puede especificar hasta cinco minutos. Esta configuración solo se aplica cuando el proxy ha alcanzado el número máximo de conexiones y todas están en uso.

Opción	Descripción
Consulta de inicialización	Añada una consulta de inicialización o modifique la actual (opcional). Puede especificar una o más instrucciones de SQL para que el proxy se ejecute al abrir cada nueva conexión de base de datos. Normalmente, el ajuste se utiliza con instrucciones de SET para garantizar que cada conexión tenga una configuración idéntica. Asegúrese de que la consulta que añada sea válida. Para incluir varias variables en una única instrucción de SET, utilice separadores de coma. Por ejemplo: `SET variable1 =value1, variable2 =value2` Para varias instrucciones, utilice punto y coma como separador. **Important** Dado que se puede acceder a la consulta de inicialización como parte de la configuración del grupo de destino, no está protegida por métodos de autenticación o criptográficos. Cualquier persona con acceso para ver o administrar la configuración del grupo de destino del proxy puede ver la consulta de inicialización. No debe agregar información confidencial, como contraseñas o claves de cifrado de larga duración, a esta opción.
Rol de AWS Identity and Access Management (IAM)	Un rol de IAM con permiso para acceder a los secretos de Secrets Manager, que representan las credenciales de las cuentas de usuario de la base de datos que puede usar el proxy. Otra opción, puede crear un rol de IAM nuevo desde la AWS Management Console.
Secretos de Secrets Manager	Elija al menos un secreto de Secrets Manager que contenga credenciales de usuario de base de datos que permita al proxy acceder a la instancia de base de datos de RDS.

Opción	Descripción
Tipo de autenticación de cliente	El tipo de autenticación que utiliza el proxy para las conexione s de los clientes. Su elección se aplica a todos los secretos de Secrets Manager que asocie a este proxy. Si tiene que especificar un tipo de autenticación de cliente diferente para cada secreto, cree su proxy mediante la AWS CLI o la API.
Autenticación de IAM	Si desea requerir, permitir o no permitir la autenticación de IAM para las conexiones al proxy. La opción de permiso solo es válida para los proxies de RDS para SQL Server. Su elección se aplica a todos los secretos de Secrets Manager que asocie a este proxy. Si tiene que especificar un tipo de autenticación de IAM diferente para cada secreto, cree su proxy mediante la AWS CLI o la API.
Requerir seguridad de capa de transporte	Aplica TLS/SSL para todas las conexiones de cliente. El proxy utiliza la misma configuración de cifrado para su conexión a la base de datos subyacente, si la conexión del cliente se cifra o no se cifra.
Subredes	Este campo se rellena previamente con todas las subredes asociadas a la VPC. Puede eliminar cualquier subred que no sea necesaria para el proxy, pero debe dejar al menos dos subredes.

Opción	Descripción
VPC security group (Grupo de seguridad de VPC)	Elija un grupo de seguridad de VPC existente o cree uno nuevo desde la AWS Management Console. Configure las reglas de entrada para permitir que las aplicaciones accedan al proxy y las reglas de salida para permitir el tráfico desde los destinos de base de datos. **Note** El grupo de seguridad debe permitir conexiones desde el proxy a la base de datos. Sirve para la entrada de las aplicaciones al proxy y para la salida del proxy a la base de datos. Por ejemplo, si utiliza el mismo grupo de seguridad para la base de datos y el proxy, asegúrese de que los recursos dentro de ese grupo de seguridad puedan comunicarse entre sí. Cuando se utiliza una VPC compartida, evite el uso del grupo de seguridad predeterminado para la VPC o uno asociado a otra cuenta. En su lugar, elija un grupo de seguridad que pertenezca a la cuenta. Si no existe ninguno, créelo. Para obtener más información, consulte Trabajar con VPC compartidas. RDS despliega un proxy en varias zonas de disponibilidad para garantizar una alta disponibilidad. Para habilitar la comunicac ión entre zonas de disponibilidad, la lista de control de acceso (ACL) a la red de la subred del proxy debe permitir la salida específica en el puerto del motor y la entrada en todos los puertos. Para obtener más información acerca de las ACL de red de, consulte Controlar el tráfico hacia las subredes utilizand o las ACL de red. Si la ACL de red del proxy y la de destino son idénticas, debe añadir una regla de entrada del protocolo TCP en la que el Origen esté configurado en el CIDR de la VPC. También debe añadir una regla de salida del protocolo

Opción	Descripción
	TCP específica del puerto del motor en la que el Destino esté configurado en el CIDR de la VPC.
Activación del registro mejorado	Habilite esta configuración para solucionar problemas de compatibilidad de proxy o rendimiento. Cuando está habilitado, RDS Proxy registra información sobre el rendimiento detallada para ayudarle a depurar el comportamiento de SQL o el rendimiento y la escalabilidad de la conexión del proxy. Habilite esta configuración solo para la depuración y asegúrese de que existan las medidas de seguridad adecuadas para proteger la información confidencial en los registros. Para minimizar la sobrecarga, RDS Proxy desactiva automáticamente esta configuración 24 horas después de la activación. Úsela temporalmente para solucionar problemas específicos.

5. Elija Create proxy (Crear proxy).

AWS CLI

Para crear un proxy utilizando el comando AWS CLI, llame al comando create-db-proxy con los siguientes parámetros requeridos:

- `--db-proxy-name`
- `--engine-family`
- `--role-arn`
- `--auth`
- `--vpc-subnet-ids`

El valor `--engine-family` distingue entre mayúsculas y minúsculas.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-proxy \
```

```
    --db-proxy-name proxy_name \
    --engine-family { MYSQL | POSTGRESQL | SQLSERVER } \
    --auth ProxyAuthenticationConfig_JSON_string \
    --role-arn iam_role \
    --vpc-subnet-ids space_separated_list \
    [--vpc-security-group-ids space_separated_list] \
    [--require-tls | --no-require-tls] \
    [--idle-client-timeout value] \
    [--debug-logging | --no-debug-logging] \
    [--tags comma_separated_list]
```

Para Windows:

```
aws rds create-db-proxy ^
    --db-proxy-name proxy_name ^
    --engine-family { MYSQL | POSTGRESQL | SQLSERVER } ^
    --auth ProxyAuthenticationConfig_JSON_string ^
    --role-arn iam_role ^
    --vpc-subnet-ids space_separated_list ^
    [--vpc-security-group-ids space_separated_list] ^
    [--require-tls | --no-require-tls] ^
    [--idle-client-timeout value] ^
    [--debug-logging | --no-debug-logging] ^
    [--tags comma_separated_list]
```

A continuación se muestra un ejemplo del valor JSON para la opción `--auth`. Este ejemplo aplica un tipo de autenticación de cliente diferente a cada secreto.

```
[
  {
    "Description": "proxy description 1",
    "AuthScheme": "SECRETS",
    "SecretArn": "arn:aws:secretsmanager:us-
west-2:123456789123:secret/1234abcd-12ab-34cd-56ef-1234567890ab",
    "IAMAuth": "DISABLED",
    "ClientPasswordAuthType": "POSTGRES_SCRAM_SHA_256"
  },

  {
    "Description": "proxy description 2",
    "AuthScheme": "SECRETS",
    "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret/1234abcd-12ab-34cd-56ef-1234567890cd",
```

```
    "IAMAuth": "DISABLED",
    "ClientPasswordAuthType": "POSTGRES_MD5"

  },

  {
    "Description": "proxy description 3",
    "AuthScheme": "SECRETS",
    "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122221111:secret/1234abcd-12ab-34cd-56ef-1234567890ef",
    "IAMAuth": "REQUIRED"
  }

]
```

> **Tip**
>
> Si aún no conoce los ID de subred que utilizar para el parámetro `--vpc-subnet-ids`, consulte Configuración de requisitos previos de red para RDS Proxy para ver ejemplos de cómo encontrarlos.

> **Note**
>
> Este grupo de seguridad debe permitir el acceso a la base de datos a la que se conecta el proxy. El mismo grupo de seguridad se utiliza para la entrada de las aplicaciones al proxy y para la salida del proxy a la base de datos. Por ejemplo, supongamos que utiliza el mismo grupo de seguridad para la base de datos y el proxy. En este caso, asegúrese de especificar que los recursos de ese grupo de seguridad pueden comunicarse con otros recursos del mismo grupo de seguridad.
>
> Cuando se utiliza una VPC compartida, no se puede utilizar el grupo de seguridad predeterminado para la VPC o uno que pertenezca a otra cuenta. Elija un grupo de seguridad que pertenezca a su cuenta. Si no existe uno, créelo. Para obtener más información acerca de esta limitación, consulte Trabajar con VPC compartidas.

Para crear las asociaciones adecuadas para el proxy, utilice también el comando register-db-proxy-targets. Especifique el nombre de grupo de destino de `default`. El proxy de RDS crea automáticamente un grupo de destino con este nombre cuando crea cada proxy.

```
aws rds register-db-proxy-targets
    --db-proxy-name value
    [--target-group-name target_group_name]
    [--db-instance-identifiers space_separated_list]  # rds db instances, or
    [--db-cluster-identifiers cluster_id]        # rds db cluster (all instances)
```

API de RDS

Para crear un proxy de RDS, llame a la operación de la API de Amazon RDS CreateDBProxy. Transfiera un parámetro con la estructura de datos AuthConfig .

El proxy de RDS crea automáticamente un grupo de destino denominado `default` cuando crea cada proxy. Se asocia una instancia de base de datos de RDS con el grupo de destino llamando a la función RegisterDBProxyTargets.

Visualización de un proxy

Después de crear uno o varios proxies de RDS, puede verlos y administrarlos en la AWS Management Console, la AWS CLI o la API de RDS. Puede revisar sus detalles de configuración, supervisar el rendimiento y determinar qué proxies modificar o eliminar según sea necesario.

Para permitir que las aplicaciones de base de datos enruten el tráfico a través de un proxy, debe especificar el punto de conexión del proxy en la cadena de conexión.

Consola

Visualización de un proxy en la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Proxies.
3. Seleccione el nombre del proxy para ver sus detalles.
4. En la página de detalles, la sección Grupos de destino muestra cómo se enlaza el proxy a una instancia de base de datos de RDS específica. Puede navegar a la página del grupo de destino predeterminado para obtener una vista más detallada de esta asociación, incluida la configuración definida durante la creación del proxy. Esta incluye el porcentaje máximo de conexión, el tiempo de espera de préstamo de la conexión, la familia de motores y los filtros de fijación de sesión.

CLI

Para consultar el proxy mediante la CLI, utilice el comando describe-db-proxies. De forma predeterminada, la solicitud devuelve todos los proxies propiedad de la cuenta de AWS. Para ver los detalles de un solo proxy, especifique su nombre con el parámetro `--db-proxy-name`.

```
aws rds describe-db-proxies [--db-proxy-name proxy_name]
```

Para consultar otra información asociada con el proxy, utilice los comandos que se muestran a continuación.

```
aws rds describe-db-proxy-target-groups  --db-proxy-name proxy_name

aws rds describe-db-proxy-targets --db-proxy-name proxy_name
```

Utilice la siguiente secuencia de comandos para ver más detalles acerca de las cosas que están asociadas con el proxy:

1. Para obtener una lista de proxies, ejecute describe-db-proxies.
2. Para mostrar parámetros de conexión como el porcentaje máximo de conexiones que puede utilizar el proxy, ejecute describe-db-proxy-target-groups `--db-proxy-name`. Utilice el nombre del proxy como el valor del parámetro.
3. Para consultar los detalles de la instancia de base de datos de RDS con asociación con el grupo de destino devuelto, ejecute describe-db-proxy-targets.

API de RDS

Para ver los proxies mediante la API de RDS, utilice la operación DescribeDBProxies . Devuelve valores del tipo de datos DBProxy.

Para consultar los detalles de la configuración de conexión del proxy, utilice los identificadores de proxy de este valor devuelto con la operación DescribeDBProxyTargetGroups. Devuelve valores del tipo de datos DBProxyTargetGroup.

Para consultar la instancia de RDS o el clúster de bases de datos de Aurora asociado con el proxy, utilice la operación DescribeDBProxyTargets. Devuelve valores del tipo de datos DBProxyTarget.

Conexión a una base de datos mediante RDS Proxy

La forma en que se conecta a una instancia de base de datos de RDS a través de un proxy es generalmente la misma que para conectarla directamente a la base de datos. Para obtener más información, consulte Información general de los puntos de enlace de proxy.

Temas

- Conexión a un proxy mediante autenticación nativa
- Conexión a un proxy mediante autenticación de IAM
- Consideraciones para conectarse a un proxy con Microsoft SQL Server
- Consideraciones para conectarse a un proxy con PostgreSQL

Conexión a un proxy mediante autenticación nativa

Utilice los siguientes pasos para conectarse a un proxy mediante autenticación nativa:

1. Buscar el punto de enlace del proxy. En la AWS Management Console, puede encontrar el punto de enlace en la página de detalles del proxy correspondiente. Con la AWS CLI, puede usar el comando describe-db-proxies. El siguiente ejemplo muestra cómo.

```
# Add --output text to get output as a simple tab-separated list.
$ aws rds describe-db-proxies --query '*[*].
{DBProxyName:DBProxyName,Endpoint:Endpoint}'
[
    [
        {
            "Endpoint": "the-proxy.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy"
        },
        {
            "Endpoint": "the-proxy-other-secret.proxy-demo.us-
east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-other-secret"
        },
        {
            "Endpoint": "the-proxy-rds-secret.proxy-demo.us-
east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-rds-secret"
        },
        {
```

```
            "Endpoint": "the-proxy-t3.proxy-demo.us-east-1.rds.amazonaws.com",
            "DBProxyName": "the-proxy-t3"
        }
    ]
]
```

2. Especifique el punto de conexión como parámetro del host en la cadena de conexión de la aplicación cliente. Por ejemplo, especifique el punto de enlace del proxy como el valor para la opción `mysql -h` o la opción `psql -h`.
3. Proporcione el mismo nombre de usuario y contraseña de la base de datos como suele hacer.

Conexión a un proxy mediante autenticación de IAM

Cuando utilice la autenticación de IAM con RDS Proxy, configure los usuarios de base de datos para que se autentiquen con nombres de usuario y contraseñas normales. La autenticación de IAM se aplica a RDS Proxy mediante la recuperación del nombre de usuario y las credenciales de contraseña de Secrets Manager. La conexión desde RDS Proxy a la base de datos subyacente no pasa a través de IAM.

Para conectarse a RDS Proxy utilizando la autenticación de IAM, utilice el mismo procedimiento general de conexión que para la autenticación de IAM con una instancia de base de datos de RDS. Para obtener más información acerca del uso de la IAM, consulte Seguridad en Amazon RDS.

Las principales diferencias en el uso de IAM para RDS Proxy incluyen las siguientes:

- No se configura cada usuario de base de datos individual con un complemento de autorización. Los usuarios de la base de datos todavía tienen nombres de usuario y contraseñas regulares dentro de la base de datos. Se configuran los secretos de Secrets Manager que contienen estos nombres de usuario y contraseñas y se autoriza al RDS Proxy para recuperar las credenciales de Secrets Manager.

  La autenticación IAM se aplica a la conexión entre el programa cliente y el proxy. A continuación, el proxy se autentica en la base de datos utilizando las credenciales de nombre de usuario y contraseña recuperadas de Secrets Manager.
- En lugar del punto de enlace de instancia, clúster o lector, se especifica el punto de enlace del proxy. Para obtener detalles sobre el punto de enlace del proxy, consulte Conexión a la instancia con la autenticación de IAM.

- En el caso de autenticación de IAM de la base de datos directa, se eligen de forma selectiva los usuarios de la base de datos y se configuran para que se identifiquen con un complemento de autenticación especial. Puede conectarse a esos usuarios mediante la autenticación de IAM.

  En el caso de uso del proxy, proporciona al proxy secretos que contengan el nombre de usuario y la contraseña de algún usuario (autenticación nativa). A continuación, se conecta al proxy mediante la autenticación de IAM. Aquí, puede hacerlo al generar un token de autenticación con el punto de conexión del proxy, no el punto de conexión de la base de datos. También utiliza un nombre de usuario que coincida con uno de los nombres de usuario de los secretos que proporcionó.
- Asegúrese de que usa Transport Layer Security (TLS)/Capa de sockets seguros (SSL) cuando se conecte a un proxy mediante la autenticación de IAM.

Puede conceder acceso al proxy a un usuario específico modificando la política de IAM. Ejemplo:

```
"Resource": "arn:aws:rds-db:us-east-2:1234567890:dbuser:prx-ABCDEFGHIJKL01234/db_user"
```

Consideraciones para conectarse a un proxy con Microsoft SQL Server

Para conectarse a un proxy mediante la autenticación de IAM, no utilice el campo de contraseña. En su lugar, debe proporcionar la propiedad de token adecuada para cada tipo de controlador de base de datos en el campo token. Por ejemplo, utilice la propiedad `accessToken` para JDBC o la propiedad `sql_copt_ss_access_token` para ODBC. O utilice la propiedad `AccessToken` del controlador .NET SqlClient. No puede usar la autenticación de IAM con clientes que no admitan propiedades de token.

En algunas condiciones, un proxy no puede compartir una conexión de base de datos y, en cambio, vincula la conexión de la aplicación cliente al proxy a una conexión de base de datos dedicada. Para más información sobre estas condiciones, consulte Cómo evitar la fijación de RDS Proxy.

Consideraciones para conectarse a un proxy con PostgreSQL

Si crea un nuevo usuario de base de datos de PostgreSQL para conectarse a RDS Proxy, asegúrese de conceder al usuario el privilegio `CONNECT` en la base de datos. Sin esto, el usuario no puede establecer una conexión. Para obtener más información, consulte the section called “Cómo añadir un nuevo usuario de base de datos a una base de datos PostgreSQL al usar RDS Proxy”.

Cuando un cliente comienza una conexión a una base de datos de PostgreSQL, envía un mensaje de inicio. Este mensaje incluye pares de cadenas de nombres y valores de parámetros. Para obtener

detalles, consulte `StartupMessage` en Formatos de mensaje de PostgreSQL en la documentación de PostgreSQL.

Al conectarse a través de un proxy de RDS, el mensaje de inicio puede incluir los siguientes parámetros reconocidos actualmente:

- `user`
- `database`

El mensaje de inicio también puede incluir los siguientes parámetros de tiempo de ejecución adicionales:

- `application_name`
- `client_encoding`
- `DateStyle`
- `TimeZone`
- `extra_float_digits`
- `search_path`

Para obtener más información acerca de la mensajería de PostgreSQL, consulte el Protocolo Frontend/Backend en la documentación de PostgreSQL.

Para PostgreSQL, si usa JDBC, recomendamos lo siguiente para evitar la fijación:

- Establezca el parámetro de conexión JDBC `assumeMinServerVersion` en al menos `9.0` para evitar la fijación. Esto evita que el controlador JDBC realice un viaje de ida y vuelta adicional durante el inicio de la conexión cuando se ejecuta `SET extra_float_digits = 3`.
- Establezca el parámetro de conexión JDBC `ApplicationName` en *`any/your-application-name`* para evitar la fijación. Al hacerlo, se evita que el JDBC driver realice un viaje de ida y vuelta adicional durante el inicio de la conexión cuando se ejecuta `SET application_name = "PostgreSQL JDBC Driver"`. Tenga en cuenta que el parámetro JDBC es `ApplicationName` pero el parámetro `StartupMessage` de PostgreSQL es `application_name`.

Para obtener más información, consulte Cómo evitar la fijación de RDS Proxy. Para obtener más información acerca de la conexión mediante JDBC, consulte Conexión a la base de datos en la documentación de PostgreSQL.

Administración de un RDS Proxy

En esta sección, se proporciona información sobre cómo administrar el funcionamiento y la configuración de RDS Proxy. Estos procedimientos ayudan a su aplicación a hacer más eficiente el uso de las conexiones de base de datos y a lograr la máxima reutilización de la conexión. Cuanto más pueda aprovechar la reutilización de la conexión, más sobrecarga de la CPU y la memoria podrá evitar. Esto, a su vez, reduce la latencia de la aplicación y permite que la base de datos dedique más recursos al procesamiento de solicitudes de la aplicación.

Temas

- Modificación de un RDS Proxy
- Cómo añadir un nuevo usuario de base de datos al usar RDS Proxy
- Observaciones sobre la conexión de RDS Proxy
- Cómo evitar la fijación de RDS Proxy
- Eliminación de un RDS Proxy

Modificación de un RDS Proxy

Puede cambiar determinadas configuraciones asociadas a un proxy después de crearlos. Para ello, modifique el propio proxy, su grupo de destino asociado o ambos. Cada proxy tiene un grupo de destino asociado.

AWS Management Console

> **Important**
>
> Los valores de los campos Client authentication type (Tipo de autenticación de cliente) y IAM authentication (Autenticación de IAM) se aplican a todos los secretos de Secrets Manager asociados a este proxy. Para especificar valores diferentes para cada secreto, modifique su proxy mediante la AWS CLI o la API.

Para modificar la configuración de un proxy

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Proxies.
3. En la lista de proxies, elija el proxy cuya configuración desea modificar o vaya a su página de detalles.
4. Para Actions (Acciones), elija Modify (Modificar).
5. Introduzca o elija las propiedades que desea modificar. Puede modificar lo siguiente:

   - Proxy identifier (Identificador de proxy: escriba un nuevo identificador para cambiar el nombre del proxy.
   - Idle client connection timeout (Tiempo de espera de inactividad de conexión de cliente): especifique un período de tiempo de espera de conexión de cliente inactiva.
   - IAM role (Rol de IAM): cambie el rol de IAM utilizado para recuperar los secretos de Secrets Manager.
   - Secrets Manager secrets (Secretos de Secrets Manager): agregue o elimine secretos de Secrets Manager. Estos secretos corresponden a nombres de usuario y contraseñas de la base de datos.
   - Client authentication type (Tipo de autenticación de cliente): (solo PostgreSQL) cambie el tipo de autenticación de las conexiones del cliente al proxy.
   - IAM Authentication (Autenticación de IAM): requiera o no permita la autenticación de IAM para las conexiones al proxy.
   - Require Transport Layer Security (Requerir Transport Layer Security): active o desactive el requisito de Transport Layer Security (TLS).
   - VPC security group (Grupo de seguridad de VPC): agregue o quite grupos de seguridad de VPC para que los utilice el proxy.
   - Enable enhanced logging (Habilitar el registro optimizado): habilite o deshabilite el registro mejorado.
6. Elija Modify.

Si no ha encontrado la configuración mostrada que desea cambiar, utilice el procedimiento siguiente para actualizar el grupo de destino del proxy. El grupo de destino asociado con un proxy controla la configuración relacionada con las conexiones de base de datos físicas. Cada proxy tiene un grupo de destino asociado llamado `default`, que se crea automáticamente junto con el proxy. No se puede cambiar el nombre del grupo de destino predeterminado.

Solo puede modificar el grupo de destino desde la página de detalles del proxy, no desde la lista de la página Proxies.

Para modificar la configuración de un grupo de destino de proxy

1. En la página Proxies, vaya a la página de detalles de un proxy.
2. En Target groups (Grupos de destino), elija el enlace `default`. Actualmente, todos los proxies tienen un único grupo de destino denominado `default`.
3. En la página de detalles del grupo de destino default (predeterminado) elija Modify (Modificar).
4. Elija nuevas configuraciones para las propiedades que puede modificar:

   - Base de datos: elija una instancia de base de datos de RDS diferente.
   - Connection pool maximum connections (Conexiones máximas de grupo de conexión): ajuste el porcentaje de conexiones disponibles máximas que puede utilizar el proxy.
   - Session pinning filters (Filtros de fijación de sesión): (opcional) elija un filtro de fijación de sesión. De este modo se eluden las medidas de seguridad predeterminadas para multiplexar las conexiones de bases de datos en las conexiones del cliente. Actualmente, la configuración no es compatible con PostgreSQL. La única opción es `EXCLUDE_VARIABLE_SETS`.

     Si se habilita esta configuración, es posible que las variables de sesión de una conexión afecten a otras conexiones. Esto puede provocar errores o problemas de corrección si las consultas dependen de valores de variables de sesión establecidos fuera de la transacción actual. Considere la posibilidad de utilizar esta opción después de comprobar que sea seguro que sus aplicaciones compartan conexiones de bases de datos en las conexiones del cliente.

     Los siguientes patrones pueden considerarse seguros:

     - Instrucciones `SET` en las que no hay ningún cambio en el valor de la variable de sesión efectiva, es decir, no hay ningún cambio en la variable de sesión.
     - Cambia el valor de la variable de sesión y ejecuta una instrucción en la misma transacción.

     Para obtener más información, consulte Cómo evitar la fijación de RDS Proxy.
   - Connection borrow timeout (Tiempo de espera de préstamo de conexión): ajuste el intervalo de tiempo de espera de préstamo de la conexión. Esta configuración se aplica cuando el número máximo de conexiones ya se está utilizando para el proxy. La configuración determina cuánto tiempo espera el proxy a que una conexión esté disponible antes de devolver un error de tiempo de espera.
   - Consutla de inicialización. Añada una consulta de inicialización o modifique la actual (opcional). Puede especificar una o más instrucciones de SQL para que el proxy se ejecute al abrir cada nueva conexión de base de datos. Normalmente, el ajuste se utiliza con

instrucciones de SET para garantizar que cada conexión tenga una configuración idéntica. Asegúrese de que la consulta que añada sea válida. Para incluir varias variables en una única instrucción de SET, utilice separadores de coma. Por ejemplo:

```
SET variable1=value1, variable2=value2
```

Para varias instrucciones, utilice punto y coma como separador.

No puede cambiar ciertas propiedades, como el identificador del grupo de destino y el motor de base de datos.

5. Elija Modify target group (Modificar grupo de destino).

AWS CLI

Para modificar un proxy mediante la AWS CLI, utilice los comandos modify-db-proxy, modify-db-proxy-target-group, deregister-db-proxy-targets y register-db-proxy-targets.

Con el comando `modify-db-proxy`, puede cambiar propiedades como las siguientes:

- El conjunto de secretos de Secrets Manager utilizados por el proxy.
- Si se requiere TLS.
- El tiempo de espera del cliente inactivo.
- Si se debe registrar información adicional de instrucciones de SQL para la depuración.
- El rol de IAM utilizado para recuperar secretos de Secrets Manager.
- Los grupos de seguridad utilizados por el proxy.

En el ejemplo siguiente se muestra cómo cambiar el nombre de un proxy existente.

```
aws rds modify-db-proxy --db-proxy-name the-proxy --new-db-proxy-name the_new_name
```

Para modificar la configuración relacionada con la conexión o cambiar el nombre del grupo de destino, utilice el comando `modify-db-proxy-target-group`. Actualmente, todos los proxies tienen un único grupo de destino denominado `default`. Cuando trabaja con este grupo de destino, debe especificar el nombre del proxy y `default` para el nombre del grupo de destino. No se puede cambiar el nombre del grupo de destino predeterminado.

En el ejemplo siguiente se muestra cómo comprobar primero la configuración de `MaxIdleConnectionsPercent` de un proxy y, a continuación, cambiarla mediante el grupo de destino.

```
aws rds describe-db-proxy-target-groups --db-proxy-name the-proxy

{
    "TargetGroups": [
        {
            "Status": "available",
            "UpdatedDate": "2019-11-30T16:49:30.342Z",
            "ConnectionPoolConfig": {
                "MaxIdleConnectionsPercent": 50,
                "ConnectionBorrowTimeout": 120,
                "MaxConnectionsPercent": 100,
                "SessionPinningFilters": []
            },
            "TargetGroupName": "default",
            "CreatedDate": "2019-11-30T16:49:27.940Z",
            "DBProxyName": "the-proxy",
            "IsDefault": true
        }
    ]
}

aws rds modify-db-proxy-target-group --db-proxy-name the-proxy --target-group-name
 default --connection-pool-config '
{ "MaxIdleConnectionsPercent": 75 }'

{
    "DBProxyTargetGroup": {
        "Status": "available",
        "UpdatedDate": "2019-12-02T04:09:50.420Z",
        "ConnectionPoolConfig": {
            "MaxIdleConnectionsPercent": 75,
            "ConnectionBorrowTimeout": 120,
            "MaxConnectionsPercent": 100,
            "SessionPinningFilters": []
        },
        "TargetGroupName": "default",
        "CreatedDate": "2019-11-30T16:49:27.940Z",
        "DBProxyName": "the-proxy",
        "IsDefault": true
```

```
    }
}
```

Con los comandos `deregister-db-proxy-targets` y `register-db-proxy-targets`, puede cambiar a qué instancias de base de datos de RDS está asociado el proxy a través de su grupo de destino. Actualmente, cada proxy puede conectarse a una instancia de base de datos de RDS. El grupo de destino realiza un seguimiento de los detalles de conexión de todas las instancias de base de datos de RDS en una configuración multi-AZ.

El ejemplo siguiente comienza con un proxy asociado a un clúster de Aurora MySQL denominado `cluster-56-2020-02-25-1399`. El ejemplo muestra cómo cambiar el proxy para que pueda conectarse a un clúster diferente denominado `provisioned-cluster`.

Cuando se trabaja con una instancia de base de datos RDS, se especifica la opción `--db-instance-identifier`.

El siguiente ejemplo modifica un proxy Aurora MySQL. Un proxy Aurora PostgreSQL tiene el puerto 5432.

```
aws rds describe-db-proxy-targets --db-proxy-name the-proxy

{
    "Targets": [
        {
            "Endpoint": "instance-9814.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-9814"
        },
        {
            "Endpoint": "instance-8898.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-8898"
        },
        {
            "Endpoint": "instance-1018.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-1018"
        },
        {
```

```
            "Type": "TRACKED_CLUSTER",
            "Port": 0,
            "RdsResourceId": "cluster-56-2020-02-25-1399"
        },
        {
            "Endpoint": "instance-4330.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "instance-4330"
        }
    ]
}

aws rds deregister-db-proxy-targets --db-proxy-name the-proxy --db-cluster-identifier
 cluster-56-2020-02-25-1399

aws rds describe-db-proxy-targets --db-proxy-name the-proxy

{
    "Targets": []
}

aws rds register-db-proxy-targets --db-proxy-name the-proxy --db-cluster-identifier
 provisioned-cluster

{
    "DBProxyTargets": [
        {
            "Type": "TRACKED_CLUSTER",
            "Port": 0,
            "RdsResourceId": "provisioned-cluster"
        },
        {
            "Endpoint": "gkldje.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "gkldje"
        },
        {
            "Endpoint": "provisioned-1.demo.us-east-1.rds.amazonaws.com",
            "Type": "RDS_INSTANCE",
            "Port": 3306,
            "RdsResourceId": "provisioned-1"
        }
```

```
    ]
}
```

API de RDS

Para modificar un proxy mediante la API de RDS, utilice las operaciones ModifyDBProxy, ModifyDBProxyTargetGroup, DeregisterDBProxyTargets y RegisterDBProxyTargets.

Con `ModifyDBProxy`, puede cambiar propiedades como las siguientes:

- El conjunto de secretos de Secrets Manager utilizados por el proxy.
- Si se requiere TLS.
- El tiempo de espera del cliente inactivo.
- Si se debe registrar información adicional de instrucciones de SQL para la depuración.
- El rol de IAM utilizado para recuperar secretos de Secrets Manager.
- Los grupos de seguridad utilizados por el proxy.

Con `ModifyDBProxyTargetGroup`, puede modificar la configuración relacionada con la conexión. Actualmente, todos los proxies tienen un único grupo de destino denominado `default`. Cuando trabaja con este grupo de destino, debe especificar el nombre del proxy y `default` para el nombre del grupo de destino. No se puede cambiar el nombre del grupo de destino predeterminado.

Con `DeregisterDBProxyTargets` y `RegisterDBProxyTargets`, puede cambiar con qué instancia de base de datos de RDS está asociado el proxy a través de su grupo de destino. Actualmente, cada proxy puede conectarse a una instancia de base de datos RDS. El grupo de destino hace un seguimiento de los detalles de conexión de las instancias de base de datos de RDS en una configuración Multi-AZ.

Cómo añadir un nuevo usuario de base de datos al usar RDS Proxy

En algunos casos, podría agregar un nuevo usuario de base de datos a un clúster o una instancia de base de datos de RDS asociado a un proxy. Si es así, agregue o reutilice un secreto de Secrets Manager para almacenar las credenciales de ese usuario. Para hacerlo, realice estos pasos:

1. Cree un nuevo secreto de Secrets Manager mediante el procedimiento descrito en Configuración de credenciales de base de datos en AWS Secrets Manager para RDS Proxy.
2. Actualice el rol de IAM para conceder acceso al RDS Proxy al nuevo secreto de Secrets Manager. Para ello, actualice la sección de recursos de la política del rol de IAM.

3. Modifique el proxy de RDS para añadir el nuevo secreto de Secrets Manager en Secretos de Secrets Manager.
4. Si el nuevo usuario toma el lugar de uno existente, actualice las credenciales almacenadas en el secreto de Secrets Manager del proxy para el usuario existente.

Cómo añadir un nuevo usuario de base de datos a una base de datos PostgreSQL al usar RDS Proxy

Al agregar un nuevo usuario a su base de datos de PostgreSQL, si ha ejecutado el siguiente comando:

```
REVOKE CONNECT ON DATABASE postgres FROM PUBLIC;
```

Otorgue al usuario `rdsproxyadmin` el privilegio `CONNECT` para que pueda supervisar las conexiones en la base de datos de destino.

```
GRANT CONNECT ON DATABASE postgres TO rdsproxyadmin;
```

También puede permitir que otros usuarios de la base de datos de destino realicen comprobaciones de estado cambiando `rdsproxyadmin` por el usuario de la base de datos del comando anterior.

Cambio de la contraseña de un usuario de base de datos al usar RDS Proxy

En algunos casos, puede cambiar la contraseña de un usuario de base de datos en una instancia de base de datos de RDS asociado a un proxy. Si es así, actualice el secreto de Secrets Manager correspondiente con la nueva contraseña.

Observaciones sobre la conexión de RDS Proxy

Configuración de los valores de conexión

Para ajustar la agrupación de conexiones de RDS Proxy, puede modificar la siguiente configuración:

- IdleClientTimeout
- MaxConnectionsPercent
- MaxIdleConnectionsPercent
- ConnectionBorrowTimeout

IdleClientTimeout

Puede especificar cuánto tiempo puede estar inactiva una conexión del cliente antes de que el proxy la cierre. El valor predeterminado es 1800 segundos (30 minutos).

Una conexión de cliente se considera inactiva cuando la aplicación no envía una nueva solicitud dentro del plazo especificado después de completar la solicitud anterior. La conexión de base de datos subyacente permanece abierta y se devuelve al grupo de conexiones. Por lo tanto, está disponible para reutilizarla para nuevas conexiones de cliente. Si quiere que el proxy elimine de forma proactiva las conexiones obsoletas, considere la posibilidad de reducir el tiempo de espera de conexión del cliente inactivo. Si la carga de trabajo establece conexiones frecuentes con el proxy, considere la posibilidad de aumentar el tiempo de espera de la conexión del cliente inactivo para ahorrar el costo del establecimiento de conexiones.

Esta configuración se representa mediante el campo Idle client connection timeout (Tiempo de espera de la conexión de cliente inactivo) en la consola de RDS y la configuración `IdleClientTimeout` en la AWS CLI y la API. Para obtener información sobre cómo cambiar el valor del campo Idle client connection timeout (Tiempo de espera de la conexión de cliente inactivo) en la consola de RDS, consulte AWS Management Console. Para obtener información sobre cómo cambiar el valor de la configuración `IdleClientTimeout`, consulte el comando de la CLI modify-db-proxy o la operación de la API ModifyDBProxy.

MaxConnectionsPercent

Puede limitar el número de conexiones que un proxy de RDS puede establecer con la base de datos de destino. Especifique el límite como porcentaje de las conexiones máximas disponibles para la base de datos. Esta configuración se representa mediante el campo Connection pool maximum connections (Conexiones máximas de grupo de conexión) en la consola de RDS y la configuración `MaxConnectionsPercent` en la AWS CLI y la API.

El valor `MaxConnectionsPercent` se expresa como un porcentaje de la configuración de `max_connections` para la instancia de base de datos de RDS que usa el grupo de destino. El proxy no crea todas estas conexiones por adelantado. Esta configuración permite que el proxy establezca estas conexiones a medida que la carga de trabajo las necesita.

Por ejemplo, en una base de datos registrada donde `max_connections` está establecido en 1000 y `MaxConnectionsPercent` está establecido en 95, el proxy de RDS establece 950 conexiones como límite máximo para las conexiones simultáneas a esa base de datos de destino.

Un efecto secundario habitual de que la carga de trabajo alcance el número máximo de conexiones a bases de datos permitidas es el aumento de la latencia general de las consultas, junto con un aumento de la métrica `DatabaseConnectionsBorrowLatency`. Puede supervisar las conexiones a bases de datos que se utilizan actualmente y el total permitido comparando las métricas `DatabaseConnections` y `MaxDatabaseConnectionsAllowed`.

Al configurar este parámetro, tenga en cuenta las siguientes prácticas recomendadas:

- Deje suficiente margen de conexión para los cambios en el patrón de carga de trabajo. Se recomienda configurar el parámetro al menos un 30 % por encima del uso supervisado máximo reciente. Dado que el proxy de RDS redistribuye las cuotas de conexión a las bases de datos entre varios nodos, los cambios en la capacidad interna pueden requerir al menos un 30 % de margen para conexiones adicionales para evitar un aumento de la latencia de préstamos.
- El proxy de RDS reserva una cantidad determinada de conexiones para la supervisión activa para facilitar una conmutación por error rápida, el enrutamiento del tráfico y las operaciones internas. La métrica `MaxDatabaseConnectionsAllowed` no incluye estas conexiones reservadas. Representa el número de conexiones disponibles para atender la carga de trabajo y puede ser inferior al valor derivado de la configuración de `MaxConnectionsPercent`.

  Valores de `MaxConnectionsPercent` mínimos recomendados

  - db.t3.small: 30
  - db.t3.medium o superior: 20

Para obtener información sobre cómo cambiar el valor del campo Connection pool maximum connections (Conexiones máximas de grupo de conexión) en la consola de RDS, consulte AWS Management Console. Para obtener información sobre cómo cambiar el valor de la configuración de `MaxConnectionsPercent`, consulte el comando de la CLI modify-db-proxy-target-group o la operación de la API ModifyDBProxyTargetGroup.

Para obtener información sobre los límites de conexión de base de datos, consulte Número máximo de conexiones de base de datos.

MaxIdleConnectionsPercent

Puede controlar el número de conexiones de base de datos inactivas que RDS Proxy puede mantener en el grupo de conexiones. De forma predeterminada, RDS Proxy considera que una conexión de base de datos en su grupo está inactiva cuando no ha habido actividad en la conexión durante cinco minutos.

El valor `MaxIdleConnectionsPercent` se expresa como un porcentaje de la configuración de `max_connections` para el grupo de destino de la instancia de base de datos de RDS. El valor predeterminado es del 50 por ciento de `MaxConnectionsPercent` y el límite superior es el valor de `MaxConnectionsPercent`. Por ejemplo, si `MaxConnectionsPercent` es 80, el valor predeterminado de `MaxIdleConnectionsPercent` es 40. Si no se especifica el valor de `MaxConnectionsPercent`, entonces `MaxIdleConnectionsPercent` es 5 para RDS para SQL Server y, para todos los demás motores, el valor predeterminado es 50.

Con un valor alto, el proxy deja un alto porcentaje de conexiones de base de datos inactivas abiertas. Con un valor bajo, el proxy cierra un alto porcentaje de conexiones de base de datos inactivas. Si sus cargas de trabajo son impredecibles, considere establecer un valor alto para `MaxIdleConnectionsPercent`. De este modo, RDS Proxy puede adaptarse a los aumentos de actividad sin abrir muchas conexiones de base de datos nuevas.

Esta configuración se representa mediante la configuración `MaxIdleConnectionsPercent` de `DBProxyTargetGroup` en la AWS CLI y la API. Para obtener información sobre cómo cambiar el valor de la configuración de `MaxIdleConnectionsPercent`, consulte el comando de la CLI modify-db-proxy-target-group o la operación de la API ModifyDBProxyTargetGroup.

Para obtener información sobre los límites de conexión de base de datos, consulte Número máximo de conexiones de base de datos.

ConnectionBorrowTimeout

Puede elegir cuánto tiempo espera RDS Proxy a que una conexión a la base de datos del grupo de conexiones esté disponible para su uso antes de devolver un error de tiempo de espera. El valor predeterminado es de 120 segundos. Esta configuración se aplica cuando el número de conexiones está al máximo, por lo que no hay conexiones disponibles en el grupo de conexiones. Esto también se aplica si no hay ninguna instancia de base de datos adecuada disponible para gestionar la solicitud, como cuando se esté realizando una operación de conmutación por error. Con esta configuración, puede establecer el mejor periodo de espera para la aplicación sin cambiar el tiempo de espera de la consulta en el código de la aplicación.

Esta configuración se representa mediante el campo Connection borrow timeout (Tiempo de espera de préstamo de conexión) en la consola de RDS o en la configuración de `ConnectionBorrowTimeout` de `DBProxyTargetGroup` de la AWS CLI o de la API. Para obtener información sobre cómo cambiar el valor del campo Connection borrow timeout (Tiempo de espera de préstamo de conexión) en la consola de RDS, consulte AWS Management Console. Para obtener información sobre cómo cambiar el valor de la configuración de

`ConnectionBorrowTimeout`, consulte el comando de la CLI modify-db-proxy-target-group o la operación de la API ModifyDBProxyTargetGroup.

Conexiones de cliente y base de datos

Las conexiones de la aplicación a RDS Proxy se conocen como conexiones de cliente. Las conexiones desde un proxy a la base de datos son conexiones de base de datos. Cuando se utiliza RDS Proxy, las conexiones de cliente terminan en el proxy, mientras que las conexiones de la base de datos se administran en RDS Proxy.

La agrupación de conexiones en la aplicación puede ofrecer la ventaja de reducir el establecimiento de conexiones recurrentes entre la aplicación y RDS Proxy.

Tenga en cuenta los siguientes elementos de configuración antes de implementar un grupo de conexiones en la aplicación:

- Duración máxima de la conexión del cliente: RDS Proxy impone una vida útil máxima de 24 horas para las conexiones del cliente. Este valor no se puede configurar. Configure su grupo con una vida útil máxima de conexión inferior a 24 horas para evitar caídas inesperadas en la conexión del cliente.
- Tiempo de espera de inactividad en la conexión de cliente: RDS Proxy impone un tiempo máximo de inactividad para las conexiones del cliente. Configure su grupo con un valor de tiempo de espera de conexión inactiva inferior al tiempo de espera de la conexión de cliente para RDS Proxy, a fin de evitar caídas inesperadas en la conexión.

El número máximo de conexiones del cliente configuradas en el grupo de conexiones de la aplicación no tiene por qué limitarse a la configuración max_connections de RDS Proxy

La agrupación de conexiones de clientes prolonga la vida útil de las conexiones del cliente. Si las conexiones se bloquean, agrupar las conexiones de cliente podría reducir la eficiencia de la multiplexación. Las conexiones del cliente que están bloqueadas pero inactivas en el grupo de conexiones de la aplicación siguen teniendo una conexión de base de datos e impiden que otras conexiones del cliente reutilicen la conexión a la base de datos. Revise los registros de proxy para comprobar si las conexiones se fijan.

> **Note**
>
> RDS Proxy cierra las conexiones de base de datos un poco después de 24 horas, cuando ya no están en uso. El proxy realiza esta acción independientemente del valor de configuración máxima de conexiones inactivas.

Cómo evitar la fijación de RDS Proxy

La multiplexación es más eficiente cuando las solicitudes de base de datos no dependen de la información de estado de solicitudes anteriores. En ese caso, RDS Proxy puede reutilizar una conexión en la conclusión de cada transacción. Algunos ejemplos de dicha información de estado incluyen la mayoría de las variables y parámetros de configuración que puede cambiar a través de instrucciones `SET` o `SELECT`. Las transacciones SQL en una conexión de cliente pueden multiplexar entre conexiones de base de datos subyacentes de forma predeterminada.

Las conexiones al proxy pueden entrar en un estado conocido como fijación. Cuando se fija una conexión, cada transacción posterior utiliza la misma conexión de base de datos subyacente hasta que finaliza la sesión. Otras conexiones de cliente tampoco pueden reutilizar esa conexión de base de datos hasta que finaliza la sesión. La sesión finaliza cuando se interrumpe la conexión del cliente.

RDS Proxy fija automáticamente una conexión de cliente a una conexión de base de datos específica cuando detecta un cambio de estado de sesión que no es apropiado para otras sesiones. La fijación reduce la eficacia de la reutilización de la conexión. Si todas o casi todas las conexiones experimentan asignación, plantéese modificar el código de la aplicación o la carga de trabajo para reducir las condiciones que provocan la fijación.

Por ejemplo, su aplicación cambia una variable de sesión o un parámetro de configuración. En este caso, las instrucciones posteriores pueden depender de que la nueva variable o parámetro esté en vigor. Por lo tanto, cuando RDS Proxy procesa solicitudes para cambiar las variables de sesión o los parámetros de configuración, fija esa sesión a la conexión de base de datos. De esta forma, el estado de la sesión permanece en vigor para todas las transacciones posteriores en la misma sesión.

Para algunos motores de base de datos, esta regla no se aplica a todos los parámetros que se pueden establecer. RDS Proxy realiza un seguimiento de ciertas sentencias y variables. Por lo tanto, RDS Proxy no fija la sesión cuando las modifica. En ese caso, RDS Proxy solo reutiliza la conexión para otras sesiones que tengan los mismos valores para esa configuración. Para obtener más información sobre lo que RDS Proxy rastrea para un motor de base de datos, consulte lo siguiente:

- Qué rastrea el proxy RDS para las bases de datos de RDS para SQL Server
- Qué seguimiento hace RDS Proxy para bases de datos de RDS para MariaDB y RDS para MySQL

Qué rastrea el proxy RDS para las bases de datos de RDS para SQL Server

A continuación se presentan las instrucciones SQL Server de las que RDS Proxy realiza un seguimiento:

- `USE`
- `SET ANSI_NULLS`
- `SET ANSI_PADDING`
- `SET ANSI_WARNINGS`
- `SET ARITHABORT`
- `SET CONCAT_NULL_YIELDS_NULL`
- `SET CURSOR_CLOSE_ON_COMMIT`
- `SET DATEFIRST`
- `SET DATEFORMAT`
- `SET LANGUAGE`
- `SET LOCK_TIMEOUT`
- `SET NUMERIC_ROUNDABORT`
- `SET QUOTED_IDENTIFIER`
- `SET TEXTSIZE`
- `SET TRANSACTION ISOLATION LEVEL`

Qué seguimiento hace RDS Proxy para bases de datos de RDS para MariaDB y RDS para MySQL

Estas son las instrucciones de MariaDB y MySQL de las que RDS Proxy realiza un seguimiento:

- DROP DATABASE
- DROP SCHEMA
- USE

A continuación se presentan las variables MySQL y MariaDB de las que RDS Proxy realiza un seguimiento:

- AUTOCOMMIT
- AUTO_INCREMENT_INCREMENT
- CHARACTER SET (or CHAR SET)
- CHARACTER_SET_CLIENT
- CHARACTER_SET_DATABASE
- CHARACTER_SET_FILESYSTEM
- CHARACTER_SET_CONNECTION
- CHARACTER_SET_RESULTS
- CHARACTER_SET_SERVER
- COLLATION_CONNECTION
- COLLATION_DATABASE
- COLLATION_SERVER
- INTERACTIVE_TIMEOUT
- NAMES
- NET_WRITE_TIMEOUT
- QUERY_CACHE_TYPE
- SESSION_TRACK_SCHEMA
- SQL_MODE
- TIME_ZONE
- TRANSACTION_ISOLATION (or TX_ISOLATION)
- TRANSACTION_READ_ONLY (or TX_READ_ONLY)
- WAIT_TIMEOUT

Minimizar la fijación

El ajuste del rendimiento para RDS Proxy implica intentar maximizar la reutilización de la conexión en el nivel de transacción (multiplexación) minimizando la fijación.

Puede minimizar la fijación, puede realizar lo siguiente:

- Evite las solicitudes de base de datos innecesarias que puedan provocar la fijación.
- Establezca variables y parámetros de configuración de forma coherente en todas las conexiones. De esta forma, es más probable que las sesiones posteriores reutilicen conexiones que tengan esa configuración particular.

  Sin embargo, en el caso de PostgreSQL, el establecimiento de una variable conduce a la fijación de sesión.
- Para una base de datos de familia de motores MySQL, aplique un filtro de sesión de fijación al proxy. Puede eximir a ciertos tipos de operaciones de asignar la sesión si sabe que hacerlo no afecta al correcto funcionamiento de la fijación.
- Consulte la frecuencia con la que se produce la fijación mediante la supervisión de la métrica de Amazon CloudWatch `DatabaseConnectionsCurrentlySessionPinned`. Para obtener información sobre esta y otras métricas de CloudWatch, consulte Supervisión de las métricas de RDS Proxy con Amazon CloudWatch.
- Si utiliza instrucciones `SET` para realizar una inicialización idéntica para cada conexión de cliente, puede hacerlo sin dejar de mantener la multiplexación en el nivel de transacción. En este caso, mueva las instrucciones que configuran el estado de la sesión inicial a la consulta de inicialización utilizada por un proxy. Esta propiedad es una cadena que contiene una o varias instrucciones SQL, separadas por punto y coma.

  Por ejemplo, puede definir una consulta de inicialización para un proxy que establezca determinados parámetros de configuración. A continuación, RDS Proxy aplica esa configuración cada vez que configura una nueva conexión para ese proxy. Puede eliminar las instrucciones `SET` correspondientes de su código de aplicación, para que no interfieran con la multiplexación en el nivel de transacción.

  Para obtener métricas acerca de la frecuencia con la que se produce la fijación de un proxy, consulte Supervisión de las métricas de RDS Proxy con Amazon CloudWatch.

Condiciones que provocan la fijación de todas las familias de motores

El proxy fija la sesión a la conexión actual en las siguientes situaciones en las que la multiplexación podría provocar un comportamiento inesperado:

- Cualquier instrucción con un tamaño de texto superior a 16 KB hace que el proxy fije la sesión.

Condiciones que provocan la fijación para RDS para Microsoft SQL Server

Para RDS para SQL Server, las siguientes interacciones también producen fijación:

- Uso de varios conjuntos de resultados activos (MARS). Para obtener información sobre MARS, consulte la documentación de SQL Server.
- Usar la comunicación del coordinador de transacciones distribuidas (DTC).
- Crear tablas, transacciones, cursores o estados preparados temporales.
- Utilizar las siguientes instrucciones:`SET`
  - `SET ANSI_DEFAULTS`
  - `SET ANSI_NULL_DFLT`
  - `SET ARITHIGNORE`
  - `SET DEADLOCK_PRIORITY`
  - `SET FIPS_FLAGGER`
  - `SET FMTONLY`
  - `SET FORCEPLAN`
  - `SET IDENTITY_INSERT`
  - `SET NOCOUNT`
  - `SET NOEXEC`
  - `SET OFFSETS`
  - `SET PARSEONLY`
  - `SET QUERY_GOVERNOR_COST_LIMIT`
  - `SET REMOTE_PROC_TRANSACTIONS`
  - `SET ROWCOUNT`
  - `SET SHOWPLAN_ALL`, `SHOWPLAN_TEXT`, y `SHOWPLAN_XML`
  - `SET STATISTICS`
  - `SET XACT_ABORT`

Condiciones que provocan la fijación para RDS para MariaDB y RDS para MySQL

Para MariaDB y MySQL, las siguientes interacciones también producen una fijación:

- Las instrucciones de bloqueo de tabla explícitas `LOCK TABLE`, `LOCK TABLES` o `FLUSH TABLES WITH READ LOCK` hacen que el proxy fije la sesión.
- Creación de bloqueos con nombre mediante`GET_LOCK`provoca que el proxy instale la sesión.
- El establecimiento de una variable de usuario o una variable de sistema (con algunas excepciones) hace que el proxy fije la sesión. Si esta situación reduce demasiado la reutilización de la conexión, puede elegir que las operaciones `SET` no provoquen la fijación. Para obtener información acerca de cómo hacerlo estableciendo la propiedad de los filtros de fijación de sesión, consulte Creación de un proxy para Amazon RDS y Modificación de un RDS Proxy.
- La creación de una tabla temporal hace que el proxy fije la sesión. De esta forma, el contenido de la tabla temporal se conserva a lo largo de la sesión con independencia de los límites de la transacción.
- La llamada a las funciones `ROW_COUNT`, `FOUND_ROWS` y `LAST_INSERT_ID` a veces provoca fijación.
- Las instrucciones preparadas hacen que el proxy fije la sesión. Esta regla se aplica si la instrucción preparada utiliza texto SQL o el protocolo binario.
- El proxy de RDS no fija las conexiones cuando se utiliza SET LOCAL.
- La llamada a procedimientos almacenados y funciones almacenadas no causa fijación. El proxy de RDS no detecta ningún cambio de estado de sesión resultante de dichas llamadas. Asegúrese de que su aplicación no cambie el estado de la sesión dentro de las rutinas almacenadas si confía en que ese estado de sesión vaya a persistir en las transacciones. Por ejemplo, RDS Proxy no es compatible actualmente con un procedimiento almacenado que crea una tabla temporal que persiste a través de todas las transacciones.

Si tiene conocimientos especializados sobre el comportamiento de la aplicación, puede omitir el comportamiento de fijación de determinadas instrucciones de aplicación. Para ello, elija la opción Session pinning filters (Filtro de fijación de sesión) al crear el proxy. Actualmente, puede desactivar la fijación de sesión para establecer variables de sesión y valores de configuración.

Condiciones que provocan la fijación para RDS para PostgreSQL

Para PostgreSQL, las siguientes interacciones también producen fijación:

- Uso de comandos `SET`.
- Uso de los comandos `PREPARE`, `DISCARD`, `DEALLOCATE` o `EXECUTE` para gestionar las instrucciones preparadas.

- Creación de secuencias, tablas o vistas temporales.
- Declaración de cursores.
- Descartar el estado de la sesión.
- Escucha en un canal de notificación.
- Carga de un módulo de biblioteca como `auto_explain`.
- Manipulación de secuencias mediante el uso de funciones como `nextval` y `setval`.
- Interacción con bloqueos mediante el uso de funciones como `pg_advisory_lock` y `pg_try_advisory_lock`.

> **Note**
>
> RDS Proxy no fija los bloqueos consultivos en la transacción, específicamente `pg_advisory_xact_lock`, `pg_advisory_xact_lock_shared`, `pg_try_advisory_xact_lock` y `pg_try_advisory_xact_lock_shared`.

- Cómo configurar un parámetro o restablecerlo a su valor predeterminado. En concreto, el uso de comandos `SET` y `set_config` para asignar valores predeterminados a las variables de sesión.
- La llamada a procedimientos almacenados y funciones almacenadas no causa fijación. El proxy de RDS no detecta ningún cambio de estado de sesión resultante de dichas llamadas. Asegúrese de que su aplicación no cambie el estado de la sesión dentro de las rutinas almacenadas si confía en que ese estado de sesión vaya a persistir en las transacciones. Por ejemplo, RDS Proxy no es compatible actualmente con un procedimiento almacenado que crea una tabla temporal que persiste a través de todas las transacciones.

Eliminación de un RDS Proxy

Puede eliminar un proxy cuando ya no lo necesite. O podría eliminar un proxy si pone la instancia de base de datos o el clúster asociado con él fuera de servicio.

AWS Management Console

Para eliminar un proxy

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Proxies.

3. Elija el proxy que desea eliminar de la lista.
4. Elija Delete Proxy (Eliminar proxy).

AWS CLI

Para eliminar un proxy de base de datos, utilice el comando de la AWS CLI delete-db-proxy. Para quitar asociaciones relacionadas, utilice también el comando deregister-db-proxy-targets.

```
aws rds delete-db-proxy --name proxy_name
```

```
aws rds deregister-db-proxy-targets
    --db-proxy-name proxy_name
    [--target-group-name target_group_name]
    [--target-ids comma_separated_list]       # or
    [--db-instance-identifiers instance_id]       # or
    [--db-cluster-identifiers cluster_id]
```

API de RDS

Para eliminar un proxy de base de datos, llame a la función de la API de Amazon RDS DeleteDBProxy. Para eliminar elementos relacionados y asociaciones, llame también a las funciones DeleteDBProxyTargetGroup y DeregisterDBProxyTargets.

Trabajo con puntos de enlace del proxy de Amazon RDS

Los puntos de conexión de RDS Proxy proporcionan formas flexibles y eficientes de administrar las conexiones de bases de datos, lo que mejora la escalabilidad, la disponibilidad y la seguridad. Con los puntos de conexión del proxy, puede:

- Simplificar la supervisión y la resolución de problemas: use varios puntos de conexión para realizar un seguimiento y administrar conexiones de diferentes aplicaciones de forma independiente.

Temas

- Información general de los puntos de enlace de proxy
- Limitaciones para los puntos de conexión de proxy
- Puntos de conexión de proxy para clústeres de bases de datos de Multi-AZ
- Acceso a las bases de datos de RDS en todas las VPC

- Creación de un punto de enlace de proxy
- Visualización de puntos de enlace de proxy
- Modificación de un punto de enlace de proxy
- Eliminación de un punto de enlace de proxy

Información general de los puntos de enlace de proxy

Trabajar con puntos de conexión de RDS Proxy implica los mismos tipos de procedimientos que con los puntos de conexión de instancia de RDS. Si no está familiarizado con los puntos de enlace de RDS, puede encontrar más información en Conexión a una instancia de base de datos que ejecuta el motor de base de datos de MySQL y Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL.

Cuando cree un punto de conexión del proxy, puede asociarlo con una nube privada virtual (VPC) diferente de la que utiliza la VPC del proxy. Esto le permite conectarse al proxy desde otra VPC, como una utilizada por una aplicación diferente dentro de la organización.

Para obtener información acerca de los límites asociados a los puntos de enlace de proxy, consulte Limitaciones para los puntos de conexión de proxy.

RDS Proxy registra el prefijo de cada entrada con el nombre del punto de conexión del proxy asociado. Este puede ser el nombre especificado para un punto de conexión definido por el usuario o el nombre `default` especial para el punto de conexión de lectura o escritura predeterminado de un proxy.

Cada punto de conexión de proxy tiene su propio conjunto de métricas de CloudWatch. Supervise las métricas de todos los puntos de conexión de proxy, un punto de conexión específico o de todos los puntos de conexión de lectura o escritura o de solo lectura de un proxy. Para obtener más información, consulte Supervisión de las métricas de RDS Proxy con Amazon CloudWatch.

Un punto de enlace del proxy utiliza el mismo mecanismo de autenticación que su proxy asociado. El proxy de RDS configura automáticamente permisos y autorizaciones para el punto de enlace definido por el usuario, de acuerdo con las propiedades del proxy asociado.

Limitaciones para los puntos de conexión de proxy

Los puntos de conexión de RDS Proxy tienen las siguientes limitaciones:

- El punto de conexión predeterminado del proxy de RDS no se puede modificar.

- El número máximo de puntos de enlace definidos por el usuario para un proxy es 20. Por lo tanto, un proxy puede tener hasta 21 puntos de enlace: el punto de enlace predeterminado, más 20 que cree.
- Cuando asocia puntos de enlace adicionales con un proxy, RDS Proxy determina automáticamente qué instancias de base de datos del clúster se utilizarán para cada punto de enlace.

Al crear un proxy, RDS crea automáticamente un punto de conexión de VPC para una comunicación segura entre las aplicaciones y la base de datos. El punto de conexión de VPC es visible y se puede acceder a él desde la consola de Amazon VPC.

Al agregar un nuevo punto de conexión de proxy, se aprovisiona un punto de conexión de interfaz de AWS PrivateLink. Si agrega uno o más puntos de conexión al proxy, incurrirá en cargos adicionales. Para obtener más información, consulte Precios de proxy de RDS.

Puntos de conexión de proxy para clústeres de bases de datos de Multi-AZ

De forma predeterminada, el punto de conexión al que se conecta cuando utiliza RDS Proxy con un clúster de bases de datos Multi-AZ tiene capacidad de lectura o escritura. Como resultado, este punto de conexión envía todas las solicitudes a la instancia del escritor del clúster. Todas esas conexiones se descontarán del valor `max_connections` de la instancia del escritor. Si su proxy está asociado con un clúster de bases de datos de Multi-AZ, puede crear puntos de conexión de lectura o escritura o de solo lectura adicionales para ese proxy.

Puede utilizar un punto de conexión de solo lectura con su proxy para consultas de solo lectura. Para hacerlo, tiene que hacer lo mismo que para usar el punto de conexión de lector para un clúster de bases de datos de Multi-AZ Esto le permite aprovechar la escalabilidad de lectura de un clúster de bases de datos de Multi-AZ con una o más instancias de base de datos de lector. Puede ejecutar más consultas simultáneas y realizar más conexiones simultáneas empleando un punto de conexión de solo lectura y agregando más instancias de base de datos de lector a su clúster de bases de datos de Multi-AZ, según sea necesario. Estos puntos de enlace del lector ayudan a mejorar la escalabilidad de lectura de sus aplicaciones que requieren un uso intensivo de consultas. Los puntos de enlace del lector también ayudan a mejorar la disponibilidad de las conexiones si una instancia de base de datos de lector del clúster deja de estar disponible.

Puntos de conexión de lector para clústeres de base de datos Multi-AZ

Con RDS Proxy, puede crear y usar puntos de enlace del lector. Sin embargo, estos puntos de conexión solo funcionan para proxies asociados con clústeres de base de datos de Multi-AZ.

Si utiliza la CLI o API de RDS, es posible que vea el atributo de `TargetRole` con un valor de `READ_ONLY`. Puede aprovechar estos proxy cambiando el destino de un proxy de una instancia de base de datos de RDS a un clúster de bases de datos multi-AZ.

Puede crear puntos de conexión de solo lectura, denominados puntos de conexión de lector, y conectarse a estos al usar RDS Proxy con los clústeres de base de datos de Multi-AZ.

Cómo los puntos de enlace del lector ayudan a la disponibilidad de las aplicaciones

A veces, es posible que alguna instancia de lector en el clúster no esté disponible. En esos casos, las conexiones que utilizan un punto de conexión de lector de un proxy de base de datos se pueden recuperar más rápidamente que las que utilizan el punto de conexión de lector del clúster de bases de datos de Multi-AZ. RDS Proxy solo enruta las conexiones a las instancias de lector disponibles en el clúster. No hay retraso debido al almacenamiento en caché de DNS cuando una instancia deja de estar disponible.

Si la conexión es multiplexada, RDS Proxy dirige las consultas posteriores a una instancia de lector diferente sin interrupciones en su aplicación. Si una instancia de lectura no está disponible, se cierran todas las conexiones de cliente a ese punto de conexión de la instancia.

Si la conexión está anclada, la siguiente consulta en la conexión devuelve un error. Sin embargo, la aplicación puede volver a conectarse inmediatamente al mismo punto de conexión de proxy. El proxy de RDS enruta la conexión a una instancia de base de datos de lector diferente que se encuentra en estado `available`. Cuando se vuelve a conectar manualmente, RDS Proxy no comprueba el retraso de reproducción entre la instancia de lector antigua y nueva.

Si su clúster de bases de datos Multi-AZ no tiene instancias de lector disponibles, RDS Proxy intentará conectarse a un punto de conexión de lector cuando esté disponible. Si no hay instancias de lector disponibles dentro del periodo de tiempo de espera de préstamo de conexión, se produce un error en el intento de conexión. Si una instancia de lector está disponible, el intento de conexión se lleva a cabo correctamente.

Cómo los puntos de enlace del lector ayudan a la escalabilidad de las consultas

Los puntos de conexión del lector de un proxy contribuyen a la escalabilidad de las consultas de clúster de bases de datos de Multi-AZ de las siguientes maneras:

- Cuando sea práctico, RDS Proxy utiliza la misma instancia de base de datos de lector para todos los problemas de consultas mediante una conexión de punto de enlace del lector en particular. De esta manera, un conjunto de consultas relacionadas en las mismas tablas puede aprovechar el

almacenamiento en caché, la optimización del plan y demás, en una instancia de base de datos particular.

- Si una instancia de base de datos de lector deja de estar disponible, el efecto en la aplicación depende de si la sesión está multiplexada o anclada. Si la sesión está multiplexada, RDS Proxy enruta las consultas posteriores a una instancia de base de datos de lector diferente sin acciones por su parte. Si la sesión está anclada, la aplicación recibe un error y debe volver a conectarse. Puede volver a conectarse al punto de enlace del lector inmediatamente y RDS Proxy enruta la conexión a una instancia de base de datos de lector disponible. Para obtener más información acerca de la multiplexación y el anclaje de sesiones de proxy, consulte Información general de los conceptos de RDS Proxy.

Acceso a las bases de datos de RDS en todas las VPC

De forma predeterminada, los componentes de su pila de tecnología de RDS están todos en la misma Amazon VPC. Por ejemplo, supongamos que una aplicación que se ejecuta en una instancia de Amazon EC2 se conecta a una instancia de base de datos de Amazon RDS. En este caso, el servidor de la aplicación y la base de datos deben estar dentro de la misma VPC.

Con RDS Proxy, puede configurar el acceso a una instancia de base de datos de Amazon RDS en una VPC a partir de recursos de otra VPC, como las instancias de EC2. Por ejemplo, la organización puede tener varias aplicaciones que tengan acceso a los mismos recursos de base de datos. Cada aplicación puede estar en su propia VPC.

A fin de habilitar el acceso entre VPC, cree un nuevo punto de enlace para el proxy. El propio proxy reside en la misma VPC que la instancia de base de datos de Amazon RDS. Sin embargo, el punto de enlace en VPC reside en la otra VPC, junto con otros recursos, como las instancias EC2. El punto de enlace en VPC está asociado con subredes y grupos de seguridad de la misma VPC que EC2 y otros recursos. Estas asociaciones permiten conectarse al punto de enlace desde las aplicaciones que, de lo contrario, no pueden acceder a la base de datos debido a las restricciones de la VPC.

Los siguientes pasos explican cómo crear y acceder a un punto de enlace en VPC a través de RDS Proxy:

1. Cree dos VPC o elija dos VPC que ya utilice para el trabajo en RDS. Cada VPC debe tener sus propios recursos de red asociados, como una puerta de enlace de Internet, tablas de enrutamiento, subredes y grupos de seguridad. Si solo tiene una VPC, puede consultar Introducción a Amazon RDS para conocer los pasos a fin de configurar otra VPC para que use

RDS con éxito. También puede examinar la VPC existente en la consola de Amazon EC2 para ver los tipos de recursos que conectar entre sí.

2. Cree un proxy de base de datos asociado con la instancia de base de datos de Amazon RDS al que desea conectarse. Siga el procedimiento indicado en Creación de un proxy para Amazon RDS.
3. En la página de Details (Detalles) para su proxy en la consola de RDS, en la pestaña de Proxy endpoints (Puntos de enlace de proxy), elija Create endpoint (Crear punto de enlace). Siga el procedimiento indicado en Creación de un punto de enlace de proxy.
4. Elija si desea que el punto de enlace en VPC sea de lectura y escritura o de solo lectura.
5. En lugar de aceptar el valor predeterminado de la misma VPC que la instancia de base de datos de Amazon RDS, elija una VPC diferente. Esta VPC debe estar en la misma región de AWS que la VPC donde reside el proxy.
6. Ahora, en lugar de aceptar los valores predeterminados para subredes y grupos de seguridad de la misma VPC que la instancia de base de datos de Amazon RDS, haga nuevas selecciones. Estos se basen en las subredes y los grupos de seguridad de la VPC que eligió.
7. No es necesario cambiar las opciones de configuración de los secretos de Secrets Manager. Las mismas credenciales funcionan para todos los puntos de enlace de proxy, independientemente de la VPC en la que se encuentre cada punto de enlace.
8. Espere a que el punto de enlace nuevo alcance el estado de Available (Disponible).
9. Anote el nombre completo del punto de enlace. Este es el valor que termina en *`Region_name`*`.rds.amazonaws.com` que proporciona como parte de la cadena de conexión para la aplicación de base de datos.
10. Acceda al punto de enlace nuevo desde un recurso en la misma VPC que el punto de enlace. Una forma sencilla de probar este proceso es crear una instancia de EC2 nueva en esta VPC. A continuación, puede iniciar sesión en la instancia de EC2 y ejecutar los comandos `mysql` o `psql` para conectarse mediante el valor de punto de conexión en la cadena de conexión.

Creación de un punto de enlace de proxy

Para crear un punto de conexión proxy, siga estas instrucciones:

Consola

Para crear un punto de enlace de proxy

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Proxies.
3. Haga clic en el nombre del proxy para el que desea crear un punto de enlace nuevo.

   Aparecerá la página de detalles de ese proxy.
4. En la sección de Proxy endpoints (Puntos de enlace de proxy), elija Crear endpoint proxy (Crear punto de enlace de proxy).

   Aparecerá la ventana de Create proxy endpoint (Crear punto de enlace de proxy).
5. Para Proxy endpoint name (Nombre del punto de enlace de proxy), escriba un nombre descriptivo de su elección.
6. Para Target role (Rol de destino), elija si desea que el punto de enlace sea de lectura o escritura o de solo lectura.

   Las conexiones que utilizan puntos de conexión de lectura/escritura pueden realizar cualquier tipo de operación, como instrucciones de lenguaje de definición de datos (DDL), instrucciones de lenguaje de manipulación de datos (DML) y consultas. Estos puntos de conexión siempre se conectan a la instancia principal del clúster de bases de datos de RDS. Puede utilizar puntos de enlace de lectura o escritura para operaciones generales de bases de datos cuando solo utiliza un punto de enlace único en la aplicación. También puede utilizar puntos de enlace de lectura o escritura para operaciones administrativas, aplicaciones de procesamiento de transacciones en línea (OLTP) y trabajos de extracción, transformación y carga (ETL).

   Las conexiones que utilizan un punto de enlace de solo lectura solo pueden realizar consultas. RDS Proxy puede utilizar una de las instancias de lector para cada conexión al punto de conexión. De esta manera, una aplicación que requiere un uso intensivo de consultas puede aprovechar la capacidad de agrupamiento en clúster del clúster de bases de datos Multi-AZ. Estas conexiones de solo lectura no imponen sobrecargas en la instancia principal del clúster. De esta manera, sus consultas de informes y análisis no ralentizan las operaciones de escritura de sus aplicaciones de OLTP.
7. En Nube privada virtual (VPC), elija el valor predeterminado para acceder al punto de conexión desde las mismas instancias de EC2 u otros recursos que normalmente utiliza para acceder al

proxy o a su base de datos asociada. Para configurar el acceso entre VPC para este proxy, elija una VPC distinta de la predeterminada. Para obtener más información sobre el acceso a través de VPC, consulte Acceso a las bases de datos de RDS en todas las VPC.

8. En Subnets (Subredes), RDS Proxy rellena las mismas subredes que el proxy asociado de forma predeterminada. Para restringir el acceso al punto de conexión para que solo una parte del intervalo de direcciones de la VPC pueda conectarse a él, quite una o varias subredes.
9. En VPC security group (Grupos de seguridad de la VPC), puede elegir un grupo de seguridad existente o crear uno nuevo. De forma predeterminada, el proxy de RDS rellena el mismo grupo o grupos de seguridad que el proxy asociado. Si las reglas entrantes y salientes del proxy son apropiadas para este punto de conexión, puede dejar la opción predeterminada.

   Si decide crear un grupo de seguridad nuevo, especifique un nombre para el grupo de seguridad en esta página. A continuación, edite la configuración del grupo de seguridad desde la consola de EC2.
10. Elija Create proxy endpoint (Crear punto de enlace de proxy).

AWS CLI

Para crear un punto de enlace de proxy, utilice el comando de AWS CLI create-db-proxy-endpoint.

Incluya los siguientes parámetros obligatorios:

- `--db-proxy-name` *`value`*
- `--db-proxy-endpoint-name` *`value`*
- `--vpc-subnet-ids` *`list_of_ids`*. Separe los ID de subred con espacios. No se especifica el ID de la VPC en sí.

También puede incluir los siguientes parámetros opcionales:

- `--target-role { READ_WRITE | READ_ONLY }`. El valor predeterminado de este parámetro es `READ_WRITE`. Cuando el proxy está asociado a un clúster de base de datos multi-AZ que solo contiene una instancia de base de datos de escritura, no puede especificar `READ_ONLY`. Para obtener más información sobre el uso previsto de puntos de conexión de solo lectura con clústeres de base de datos multi-AZ, consulte Puntos de conexión de lector para clústeres de base de datos Multi-AZ.

- `--vpc-security-group-ids` *`value`*. Separe los ID de grupo de seguridad con espacios. Si omite este parámetro, el proxy de RDS utiliza el grupo de seguridad predeterminado de la VPC. El proxy de RDS determina la VPC en función de los ID de subred que especifique para el parámetro `--vpc-subnet-ids`.

Example

En el ejemplo siguiente se crea un punto de enlace de proxy denominado `my-endpoint`.

Para Linux, macOS o:Unix

```
aws rds create-db-proxy-endpoint \
  --db-proxy-name my-proxy \
  --db-proxy-endpoint-name my-endpoint \
  --vpc-subnet-ids subnet_id subnet_id subnet_id ... \
  --target-role READ_ONLY \
  --vpc-security-group-ids security_group_id ]
```

En:Windows

```
aws rds create-db-proxy-endpoint ^
  --db-proxy-name my-proxy ^
  --db-proxy-endpoint-name my-endpoint ^
  --vpc-subnet-ids subnet_id_1 subnet_id_2 subnet_id_3 ... ^
  --target-role READ_ONLY ^
  --vpc-security-group-ids security_group_id
```

API de RDS

Para crear un punto de conexión proxy, utilice la acción CreateDBProxyEndpoint de la API de RDS.

Visualización de puntos de enlace de proxy

Para ver los puntos de conexión proxy existentes, siga estas instrucciones:

Consola

Para ver los detalles de un punto de enlace de proxy

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Proxies.
3. En la lista, elija el proxy cuyo punto de enlace desea ver. Haga clic en el nombre del proxy para ver su página de detalles.
4. En la sección Proxy endpoints (Puntos de enlace de proxy), elija el punto de enlace que desea ver. Haga clic en su nombre para ver la página de detalles.
5. Examine los parámetros cuyos valores le interesan. Puede comprobar propiedades como las siguientes:
   - Si el punto de enlace es de lectura o escritura o de solo lectura.
   - La dirección de punto de enlace que se utiliza en una cadena de conexión de base de datos.
   - La VPC, las subredes y los grupos de seguridad asociados con el punto de enlace.

AWS CLI

Para ver uno o más puntos de conexión de proxy, utilice el comando de AWS CLI describe-db-proxy-endpoints.

Puede incluir los siguientes parámetros opcionales:

- `--db-proxy-endpoint-name`
- `--db-proxy-name`

En el siguiente ejemplo se describe el punto de enlace de proxy de `my-endpoint`.

Example

Para Linux, macOS o:Unix

```
aws rds describe-db-proxy-endpoints \
  --db-proxy-endpoint-name my-endpoint
```

En:Windows

```
aws rds describe-db-proxy-endpoints ^
  --db-proxy-endpoint-name my-endpoint
```

API de RDS

Para describir uno o más puntos de enlace de proxy, utilice la operación de API de RDS DescribeDBProxyEndpoints.

Modificación de un punto de enlace de proxy

Para modificar los puntos de conexión proxy, siga estas instrucciones:

Consola

Para modificar uno o varios puntos de enlace de proxy

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Proxies.
3. En la lista, elija el proxy cuyo punto de enlace desea modificar. Haga clic en el nombre del proxy para ver su página de detalles.
4. En la sección Proxy endpoints (Puntos de enlace de proxy), elija el punto de enlace que desea modificar. Puede seleccionarlo en la lista o hacer clic en su nombre para ver la página de detalles.
5. En la página de detalles del proxy, en la sección de Proxy endpoints (Puntos de enlace de proxy), elija Edit (Editar). O en la página de detalles del punto de conexión de proxy, en Acciones, elija Editar.
6. Cambie los valores de los parámetros que desee modificar.
7. Elija Guardar cambios.

AWS CLI

Para modificar un punto de conexión de proxy, utilice el comando de AWS CLI modify-db-proxy-endpoint con los siguientes parámetros requeridos:

- `--db-proxy-endpoint-name`

Especifique los cambios en las propiedades del punto de enlace mediante uno o varios de los siguientes parámetros:

- `--new-db-proxy-endpoint-name`

- `--vpc-security-group-ids`. Separe los ID de grupo de seguridad con espacios.

En el ejemplo siguiente se cambia el nombre del punto de enlace de proxy de `my-endpoint` a `new-endpoint-name`.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-proxy-endpoint \
  --db-proxy-endpoint-name my-endpoint \
  --new-db-proxy-endpoint-name new-endpoint-name
```

Para Windows:

```
aws rds modify-db-proxy-endpoint ^
  --db-proxy-endpoint-name my-endpoint ^
  --new-db-proxy-endpoint-name new-endpoint-name
```

API de RDS

Para modificar un punto de enlace de proxy, utilice la operación de API de RDS ModifyDBProxyEndpoint.

Eliminación de un punto de enlace de proxy

Para eliminar un punto de conexión para su proxy, siga estas instrucciones:

> **Note**
>
> No puede eliminar el punto de conexión de proxy predeterminado que RDS Proxy crea automáticamente para cada proxy.
> Cuando elimina un proxy, RDS Proxy elimina automáticamente todos los puntos de enlace asociados.

Consola

Para eliminar un punto de enlace de proxy mediante AWS Management Console

1. En el panel de navegación, seleccione Proxies.

2. En la lista, elija el proxy cuyo punto de enlace desea establecer como punto de enlace. Haga clic en el nombre del proxy para ver su página de detalles.
3. En la sección Proxy endpoints (Puntos de enlace de proxy), elija el punto de enlace que desea eliminar. Puede seleccionar uno o varios puntos de enlace de la lista o hacer clic en el nombre de un punto de enlace único para ver la página de detalles.
4. En la página de detalles del proxy, en la sección de Proxy endpoints (Puntos de enlace de proxy), elija Delete (Eliminar). O en la página de detalles del punto de conexión de proxy, en Acciones, elija Eliminar.

AWS CLI

Para eliminar un punto de enlace de proxy, ejecute el comando delete-db-proxy-endpoint con los siguientes parámetros requeridos:

- `--db-proxy-endpoint-name`

El siguiente comando elimina el punto de enlace de proxy denominado `my-endpoint`.

Para Linux, macOS o:Unix

```
aws rds delete-db-proxy-endpoint \
  --db-proxy-endpoint-name my-endpoint
```

En:Windows

```
aws rds delete-db-proxy-endpoint ^
  --db-proxy-endpoint-name my-endpoint
```

API de RDS

Para eliminar un punto de enlace de proxy con la API de RDS, ejecute la operación DeleteDBProxyEndpoint. Especifique el nombre del punto de enlace de proxy para el parámetro `DBProxyEndpointName`.

Supervisión de las métricas de RDS Proxy con Amazon CloudWatch

Puede monitorear el proxy de RDS mediante Amazon CloudWatch. CloudWatch recopila y procesa los datos sin procesar de los proxies en métricas legibles y casi en tiempo real. Para buscar estas métricas en la consola de CloudWatch, seleccione Metrics (Métricas), a continuación, RDS y, a continuación, Per-Proxy Metrics (Métricas por proxy). Para obtener más información, consulte Uso de métricas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

> **Note**
>
> RDS publica estas métricas para cada instancia Amazon EC2 subyacente asociada con un proxy. Es posible que más de una instancia EC2 sirva un proxy único. Utilice estadísticas de CloudWatch para agregar los valores de un proxy en todas las instancias asociadas.
> Es posible que algunas de estas métricas no estén visibles hasta después de la primera conexión correcta a través de un proxy.

En los registros de RDS Proxy, cada entrada tiene el prefijo del nombre del punto de enlace de proxy asociado. Este nombre puede ser el especificado para un punto de conexión definido por el usuario, o el nombre especial `default` para el punto de conexión predeterminado de un proxy que realiza las solicitudes de lectura/escritura.

Todas las métricas de RDS Proxy están en el grupo `proxy`.

Cada punto de enlace de proxy tiene sus propias métricas de CloudWatch. Puede monitorear el uso de cada punto de enlace de proxy de forma independiente. Para obtener más información acerca de los puntos de enlace de proxy, consulte Trabajo con puntos de enlace del proxy de Amazon RDS.

Puede agregar los valores de cada métrica mediante uno de los siguientes conjuntos de dimensiones. Por ejemplo, mediante el uso del conjunto de dimensiones de `ProxyName`, puede analizar todo el tráfico de un proxy determinado. Mediante el uso de los otros conjuntos de dimensiones, puede dividir las métricas de diferentes maneras. Puede dividir las métricas en función de los diferentes puntos de enlace o bases de datos de destino de cada proxy, o el tráfico de lectura o escritura y de solo lectura a cada base de datos.

- Conjunto de dimensiones 1 : `ProxyName`
- Conjunto de dimensiones 2 : `ProxyName`, `EndpointName`

- Conjunto de dimensiones 3 : `ProxyName`, `TargetGroup`, `Target`
- Conjunto de dimensiones 4 : `ProxyName`, `TargetGroup`, `TargetRole`

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
`AvailabilityPercentage`	El porcentaje de tiempo para el que el grupo de destino estaba disponible en el rol indicado por la dimensión. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 4
`ClientConnections`	El número actual de conexiones de cliente. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 2
`ClientConnectionsClosed`	El número de conexiones de cliente cerradas. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 2
`ClientConnectionsInSetup`	El número actual de conexiones de cliente abiertas, pero que no han completado la configuración.	1 minuto	Dimension set 1, Dimension set 2

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
	Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es Suma.		
`ClientConnectionsNoTLS`	Número actual de conexiones de cliente sin Transport Layer Security (TLS). Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 2
`ClientConnectionsReceived`	El número de solicitudes de conexión de cliente recibidas. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 2
`ClientConnectionsSetupFailedAuth`	El número de intentos de conexión de cliente que produjeron un error debido a una autenticación o TLS mal configurada. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 2

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
`ClientConnectionsSetupSucceeded`	El número de conexiones de cliente establecidas correctamente con cualquier mecanismo de autenticación con o sin TLS. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 2
`ClientConnectionsTLS`	El número actual de conexiones de cliente con TLS. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 2
`DatabaseConnectionRequests`	El número de solicitudes para crear una conexión de base de datos. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionRequestsWithTLS`	El número de solicitudes para crear una conexión de base de datos con TLS. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 3, Dimension set 4

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
DatabaseConnections	El número actual de conexiones de base de datos. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es Sum.	1 minuto	Dimension set 1, Dimension set 3, Dimension set 4
DatabaseConnectionsBorrowLatency	El tiempo en microsegundos que tarda el proxy que se monitorea en obtener una conexión de base de datos. La estadística más útil para esta métrica es Sum.	1 minuto o más	Dimension set 1, Dimension set 2
DatabaseConnectionsCurrentlyBorrowed	El número actual de conexiones de base de datos en estado de préstamo. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es Sum.	1 minuto	Dimension set 1, Dimension set 3, Dimension set 4

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
`DatabaseConnectionsCurrentlyInTransaction`	El número actual de conexiones de base de datos en una transacción. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionsCurrentlySessionPinned`	El número actual de conexiones de base de datos fijadas actualmente debido a operaciones en solicitudes de cliente que cambian el estado de la sesión. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionsSetupFailed`	El número de solicitudes de conexión de base de datos que produjeron un error. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 3, Dimension set 4

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
`DatabaseConnectionsSetupSucceeded`	El número de conexiones de base de datos establecidas correctamente con o sin TLS. La estadística más útil para esta métrica es `Sum`.	1 minuto o más	Dimension set 1, Dimension set 3, Dimension set 4
`DatabaseConnectionsWithTLS`	El número actual de conexiones de base de datos con TLS. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 3, Dimension set 4
`MaxDatabaseConnectionsAllowed`	El número máximo de conexiones de base de datos permitidas. Se informa de esta métrica cada minuto. La estadística más útil para esta métrica es `Sum`.	1 minuto	Dimension set 1, Dimension set 3, Dimension set 4
`QueryDatabaseResponseLatency`	El tiempo en microsegundos que la base de datos tardó en responder a la consulta. La estadística más útil para esta métrica es `Average`.	1 minuto o más	Dimension set 1, Dimension set 2, Dimension set 3, Dimension set 4

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
QueryRequests	El número de consultas recibidas . Una consulta que incluye varias instrucciones se cuenta como una consulta. La estadística más útil para esta métrica es Sum.	1 minuto o más	Dimension set 1, Dimension set 2
QueryRequestsNoTLS	El número de consultas recibidas de conexiones que no son TLS. Una consulta que incluye varias instrucciones se cuenta como una consulta. La estadística más útil para esta métrica es Sum.	1 minuto o más	Dimension set 1, Dimension set 2
QueryRequestsTLS	El número de consultas recibidas de conexiones TLS. Una consulta que incluye varias instrucciones se cuenta como una consulta. La estadística más útil para esta métrica es Sum.	1 minuto o más	Dimension set 1, Dimension set 2

Métrica	Descripción	Período de validez	Conjunto de dimensiones de CloudWatch
`QueryResponseLatency`	El tiempo en microsegundos entre obtener una solicitud de consulta y que el proxy la responda. La estadística más útil para esta métrica es `Average`.	1 minuto o más	Dimension set 1, Dimension set 2

Puede encontrar registros de actividad del proxy de RDS en CloudWatch en la AWS Management Console. Cada proxy tiene una entrada en la página Log groups (Grupos de registro).

> **Important**
>
> Estos registros están destinados al consumo humano para solucionar problemas y no para el acceso mediante programación. El formato y el contenido de los registros están sujetos a cambios.
>
> En particular, los registros más antiguos no contienen prefijos que indiquen el punto de enlace de cada solicitud. En los registros más recientes, cada entrada tiene el prefijo del nombre del punto de enlace de proxy asociado. Este nombre puede ser el que especificó para un punto de enlace definido por el usuario, o el nombre especial `default` para las solicitudes que utilizan el punto de enlace predeterminado de un proxy.

Trabajo con eventos de RDS Proxy

Un evento indica un cambio en un entorno, como un entorno de AWS, un servicio o aplicación de un socio de software como servicio (SaaS). O bien, puede ser una de sus propias aplicaciones o servicios personalizados. Por ejemplo, Amazon RDS genera un evento al crear o modificar una instancia de RDS Proxy. Amazon RDS envía eventos a Amazon EventBridge casi en tiempo real. A continuación, encontrará una lista de eventos de RDS Proxy a los que puede suscribirse y un ejemplo de evento de RDS Proxy.

Para obtener más información acerca de cómo trabajar con eventos, consulte lo siguiente:

- Para obtener instrucciones acerca de cómo ver los eventos mediante la AWS Management Console, la AWS CLI o la API de RDS, consulte Consulta de eventos de Amazon RDS.
- Para obtener información sobre cómo configurar Amazon RDS para enviar eventos a EventBridge, consulte Creación de una regla que se desencadena en función de un evento Amazon RDS.

Eventos de RDS Proxy

En la siguiente tabla se muestran las categorías de eventos y una lista de los eventos que pueden producirse cuando el tipo de origen es una instancia de RDS Proxy.

Categoría	ID de evento de RDS	Mensaje	Notas
configuration change	RDS-EVENT-0204	RDS ha modificado el proxy de la base de datos *nombre*.	Ninguna
configuration change	RDS-EVENT-0207	RDS ha modificado el punto de conexión del proxy de la base de datos *nombre*.	Ninguna
configuration change	RDS-EVENT-0213	RDS ha detectado la adición de la instancia de base de datos y la ha agregado automáticamente al grupo de destino del proxy de la base de datos *nombre*.	Ninguna
configuration change	RDS-EVENT-0214	RDS ha detectado la eliminación de la instancia de base de datos *nombre* y la ha borrado automátic amente del grupo de	Ninguna

Categoría	ID de evento de RDS	Mensaje	Notas
		destino *nombre* del proxy de la base de datos *nombre*.	
configuration change	RDS-EVENT-0215	RDS ha detectado la eliminación del clúster de base de datos *nombre* y la ha borrado automátic amente del grupo de destino *nombre* del proxy de la base de datos *nombre*.	Ninguna
creación	RDS-EVENT-0203	RDS ha creado el proxy de la base de datos *nombre*.	Ninguna
creación	RDS-EVENT-0206	RDS ha creado el punto de conexión *nombre* del para el proxy de la base de datos *nombre*.	Ninguna
deletion	RDS-EVENT-0205	RDS ha eliminado el proxy de la base de datos *nombre*.	Ninguna
deletion	RDS-EVENT-0208	RDS ha eliminado el punto de conexión *nombre* del proxy de la base de datos *nombre*.	Ninguna

Categoría	ID de evento de RDS	Mensaje	Notas
failure	RDS-EVENT-0243	RDS no ha podido aprovisionar capacidad para el proxy *nombre* porque no hay suficientes direcciones IP disponibles en las subredes: *nombre*. Para resolver el problema, asegúrese de que sus subredes tengan el número mínimo de direcciones IP sin usar, tal como se recomienda en la documentación de RDS Proxy.	Para determinar el número recomendado para la clase de instancia, consulte Planificación de la capacidad de direcciones IP.
failure	RDS-EVENT-0275	RDS ha limitado algunas conexiones al proxy de base de datos *nombre*. El número de solicitudes de conexión simultáneas del cliente al proxy ha superado el límite.	Ninguna

A continuación, se muestra un ejemplo de un evento de RDS Proxy en formato JSON. El evento muestra que RDS modificó el punto de conexión denominado `my-endpoint` de la instancia de RDS Proxy denominada `my-rds-proxy`. El ID de evento es RDS-EVENT-0207.

```
{
  "version": "0",
  "id": "68f6e973-1a0c-d37b-f2f2-94a7f62ffd4e",
  "detail-type": "RDS DB Proxy Event",
  "source": "aws.rds",
  "account": "123456789012",
  "time": "2018-09-27T22:36:43Z",
```

```
  "region": "us-east-1",
  "resources": [
     "arn:aws:rds:us-east-1:123456789012:db-proxy:my-rds-proxy"
  ],
  "detail": {
    "EventCategories": [
      "configuration change"
    ],
    "SourceType": "DB_PROXY",
    "SourceArn": "arn:aws:rds:us-east-1:123456789012:db-proxy:my-rds-proxy",
    "Date": "2018-09-27T22:36:43.292Z",
    "Message": "RDS modified endpoint my-endpoint of DB Proxy my-rds-proxy.",
    "SourceIdentifier": "my-endpoint",
    "EventID": "RDS-EVENT-0207"
  }
}
```

Solución de problemas de RDS Proxy

A continuación, puede encontrar ideas de solución de problemas para algunos problemas de RDS Proxy comunes e información sobre registros de CloudWatch para RDS Proxy.

En los registros de RDS Proxy, cada entrada tiene el prefijo del nombre del punto de enlace de proxy asociado. Este nombre puede ser el especificado para un punto de conexión definido por el usuario. O puede ser el nombre especial `default` para el punto de conexión predeterminado de un proxy que lleva a cabo solicitudes de lectura/escritura. Para obtener más información acerca de los puntos de enlace de proxy, consulte Trabajo con puntos de enlace del proxy de Amazon RDS.

Temas

- Verificación de la conectividad para un proxy
- Problemas y soluciones comunes de
- Solución de problemas de RDS Proxy con RDS para MySQL
- Solución de problemas de RDS Proxy con RDS para PostgreSQL

Verificación de la conectividad para un proxy

Puede utilizar los siguientes comandos para comprobar que todos los componentes, como el proxy, la base de datos y las instancias de computación de la conexión, se pueden comunicar entre sí.

Examine el propio proxy usando el comando describe-db-proxies. Examine también el grupo de destino asociado mediante el comando describe-db-proxy-target-groups. Compruebe que los detalles de los destinos coincidan con la instancia de base de datos de RDS que desea asociar con el proxy. Utilice comandos como los siguientes.

```
aws rds describe-db-proxies --db-proxy-name $DB_PROXY_NAME
aws rds describe-db-proxy-target-groups --db-proxy-name $DB_PROXY_NAME
```

Para confirmar que el proxy puede conectarse a la base de datos subyacente, examine los destinos especificados en los grupos de destino mediante el comando describe-db-proxy-targets. Utilice un comando como el siguiente.

```
aws rds describe-db-proxy-targets --db-proxy-name $DB_PROXY_NAME
```

El resultado del comando describe-db-proxy-targets incluye un campo `TargetHealth`. Puede examinar los campos `State`, `Reason` y `Description` dentro de `TargetHealth` para comprobar si el proxy puede comunicarse con la instancia de base de datos subyacente.

- Un valor `State` de `AVAILABLE` indica que el proxy puede conectarse a la instancia de base de datos.
- Un valor `State` de `UNAVAILABLE` indica un problema de conexión temporal o permanente. En este caso, examine los campos `Reason` y `Description`. Por ejemplo, si `Reason` tiene un valor de `PENDING_PROXY_CAPACITY`, intente conectarse de nuevo después de que el proxy finalice su operación de escalado. Si `Reason` tiene un valor de `UNREACHABLE`, `CONNECTION_FAILED` o `AUTH_FAILURE`, utilice la explicación del campo `Description` que le ayudará a diagnosticar el problema.
- El campo `State` es posible que tenga un valor de `REGISTERING` durante un breve tiempo antes de cambiar a `AVAILABLE` o `UNAVAILABLE`.

Si el siguiente comando Necat (`nc`) se ejecuta correctamente, puede acceder al punto de enlace del proxy desde la instancia de EC2 u otro sistema en el que haya iniciado sesión. Este comando notifica un error si no está en la misma VPC que el proxy y la base de datos asociada. Es posible que pueda iniciar sesión directamente en la base de datos sin estar en la misma VPC. Sin embargo, no puede iniciar sesión en el proxy a menos que esté en la misma VPC.

```
nc -zx MySQL_proxy_endpoint 3306
```

```
nc -zx PostgreSQL_proxy_endpoint 5432
```

Puede utilizar los siguientes comandos para asegurarse de que la instancia de EC2 tenga las propiedades requeridas. Algo especialmente importante es que la VPC para la instancia de EC2 debe ser la misma que la VPC para donde se conecta el proxy.

```
aws ec2 describe-instances --instance-ids your_ec2_instance_id
```

Examine los secretos de Secrets Manager utilizados para el proxy.

```
aws secretsmanager list-secrets
aws secretsmanager get-secret-value --secret-id your_secret_id
```

Asegúrese de que el campo `SecretString` que muestra `get-secret-value` está codificado como una cadena JSON que incluye los campos `username` y `password`. En el ejemplo siguiente se muestra el formato del campo `SecretString`.

```
{
  "ARN": "some_arn",
  "Name": "some_name",
  "VersionId": "some_version_id",
  "SecretString": '{"username":"some_username","password":"some_password"}',
  "VersionStages": [ "some_stage" ],
  "CreatedDate": some_timestamp
}
```

Problemas y soluciones comunes de

En esta sección, se describen algunos problemas comunes y posibles soluciones al utilizar RDS Proxy.

Después de ejecutar el comando de la CLI `aws rds describe-db-proxy-targets`, si en la descripción `TargetHealth` se indica `Proxy does not have any registered credentials`, verifique lo siguiente:

- Hay credenciales registradas para que el usuario acceda al proxy.
- El rol de IAM para acceder al secreto de Secrets Manager utilizado por el proxy es válido.

Es posible que encuentre los siguientes eventos de RDS al crear o conectarse a un proxy de base de datos.

Categoría	ID de evento de RDS	Descripción
error	RDS-EVENT-0243	RDS no ha podido aprovisionar capacidad para el proxy porque no hay suficientes direcciones IP disponibles en las subredes. Para resolver el problema, asegúrese de que sus subredes tengan el número mínimo de direcciones IP sin usar. Para determinar el número recomendado para la clase de instancia, consulte Planificación de la capacidad de direcciones IP.
error	RDS-EVENT-0275	RDS ha limitado algunas conexiones al proxy de base de datos *nombre*. El número de solicitudes de conexión simultáneas del cliente al proxy ha superado el límite.

Es posible que encuentre los siguientes problemas al crear un nuevo proxy o al conectarse a un proxy.

Error	Causas o soluciones provisionales
`403: The security token included in the request is invalid`	Seleccione un rol de IAM existente en lugar de elegir crear uno nuevo.

Solución de problemas de RDS Proxy con RDS para MySQL

Es posible que encuentre los siguientes problemas al conectarse a un proxy MySQL.

Error	Causas o soluciones provisionales
`ERROR 1040 (HY000): Connections rate limit exceeded (`*`limit_value`*` )`	La tasa de solicitudes de conexión del cliente al proxy ha superado el límite.
`ERROR 1040 (HY000): IAM authentication rate limit exceeded`	El número de solicitudes simultáneas con autenticación de IAM desde el cliente al proxy ha superado el límite.
`ERROR 1040 (HY000): Number simultaneous connections exceeded (`*`limit_value`*` )`	El número de solicitudes de conexión simultáneas del cliente al proxy ha superado el límite.
`ERROR 1045 (28000): Access denied for user '`*`DB_USER`*`'@'%' (using password: YES)`	El secreto de Secrets Manager utilizado por el proxy no coincide con el nombre de usuario y la contraseña de un usuario de base de datos existente. Actualice las credenciales en el secreto de Secrets Manager o asegúrese de que el usuario de la base de datos existe y tiene la misma contraseña que en el secreto.
`ERROR 1105 (HY000): Unknown error`	Se ha producido un error desconocido.

Error	Causas o soluciones provisionales
`ERROR 1231 (42000): Variable ''character_set_client'' can't be set to the value of` *`value`*	El valor establecido para el parámetro `character_set_client` no es válido. Por ejemplo, el valor `ucs2` no es válido porque puede bloquear el servidor MySQL.
`ERROR 3159 (HY000): This RDS Proxy requires TLS connections.`	Ha habilitado la configuración Exigir Transport Layer Security en el proxy pero su conexión incluyó el parámetro `ssl-mode=DISABLED` en el cliente de MySQL. Haga una de estas dos operaciones: • Desactive la configuración Exigir Transport Layer Security para el proxy. • Conéctese a la base de datos mediante la configuración mínima de `ssl-mode=REQUIRED` en el cliente de MySQL.
`ERROR 2026 (HY000): SSL connection error: Internal Server` *`Error`*	Error en el protocolo de enlace TLS al proxy. Algunas posibles razones incluyen las siguientes: • Se requiere SSL, pero el servidor no lo admite. • Se ha producido un error interno del servidor. • Se ha producido un protocolo de enlace erróneo.
`ERROR 9501 (HY000): Timed-out waiting to acquire database connection`	Se agotó el tiempo de espera del proxy mientras esperaba a adquirir una conexión a la base de datos. Algunas posibles razones incluyen las siguientes: • El proxy no puede establecer una conexión con la base de datos porque se ha llegado al máximo de conexiones. • El proxy no puede establecer una conexión a base de datos porque la base de datos no está disponible.

Solución de problemas de RDS Proxy con RDS para PostgreSQL

Es posible que encuentre los siguientes problemas al conectarse a un proxy PostgreSQL.

Error	Causa	Solución
`ERROR 28000: IAM authentication is allowed only with SSL connections.`	El usuario ha intentado conectarse a la base de datos mediante la autenticación de IAM con la configuración `sslmode=disable` en el cliente PostgreSQL.	El usuario necesita conectarse a la base de datos utilizando la configuración mínima de `sslmode=require` en el cliente PostgreSQL. Para obtener más información, consulte la documentación de Soporte de SSL de PostgreSQL.
`ERROR 28000: This RDS proxy has no credentials for the role` *`role_name`* `. Check the credentials for this role and try again.`	No hay ningún secreto de Secrets Manager para este rol.	Agregue un secreto de Secrets Manager para este rol. Para obtener más información, consulte Configuración de políticas de AWS Identity and Access Management (IAM) para RDS Proxy.
`ERROR 28000: RDS supports only IAM, MD5, or SCRAM authentication.`	El cliente de base de datos que se utiliza para conectarse al proxy utiliza un mecanismo de autenticación que actualmente no admite el proxy.	Si no utiliza la autenticación IAM, utilice la autenticación de contraseñas MD5 o SCRAM.
`ERROR 28000: A user name is missing from the connection startup packet.`	El cliente de base de datos que se utiliza para conectarse al proxy no envía un nombre de usuario al intentar establecer una conexión.	Asegúrese de definir un nombre de usuario al configurar una conexión con el proxy utilizando el cliente PostgreSQL de su elección.

Error	Causa	Solución
`Provide a user name for this connection.`		
`ERROR 28000: IAM is allowed only with SSL connections.`	Un cliente intentó conectarse mediante la autenticación de IAM, pero SSL no estaba habilitado.	Habilite SSL en el cliente PostgreSQL.
`ERROR 28000: This RDS Proxy requires TLS connections.`	El usuario habilitó la opción Exigir Transport Layer Security pero intentó conectarse con `sslmode=disable` en el cliente de PostgreSQL.	Para corregir este error, realice alguna de las siguientes acciones: • Desactive la opción del proxy Exigir Transport Layer Security. • Conectarse a la base de datos mediante la configuración mínima de `sslmode=allow` en el cliente PostgreSQL.

Error	Causa	Solución
`ERROR 28P01: IAM authentication failed for user` *`user_name`* `. Check the IAM token for this user and try again.`	Este error es posible que se deba a las siguientes razones: • El cliente proporcionó el nombre de usuario de IAM incorrecto. • El cliente proporcionó un token de autorización de IAM incorrecto para el usuario. • El cliente está utilizando una política de IAM que no tiene los permisos necesarios. • El cliente proporcionó un token de autorización de IAM caducado para el usuario.	Para corregir este error, haga lo siguiente: 1. Confirme que existe el usuario de IAM proporcio nado. 2. Confirme que el token de autorización de IAM pertenece al usuario de IAM proporcionado. 3. Confirme que la política de IAM tiene los permisos adecuados para RDS. 4. Compruebe la validez del token de autorización de IAM utilizado.
`ERROR 28P01: The password that was provided for the role` *`role_name`* `is wrong.`	La contraseña de este rol no coincide con el secreto de Secrets Manager.	Compruebe el secreto de este rol en Secrets Manager para ver si la contraseña es la misma que la que se está utilizando en su cliente PostgreSQL.
`ERROR 28P01: The IAM authentication failed for the role` *`role_name`* `. Check the IAM token for this role and try again.`	Hay un problema con el token de IAM utilizado para la autenticación de IAM.	Genere un nuevo token de autenticación y úselo en una nueva conexión.

Error	Causa	Solución
`ERROR 0A000: Feature not supported: RDS Proxy supports only version 3.0 of the PostgreSQL messaging protocol.`	El cliente PostgreSQL utilizado para conectarse al proxy utiliza un protocolo anterior a 3.0.	Utilice un cliente PostgreSQL más reciente que sea compatible con el protocolo de mensajería 3.0. Si está utilizando la CLI `psql` de PostgreSQL, utilice una versión mayor o igual a 7.4.
`ERROR 0A000: Feature not supported: RDS Proxy currently doesn't support streaming replication mode.`	El cliente PostgreSQL utilizado para conectarse al proxy está intentando utilizar el modo de replicación de streaming, que actualmente no es compatible con el proxy RDS.	Desactive el modo de replicación de streaming en el cliente de PostgreSQL que se utiliza para conectarse.
`ERROR 0A000: Feature not supported: RDS Proxy currently doesn't support the option` *`option_name`* `.`	A través del mensaje de inicio, el cliente PostgreSQL utilizado para conectarse al proxy solicita una opción que actualmente no es compatible con el proxy RDS.	Desactive la opción que se muestra como no compatible con el mensaje anterior en el cliente de PostgreSQL que se utiliza para conectarse.
`ERROR 53300: The IAM authentication failed because of too many competing requests.`	El número de solicitudes simultáneas con autenticación de IAM desde el cliente al proxy ha superado el límite.	Reduzca la velocidad en la que se establecen las conexiones que utilizan la autenticación de IAM desde un cliente PostgreSQL.
`ERROR 53300: The maximum number of client connections to the proxy exceeded` *`number_value`* `.`	El número de solicitudes de conexión simultáneas del cliente al proxy ha superado el límite.	Reduzca el número de conexiones activas de clientes PostgreSQL a este proxy RDS.

Error	Causa	Solución
`ERROR 53300: Rate of connection to proxy exceeded` *`number_value`* `.`	La tasa de solicitudes de conexión del cliente al proxy ha superado el límite.	Reduzca la velocidad en la que se establecen las conexiones de un cliente PostgreSQL.
`ERROR XX000: Unknown error.`	Se ha producido un error desconocido.	Contacte con AWS Support para que investiguemos el problema.
`ERROR 08000: Timed-out waiting to acquire database connection.`	El proxy ha agotado el tiempo de espera para adquirir una conexión de base de datos en el tiempo especificado por la configuración `ConnectionBorrowTimeout` . Algunas posibles razones incluyen las siguientes: • El proxy no puede establecer una conexión con la base de datos porque se ha alcanzado el número máximo de conexiones. • El proxy no puede establecer una conexión con la base de datos porque esta no está disponible o porque el establecimiento de la conexión con la base de datos tarda más que valor de `ConnectionBorrowTimeout` configurado.	Las posibles soluciones son las siguientes: • Evite fijar las conexiones de proxy. Consulte Cómo evitar la fijación de RDS Proxy. • Revise las configuraciones `ConnectionBorrowTimeout` y `MaxConnectionsPercent` . Consulte Observaciones sobre la conexión de RDS Proxy. • Revise la disponibilidad del destino. Consulte `AvailabilityPercentage` en Supervisión de las métricas de RDS Proxy con Amazon CloudWatch.

Error	Causa	Solución
`ERROR XX000: Request returned an error: database_error .`	La conexión de base de datos establecida desde el proxy devolvió un error.	La solución depende del error específico de la base de datos. Un ejemplo es: `Request returned an error: database "your-database-name" does not exist`. Esto significa que el nombre de base de datos especificado no existe en el servidor de bases de datos. O significa que el nombre de usuario utilizado como nombre de base de datos (si no se especifica un nombre de base de datos) no existe en el servidor.

Se ha eliminado la solución de problemas de una base de datos de **`postgres`**

Si elimina la base de datos de `postgres` de la instancia por error, tendrá que restaurarla para restablecer la conectividad con la instancia. Ejecute los siguientes comandos dentro de la instancia de base de datos:

```
CREATE DATABASE postgres;
GRANT CONNECT ON DATABASE postgres TO rdsproxyadmin;
```

Uso del proxy de RDS con AWS CloudFormation

Puede usar el proxy de RDS con AWS CloudFormation. Esto le ayuda a crear grupos de recursos relacionados. Dicho grupo puede incluir un proxy que se puede conectar a una instancia de base de datos de Amazon RDS. La compatabilidad del proxy de RDS en AWS CloudFormation implica dos nuevos tipos de registro: `DBProxy` y `DBProxyTargetGroup`.

En la siguiente descripción, se muestra una plantilla de AWS CloudFormation de ejemplo para el proxy de RDS.

```
Resources:
 DBProxy:
   Type: AWS::RDS::DBProxy
   Properties:
     DBProxyName: CanaryProxy
     EngineFamily: MYSQL
     RoleArn:
      Fn::ImportValue: SecretReaderRoleArn
     Auth:
       - {AuthScheme: SECRETS, SecretArn: !ImportValue ProxySecret, IAMAuth: DISABLED}
     VpcSubnetIds:
       Fn::Split: [",", "Fn::ImportValue": SubnetIds]

 ProxyTargetGroup:
   Type: AWS::RDS::DBProxyTargetGroup
   Properties:
     DBProxyName: CanaryProxy
     TargetGroupName: default
     DBInstanceIdentifiers:
       - Fn::ImportValue: DBInstanceName
   DependsOn: DBProxy
```

Para obtener más información sobre los recursos de este ejemplo, consulte DBProxy y DBProxyTargetGroup.

Para obtener más información acerca de los recursos que puede crear mediante AWS CloudFormation, consulte la Referencia del tipo de recurso de RDS.

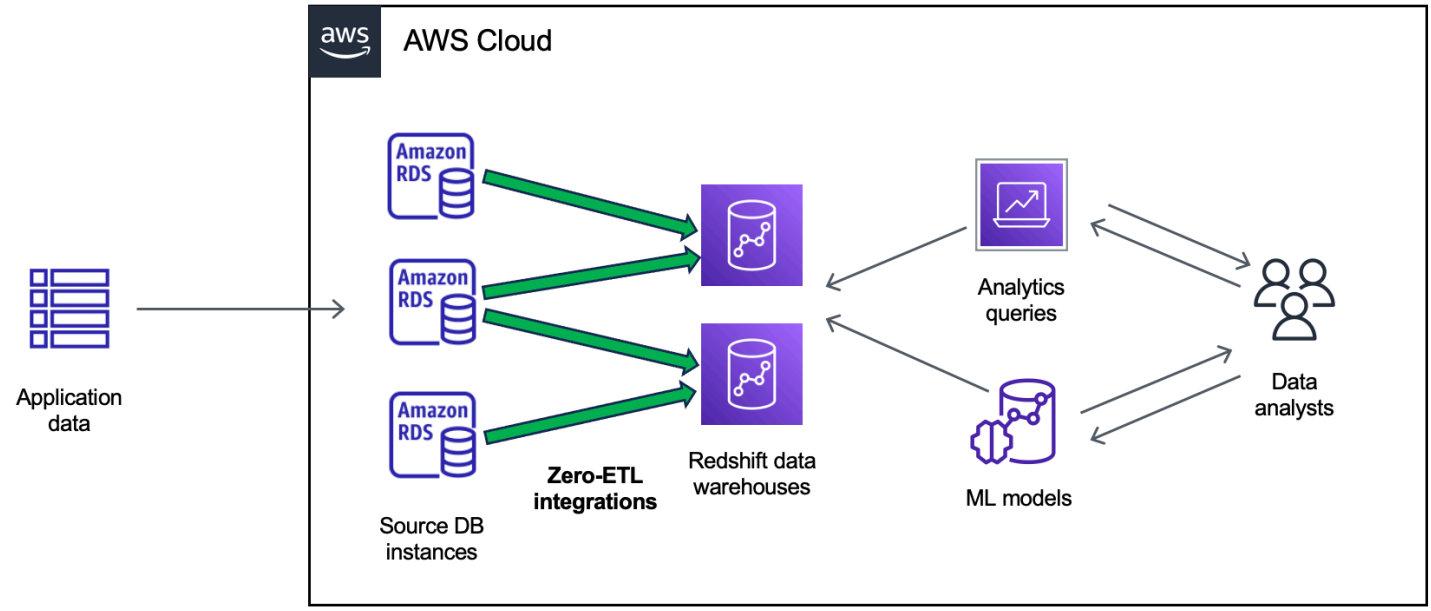
Integraciones sin ETL de Amazon RDS

Una integración sin ETL de Amazon RDS con Amazon Redshift y Amazon SageMaker permite realizar análisis y machine learning (ML) casi en tiempo real mediante datos de RDS. Es una solución totalmente administrada que permite que los datos transaccionales estén disponibles en el destino de análisis después de escribirlos en una base de datos de RDS. La extracción, transformación y carga (ETL) es un proceso en el que se combinan datos de numerosos orígenes en un gran almacenamiento de datos central.

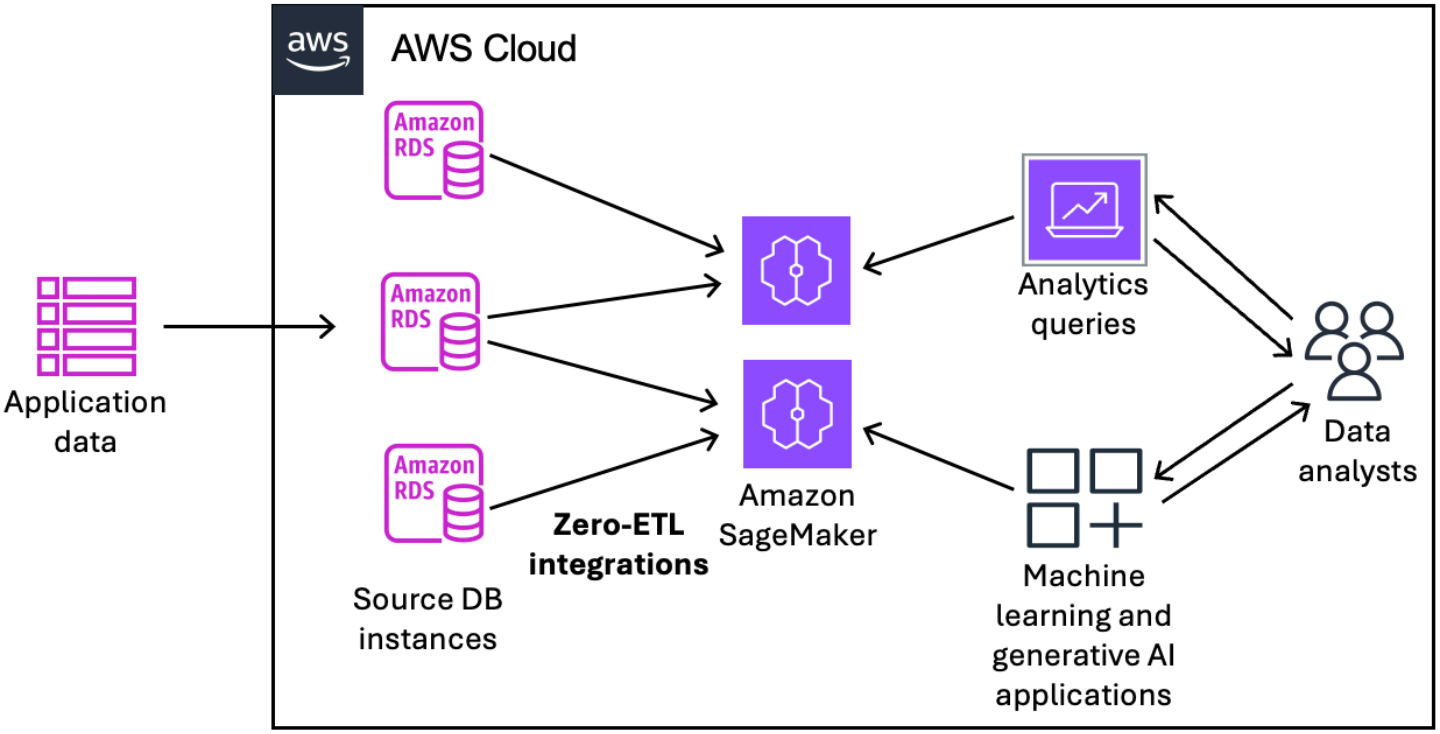
La integración sin ETL hace que los datos de base de datos de RDS estén disponibles en Amazon Redshift o un Amazon SageMaker Lakehouse prácticamente en tiempo real. Una vez que los datos están en el almacén de datos de destino o lago de datos, puede alimentar cargas de trabajo de análisis, ML e IA con las capacidades integradas, como el machine learning, las vistas materializadas, el uso compartido de datos, el acceso federado a varios almacenamientos de datos y lagos de datos, y las integraciones con Amazon SageMaker AI, QuickSight y otros Servicios de AWS.

Para crear una integración sin ETL, especifique una base de datos de RDS como origen y un almacén de datos o almacén de lago compatible como destino. La integración replica los datos de la base de datos de origen en el almacén de datos de destino o almacén de lago.

El siguiente diagrama ilustra esta funcionalidad para una integración sin ETL con Amazon Redshift:



En el siguiente diagrama se ilustra esta funcionalidad para la integración sin ETL con un Amazon SageMaker Lakehouse:



La integración supervisa el estado de la canalización de datos y se recupera de los problemas cuando es posible. Puede crear integraciones a partir de varias bases de datos de RDS en un único almacén de datos o almacén de lago de destino, lo que le permite obtener información en varias aplicaciones.

Temas

- Ventajas
- Conceptos clave
- Limitaciones
- Cuotas
- Regiones compatibles
- Introducción a las integraciones sin ETL de Amazon RDS con Amazon Redshift
- Creación de integraciones sin ETL de Amazon RDS con Amazon Redshift
- Creación de integraciones sin ETL de Amazon RDS con un Amazon SageMaker Lakehouse
- Filtrado de datos para integraciones sin ETL de Amazon RDS
- Cómo agregar datos en una base de datos de RDS de origen y dirigirle consultas en Amazon Redshift
- Visualización y supervisión de las integraciones sin ETL de Amazon RDS

- Modificación de las integraciones sin ETL de Amazon RDS
- Eliminación de las integraciones sin ETL de Amazon RDS
- Solución de problemas de integraciones sin ETL de Amazon RDS con Amazon Redshift

Ventajas

Las integraciones sin ETL de RDS tienen los siguientes beneficios:

- Le ayudan a obtener información holística a partir de numerosos orígenes de datos.
- Eliminan la necesidad de crear y mantener canalizaciones de datos complejas que realicen operaciones de extracción, transformación y carga (ETL). Las integraciones sin ETL eliminan los inconvenientes derivados de la creación y administración de canalizaciones, ya que las aprovisionan y administran por usted.
- Reducen la carga operativa y los costos para que pueda centrarse en mejorar sus aplicaciones.
- Le permite aprovechar las capacidades de análisis y ML de destino para obtener información a partir de datos transaccionales y de otro tipo, a fin de responder de manera eficaz a eventos críticos y urgentes.

Conceptos clave

Cuando empiece a utilizar las integraciones sin ETL, tenga en cuenta los siguientes conceptos:

Integración

Una canalización de datos totalmente administrada que replica automáticamente los datos y esquemas transaccionales de una base de datos de RDS a un almacén de datos o catálogo.

Base de datos de origen

La base de datos de RDS desde donde se replican los datos. Puede especificar una instancia de base de datos single-AZ o multi-AZ o un clúster de base de datos multi-AZ.

Destino

El almacén de datos o almacén de lago en el que se replican los datos. Hay dos tipos de almacenamientos de datos: un almacenamiento de datos de clústeres aprovisionados y un almacenamiento de datos sin servidor. Un almacenamiento de datos de clústeres aprovisionados

es una colección de recursos de computación denominados nodos que están organizados en un grupo llamado clúster. Un almacenamiento de datos sin servidor se compone de un grupo de trabajo que almacena los recursos de computación y un espacio de nombres que aloja los objetos y usuarios de la base de datos. Ambos almacenes de datos ejecutan un motor de análisis y contienen una o más bases de datos.

Un almacén de lago de destino consta de catálogos, bases de datos, tablas y vistas. Para obtener más información sobre la arquitectura del almacén de lago, consulte Amazon SageMaker Lakehouse components en la Guía del usuario de Amazon SageMaker Unified Studio.

Múltiples bases de datos de origen pueden escribir en el mismo destino.

Para obtener más información, consulte Arquitectura del sistema de almacenamiento de datos en la Guía del desarrollador de Amazon Redshift.

Limitaciones

Las siguientes limitaciones se aplican a las integración sin ETL de RDS.

Temas

- Limitaciones generales
- Limitaciones de RDS for MySQL
- Limitaciones de Amazon Redshift
- Limitaciones de Amazon SageMaker Lakehouse

Limitaciones generales

- La base de datos de origen debe estar en la misma región que el destino.
- No puede cambiar el nombre de una base de datos si ya tiene integraciones.
- No se pueden crear varias integraciones entre las mismas bases de datos de origen y de destino.
- No puede eliminar una base de datos que ya tenga integraciones. Primero debes eliminar todas las integraciones asociadas.
- Si detiene la base de datos de origen, es posible que las últimas transacciones no se repliquen en el destino hasta que reanude la base de datos.
- No puede eliminar una integración si la base de datos de origen está detenida.

- Si la base de datos es el origen de una implementación azul/verde, los entornos azul y verde no pueden tener integraciones sin ETL existentes durante la transición. Primero debe eliminar la integración, realizar la transición y, a continuación, volver a crear la integración.
- No puede crear una integración para una base de datos de origen en la que se esté creando otra integración de forma activa.
- Cuando se crea una integración por primera vez, o cuando se vuelve a sincronizar una tabla, la transferencia de datos del origen al destino puede tardar entre 20 y 25 minutos o más, en función del tamaño de la base de datos de origen. Este retardo puede provocar un aumento del retardo en la réplica.
- Algunos tipos de datos no son compatibles. Para obtener más información, consulte the section called “Diferencias de tipos de datos”.
- Las tablas del sistema, las tablas temporales y las vistas no se replican en almacenes de destino.

Limitaciones de RDS for MySQL

- La base de datos de origen debe ejecutar una versión compatible de RDS para MySQL. Para obtener una lista de las versiones compatibles, consulte the section called “Integraciones sin ETL ”.
- Las integraciones sin ETL se basan en el registro binario de MySQL (binlog) para capturar los cambios en los datos en curso. No utilice el filtrado de datos basado en binlog, ya que puede provocar incoherencias entre los datos de las bases de datos de origen y de destino.
- Las integraciones sin ETL solo son compatibles con bases de datos configuradas para usar el motor de almacenamiento de InnoDB.
- No se admiten referencias de clave externas con actualizaciones de tablas predefinidas. En concreto, las reglas `ON DELETE` y `ON UPDATE` no son compatibles con las acciones `CASCADE`, `SET NULL` y `SET DEFAULT`. Si se intenta crear o actualizar una tabla con este tipo de referencias a otra tabla, se producirá un error en la tabla.
- Las operaciones de partición de `ALTER TABLE` provocan que se vuelva a sincronizar la tabla para cargar los datos de RDS de nuevo en el almacén de destino. Durante este proceso, la tabla no se podrá consultar. Para obtener más información, consulte the section called “Una o más de mis tablas de Amazon Redshift requieren una resincronización”.

Limitaciones de Amazon Redshift

Para obtener una lista de limitaciones de Amazon Redshift relacionadas con las integraciones sin ETL, consulte Consideraciones al utilizar las integraciones sin ETL con Amazon Redshift de la Guía de administración de Amazon Redshift.

Limitaciones de Amazon SageMaker Lakehouse

La siguiente es una limitación para las integraciones sin ETL de Amazon SageMaker Lakehouse.

- Los nombres de catálogo están limitados a 19 caracteres de longitud.

Cuotas

La cuenta tiene las siguientes cuotas relacionadas con las integraciones sin ETL de RDS. Cada una de las cuotas se aplica a una sola región, a no ser que se especifique otra cosa.

Nombre	Predeterminado/a	Descripción
Integraciones	100	El número total de integraciones dentro de una Cuenta de AWS.
Integraciones por destino	50	El número de integraciones que envían datos a un único almacén de datos o almacén de lago de destino.
Integraciones por instancia de origen	5	La cantidad de integraciones que envían datos desde una sola instancia de base de datos de origen.

Además, el almacén de destino establece algunos límites en la cantidad de tablas permitidas en cada instancia de base de datos o nodo de clúster. Para obtener más información sobre cuotas y límites de Amazon Redshift, consulte Cuotas y límites de Amazon Redshift en la Guía de administración de Amazon Redshift.

Regiones compatibles

Las integraciones sin ETL de RDS están disponibles en un subconjunto de Regiones de AWS. Para obtener una lista de las regiones admitidas, consulte the section called “Integraciones sin ETL ”.

Introducción a las integraciones sin ETL de Amazon RDS con Amazon Redshift

> Esta es la documentación previa al lanzamiento de las integraciones sin ETL de Amazon RDS con Amazon Redshift, que se encuentra en la versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

Antes de crear una integración sin ETL con Amazon Redshift, configure su base de datos de RDS y el almacenamiento de datos de Amazon Redshift con los parámetros y permisos necesarios. Durante la configuración, realizará los siguientes pasos:

1. Cree un grupo de parámetros de de base de datos personalizado.
2. Cree una base de datos.
3. Creación de un almacén de datos de Amazon Redshift de destino.

Una vez que haya completado estos pasos, continúe con la the section called “Creación de integraciones sin ETL con Amazon Redshift”.

Crear un grupo de parámetros de de base de datos personalizado

Las integraciones sin ETL de Amazon RDS con Amazon Redshift requieren valores específicos para los parámetros de base de datos que controlan el registro binario (binlog). Para configurar el registro binario, primero debe crear un grupo de parámetros personalizado de base de datos y, a continuación, asociarlo a la base de datos de origen.

Cree un grupo de parámetros de de base de datos personalizado con los siguientes ajustes. Para obtener instrucciones sobre cómo crear un grupo de parámetros, consulte the section called “Grupos de parámetros de base de datos”.

- `binlog_format=ROW`
- `binlog_row_image=full`
- `binlog_checksum=NONE`

Compruebe también que el parámetro `binlog_row_value_options` no esté establecido en `PARTIAL_JSON`.

Paso 2: seleccionar o crear una base de datos de origen

Tras crear un grupo de parámetros personalizado del de base de datos, elija o cree una instancia de base de datos de RDS para MySQL multi-AZ o single-AZ. Esta base de datos será el origen de la réplica de datos en Amazon Redshift.

La base de datos debe ejecutar RDS para MySQL versión 8.0.32 o posterior. Para obtener instrucciones sobre cómo crear una instancia de base de datos multi-AZ o single-AZ, consulte the section called “Creación de una instancia de base de datos”.

En Configuración adicional, cambie el Grupo de parámetros de base de datos por el grupo de parámetros personalizado que creó en el paso anterior.

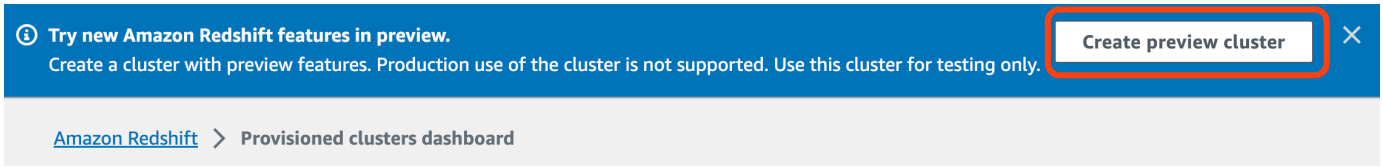
> **Note**
>
> si asocia el grupo de parámetros a la base de datos después de haber creado la base de datos, debe reiniciar la base de datos a fin de aplicar los cambios antes de poder crear una integración sin ETL. Para obtener instrucciones, consulte the section called “Reinicio de una instancia de base de datos”.

Además, asegúrese de que las copias de seguridad automáticas están activadas en la base de datos. Para obtener más información, consulte the section called “Habilitar las copias de seguridad automatizadas”.

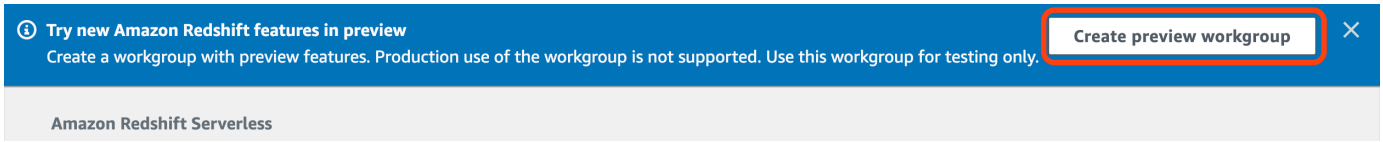
Paso 3: Creación de un almacén de datos de destino en Amazon Redshift

Tras crear la base de datos de origen, debe crear y configurar un almacenamiento de datos de destino en Amazon Redshift. El almacenamiento de datos debe cumplir los siguientes requisitos:

- Creado en vista previa
  - Para crear un clúster aprovisionado en versión preliminar, seleccione Crear clúster de vista previa en el encabezado del panel de clústeres aprovisionados. Para obtener más información, consulte Creación de un clúster de previsualización..



    Al crear el clúster, configure la pista Vista previa en `preview_2023`.
  - Para crear un grupo de trabajo Redshift sin servidor en versión preliminar, seleccione Crear grupo de trabajo de vista previa en el encabezado del panel de control sin servidor.. Para obtener más información, consulte Crear un grupo de trabajo de vista previa.



- Uso de un tipo de nodo RA3 (`ra3.xlplus`, `ra3.4xlarge` o `ra3.16xlarge`) con al menos dos nodos o Redshift sin servidor.
- Cifrado (si se utiliza un clúster aprovisionado). Para obtener más información, consulte Cifrado de base de datos de Amazon Redshift.

Para obtener instrucciones sobre cómo crear un almacenamiento de datos, consulte la sección Creación de un clúster para clústeres aprovisionados o Creación de un grupo de trabajo con un espacio de nombres para Redshift Serverless.

Activar la distinción entre mayúsculas y minúsculas en el almacén de datos

Para que la integración funcione, el parámetro de distinción entre mayúsculas y minúsculas (`enable_case_sensitive_identifier`) debe estar habilitado en el almacenamiento de datos. De forma predeterminada, la distinción entre mayúsculas y minúsculas está desactivada en todos los clústeres y grupos de trabajo sin servidor de Redshift suministrados.

Para activar la distinción entre mayúsculas y minúsculas, realice los siguientes pasos en función del tipo de almacén de datos:

- Clúster aprovisionado: para habilitar la distinción entre mayúsculas y minúsculas en un clúster aprovisionado, cree un grupo de parámetros personalizado con el parámetro `enable_case_sensitive_identifier` habilitado. A continuación, asocie el grupo de parámetros al clúster. Para obtener instrucciones, consulte la sección Administración de grupos de parámetros mediante la consola o Configuración de los valores de parámetros mediante la AWS CLI.

  > **Note**
  >
  > Recuerde reiniciar el clúster después de asociarlo el grupo de parámetros personalizado.

- Grupo de trabajo sin servidor: para habilitar la distinción entre mayúsculas y minúsculas en un grupo de trabajo sin servidor de Redshift, debe usar AWS CLI. Actualmente, la consola de Amazon Redshift no permite modificar los valores de los parámetros de Redshift sin servidor. Envíe la siguiente solicitud de update-workgroup:

  ```
  aws redshift-serverless update-workgroup \
    --workgroup-name target-workgroup \
    --config-parameters
   parameterKey=enable_case_sensitive_identifier,parameterValue=true
  ```

  No es necesario reiniciar un grupo de trabajo después de modificar los valores de los parámetros.

Configure la autorización para el almacenamiento de datos

Tras crear un almacenamiento de datos, debe configurar la base de datos de RDS de origen como origen de integración autorizado. Para obtener instrucciones, consulte Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.

Siguientes pasos

Ahora que tiene una base de datos de RDS de origen y un almacenamiento de datos de destino de Amazon Redshift, puede crear una integración sin ETL y empezar a replicar los datos. Para obtener instrucciones, consulte the section called “Creación de integraciones sin ETL con Amazon Redshift”.

Creación de integraciones sin ETL de Amazon RDS con Amazon Redshift

Al crear una integración sin ETL de Amazon RDS, debe especificar una base de datos de RDS de origen y un almacenamiento de datos de Amazon Redshift de destino. También puede personalizar la configuración de cifrado y añadir etiquetas. Amazon RDS crea una integración entre la base de datos de origen y su destino. Una vez que la integración esté activa, todos los datos que inserte en la base de datos de origen se replicarán en el destino configurado de Amazon Redshift.

Requisitos previos

Antes de crear una integración sin ETL, debe crear una base de datos de origen y un almacenamiento de datos de Amazon Redshift de destino. También debe permitir la réplica en el almacenamiento de datos añadiendo la base de datos como origen de integración autorizado.

Para obtener instrucciones para completar cada uno de estos pasos, consulte the section called "Introducción a las integraciones sin ETL".

Permisos necesarios

Para crear una integración sin ETL se necesitan determinados permisos de IAM. Como mínimo, necesita permisos para realizar las siguientes acciones:

- Crear integraciones sin ETL para la base de datos RDS de origen.
- Ver y eliminar todas las integraciones sin ETL.
- Crear integraciones entrantes en el almacenamiento de datos de destino.

Las políticas de ejemplo siguiente muestran los permisos con privilegios mínimos necesarios para crear y administrar integraciones. Es posible que no necesite estos permisos exactos si su usuario o rol tiene permisos más amplios, como una política administrada `AdministratorAccess`.

> **Note**
>
> Los nombres de recurso de Amazon (ARN) de Redshift tienen el siguiente formato. Tenga en cuenta el uso de la barra diagonal (`/`) en lugar de dos puntos (`:`) antes del UUID del espacio de nombres sin servidor.

- Clúster aprovisionado: `arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid`
- Sin servidor: `arn:aws:redshift-serverless:{region}:{account-id}:namespace/namespace-uuid`

Política de ejemplo para el destino de Redshift

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rds:CreateIntegration"
        ],
        "Resource": [
            "arn:aws:rds:{region}:{account-id}:db:source-db",
            "arn:aws:rds:{region}:{account-id}:integration:*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "rds:DescribeIntegrations"
        ],
        "Resource": ["*"]
    },
    {
        "Effect": "Allow",
        "Action": [
            "rds:DeleteIntegration",
            "rds:ModifyIntegration"
        ],
        "Resource": [
            "arn:aws:rds:{region}:{account-id}:integration:*"
        ]
    },
    {
        "Effect": "Allow",
```

```
        "Action": [
            "redshift:CreateInboundIntegration"
        ],
        "Resource": [
            "arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid"
        ]
    }]
}
```

Elegir un almacenamiento de datos de destino en una cuenta diferente

Si tiene previsto especificar un almacenamiento de datos de Amazon Redshift de destino distinto de una Cuenta de AWS, debe crear un rol que permita a los usuarios de la cuenta actual acceder a los recursos de la cuenta de destino. Para obtener más información, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS propia.

El rol debe tener los siguientes permisos, que permiten al usuario ver los clústeres aprovisionados de Amazon Redshift y los espacios de nombres de Redshift sin servidor disponibles en la cuenta de destino.

Permisos necesarios y política de confianza

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "redshift:DescribeClusters",
            "redshift-serverless:ListNamespaces"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

El rol debe tener la siguiente política de confianza, que especifica el ID de la cuenta de destino.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS": "arn:aws:iam::{external-account-id}:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Para obtener instrucciones sobre cómo crear los roles, consulte Creación de un rol mediante políticas de confianza personalizadas.

Creación de integraciones sin ETL

Puede crear la integración sin ETL mediante la AWS Management Console, la AWS CLI o la API de RDS.

> **Important**
>
> Las integraciones sin ETL no admiten operaciones de actualización o resincronización. Si encuentra problemas con una integración después de la creación, debe eliminarla y crear una nueva.

De forma predeterminada, RDS para MySQL purga inmediatamente los archivos de registro binarios. Como las integraciones sin ETL se basan en registros binarios para replicar los datos de origen en el destino, el periodo de retención de la base de datos de origen debe ser de al menos una hora. Al crear una integración, Amazon RDS comprueba el periodo de retención del archivo de registro binario para la base de datos de origen seleccionada. Si el valor actual es 0 horas, Amazon RDS lo cambia automáticamente a 1 hora. De lo contrario, el valor sigue siendo el mismo.

Consola de RDS

Para eliminar una integración sin ETL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación izquierdo, elija Integraciones sin ETL.
3. Elija Crear integración sin ETL.
4. En Identificador de la integración, introduzca un nombre para la integración. El nombre puede tener hasta 63 caracteres alfanuméricos y puede incluir guiones.

   > **Important**
   >
   > Los nombres de catálogo están limitados a 19 caracteres de longitud. Asegúrese de que el identificador de integración cumpla este requisito si se va a utilizar como nombre de catálogo.

5. Elija Siguiente.
6. En Origen, seleccione la base de datos de RDS donde se originarán los datos.

   > **Note**
   >
   > RDS le avisa si los parámetros del de base de datos no están configurados correctamente. Si aparece este mensaje, puede elegir la opción Corregir automáticamente o configurarlos manualmente. Para obtener instrucciones sobre cómo corregirlos manualmente, consulte the section called “Crear un grupo de parámetros de de base de datos personalizado”.
   > Para modificar los parámetros del de base de datos es necesario reiniciar. Para crear la integración, es necesario completar el reinicio y aplicar correctamente los nuevos valores de parámetros en la base de datos.

7. Cuando la base de datos de origen esté configurado correctamente, seleccione Siguiente.
8. En Destino, haga lo siguiente:

   1. (Opcional) Para utilizar una cuenta diferente a la Cuenta de AWS para el destino de Amazon Redshift, elija Especificar una cuenta diferente. A continuación, introduzca el ARN del rol de IAM con permisos para mostrar sus almacenamientos de datos. Para obtener instrucciones

para crear el rol de IAM, consulte the section called “Elegir un almacenamiento de datos de destino en una cuenta diferente”.

2. Para el almacenamiento de datos de Amazon Redshift, seleccione el destino para los datos replicados de la base de datos de origen. Puede elegir un clúster de Amazon Redshift aprovisionado o un espacio de nombres Redshift sin servidor como destino.

> **Note**
>
> RDS le avisa si la política de recursos o la configuración de distinción entre mayúsculas y minúsculas del almacenamiento de datos especificado no están configuradas correctamente. Si aparece este mensaje, puede elegir la opción Corregir automáticamente o configurarlas manualmente. Para obtener instrucciones sobre cómo corregirlas manualmente, consulte Activación de la distinción entre mayúsculas y minúsculas en el almacenamiento de datos y Configuración de la autorización para el almacenamiento de datos en la Guía de administración de Amazon Redshift.
> Para modificar la distinción entre mayúsculas y minúsculas en un clúster de Redshift aprovisionado es necesario reiniciar. Para crear la integración, es necesario completar el reinicio y aplicar correctamente el nuevo valor del parámetro al clúster.
> Si el origen y el destino seleccionados están en Cuentas de AWS diferentes, Amazon RDS no podrá corregir esta configuración automáticamente. Debe acceder a la otra cuenta y corregirla manualmente en Amazon Redshift.

9. Una vez que el almacenamiento de datos de destino esté configurado correctamente, seleccione Siguiente.
10. (Opcional) En Etiquetas, añada una o más etiquetas al trabajo de integración. Para obtener más información, consulte the section called “Etiquetado de los recursos de RDS”.
11. En el caso del cifrado, especifique cómo desea que se cifra la integración. De forma predeterminada, RDS cifra todas las integraciones con una Clave propiedad de AWS. Para elegir una clave administrada por el cliente en su lugar, active Personalizar la configuración de cifrado y elija una clave de KMS para usarla en el cifrado. Para obtener más información, consulte the section called “Cifrado de recursos de Amazon RDS”.

    Si lo desea, añada un contexto de cifrado. Para obtener más información, consulte Contexto de cifrado en la Guía para desarrolladores de AWS Key Management Service.

> **Note**
>
> Amazon RDS añade los siguientes pares de contexto de cifrado (además de los que usted incluya):
>
> - `aws:redshift:integration:arn` - `IntegrationArn`
> - `aws:servicename:id` - `Redshift`
>
> Esto reduce el número total de pares que se pueden añadir (de 8 a 6) y contribuye al límite total de caracteres en la restricción de concesiones. Para obtener más información, consulte Uso de restricciones de concesiones en la Guía para desarrolladores de AWS Key Management Service.

12. Elija Siguiente.
13. Revise la configuración de integración y elija Crear integración sin ETL.

    Si se produce un error en la creación, consulte the section called “No puedo crear una integración sin ETL” para ver los pasos de solución de problemas.

La integración tiene un estado de `Creating` mientras se crea y el almacenamiento de datos de Amazon Redshift de destino tiene un estado de `Modifying`. Durante este tiempo, no puede consultar el almacenamiento de datos ni realizar ningún cambio de configuración en él.

Cuando la integración se crea correctamente, tanto el estado de la integración como el almacenamiento de datos de Amazon Redshift de destino cambian a `Active`.

AWS CLI

Para crear una integración sin ETL mediante la AWS CLI, utilice el comando create-integration con las siguientes opciones:

> **Note**
>
> Recuerde que los nombres de catálogo están limitados a 19 caracteres. Elija el nombre de la integración en consecuencia si se va a utilizar como nombre de catálogo.

- `--integration-name`: especifique un nombre para la integración.
- `--source-arn`: especifique el ARN de la base de datos de RDS que será el origen de la integración.
- `--target-arn`: especifique el ARN del almacenamiento de datos de Amazon Redshift que será el destino de la integración.

Example

Para Linux, macOS o Unix:

```
aws rds create-integration \
    --integration-name my-integration \
    --source-arn arn:aws:rds:{region}:{account-id}:my-db \
    --target-arn arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid
```

Para Windows:

```
aws rds create-integration ^
    --integration-name my-integration ^
    --source-arn arn:aws:rds:{region}:{account-id}:my-db ^
    --target-arn arn:aws:redshift:{region}:{account-id}:namespace:namespace-uuid
```

API de RDS

Para crear una integración sin ETL mediante la API de Amazon RDS, utilice la operación `CreateIntegration` con los siguientes parámetros:

> **Note**
>
> Los nombres de catálogo están limitados a 19 caracteres. Asegúrese de que el parámetro IntegrationName cumpla este requisito si se va a utilizar como nombre de catálogo.

- `IntegrationName`: especifique un nombre para la integración.
- `SourceArn`: especifique el ARN de la base de datos de RDS que será el origen de la integración.
- `TargetArn`: especifique el ARN del almacenamiento de datos de Amazon Redshift que será el destino de la integración.

Cifrado de integraciones con una clave administrada por el cliente

Si especifica una clave de KMS personalizada en lugar de una Clave propiedad de AWS al crear una integración, la política de claves debe darle a la entidad principal del servicio Amazon Redshift acceso principal a la acción `CreateGrant`. Además, debe permitir al usuario actual realizar las acciones `DescribeKey` y `CreateGrant`.

En la siguiente política de muestra se demuestra cómo proporcionar los permisos necesarios en su política de claves. Incluye claves de contexto que sirven para reducir aún más el alcance de los permisos.

Política de claves de muestra

JSON

```
{
    "Version": "2012-10-17",
    "Id": "Key policy",
    "Statement": [
        {
            "Sid": "Enables IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{account-ID}:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allows the Redshift service principal to add a grant to a KMS
 key",
            "Effect": "Allow",
            "Principal": {
                "Service": "redshift.amazonaws.com"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:{context-key}":"{context-value}"
                },
                "ForAllValues:StringEquals": {
```

```
                    "kms:GrantOperations": [
                        "Decrypt",
                        "GenerateDataKey",
                        "CreateGrant"
                    ]
                }
            }
        },
        {
            "Sid": "Allows the current user or role to add a grant to a KMS key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{account-ID}:role/{role-name}"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:{context-key}":"{context-value}",
                    "kms:ViaService": "rds.us-east-1.amazonaws.com"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "GenerateDataKey",
                        "CreateGrant"
                    ]
                }
            }
        },
        {
            "Sid": "Allows the current uer or role to retrieve information about
 a KMS key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{account-ID}:role/{role-name}"
            },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Creating a key policy en la Guía del desarrollador de AWS Key Management Service.

Pasos a seguir a continuación

Tras crear correctamente una integración sin ETL, debe crear una base de datos de destino dentro del clúster o grupo de trabajo de Amazon Redshift de destino. A continuación, puede empezar a agregar datos a la base de datos de RDS de origen y a dirigirle consultas en Amazon Redshift. Para obtener instrucciones, consulte Creating destination databases in Amazon Redshift.

Creación de integraciones sin ETL de Amazon RDS con un Amazon SageMaker Lakehouse

Cuando crea una integración sin ETL de Amazon RDS con un Amazon SageMaker Lakehouse, debe especificar una base de datos de RDS de origen y el catálogo administrado por AWS Glue de destino. También puede personalizar la configuración de cifrado y añadir etiquetas. Amazon RDS crea una integración entre la base de datos de origen y su destino. Una vez que la integración esté activa, todos los datos que inserte en la base de datos de origen se replicarán en el destino configurado.

Requisitos previos

Antes de crear una integración sin ETL con un Amazon SageMaker Lakehouse, debe crear una base de datos de origen y un catálogo administrado por AWS Glue de destino. También debe permitir la replicación en el catálogo agregando la base de datos como origen de integración autorizado.

Para obtener instrucciones para completar cada uno de estos pasos, consulte the section called “Introducción a las integraciones sin ETL”.

Permisos necesarios

Se necesitan determinados permisos de IAM para crear una integración sin ETL con un Amazon SageMaker Lakehouse. Como mínimo, necesita permisos para realizar las siguientes acciones:

- Crear integraciones sin ETL para la base de datos RDS de origen.
- Ver y eliminar todas las integraciones sin ETL.
- Cree integraciones entrantes en el catálogo administrado por AWS Glue de destino.

- Acceda a los buckets de Amazon S3 que utiliza el catálogo administrado por AWS Glue.
- Utilice claves de AWS KMS para el cifrado si está configurado un cifrado personalizado.
- Registre recursos con Lake Formation.
- Incluya la política de recursos en el catálogo administrado por AWS Glue para autorizar las integraciones entrantes.

La política de ejemplo siguiente demuestra los permisos con privilegios mínimos necesarios para crear y administrar integraciones con un Amazon SageMaker Lakehouse. Es posible que no necesite estos permisos exactos si su usuario o rol tiene permisos más amplios, como una política administrada `AdministratorAccess`.

Además, debe configurar una política de recursos en el catálogo administrado por AWS Glue de destino para autorizar las integraciones entrantes. Use el comando de la AWS CLI siguiente para aplicar la política de recursos.

Comando de la AWS CLI de ejemplo para autorizar las integraciones entrantes en el catálogo de destino

```
aws glue put-resource-policy \
      --policy-in-json  '{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "glue.amazonaws.com"
        },
        "Action": [
            "glue:AuthorizeInboundIntegration"
        ],
        "Resource": ["arn:aws:glue:region:account_id:catalog/catalog_name"],
        "Condition": {
            "StringEquals": {
                "aws:SourceArn": "arn:aws:rds:region:account_id:db:source_name"
            }
        }
    },
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "account_id"
```

```
        },
        "Action": ["glue:CreateInboundIntegration"],
        "Resource": ["arn:aws:glue:region:account_id:catalog/catalog_name"]
    }
    ]
}' \
      --region region
```

> **Note**
>
> Los nombres de recurso de Amazon (ARN) del catálogo de Glue tienen el siguiente formato:
>
> - Catálogo de Glue: `arn:aws:glue:{region}:{account-id}:catalog/catalog-name`

Elección de un catálogo administrado por AWS Glue de destino en una cuenta diferente

Si piensa especificar un catálogo administrado por AWS Glue de destino que está en otra Cuenta de AWS, debe crear un rol que permita a los usuarios de la cuenta actual acceder a los recursos de la cuenta de destino. Para obtener más información, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS propia.

El rol debe tener los siguientes permisos, que permiten al usuario ver los catálogos de AWS Glue disponibles en la cuenta de destino.

Permisos necesarios y política de confianza

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "glue:GetCatalog"
         ],
         "Resource":[
            "*"
         ]
      }
```

```
   ]
}
```

El rol debe tener la siguiente política de confianza, que especifica el ID de la cuenta de destino.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS": "arn:aws:iam::{external-account-id}:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Para obtener instrucciones sobre cómo crear los roles, consulte Creación de un rol mediante políticas de confianza personalizadas.

Creación de integraciones sin ETL con un Amazon SageMaker Lakehouse

Puede crear una integración sin ETL con un Amazon SageMaker Lakehouse mediante la AWS Management Console, la AWS CLI o la API de RDS.

> **Important**
>
> Las integraciones sin ETL con un Amazon SageMaker Lakehouse no admiten operaciones de actualización o resincronización. Si encuentra problemas con una integración después de la creación, debe eliminarla y crear una nueva.

De forma predeterminada, RDS para MySQL purga inmediatamente los archivos de registro binarios. Como las integraciones sin ETL se basan en registros binarios para replicar los datos de origen en el destino, el periodo de retención de la base de datos de origen debe ser de al menos una hora. Al crear una integración, Amazon RDS comprueba el periodo de retención del archivo de registro binario para la base de datos de origen seleccionada. Si el valor actual es 0 horas, Amazon RDS lo cambia automáticamente a 1 hora. De lo contrario, el valor sigue siendo el mismo.

Consola de RDS

Creación de una integración sin ETL con un Amazon SageMaker Lakehouse

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación izquierdo, elija Integraciones sin ETL.
3. Elija Crear integración sin ETL.
4. En Identificador de la integración, introduzca un nombre para la integración. El nombre puede tener hasta 63 caracteres alfanuméricos y puede incluir guiones.
5. Elija Siguiente.
6. En Origen, seleccione la base de datos de RDS donde se originarán los datos.

> **Note**
>
> RDS le avisa si los parámetros del de base de datos no están configurados correctamente. Si aparece este mensaje, puede elegir la opción Corregir automáticamente o configurarlos manualmente. Para obtener instrucciones sobre cómo corregirlos manualmente, consulte the section called “Crear un grupo de parámetros de de base de datos personalizado”.
> Para modificar los parámetros del de base de datos es necesario reiniciar. Para crear la integración, es necesario completar el reinicio y aplicar correctamente los nuevos valores de parámetros en la base de datos.

7. Cuando la base de datos de origen esté configurado correctamente, seleccione Siguiente.
8. En Destino, haga lo siguiente:
    1. (Opcional) Para utilizar una Cuenta de AWS diferente para el Amazon SageMaker Lakehouse de destino, elija Especificar una cuenta diferente. A continuación, ingrese el ARN de un rol de IAM con permisos para mostrar los catálogos de AWS Glue. Para obtener instrucciones para crear el rol de IAM, consulte the section called “Elección de un catálogo administrado por AWS Glue de destino en una cuenta diferente”.
    2. Para el catálogo de AWS Glue, seleccione el destino de los datos replicados de la base de datos de origen. Puede elegir un catálogo administrado por AWS Glue existente como destino.

3. El rol de IAM de destino necesita permisos de descripción en el catálogo de destino y debe tener los siguientes permisos:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "glue:GetCatalog",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog/*",
                "arn:aws:glue:region:account-id:catalog"
            ]
        }
    ]
}
```

   El rol de IAM de destino debe tener la siguiente relación de confianza:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "glue.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

4. Debe conceder al rol de IAM de destino permisos de descripción para el catálogo administrado por AWS Glue de destino con el rol de administrador de Lake Formation creado en ???.

> **Note**
>
> RDS le notificará si la política de recursos o la configuración del catálogo administrado por AWS Glue especificado no están configurados correctamente. Si aparece este mensaje, puede elegir la opción Corregir automáticamente o configurarlas manualmente. Si el origen y el destino seleccionados están en Cuentas de AWS diferentes, Amazon RDS no podrá corregir esta configuración automáticamente. Debe acceder a la otra cuenta y corregirla manualmente en SageMaker Unified Studio.

9. Una vez que el catálogo administrado por AWS Glue de destino esté configurado correctamente, elija Siguiente.
10. (Opcional) En Etiquetas, añada una o más etiquetas al trabajo de integración. Para obtener más información, consulte the section called “Etiquetado de los recursos de RDS”.
11. En el caso del cifrado, especifique cómo desea que se cifra la integración. De forma predeterminada, RDS cifra todas las integraciones con una Clave propiedad de AWS. Para elegir una clave administrada por el cliente en su lugar, active Personalizar la configuración de cifrado y elija una clave de KMS para usarla en el cifrado. Para obtener más información, consulte the section called “Cifrado de recursos de Amazon RDS”.

    Si lo desea, añada un contexto de cifrado. Para obtener más información, consulte Contexto de cifrado en la Guía para desarrolladores de AWS Key Management Service.

    > **Note**
    >
    > Amazon RDS añade los siguientes pares de contexto de cifrado (además de los que usted incluya):
    >
    > - `aws:glue:integration:arn` - `IntegrationArn`
    > - `aws:servicename:id` - `glue`
    >
    > Esto reduce el número total de pares que se pueden añadir (de 8 a 6) y contribuye al límite total de caracteres en la restricción de concesiones. Para obtener más información, consulte Uso de restricciones de concesiones en la Guía para desarrolladores de AWS Key Management Service.

12. Elija Siguiente.
13. Revise la configuración de integración y elija Crear integración sin ETL.

    Si se produce un error en la creación, consulte the section called “Solución de problemas de integración sin ETL” para ver los pasos de solución de problemas.

La integración tiene un estado de `Creating` mientras se crea y el Amazon SageMaker Lakehouse de destino tiene un estado de `Modifying`. Durante este tiempo, no puede consultar el catálogo ni realizar ningún cambio de configuración en él.

Cuando la integración se crea correctamente, el estado de la integración y el Amazon SageMaker Lakehouse de destino cambian a `Active`.

AWS CLI

Para preparar un catálogo administrado por AWS Glue de destino para una integración sin ETL utilizando la AWS CLI, primero debe utilizar el comando create-integration-resource-property con las siguientes opciones:

- `--resource-arn`: especifique el ARN del catálogo administrado por AWS Glue que será el destino de la integración.
- `--target-processing-properties`: especifique el ARN del rol de IAM para acceder al catálogo administrado por AWS Glue de destino

```
aws glue create-integration-resource-property --region us-east-1
 --resource-arn arn:aws:glue:region:account_id:catalog/catalog_name \
 --target-processing-properties '{"RoleArn" : "arn:aws:iam::account_id:role/
TargetIamRole"}'
```

Para crear una integración sin ETL mediante un Amazon SageMaker Lakehouse, utilice la AWS CLI, use el comando create-integration con las siguientes opciones:

- `--integration-name`: especifique un nombre para la integración.
- `--source-arn`: especifique el ARN de la base de datos de RDS que será el origen de la integración.
- `--target-arn`: especifique el ARN del catálogo administrado por AWS Glue que será el destino de la integración.

Example

Para Linux, macOS o Unix:

```
aws rds create-integration \
    --integration-name my-sagemaker-integration \
    --source-arn arn:aws:rds:{region}:{account-id}:my-db \
    --target-arn arn:aws:glue:{region}:{account-id}:catalog/catalog-name
```

Para Windows:

```
aws rds create-integration ^
    --integration-name my-sagemaker-integration ^
    --source-arn arn:aws:rds:{region}:{account-id}:my-db ^
    --target-arn arn:aws:glue:{region}:{account-id}:catalog/catalog-name
```

API de RDS

Para crear una integración sin ETL con Amazon SageMaker mediante la API de Amazon RDS, utilice la operación `CreateIntegration` con los siguientes parámetros:

> **Note**
>
> Los nombres de catálogo están limitados a 19 caracteres. Asegúrese de que el parámetro IntegrationName cumpla este requisito si se va a utilizar como nombre de catálogo.

- `IntegrationName`: especifique un nombre para la integración.
- `SourceArn`: especifique el ARN de la base de datos de RDS que será el origen de la integración.
- `TargetArn`: especifique el ARN del catálogo administrado por AWS Glue que será el destino de la integración.

Cifrado de integraciones con una clave administrada por el cliente

Si especifica una clave de KMS personalizada en lugar de una Clave propiedad de AWS al crear una integración con Amazon SageMaker, la política de claves debe proporcionar a la entidad principal de servicio SageMaker Unified Studio acceso a la acción `CreateGrant`. Además, debe permitir al usuario actual realizar las acciones `DescribeKey` y `CreateGrant`.

En la siguiente política de muestra se demuestra cómo proporcionar los permisos necesarios en su política de claves. Incluye claves de contexto que sirven para reducir aún más el alcance de los permisos.

Política de claves de muestra

```
{
    "Version": "2012-10-17",
    "Id": "Key policy",
    "Statement": [
        {
            "Sid": "Enables IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{account-ID}:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allows the Glue service principal to add a grant to an AWS KMS
 key",
            "Effect": "Allow",
            "Principal": {
                "Service": "glue.amazonaws.com"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:{context-key}":"{context-value}"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "GenerateDataKey",
                        "CreateGrant"
                    ]
                }
            }
        },
        {
            "Sid": "Allows the current user or role to add a grant to a KMS key",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{account-ID}:role/{role-name}"
            },
            "Action": "kms:CreateGrant",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:{context-key}":"{context-value}",
                    "kms:ViaService": "rds.us-east-1.amazonaws.com"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "GenerateDataKey",
                        "CreateGrant"
                    ]
                }
            }
        },
        {
            "Sid": "Allows the current uer or role to retrieve information about a KMS
 key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{account-ID}:role/{role-name}"
            },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        }
    ]
}
```

Para obtener más información, consulte Creating a key policy en la Guía del desarrollador de AWS Key Management Service.

Pasos a seguir a continuación

Después de crear correctamente una integración sin ETL con Amazon SageMaker, puede comenzar a agregar datos a base de datos de RDS de destino, y consultarlos en el Amazon SageMaker Lakehouse. Los datos se replicarán automáticamente y estarán disponibles para las cargas de trabajo de análisis y machine learning.

Filtrado de datos para integraciones sin ETL de Amazon RDS

Las integraciones sin ETL de Amazon RDS admiten el filtrado de datos, lo que le permite controlar qué datos se replican desde la base de datos de Amazon RDS de origen al almacén de datos de destino. En lugar de replicar toda la base de datos, puede aplicar uno o más filtros para incluir o excluir selectivamente tablas específicas. Esto lo ayuda a optimizar el almacenamiento y el rendimiento de las consultas al garantizar que solo se transfieran los datos relevantes. Actualmente, el filtrado está limitado a los niveles de base de datos y tabla. No se admite el filtrado a nivel de columna y fila.

El filtrado de datos puede resultar útil cuando desee:

- Una determinadas tablas de dos o más bases de datos de origen diferentes y no necesita datos completos de la base de datos.
- Ahorrar costos realizando análisis utilizando únicamente un subconjunto de tablas en lugar de una flota completa de bases de datos.
- Filtrar la información confidencial (como números de teléfono, direcciones o datos de tarjetas de crédito) de determinadas tablas.

Puede agregar filtros de datos a una integración sin ETL mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de Amazon RDS.

Si la integración tiene un clúster aprovisionado como destino, el clúster debe tener la revisión 180 o uno posterior para usar el filtrado de datos.

Temas

- Formato de un filtro de datos
- Lógica de filtros
- Prioridad del filtro
- Ejemplos
- Adición de filtros de datos a una integración
- Eliminación de filtros de datos de una integración

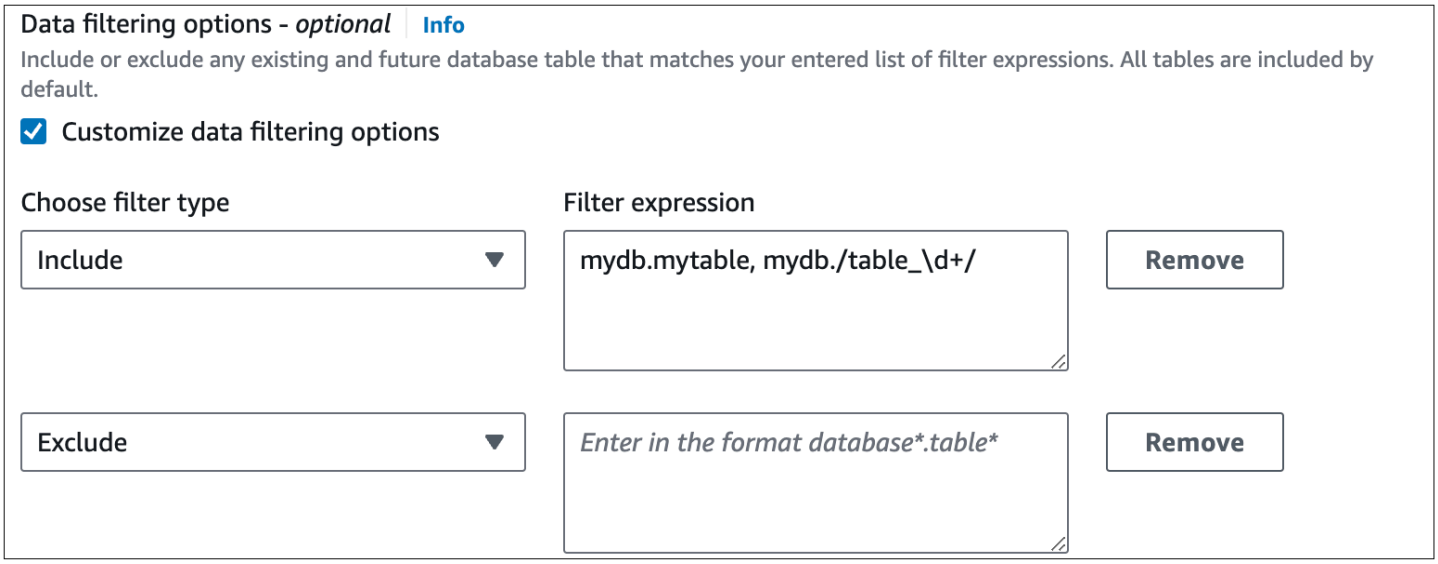
Formato de un filtro de datos

Puede definir varios filtros para una sola integración. Cada filtro incluye o excluye cualquier tabla de base de datos existente y futura que coincida con uno de los patrones de la expresión del filtro. Las integraciones sin ETL de Amazon RDS utilizan la sintaxis de filtro Maxwell para el filtrado de datos.

Cada filtro tiene los siguientes elementos:

Elemento	Descripción
Tipo de filtro	Un tipo de filtro `Include` incluye todas las tablas que coinciden con uno de los patrones de la expresión de filtro. Un tipo de filtro `Exclude` excluye todas las tablas que coinciden con uno de los patrones.
Expresión de filtro	Una lista separada por comas de patrones. Las expresiones deben usar la sintaxis de filtro Maxwell.
Patrón	Un patrón de filtro en el formato *`database`*`.`*`table`* . Puede especificar nombres literales o definir expresiones regulares. No pueden incluir filtros en columnas ni listas de denegación. Una sola integración puede tener un máximo de 99 patrones en total. En la consola, puede introducir patrones dentro de una sola expresión de filtro o distribuirlos entre varias expresiones. Un único patrón no puede superar los 256 caracteres de longitud.

En la imagen siguiente, se muestra la estructura de los filtros de datos de en la consola:



> **Important**
>
> No incluya información de identificación personal, confidencial o sensible en sus patrones de filtros.

Filtros de datos en la AWS CLI

Cuando se utiliza la AWS CLI para agregar un filtro de datos, la sintaxis es ligeramente diferente a la de la consola. Debe asignar un tipo de filtro (`Include` o `Exclude`) a cada patrón individualmente, por lo que no puede agrupar varios patrones en un mismo tipo de filtro.

Por ejemplo, en la consola puede agrupar los siguientes patrones separados por comas en una sola instrucción `Include`:

```
mydb.mytable, mydb./table_\d+/
```

Sin embargo, al utilizar la AWS CLI, el mismo filtro de datos debe tener el siguiente formato:

```
'include: mydb.mytable, include: mydb./table_\d+/'
```

Lógica de filtros

Si no especifica ningún filtro de datos en la integración, Amazon RDS asume un filtro predeterminado de `include:*.*`, que replica todas las tablas en el almacén de datos de destino. No obstante, si

agrega al menos un filtro, la lógica predeterminada cambia a `exclude:*.*`, que excluye todas las tablas de forma predeterminada. Esto le permite definir explícitamente qué bases de datos y tablas se incluirán en la replicación.

Por ejemplo, si hace lo siguiente:

```
'include: db.table1, include: db.table2'
```

Amazon RDS evalúa el filtro de la siguiente manera:

```
'exclude:*.*, include: db.table1, include: db.table2'
```

Por lo tanto, Amazon RDS solo replica `table1` y `table2` de la base de datos denominada db se replican en el almacén de datos de destino.

Prioridad del filtro

Amazon RDS evalúa los filtros de datos en el orden que especifique. En la AWS Management Console, procesa las expresiones de filtro de izquierda a derecha y de arriba abajo. Un segundo filtro o un patrón individual que siga al primero puede anularlo.

Por ejemplo, si el primer filtro es `Include books.stephenking`, solo incluye la tabla `stephenking` de la base de datos `books`. Sin embargo, si agrega un segundo filtro, `Exclude books.*`, este anulará el primer filtro. Esto evita que las tablas del índice de `books` se repliquen en el almacén de datos de destino.

Cuando especifica al menos un filtro, la lógica comienza con la suposición de `exclude:*.*` de forma predeterminada, lo que excluye automáticamente todas las tablas de la replicación. Como práctica recomendada, defina los filtros de más amplio a más específico. Comience con una o más instrucciones `Include` para especificar los datos que desea replicar; a continuación, agregue filtros `Exclude` para eliminar selectivamente ciertas tablas.

El mismo principio se aplica a los filtros que se definen mediante la AWS CLI. Amazon RDS evalúa estos patrones de filtro en el orden en que los especifique, por lo que un patrón podría anular a otro especificado antes que él.

Ejemplos

En los siguientes ejemplos, se muestra cómo funciona el filtrado de datos para las integraciones sin ETL de :

- Incluir todas las bases de datos y todas las tablas:

```
'include: *.*'
```

- Incluir todas las tablas en la base de datos `books`:

```
'include: books.*'
```

- Excluya cualquier tabla con el nombre `mystery`:

```
'include: *.*, exclude: *.mystery'
```

- Incluir dos tablas específicas en la base de datos `books`:

```
'include: books.stephen_king, include: books.carolyn_keene'
```

- Incluya todas las tablas de la base de datos `books`, excepto las que contengan la subcadena `mystery`:

```
'include: books.*, exclude: books./.*mystery.*/'
```

- Incluya todas las tablas de la base de datos `books`, excepto las que comiencen por `mystery`:

```
'include: books.*, exclude: books./mystery.*/'
```

- Incluya todas las tablas de la base de datos `books`, excepto las que finalicen por `mystery`:

```
'include: books.*, exclude: books./.*mystery/'
```

- Incluya todas las tablas de la base de datos `books` que comiencen por `table_`, excepto la que se llama `table_stephen_king`. Por ejemplo, `table_movies` o `table_books` se replicaría, pero no `table_stephen_king`.

```
'include: books./table_.*/, exclude: books.table_stephen_king'
```

Adición de filtros de datos a una integración

Puede configurar el filtrado de datos mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS.

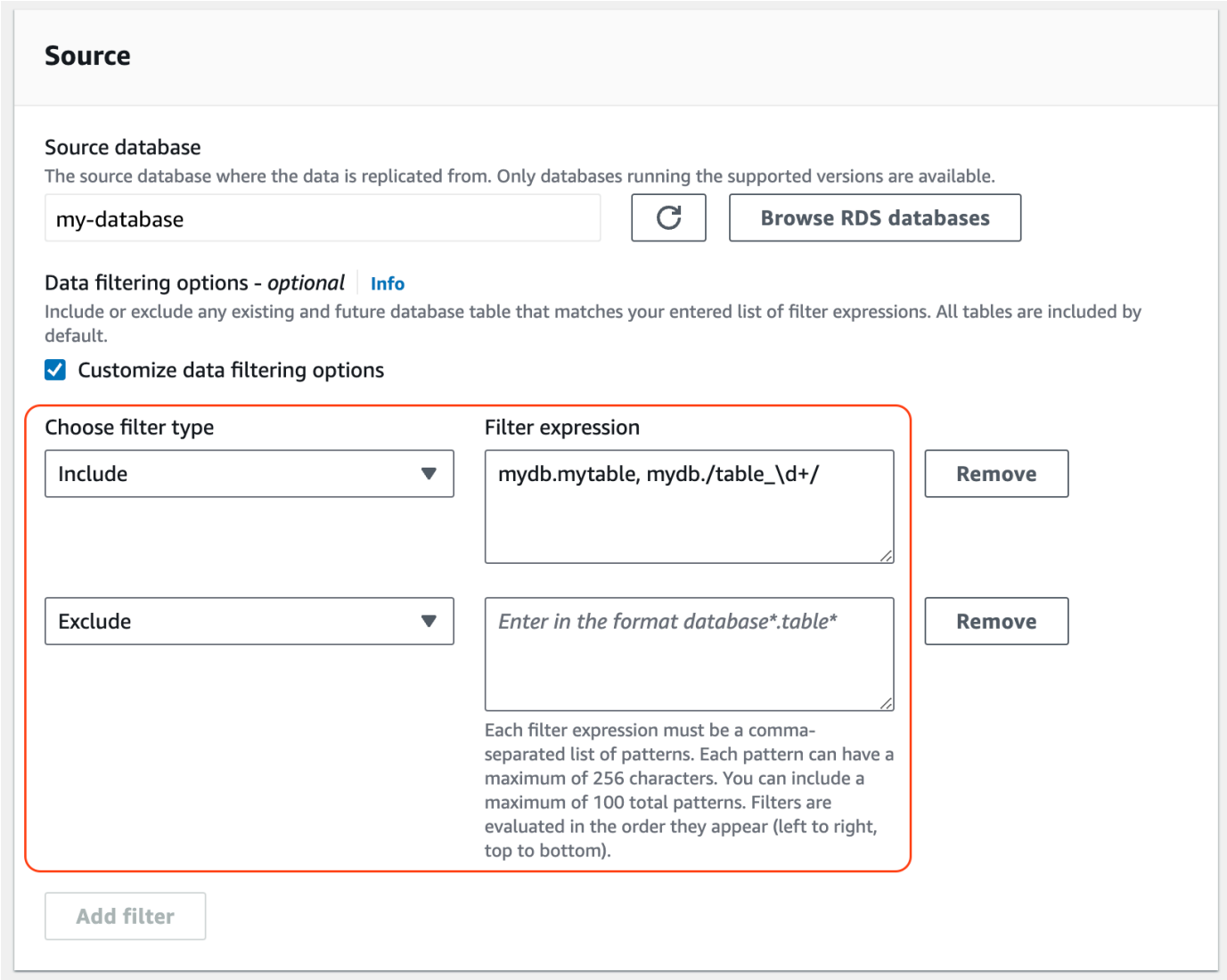
> **Important**
>
> Si agrega un filtro después de crear una integración, Amazon RDS lo trata como si hubiera existido siempre. Elimina todos los datos del almacén de datos de destino que no coincidan con los nuevos criterios de filtrado y vuelve a sincronizar todas las tablas afectadas.

Consola de RDS

Adición de filtros de datos a una integración sin ETL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Integraciones sin ETL. Seleccione la integración a la que desea agregar filtros de datos y, a continuación, elija Modificar.
3. En Origen, agregue una o más instrucciones `Include` y `Exclude`.

   En la imagen siguiente, se muestra un ejemplo de filtros de datos para una integración de MySQL:



4. Cuando esté satisfecho con los cambios, elija Continuar y Guardar cambios.

AWS CLI

Para agregar filtros de datos a una integración sin ETL mediante la AWS CLI, llame al comando modify-integration. Además del identificador de integración, especifique el parámetro `--data-filter` con una lista separada por comas de filtros `Include` y `Exclude` Maxwell.

Example

En el siguiente ejemplo, se agregan patrones de filtro a `my-integration`.

Para Linux, macOS o Unix:

```
aws rds modify-integration \
```

```
    --integration-identifier my-integration \
    --data-filter 'include: foodb.*, exclude: foodb.tbl, exclude: foodb./table_\d+/'
```

Para Windows:

```
aws rds modify-integration ^
    --integration-identifier my-integration ^
    --data-filter 'include: foodb.*, exclude: foodb.tbl, exclude: foodb./table_\d+/'
```

API de RDS

Para modificar una integración sin ETL mediante la API de RDS, llame a la operación ModifyIntegration. Especifique el identificador de integración y proporcione una lista separada por comas de patrones de filtro.

Eliminación de filtros de datos de una integración

Al eliminar un filtro de datos de una integración, Amazon RDS vuelve a evaluar los filtros restantes como si el filtro eliminado nunca hubiera existido. A continuación, replica en el almacén de datos de destino cualquier dato excluido anteriormente que ahora cumpla los criterios. Esto desencadena una nueva sincronización de todas las tablas afectadas.

Cómo agregar datos en una base de datos de RDS de origen y dirigirle consultas en Amazon Redshift

Esta es la documentación previa al lanzamiento de las integraciones sin ETL de Amazon RDS con Amazon Redshift, que se encuentra en la versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

Para terminar de crear una integración sin ETL que replique los datos de Amazon RDS en Amazon Redshift, debe crear una base de datos de destino en Amazon Redshift.

Primero, conéctese a su clúster o grupo de trabajo de Amazon Redshift y cree una base de datos con una referencia a su identificador de integración. A continuación, puede empezar a añadir datos a la base de datos de RDS de origen y ver la réplica en Amazon Redshift.

Temas

- Creación de bases de datos de destino en Amazon Redshift
- Añadir datos a la base de datos de origen
- Consulta de los datos de Amazon RDS en Amazon Redshift
- Diferencias de tipos de datos entre las bases de datos RDS y Amazon Redshift

Creación de bases de datos de destino en Amazon Redshift

Antes de empezar a replicar datos en Amazon Redshift, debe crear una base de datos de destino en su almacén de datos de destino después de crear una integración. Esta base de datos de destino debe incluir una referencia al identificador de integración. También puede utilizar la consola de Amazon Redshift o el editor de consultas v2 para crear la base de datos.

Para obtener instrucciones sobre cómo crear una base de datos de destino, consulte Creación de una base de datos de destino en Amazon Redshift.

Añadir datos a la base de datos de origen

Tras configurar la integración, puede añadir algunos datos a la base de datos de RDS que desee replicar en su almacenamiento de datos de Amazon Redshift.

> **Note**
>
> Existen diferencias entre los tipos de datos en Amazon RDS, y Amazon Redshift. Para consultar una tabla de correspondencias de tipos de datos, consulte the section called “Diferencias de tipos de datos”.

Primero, conéctese a la base de datos de origen mediante el cliente MySQL que prefiera. Para obtener instrucciones, consulte the section called “Conexión a una instancia de base de datos que ejecuta MySQL”.

A continuación, cree una tabla e inserte una fila de datos de muestra.

> **Important**
>
> Asegúrese de que la tabla tenga una clave principal. De lo contrario, no se podrá replicar en el almacenamiento de datos de destino.

En el siguiente ejemplo se usa la utilidad MySQL Workbench.

```
CREATE DATABASE my_db;

USE my_db;

CREATE TABLE books_table (ID int NOT NULL, Title VARCHAR(50) NOT NULL, Author
 VARCHAR(50) NOT NULL,
Copyright INT NOT NULL, Genre VARCHAR(50) NOT NULL, PRIMARY KEY (ID));

INSERT INTO books_table VALUES (1, 'The Shining', 'Stephen King', 1977, 'Supernatural
 fiction');
```

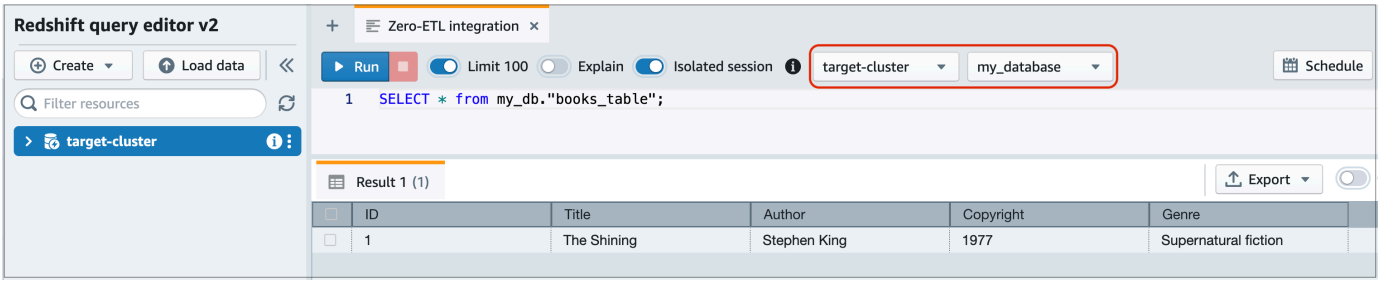
Consulta de los datos de Amazon RDS en Amazon Redshift

Después de añadir datos en la base de datos de RDS, se replican en Amazon Redshift y ya se pueden consultar.

Consulta de datos replicados

1. Vaya a la consola de Amazon Redshift y seleccione el editor de consultas v2 en el panel de navegación izquierdo.
2. Conéctese a su clúster o grupo de trabajo y elija su base de datos de destino (la que creó a partir de la integración) en el menú desplegable (destination_database en este ejemplo). Para obtener instrucciones sobre cómo crear una base de datos de destino, consulte Creación de una base de datos de destino en Amazon Redshift.
3. Utilice una instrucción SELECT para consultar los datos. En este ejemplo, puede ejecutar el siguiente comando para seleccionar todos los datos de la tabla que creó en la base de datos de RDS de origen:

   ```
   SELECT * from my_db."books_table";
   ```



- *my_db* es el nombre del esquema de la base de datos de RDS.
- *books_table* es el nombre de la tabla RDS.

También puede consultar los datos mediante un cliente de línea de comandos. Por ejemplo:

```
destination_database=# select * from my_db."books_table";

 ID |       Title |        Author |   Copyright |                 Genre |  txn_seq |
 txn_id
----+-------------+---------------+-------------+-----------------------+----------
+--------+
  1 | The Shining |  Stephen King |        1977 |   Supernatural fiction |        2 |
 12192
```

> **Note**
>
> Para distinguir entre mayúsculas y minúsculas, utilice comillas dobles (" ") para los nombres de esquemas, tablas y columnas. Para obtener más información, consulte enable_case_sensitive_identifier.

Diferencias de tipos de datos entre las bases de datos RDS y Amazon Redshift

En la siguiente tabla se muestra la asignación de un tipo de datos de RDS para MySQL a un tipo de datos de Amazon Redshift correspondiente. Actualmente, Amazon RDS solo admite estos tipos de datos para integraciones sin ETL.

Si una tabla del clúster de base de datos de origen incluye un tipo de datos no compatible, la tabla no se sincroniza y el destino de Amazon Redshift no puede utilizarla. La transmisión desde el origen

al destino continúa, pero la tabla con el tipo de datos no admitido no está disponible. Para corregir la tabla y hacer que esté disponible en Amazon Redshift, debe revertir manualmente el cambio de ruptura y, a continuación, actualizar la integración ejecutando `ALTER DATABASE...INTEGRATION REFRESH`.

RDS para MySQL

Tipo de datos de RDS para MySQL o	Tipos de datos de Amazon Redshift	Descripción	Limitaciones
INT	INTEGER	Entero firmado de cuatro bytes	
SMALLINT	SMALLINT	Entero firmado de dos bytes	
TINYINT	SMALLINT	Entero firmado de dos bytes	
MEDIUMINT	INTEGER	Entero firmado de cuatro bytes	
BIGINT	BIGINT	Entero firmado de ocho bytes	
INT UNSIGNED	BIGINT	Entero firmado de ocho bytes	
TINYINT UNSIGNED	SMALLINT	Entero firmado de dos bytes	
MEDIUMINT UNSIGNED	INTEGER	Entero firmado de cuatro bytes	
BIGINT UNSIGNED	DECIMAL(20,0)	Numérico exacto de precisión seleccionable	

Tipo de datos de RDS para MySQL o	Tipos de datos de Amazon Redshift	Descripción	Limitaciones
DECIMAL(p,s) = NUMERIC(p,s)	DECIMAL (p,s)	Numérico exacto de precisión seleccionable	No se admiten precisiones superiores a 38 ni escalas superiores a 37
DECIMAL(p,s) UNSIGNED = NUMERIC(p,s) UNSIGNED	DECIMAL (p,s)	Numérico exacto de precisión seleccionable	No se admiten precisiones superiores a 38 ni escalas superiores a 37
FLOAT4/REAL	REAL	Número en coma flotante de precisión única	
FLOAT4/REAL SIN FIRMAR	REAL	Número en coma flotante de precisión única	
DOBLE/REAL/FLOAT8	DOUBLE PRECISION	Número en coma flotante de precisión doble	
DOBLE/REAL/FLOAT8 SIN FIRMAR	DOUBLE PRECISION	Número en coma flotante de precisión doble	
BIT(n)	VARBYTE (8)	Valor binario de longitud variable	
BINARY(n)	VARBYTE(n)	Valor binario de longitud variable	
VARBINARY (n)	VARBYTE(n)	Valor binario de longitud variable	

Tipo de datos de RDS para MySQL o	Tipos de datos de Amazon Redshift	Descripción	Limitaciones
CHAR(n)	VARCHAR (n)	Valor de cadena de longitud variable	
VARCHAR (n)	VARCHAR (n)	Valor de cadena de longitud variable	
TEXT	VARCHAR(6535)	Valor de cadena de longitud variable de hasta 65535 bytes	
TINYTEXT	VARCHAR (255)	Valor de cadena de longitud variable de hasta 255 bytes	
ENUM	VARCHAR(1020)	Valor de cadena de longitud variable de hasta 1020 bytes	
SET	VARCHAR(1020)	Valor de cadena de longitud variable de hasta 1020 bytes	
FECHA	FECHA	Fecha de calendario (año, mes, día)	
DATETIME	MARCA DE TIEMPO	Fecha y hora (sin zona horaria)	

Tipo de datos de RDS para MySQL o	Tipos de datos de Amazon Redshift	Descripción	Limitaciones
TIMESTAMP(p)	MARCA DE TIEMPO	Fecha y hora (sin zona horaria)	
HORA	VARCHAR(18)	Valor de cadena de longitud variable de hasta 18 bytes	
YEAR	VARCHAR(4)	Valor de cadena de longitud variable de hasta 4 bytes	
JSON	SUPER	Datos o documento s semiestru cturados como valores	

Visualización y supervisión de las integraciones sin ETL de Amazon RDS

Puede acceder a los detalles de una integración sin ETL de Amazon RDS para ver su información de configuración y su estado actual. También puede supervisar el estado de la integración consultando vistas concretas del sistema en Amazon Redshift. Además, Amazon Redshift publica determinadas métricas relacionadas con la integración en Amazon CloudWatch, que puede ver en la consola de Amazon Redshift.

Temas

- Visualización de las integraciones
- Supervisión de las integraciones mediante tablas del sistema para Amazon Redshift
- Supervisión de las integraciones con Amazon EventBridge para Amazon Redshift

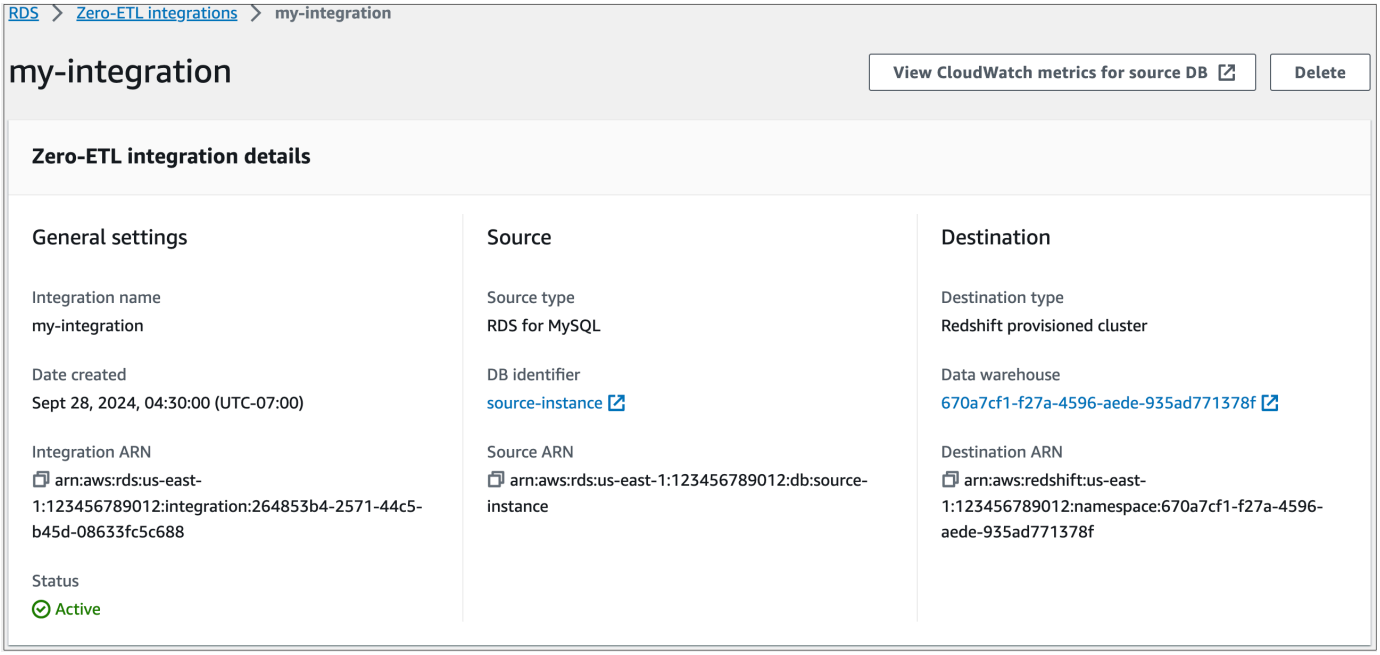
Visualización de las integraciones

Puede ver integraciones sin ETL de Amazon RDS con la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para ver los detalles de una integración sin ETL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Integraciones sin ETL en el panel de navegación izquierdo.
3. Seleccione una integración para ver más detalles sobre ella, como la base de datos de origen y el almacenamiento de datos de destino.



Una integración puede tener los siguientes estados:

- `Creating`: la integración se está creando.
- `Active`: la integración envía datos transaccionales al almacenamiento de datos de destino.
- `Syncing`: la integración detectó un error recuperable y vuelve a almacenar los datos. Las tablas afectadas no están disponibles para consultas hasta que no terminen la resincronización.

- `Needs attention`: la integración detectó un evento o error que requiere la intervención manual para su resolución. Para solucionar el problema, siga las instrucciones del mensaje de error que aparece en la página de detalles de la integración.
- `Failed`: la integración detectó un evento o error irrecuperable que no se puede corregir. Debe eliminar y volver a crear la integración.
- `Deleting`: la integración se está eliminando.

AWS CLI

Para ver todas las integraciones sin ETL de la cuenta actual mediante la AWS CLI, utilice el comando describe-integrations y especifique la opción `--integration-identifier`.

Example

Para Linux, macOS o Unix:

```
aws rds describe-integrations \
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

Para Windows:

```
aws rds describe-integrations ^
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

API de RDS

Para ver una integración sin ETL mediante la API de Amazon RDS, utilice la operación `DescribeIntegrations` con el parámetro `IntegrationIdentifier`.

Supervisión de las integraciones mediante tablas del sistema para Amazon Redshift

Amazon Redshift dispone de muchas tablas y vistas de sistema que contienen información acerca de cómo funciona el sistema. Puede consultar estas tablas y vistas de sistema de la misma forma que lo haría con cualquier otra tabla de bases de datos. Para obtener más información acerca de las vistas y tablas del sistema en Amazon Redshift, consulte la Referencia de las tablas y vistas de sistema en la Guía del desarrollador de bases de datos de Amazon Redshift.

Puede consultar las siguientes vistas y tablas del sistema para obtener información sobre las integraciones sin ETL de :

- SVV_INTEGRATION: proporciona detalles de configuración de sus integraciones.
- SVV_INTEGRATION_TABLE_STATE: describe el estado de cada tabla de una integración.
- SYS_INTEGRATION_TABLE_STATE_CHANGE: muestra los cambios de estado de las tablas de una integración.
- SYS_INTEGRATION_ACTIVITY: proporciona información sobre las ejecuciones de integración finalizadas.

Todas las métricas de Amazon CloudWatch provienen de Amazon Redshift. Para obtener información, consulte Métricas para integraciones sin ETL en la Guía de administración de Amazon Redshift. Actualmente, Amazon RDS no publica ninguna métrica relacionada con la integración en CloudWatch.

Supervisión de las integraciones con Amazon EventBridge para Amazon Redshift

Amazon Redshift envía eventos relacionados con la integración a Amazon EventBridge. Para obtener una lista de los eventos y sus correspondientes ID, consulte la sección sobre notificaciones de eventos de integración sin ETL con Amazon EventBridge en la Guía de administración de Amazon Redshift.

Modificación de las integraciones sin ETL de Amazon RDS

Solo puede modificar el nombre, la descripción y las opciones de filtrado de datos para una integración sin ETL en un almacén de datos compatible. No puede modificar la clave AWS KMS utilizada para cifrar la integración ni las bases de datos de origen o destino.

Si agrega un filtro a una integración existente, Amazon RDS volverá a evaluar el filtro como si hubiera existido siempre. Elimina cualquier dato que se encuentre actualmente en el almacén de datos de destino y que no coincida con los nuevos criterios de filtrado. Si elimina un filtro de datos de una integración, este replica todos los datos que anteriormente no coincidían con los criterios de filtrado (pero que ahora sí) en el almacenamiento de datos de destino. Para obtener más información, consulte the section called “Filtrado de datos para integraciones sin ETL”.

Puede modificar la integración sin ETL mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS.

Consola de RDS

Modificación de una integración sin ETL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Integraciones sin ETL y, a continuación, elija la integración que desee modificar.
3. Elija Modificar y modifique cualquier configuración disponible.
4. Cuando haya realizado todos los cambios que desee, elija Modificar.

AWS CLI

Para modificar una integración sin ETL utilizando la AWS CLI, llame al comando modify-integration. Junto con `--integration-identifier`, especifique cualquiera de las siguientes opciones:

- `--integration-name`: especifique un nombre nuevo para la integración.
- `--description`: especifique una descripción nueva para la integración.
- `--data-filter`: especifique las opciones de filtrado de datos para la integración. Para obtener más información, consulte the section called “Filtrado de datos para integraciones sin ETL”.

Example

La siguiente solicitud modifica una integración existente.

Para Linux, macOS o Unix:

```
aws rds modify-integration \
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374 \
    --integration-name my-renamed-integration
```

Para Windows:

```
aws rds modify-integration ^
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374 ^
```

```
    --integration-name my-renamed-integration
```

API de RDS

Para modificar una integración sin ETL mediante la API de RDS, llame a la operación ModifyIntegration. Especifique el identificador de integración y los parámetros que desee modificar.

Eliminación de las integraciones sin ETL de Amazon RDS

Al eliminar una integración sin ETL, Amazon RDS la elimina de la base de datos de origen. Los datos transaccionales no se eliminan de Amazon RDS ni del destino de los análisis, pero Amazon RDS no envía nuevos datos a Amazon Redshift o Amazon SageMaker.

Solo puede eliminar una integración si su estado es `Active`, `Failed`, `Syncing`, o `Needs attention`.

Puede eliminar las integraciones sin ETL mediante la AWS Management Console, AWS CLI o la API de RDS.

Consola

Eliminación de una integración sin ETL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Integraciones sin ETL en el panel de navegación.
3. Seleccione la integración sin ETL que desea eliminar.
4. Elija Acciones, Eliminar dominio y confirme la eliminación.

AWS CLI

Para eliminar una integración sin ETL, utilice el comando delete-integration y especifique la opción `--integration-identifier`.

Example

Para Linux, macOS o Unix:

```
aws rds delete-integration \
```

```
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

Para Windows:

```
aws rds delete-integration ^
    --integration-identifier ee605691-6c47-48e8-8622-83f99b1af374
```

API de RDS

Para eliminar una integración sin ETL mediante la API de Amazon RDS, utilice la operación `DeleteIntegration` con el parámetro `IntegrationIdentifier`.

Solución de problemas de integraciones sin ETL de Amazon RDS con Amazon Redshift

> Esta es la documentación previa al lanzamiento de las integraciones sin ETL de Amazon RDS con Amazon Redshift, que se encuentra en la versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio de AWS.

Para comprobar el estado de una integración sin ETL, consulte la tabla del sistema SVV_INTEGRATION en Amazon Redshift. Si la columna `state` tiene un valor de `ErrorState`, significa que algo está mal. Para obtener más información, consulte the section called "Monitorización mediante tablas del sistema".

Utilice la siguiente información para solucionar problemas habituales relacionados con las integraciones sin ETL de Amazon RDS con Amazon Redshift.

Temas

- No puedo crear una integración sin ETL
- Mi integración está atascada en un estado de Syncing
- Mis tablas no se replican en Amazon Redshift
- Una o más de mis tablas de Amazon Redshift requieren una resincronización

No puedo crear una integración sin ETL

Si no puede crear una integración sin ETL, asegúrese de que los siguientes elementos son correctos para su instancia de base de datos de origen:

- La base de datos de origen ejecuta RDS para MySQL versión 8.0.32 o posterior. Para validar la versión del motor, elija la pestaña Configuración de la base de datos y compruebe la versión del motor.
- Ha configurado correctamente los parámetros del de base de datos. Si los parámetros requeridos están configurados incorrectamente o no están asociados a la instancia de base de datos, se produce un error en la creación. Consulte the section called “Crear un grupo de parámetros de de base de datos personalizado”.

Además, asegúrese de que lo siguiente sea correcto para su almacenamiento de datos de destino:

- La distinción entre mayúsculas y minúsculas está activada. Consulte Turn on case sensitivity for your data warehouse.
- Ha añadido la entidad principal autorizado y el origen de integración correctos. Consulte Configuración de la autorización para el almacenamiento de datos de Amazon Redshift.
- El almacenamiento de datos está cifrado (si se trata de un clúster aprovisionado). Consulte Cifrado de la base de datos de Amazon Redshift.

Mi integración está atascada en un estado de **`Syncing`**

Es posible que su integración muestre continuamente el estado `Syncing` si cambia el valor de uno de los parámetros de base de datos necesarios.

Para solucionarlo, compruebe los valores de los parámetros del grupo de parámetros asociado a la base de datos de origen y asegúrese de que coincidan con los valores requeridos. Para obtener más información, consulte the section called “Crear un grupo de parámetros de de base de datos personalizado”.

Si modifica algún parámetro, asegúrese de reiniciar la base de datos para aplicar los cambios.

Mis tablas no se replican en Amazon Redshift

Si no ve reflejadas una o varias tablas en Amazon Redshift, puede ejecutar el siguiente comando para volver a sincronizarlas:

```
ALTER DATABASE dbname INTEGRATION REFRESH TABLES table1, table2;
```

Para obtener más información, consulte ALTER DATABASE en la Referencia de SQL de Amazon Redshift.

Es posible que los datos no se estén replicando porque una o varias de las tablas de origen no tienen una clave principal. El panel de supervisión de Amazon Redshift muestra el estado de estas tablas como `Failed` y el estado de la integración sin ETL global cambia a `Needs attention`. Para resolver este problema, puede identificar una clave existente en la tabla que pueda convertirse en clave principal o puede añadir una clave principal sintética. Para obtener soluciones detalladas, consulte Handle tables without primary keys while creating Amazon Aurora MySQL or Amazon RDS for MySQL zero-ETL integrations with Amazon Redshift.

Una o más de mis tablas de Amazon Redshift requieren una resincronización

La ejecución de algunos comandos en la instancia de base de datos de origen puede requerir que las tablas se vuelvan a sincronizar. En estos casos, la vista del sistema SVV_INTEGRATION_TABLE_STATE muestra un `table_state` de `ResyncRequired`, lo que significa que la integración debe volver a cargar por completo los datos de esa tabla de MySQL a Amazon Redshift.

Cuando la tabla comienza a resincronizarse, entra en un estado de `Syncing`. No es necesario realizar ninguna acción manual para volver a sincronizar una tabla. Mientras se vuelven a sincronizar los datos de la tabla, no puede acceder a ellos en Amazon Redshift.

A continuación se muestran algunos ejemplos de operaciones que pueden poner una tabla en estado `ResyncRequired` y las posibles alternativas que se pueden considerar.

Operación	Ejemplo	Alternativa

Añadir una columna a una posición específica	`ALTER TABLE table_name`
	`  ADD COLUMN column_name  INTEGER`
	`  NOT NULL first;`
		Amazon Redshift no admite la adición de columnas en posiciones específic

Operación	Ejemplo	Alternativa
		as mediante las palabras clave `first` o `after`. Si el orden de las columnas de la tabla de destino no es crucial, añada la columna al final de la tabla con un comando más sencillo: `ALTER TABLE table_name ADD COLUMN column_name column_type ;`

Operación	Ejemplo	Alternativa

Añadir una columna de marca temporal con la opción predeterminada `CURRENT_TIMESTAMP`	`ALTER TABLE table_name`
	`  ADD COLUMN column_name  TIMESTAMP`
	`  NOT NULL DEFAULT CURRENT_TIMESTAMP;`
		RDS para MySQL calcula el valor `CURRENT_TIMESTAMP` de las filas de la tabla existentes y no se puede simular en Amazon Redshift sin una resincronización completa de los datos de la tabla.
		
		Si es posible, cambie el valor predeterminado a una constante literal, por ejemplo, `2023-01-01 00:00:15` para evitar la latencia en la disponibilidad de la tabla.

Operación	Ejemplo	Alternativa
Realizar operaciones en varias columnas con un solo comando	`ALTER TABLE table_name ADD COLUMN column_1, RENAME COLUMN column_2 TO column_3;`	Considere la posibilidad de dividir el comando en dos operaciones distintas ADD y RENAM que no requerirá resincronización.

Amazon RDS para Db2

Amazon RDS admite instancias de base de datos que ejecutan las siguientes ediciones de IBM Db2:

- Db2 Standard Edition
- Db2 Advanced Edition

Amazon RDS admite instancias de base de datos que ejecutan las siguientes versiones de Db2:

- Db2 11.5

Para obtener más información acerca de la compatibilidad con las versiones secundarias, consulte Versiones de Db2 en Amazon RDS.

Antes de crear una instancia de base de datos, complete los pasos que se describen en la sección Configuración del entorno para Amazon RDS de esta guía del usuario. Cuando crea una instancia de base de datos con su usuario maestro, el usuario obtiene autoridad `DBADM`, con algunas limitaciones. Utilice este usuario para tareas administrativas, como crear cuentas de base de datos adicionales. No puede usar `SYSADM`, `SYSCTRL`, autoridad a nivel de instancia `SYSMAINT` ni autoridad a nivel de base de datos `SECADM`.

Puede crear lo siguiente:

- Instancias de base de datos
- Instantáneas de base de datos
- Restauraciones a un momento dado
- Copias de seguridad de almacenamiento automatizadas
- Copias de seguridad de almacenamiento manuales

Puede utilizar instancias de base de datos que ejecuten Db2 en una nube privada virtual (VPC). También puede agregar características a la instancia de base de datos de Amazon RDS para Db2 habilitando diversas opciones. Amazon RDS admite implementaciones multi-AZ para RDS para Db2 como una solución de conmutación por error de alta disponibilidad.

> **Important**
>
> Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios elevados. Puede acceder a la base de datos con clientes estándar de SQL, como IBM Db2 CLP. No obstante, no puede acceder al host directamente mediante Telnet o Secure Shell (SSH).

Temas

- Información general de Db2 en Amazon RDS
- Requisitos previos para crear una instancia de base de datos de Amazon RDS para Db2
- Varias bases de datos en una instancia de base de datos de Amazon RDS para Db2
- Conexión a la instancia de base de datos de Db2
- Protección de conexiones de instancias de bases de datos de Amazon RDS para Db2
- Administración de la instancia de base de datos de Amazon RDS para Db2
- Integración de una instancia de base de datos de Amazon RDS para Db2 con Amazon S3
- Migración de datos a Amazon RDS para Db2
- Federación de Amazon RDS para Db2
- Trabajo con las réplicas de Amazon RDS para Db2
- Opciones de instancias de base de datos de Amazon RDS para Db2
- Procedimientos almacenados externos de Amazon RDS para Db2
- Problemas conocidos y limitaciones para Amazon RDS para Db2
- Referencia de procedimientos almacenados de Amazon RDS para Db2
- Referencia de funciones definidas por el usuario de Amazon RDS para Db2
- Resolución de problemas de Amazon RDS para Db2

Información general de Db2 en Amazon RDS

Puede leer las siguientes secciones para obtener una descripción general de Db2 en Amazon RDS.

Temas

- Características de Amazon RDS para Db2

- Versiones de Db2 en Amazon RDS
- Opciones de licencias de Amazon RDS para Db2
- Amazon RDS para clases de instancia de Db2
- Roles predeterminados de Amazon RDS para Db2
- Parámetros de Amazon RDS para Db2
- Intercalación EBCDIC para bases de datos Db2 en Amazon RDS
- Zona horaria local para instancias de base de datos de Amazon RDS para Db2

Características de Amazon RDS para Db2

Amazon RDS para Db2 admite la mayoría de las características y capacidades de la base de datos IBM Db2. Algunas características pueden disponer de una compatibilidad limitada o de privilegios restringidos. Para obtener más información sobre las características de la base de datos Db2 para versiones específicas de Db2, consulte la documentación de IBM Db2.

Puede filtrar nuevas características de Amazon RDS en la página Novedades de Database. En el filtro Products (Productos), elija Amazon RDS. A continuación, puede buscar con palabras clave como **`Db2 2023`**.

> **Note**
>
> Las listas que siguen no son exhaustivas.

Temas

- Características admitidas de RDS para Db2
- Características no admitidas de RDS para Db2

Características admitidas de RDS para Db2

RDS para Db2 admite características que incluyen las características nativas de IBM Db2 y las que son fundamentales de Amazon RDS.

Características nativas de IBM Db2

RDS para Db2 admite las siguientes características de bases de datos de Db2:

- Creación de una base de datos estándar que utilice un conjunto de códigos, una intercalación, un tamaño de página y un territorio definidos por el cliente. Uso del procedimiento almacenado rdsadmin.create_database de Amazon RDS.
- Adición, eliminación o modificación de usuarios y grupos locales. Uso de los procedimientos almacenados de Amazon RDS para Concesión y revocación de privilegios.
- Creación de roles con el procedimiento almacenado rdsadmin.create_role de Amazon RDS.
- Compatibilidad para tablas estándar organizadas en filas.
- Compatibilidad para la carga de trabajo analítica para tablas organizadas en columnas.
- Capacidad para definir características de compatibilidad con Db2, como Oracle y MySQL.
- Compatibilidad con procedimientos almacenados externos basados en Java.
- Compatibilidad con el cifrado de datos en tránsito mediante SSL/TLS.
- Monitorización del estado de una base de datos (`ALIVE`, `DOWN`, `STORAGE_FULL`, `UNKNOWN` y `STANDBY_CONNECTABLE`).
- Restauración de una base de datos Linux (LE) en línea o fuera de línea proporcionada por el cliente. Uso de procedimientos almacenados de Amazon RDS para Administración de bases de datos.
- Aplicación de registros de archivo Db2 proporcionados por el cliente para mantener la base de datos sincronizada con las bases de datos Db2 autoadministradas. Uso de procedimientos almacenados de Amazon RDS para Administración de bases de datos.
- Compatibilidad para la auditoría en el nivel de instancia y de base de datos de Db2.
- Compatibilidad para la federación homogénea.
- Capacidad para cargar una tabla a partir de archivos de datos en Amazon Simple Storage Service (Amazon S3).
- Autorizaciones concedidas a usuarios, grupos o roles, tales como `CONNECT`, `SYSMON`, `ACCESSCTRL`, `DATAACCESS`, `SQLADM`, `WLMADM`, `EXPLAIN`, `LOAD` o `IMPLICIT_SCHEMA`.
- Creación de varias bases de datos.

> **Note**
>
> Una instancia de base de datos de RDS para Db2 puede contener hasta 50 bases de datos. Para obtener más información, consulte the section called “Múltiples bases de datos Db2”.

Características fundamentales de Amazon RDS

RDS para Db2 es compatible con las siguientes características fundamentales de Amazon RDS:

- Grupos de parámetros personalizados para asignar a las instancias de base de datos
- Creación, modificación y eliminación de instancias de bases de datos
- Restauración de una copia de seguridad autoadministrada de una base de datos Linux (LE) de Db2 en línea o sin conexión
- Compatibilidad con los tipos de almacenamiento gp3, io2 e io1
- Uso de AWS Managed Microsoft AD para la autenticación de Kerberos y la autorización de grupos LDAP para RDS para Db2
- Modificación de los grupos de seguridad, los puertos, los tipos de instancias, el almacenamiento, los períodos de retención de las copias de seguridad y otros ajustes de las instancias de Db2 existentes
- Protección contra eliminación para instancias de bases de datos
- Recuperación en un momento dado (PITR) entre regiones
- Uso de AWS Key Management Service (AWS KMS) para el cifrado de almacenamiento y el cifrado en reposo
- Instancias de base de datos multi-AZ con una en espera para alta disponibilidad
- Reinicios de instancias de bases de datos
- Actualizaciones de contraseñas maestras
- Restauración de instancias de bases de datos a un momento especificado
- Copia de seguridad y restauración de instancias de bases de datos mediante copias de seguridad de almacenamiento
- Inicio y detención de instancias de bases de datos
- Mantenimiento de instancias de bases de datos

Características no admitidas de RDS para Db2

RDS para Db2 no admite las siguientes funciones de bases de datos de Db2:

- Acceso a `SYSADM`, `SECADM` y `SYSMAINT` para el usuario maestro.
- Procedimientos almacenados externos escritos en C, C++ o Cobol.
- Varias instancias de bases de datos Db2 en un único host.

- Complementos GSS-API externos para la autenticación.
- Complementos externos de terceros para realizar copias de seguridad o restaurar bases de datos de Db2.
- Procesamiento masivo en paralelo (MPP) multinodo, como IBM Db2 Warehouse.
- IBM Db2 pureScale.
- Configuración manual de recuperación ante desastres de alta disponibilidad (HADR) para RDS para Db2.

> **Note**
>
> Amazon RDS admite y administra HADR para RDS para Db2 a través de réplicas. Para obtener más información, consulte Trabajo con las réplicas de Amazon RDS para Db2. RDS para Db2 admite implementaciones multi-AZ, copias de seguridad automatizadas entre regiones y replicación. Para obtener más información, consulte Habilitación de implementaciones de instancias de bases de datos multi-AZ para Amazon RDS y Replicación de las copias de seguridad automatizadas en otra Región de AWS.

- Cifrado de bases de datos nativo.
- Federación heterogénea para Informix, Sybase y Teradata. Para obtener más información, consulte the section called “Federación”.
- Recuperación en un momento dado (PITR) entre regiones para las copias de seguridad cifradas.
- Creación de rutinas no restringidas y migración de las rutinas no restringidas existentes mediante la creación de copias de seguridad y la restauración de los datos. Para obtener más información, consulte Rutinas no restringidas.
- Creación de nuevos espacios de tablas de almacenamiento no automáticos. Para obtener más información, consulte Espacios de tablas de almacenamiento no automáticos durante la migración.
- Tablas externas.

Versiones de Db2 en Amazon RDS

En el caso de Db2, los números de versión adoptan la forma major.minor.build.revision, por ejemplo, 11.5.9.0.sb00000000.r1. La implementación de nuestra versión coincide con la de Db2.

principal

El número de versión principal es tanto el entero como la primera parte fraccional del número de versión, por ejemplo, 11.5. Un cambio de versión se considera principal si el número de versión principal cambia, por ejemplo, si se pasa de la versión 11.5 a la 12.1.

secundaria

El número de versión secundaria es tanto la tercera como la cuarta parte del número de versión, por ejemplo, el 9.0 de 11.5.9.0. La tercera parte indica el modpack de Db2, por ejemplo, el 9 en 9.0. La cuarta parte indica el fixpack de Db2, por ejemplo, el 0 en 9.0. Un cambio de versión se considera secundario si el modpack de Db2 o el fixpack de Db2 cambian; por ejemplo, si se pasa de la versión 11.5.9.0 a la 11.5.9.1 o de la 11.5.9.0 a la 11.5.10.0, con excepciones para actualizar las tablas del catálogo. (Amazon RDS se ocupa de estas excepciones).

build

El número de compilación es la quinta parte del número de versión, por ejemplo, sb00000000 en 11.5.9.0.sb00000000. Un número de compilación en el que la parte numérica está compuesta exclusivamente por ceros indica que se trata de una compilación estándar. Un número de compilación en el que la parte numérica no está compuesta exclusivamente por ceros indica que se trata de una compilación especial. El número de compilación cambia si hay una corrección de seguridad o una compilación especial de una versión de Db2 existente. Un cambio en el número de compilación también indica que Amazon RDS ha aplicado automáticamente una nueva versión secundaria.

revision

El número de revisión es la sexta parte del número de versión, por ejemplo, r1 en 11.5.9.0.sb00000000.r1. Una revisión es una revisión de Amazon RDS de una versión de Db2 existente. Un cambio en el número de revisión indica que Amazon RDS ha aplicado automáticamente una nueva versión secundaria.

Temas

- Versiones secundarias de Db2 compatibles en Amazon RDS
- Versiones principales de Db2 compatibles en Amazon RDS

Versiones secundarias de Db2 compatibles en Amazon RDS

En la siguiente tabla se muestran las versiones secundarias de Db2 11.5 compatibles actualmente con Amazon RDS.

> **Note**
>
> Las fechas con solo un mes y un año son aproximadas y se actualizan con una fecha exacta cuando se conoce.

Versión del motor de base de datos	Fecha de versión de IBM	Fecha de versión de RDS	
11.5.9.0	15 de noviembre de 2023	27 de noviembre de 2023	

Puede especificar cualquier versión admitida actualmente de Db2 al crear una nueva instancia de base de datos. Puede especificar la versión principal (como Db2 11.5) y cualquier versión secundaria admitida para la versión principal especificada. Si no se especifica ninguna versión, Amazon RDS cambia de forma predeterminada a una versión admitida, normalmente la más reciente. Si se especifica una versión principal pero no una versión secundaria, Amazon RDS usa de manera predeterminada una versión reciente de la versión principal especificada. Para ver una lista de las versiones admitidas, así como de las versiones predeterminadas para instancias de bases de datos recién creadas, utilice el comando describe-db-engine-versions de la AWS Command Line Interface (AWS CLI).

Por ejemplo, para enumerar las versiones de motor compatibles con Amazon RDS para Db2, ejecute el siguiente comando de la AWS CLI. Sustituya *region* por su Región de AWS.

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
    --filters Name=engine,Values=db2-ae,db2-se \
    --query "DBEngineVersions[].{Engine:Engine, EngineVersion:EngineVersion,
 DBParameterGroupFamily:DBParameterGroupFamily}" \
    --region region
```

Para Windows:

```
aws rds describe-db-engine-versions ^
    --filters Name=engine,Values=db2-ae,db2-se ^
    --query "DBEngineVersions[].{Engine:Engine, EngineVersion:EngineVersion,
 DBParameterGroupFamily:DBParameterGroupFamily}" ^
    --region region
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
[
    {
    "Engine": "db2-ae",
    "EngineVersion": "11.5.9.0.sb00000000.r1",
    "DBParameterGroupFamily": "db2-ae-11.5"
    },
    {
    "Engine": "db2-se",
    "EngineVersion": "11.5.9.0.sb00000000.r1",
    "DBParameterGroupFamily": "db2-se-11.5"
    }
]
```

La versión predeterminada de Db2 puede variar según la Región de AWS. Para crear una instancia de base de datos con una versión secundaria concreta, especifique la versión secundaria durante la creación de la instancia de base de datos. Puede determinar la versión predeterminada de una Región de AWS para los motores de bases de datos `db2-ae` y `db2-se`ejecutando el comando `describe-db-engine-versions`. En el siguiente ejemplo, se devuelve la versión predeterminada de `db2-ae` para Este de EE. UU. (Norte de Virginia).

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
    --default-only --engine db2-ae \
    --query "DBEngineVersions[].{Engine:Engine, EngineVersion:EngineVersion,
 DBParameterGroupFamily:DBParameterGroupFamily}" \
    --region us-east-1
```

Para Windows:

```
aws rds describe-db-engine-versions ^
```

```
    --default-only --engine db2-ae ^
    --query "DBEngineVersions[].{Engine:Engine, EngineVersion:EngineVersion,
 DBParameterGroupFamily:DBParameterGroupFamily}" ^
    --region us-east-1
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
[
    {
    "Engine": "db2-ae",
    "EngineVersion": "11.5.9.0.sb00000000.r1",
    "DBParameterGroupFamily": "db2-ae-11.5"
    }
]
```

Con Amazon RDS, puede controlar cuándo se actualiza una instancia de Db2 a una nueva versión principal admitida por Amazon RDS. Puede mantener la compatibilidad con versiones específicas de Db2, probar nuevas versiones con una aplicación antes de implementarlas en producción y realizar las actualizaciones de versiones principales en el momento que le resulte más conveniente.

Cuando se habilita la actualización automática de versiones secundarias, Amazon RDS actualiza automáticamente sus instancias de bases de datos a nuevas versiones secundarias de Db2 a medida que sean compatibles con Amazon RDS. Los parches se instalan durante el periodo de mantenimiento programado. Puede modificar una instancia de base de datos para habilitar o desactivar actualizaciones automáticas de versiones secundarias.

A excepción de las versiones 11.5.9.1 y 11.5.10.0 de Db2, las actualizaciones automáticas a la nueva versión secundaria de Db2 incluyen actualizaciones automáticas a nuevas versiones y revisiones. Para las versiones 11.5.9.1 y 11.5.10.0, actualice manualmente las versiones secundarias.

Si desactiva las actualizaciones programadas automáticamente, puede actualizar manualmente a una versión secundaria admitida siguiendo el mismo procedimiento que utilizaría para una actualización de la versión principal. Para obtener información, consulte Actualización de una versión del motor de una instancia de base de datos.

Versiones principales de Db2 compatibles en Amazon RDS

Las versiones principales de RDS para Db2 están disponibles bajo soporte estándar al menos hasta el final de la vida útil de IBM (base) para la versión de IBM correspondiente. En la siguiente tabla se muestran las fechas que puede utilizar para planificar sus ciclos de prueba y actualización.

Si Amazon amplía la compatibilidad con una versión de RDS para Db2 durante más tiempo de lo previsto originalmente, esta tabla se actualizará para reflejar la fecha posterior.

Puede utilizar las siguientes fechas para planificar sus ciclos de prueba y actualización.

> **Note**
>
> Las fechas con solo un mes y un año son aproximadas y se actualizan con una fecha exacta cuando se conoce.
> Puede ver las versiones principales de las bases de datos de Db2 ejecutando el comando describe-db-major-engine-versions de la AWS CLI o mediante la operación de la API de RDS DescribeDBMajorEngineVersions.

Versión principal de Db2	Fecha de versión de IBM	Fecha de versión de RDS	Fin del soporte de IBM (edición Estándar y Avanzada)	Fin del soporte de IBM (extendido)	
Db2 11.5	27 de junio de 2019	27 de noviembre de 2023	Aún no anunciado por IBM.[1]	4 años después del fin del soporte	

[1] Para obtener la información más reciente, consulte Db2 product end-of-support dates en la documentación de IBM Db2.

Opciones de licencias de Amazon RDS para Db2

Amazon RDS para Db2 tiene dos opciones de licencias: Traiga su propia licencia (BYOL) y licencia de Db2 a través de AWS Marketplace.

Temas

- Traiga su propia licencia para Db2
- Licencia de Db2 a través de AWS Marketplace
- Cambio entre licencias de Db2

Traiga su propia licencia para Db2

En el modelo BYOL, utiliza sus licencias existentes de Db2 para desplegar bases de datos en Amazon RDS. Compruebe que tiene la licencia de base de datos de Db2 adecuada para la clase de instancia de base de datos y la edición de base de datos de Db2 que desee ejecutar. También debe seguir las políticas de IBM en cuanto a licencias de software de bases de datos de IBM en el entorno de computación en la nube.

> **Note**
>
> Las instancias de base de datos multi-AZ están en modo de espera inactivo porque la base de datos Db2 está instalada, pero no en ejecución. Las instancias en espera no son legibles, no se ejecutan ni atienden las solicitudes. Para obtener más información, consulte la información sobre licencias de IBM Db2 en el sitio web de IBM.

En este modelo, continuará utilizando su cuenta de soporte de IBM activa y se pondrá en contacto con IBM directamente para las solicitudes de servicio relacionadas con las bases de datos Db2. Si tiene una cuenta de Soporte con soporte para incidencias, puede contactar a Soporte para solucionar problemas relacionados con Amazon RDS. Amazon Web Services y IBM tienen un proceso de soporte multiproveedor para las incidencias que necesitan asistencia por parte de las dos organizaciones.

Amazon RDS admite el modelo BYOL para Db2 Standard Edition y Db2 Advanced Edition.

Temas

- ID de IBM para Traiga su propia licencia para Db2
- Adición de ID de IBM a un grupo de parámetros para instancias de base de datos de RDS para Db2
- Integración con AWS License Manager

ID de IBM para Traiga su propia licencia para Db2

En el modelo BYOL, necesita su IBM Customer ID y su IBM Site ID para crear, modificar o restaurar instancias de base de datos RDS para Db2. Debe crear un grupo de parámetros personalizado con su IBM Customer ID y su IBM Site ID antes de crear una instancia de base de datos de RDS para Db2. Para obtener más información, consulte Adición de ID de IBM a un grupo de parámetros para instancias de base de datos de RDS para Db2. Puede ejecutar varias instancias de base de datos de

RDS para Db2 con distintos IBM Customer IDs y IBM Site IDs en la misma Cuenta de AWS o Región de AWS.

> **Important**
>
> Si no podemos verificar su licencia con su IBM Customer ID y su IBM Site ID, podríamos cancelar cualquier instancia de base de datos que se ejecute con estas licencias no verificadas.

Si es un cliente nuevo de IBM Db2, primero debe comprar una licencia de software de Db2 en IBM. Tras adquirir una licencia de software de Db2, recibirá un certificado de titularidad de IBM, en el que figuran su IBM Customer ID y su IBM Site ID.

Si ya es cliente de IBM Db2, puede encontrar su IBM Customer ID y su IBM Site ID en su certificado de titularidad de IBM.

También puede encontrar su IBM Customer ID y su IBM Site ID en su cuenta de IBM Passport Advantage Online. Tras iniciar sesión, podrá ver ambos ID en la página principal o en la página de descargas de software.

Adición de ID de IBM a un grupo de parámetros para instancias de base de datos de RDS para Db2

Como no puede modificar los grupos de parámetros predeterminados, debe crear un grupo de parámetros personalizado y, a continuación, modificarlo para incluir los valores de su IBM Customer ID y su IBM Site ID. Para obtener información acerca de los grupos de parámetros, consulte Grupos de parámetros de base de datos para instancias de Amazon RDS.

> **Important**
>
> Debe crear un grupo de parámetros personalizado con su IBM Customer ID y su IBM Site ID antes de crear una instancia de base de datos de RDS para Db2.

Utilice la configuración de parámetros en la tabla siguiente.

Parámetro	Valor
`rds.ibm_customer_id`	`<your IBM Customer ID>`

Parámetro	Valor
`rds.ibm_site_id`	`<your IBM Site ID>`
`ApplyMethod`	`immediate` , `pending-reboot`

Estos parámetros son dinámicos, lo que significa que cualquier cambio en ellos se produce de forma inmediata y no es necesario reiniciar la instancia de base de datos. Si no desea que los cambios se apliquen de forma inmediata, puede configurar `ApplyMethod` como `pending-reboot` y programar estos cambios para que se realicen durante un período de mantenimiento.

Puede crear y modificar una instancia de base de datos mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS.

Consola

Para agregar su IBM Customer ID y su IBM Site ID a un grupo de parámetros

1. Cree un nuevo grupo de parámetros de base de datos. Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Modifique el grupo de parámetros que ha creado. Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

AWS CLI

Para agregar su IBM Customer ID y su IBM Site ID a un grupo de parámetros

1. Cree un grupo de parámetros personalizado ejecutando el comando create-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: un nombre para el grupo de parámetros que se está creando.
   - `--db-parameter-group-family`: la edición y la versión principal del motor de Db2. Valores válidos: `db2-se-11.5`, `db2-ae-11.5`.
   - `--description`: la descripción para este grupo de parámetros.

Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.

2. Modifique los parámetros del grupo de parámetros personalizado que creó ejecutando el comando modify-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: el nombre del grupo de parámetros creado.
   - `--parameters`: una matriz de los nombres de parámetros, valores y métodos de aplicación para la actualización del parámetro.

   Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

API de RDS

Para agregar su IBM Customer ID y su IBM Site ID a un grupo de parámetros

1. Creación de un grupo de parámetros de base de datos personalizado con la operación CreateDBParameterGroup de la API de Amazon RDS.

   Incluya los siguientes parámetros obligatorios:

   - `DBParameterGroupName`
   - `DBParameterGroupFamily`
   - `Description`

   Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.

2. Modifique los parámetros del grupo de parámetros personalizado que creó mediante la operación ModifyDBParameterGroup de la API de RDS.

   Incluya los siguientes parámetros obligatorios:

   - `DBParameterGroupName`
   - `Parameters`

Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Ahora está listo para crear una instancia de base de datos y asociar el grupo de parámetros personalizado a la instancia de base de datos. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS y Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS.

Integración con AWS License Manager

Para ayudar a monitorear el uso de licencias de RDS para Db2 en el modelo BYOL, AWS License Manager se integra con RDS para Db2. License Manager admite el seguimiento de las ediciones del motor de RDS para Db2 basadas en CPU virtuales (vCPU). También puede utilizar License Manager con AWS Organizations para administrar todas las cuentas de su organización de forma centralizada.

Para hacer un seguimiento del uso de licencias de las instancias de base de datos de RDS para Db2, debe crear licencias autoadministradas. Puede crear licencias autoadministradas mediante la AWS Management Console, la CLI de AWS License Manager y la API de AWS License Manager. O bien, puede automatizar la creación de licencias autoadministradas con plantillas AWS CloudFormation y Terraform.

Los recursos de RDS para Db2 que coinciden con el filtro de información del producto se asocian automáticamente a la configuración de la licencia autoadministrada. La detección de instancias de base de datos de RDS para Db2 puede tardar hasta 24 horas.

En la siguiente tabla, se muestran los valores disponibles para el filtro de información del producto Edición del motor de RDS para Db2.

Valor	Descripción
`db2-se`	Db2 Standard Edition
`db2-ae`	Db2 Advanced Edition

Temas

- Terminología

- Creación de una licencia autoadministrada en AWS License Manager
- Automatización de la creación de licencias autoadministradas en AWS License Manager con plantillas
- Ajustes para crear licencias autoadministradas

Terminología

En esta página se utilizan los siguientes términos al hablar de la integración de Amazon RDS con AWS License Manager.

Licencia autoadministrada

> La licencia autoadministrada es un término que se utiliza en AWS License Manager. La consola de Amazon RDS hace referencia a la licencia como una configuración de AWS License Manager. Una licencia autoadministrada incluye reglas de asignación de licencias que se basan en las condiciones de los acuerdos de su empresa. Las reglas que cree determinan el modo en que AWS procesa los comandos que consumen licencias. Cuando cree una licencia autoadministrada, trabaje en estrecha colaboración con el equipo de conformidad de su organización para revisar los acuerdos de su empresa. Para obtener más información, consulte Self-managed licenses in License Manager.

Creación de una licencia autoadministrada en AWS License Manager

Puede crear una licencia autoadministrada mediante la AWS Management Console, la CLI de AWS License Manager y la API de AWS License Manager.

> **Note**
>
> Si crea una instancia de base de datos de RDS para Db2 mediante la AWS Management Console, creará una licencia autoadministrada al introducir un nombre para la licencia. A continuación, Amazon RDS asocia la instancia de base de datos a esta licencia. (en la consola de Amazon RDS, se hace referencia a esta licencia como una configuración de AWS License Manager). Si desea crear una instancia de base de datos de RDS para Db2 mediante la CLI de AWS License Manager o la API de AWS License Manager, primero debe crear una licencia autoadministrada con los siguientes pasos. La misma situación se aplica a la restauración de una instancia de base de datos de RDS para Db2 a un momento determinado o a partir de una instantánea.

Consola

Creación de una licencia autoadministrada para realizar un seguimiento del uso de licencias de sus instancias de base de datos de RDS para Db2

1. Vaya a https://console.aws.amazon.com/license-manager/.
2. Cree una licencia autoadministrada.

   Para obtener instrucciones, consulte Create a self-managed license en la Guía del usuario de AWS License Manager.

   Agregue una regla para un RDS Product Information Filter (Filtro de información del producto de RSD) en el panel Product Information (Información del producto).

   Para obtener más información, consulte ProductInformation en la Referencia de la API de AWS License Manager.

AWS License Manager CLI

> **Note**
>
> Este procedimiento utiliza el comando de la CLI de AWS License Manager.

Para crear una licencia autoadministrada mediante la AWS CLI, ejecute el comando create-license-configuration de AWS License Manager. Utilice las opciones `--cli-input-json` o `--cli-input-yaml` para pasar las opciones al comando.

Para obtener más información, consulte the section called “Ajustes para crear licencias autoadministradas”.

El siguiente código crea una licencia autoadministrada para Db2 Standard Edition.

```
aws license-manager create-license-configuration --cli-input-json file://rds-db2-
se.json
```

El siguiente JSON es el contenido del archivo `rds-db2-se.json` utilizado en el comando anterior.

```
{
    "Name": "rds-db2-se",
```

```
    "Description": "RDS Db2 Standard Edition",
    "LicenseCountingType": "vCPU",
    "LicenseCountHardLimit": false,
    "ProductInformationList": [
        {
            "ResourceType": "RDS",
            "ProductInformationFilterList": [
                {
                    "ProductInformationFilterName": "Engine Edition",
                    "ProductInformationFilterValue": ["db2-se"],
                    "ProductInformationFilterComparator": "EQUALS"
                }
            ]
        }
    ]
}
```

Para obtener más información acerca de la información del producto, consulte Detección automatizada del inventario de recursos en la Guía del usuario de AWS License Manager.

Para obtener más información sobre el parámetro `--cli-input`, consulte Generar AWS CLIel esqueleto y los parámetros de entrada a partir de un archivo de entrada JSON o YAML en la AWS CLIGuía del usuario de

API AWS License Manager

> **Note**
>
> Este procedimiento utiliza el comando de la API de AWS License Manager.

Para crear una licencia autoadministrada, utilice la operación de la API de AWS License Manager `CreateLicenseConfiguration` con los siguientes parámetros obligatorios:

- `Name`
- `LicenseCountingType`
- `ProductInformationList`
- `ResourceType`
- `ProductInformationFilterList`
- `ProductInformationFilterName`

- `ProductInformationFilterValue`
- `ProductInformationFilterComparator`

Para obtener más información sobre los parámetros, consulte the section called “Ajustes para crear licencias autoadministradas”.

Automatización de la creación de licencias autoadministradas en AWS License Manager con plantillas

Puede automatizar la creación de licencias autoadministradas usando las plantillas AWS CloudFormation y Terraform.

La siguiente plantilla AWS CloudFormation de ejemplo crea licencias autoadministradas para Db2 Standard Edition en RDS for Db2. Para una plantilla para Db2 Advanced Edition, actualice los valores de `Name`, `Description` y `ProductInformationFilter`.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: CloudFormation template to create a License Configuration for Db2 Standard
 Edition on RDS for Db2.

Resources:
  Db2LicenseConfiguration:
    Type: "AWS::LicenseManager::LicenseConfiguration"
    Properties:
      Name: "rds-db2-se"
      Description: "Db2 Standard Edition on RDS for Db2"
      LicenseCountingType: "vCPU"
      LicenseCountHardLimit: false
      ProductInformationList:
        - ResourceType: "RDS"
          ProductInformationFilterList:
            - ProductInformationFilterName: "Engine Edition"
              ProductInformationFilterValue:
                - "db2-se"
              ProductInformationFilterComparator: "EQUALS"
```

Para obtener más información sobre el uso de AWS CloudFormation con Amazon RDS, consulte Creación de recursos de Amazon RDS con AWS CloudFormation.

La siguiente plantilla Terraform de ejemplo crea licencias autoadministradas para Db2 Standard Edition en RDS for Db2. Sustituya *`us-east-1`* por su Región de AWS. Para

una plantilla para Db2 Advanced Edition, actualice los valores de `name`, `description` y `product_information_filter`.

```
provider "aws" {
  region = "us-east-1"
}

resource "aws_licensemanager_license_configuration" "rds_db2_license_config" {
  name                     = "rds-db2-se"
  description              = "Db2 Standard Edition on RDS for Db2
  license_counting_type    = "vCPU"
  license_count_hard_limit = false

  product_information_list {
    resource_type = "RDS"

    product_information_filter {
      name       = "Engine Edition"
      comparator = "EQUALS"
      value      = ["db2-se"]
    }
  }
}
```

Para obtener más información sobre el uso de Terraform y Amazon RDS, consulte Using Terraform as an IaC tool for the Nube de AWS y Best practices for using the Terraform AWS Provider en Recomendaciones de AWS.

Ajustes para crear licencias autoadministradas

En la siguiente tabla, podrá encontrar información sobre la configuración para crear licencias autoadministradas mediante la CLI de AWS License Manager, la API de AWS License Manager, una plantilla de AWS CloudFormation y una plantilla de Terraform. El nombre del parámetro de la siguiente tabla aparece en el formato del nombre utilizado en la API de AWS License Manager y la plantilla de AWS CloudFormation.

Nombre del parámetro	Tipo de datos	Obligatorio	Descripción
Nombre	cadena	Sí	El nombre de la configuración de la licencia.
Descripción	cadena	No	La descripción de la configuración de la licencia.
LicenseCountingType	cadena	Sí	La dimensión utilizada para realizar un seguimiento del inventario de licencias . Valor válido: `vCPU`.
LicenseCountHardLimit	booleano	No	Indica si se utiliza una aplicación de licencias estricta o flexible. Si se supera el límite estricto, se bloqueará el lanzamiento de nuevas instancias.
ProductInformationList	matriz de objetos	Sí	Una lista de información del producto para la configuración de una licencia.
ResourceType	cadena	Sí	El tipo de recurso. Valor válido: `RDS`.
ProductInformationFilterList	matriz de objetos	Sí	Una lista de filtros de información del producto para la configuración de una licencia.

Nombre del parámetro	Tipo de datos	Obligatorio	Descripción
ProductInformation FilterName	cadena	Sí	El nombre del tipo de filtro que se está declarando. Valor válido: `Engine Edition`.
ProductInformation FilterValue	matriz de cadenas	Sí	Valor para filtrar. Puede especificar solo un valor. Valores válidos: `db2-se` o `db2-ae`.
ProductInformation FilterComparator	cadena	Sí	El operador lógico de `ProductInformation FilterName` . Valor válido: `EQUALS`.

Licencia de Db2 a través de AWS Marketplace

En la licencia Db2 a través del modelo AWS Marketplace, se paga una tarifa por hora para suscribirse a licencias de Db2. Este modelo le ayuda a empezar rápidamente con RDS para Db2 sin necesidad de adquirir licencias.

Para utilizar la licencia Db2 a través de AWS Marketplace, necesita una suscripción de AWS Marketplace activa para la edición de IBM Db2 concreta que quiera usar. Si aún no tiene una, suscríbase a AWS Marketplace para esa edición IBM Db2.

Amazon RDS admite la licencia de Db2 a través de AWS Marketplace para la edición estándar de IBM Db2 y la edición avanzada de IBM Db2.

Temas

- Terminología
- Pagos y facturación

- Suscripción a listados de Db2 Marketplace y registro con IBM
- Obtención de una oferta privada

Terminología

En esta página se utilizan los siguientes términos al hablar de la integración de Amazon RDS con AWS Marketplace.

Suscripción a SaaS

: En AWS Marketplace, los productos de software como servicio (SaaS), como el modelo de licencia de pago por uso, adoptan un modelo de suscripción basado en el uso. IBM, que es el vendedor de software de Db2, realiza un seguimiento de su uso y usted solo paga por lo que usa.

Oferta pública

: Las ofertas públicas le permiten adquirir productos de AWS Marketplace directamente desde la AWS Management Console.

Oferta privada

: Las ofertas privadas son un programa de compra que permite a los vendedores y compradores negociar unas condiciones del contrato de licencia del usuario final (CLUF) y unos precios personalizados para compras en AWS Marketplace.

Tarifas de Db2 Marketplace

: Las tarifas que cobra IBM por el uso de la licencia de software de Db2. Estas tarifas de servicio se calculan íntegramente a través de AWS Marketplace y aparecen en su factura de AWS, en la sección AWS Marketplace correspondiente.

Cuotas de Amazon RDS

: Las tarifas que cobra AWS por el RDS para los servicios de Db2, que no incluyen las licencias cuando se utiliza AWS Marketplace para licencias de Db2. Las tarifas se calculan a través de los servicios de Amazon RDS que se utilizan y aparecen en su factura de AWS.

Pagos y facturación

RDS para Db2 se integra con AWS Marketplace para ofrecer licencias de Db2 de pago por uso y por hora. Las tarifas de Db2 Marketplace incluyen los costos de licencia del software de Db2 y las tarifas

de Amazon RDS incluyen los costos del uso que haga de la instancia de base de datos de RDS para Db2. Para obtener más información acerca de los precios, consulte Precios de Amazon RDS para Db2.

Para cancelar las tarifas, debe eliminar cualquier instancia de base de datos de RDS para Db2. Además, puede eliminar sus suscripciones a AWS Marketplace de las licencias de Db2. Si elimina las suscripciones sin eliminar las instancias de base de datos, Amazon RDS seguirá facturándole por el uso de las instancias de base de datos. Para obtener más información, consulte the section called "Eliminación de una instancia de base de datos".

Puede ver las facturas y administrar los pagos de sus instancias de base de datos de RDS para Db2 que utilizan una licencia de Db2 a través AWS Marketplace en la consola de AWS Billing. Sus facturas incluyen dos cargos: uno por el uso de la licencia de Db2 a través de AWS Marketplace y otro por el uso de Amazon RDS. Para obtener más información, consulte Viewing your bill en la Guía de usuario de Administración de facturación y costos de AWS.

Suscripción a listados de Db2 Marketplace y registro con IBM

Para utilizar la licencia de Db2 a través de AWS Marketplace, debe utilizar la AWS Management Console para completar las dos tareas siguientes. No puede completar estas tareas a través de la AWS CLI o de la API de RDS.

> **Note**
>
> Si quiere crear sus instancias de base de datos mediante la AWS CLI o la API de RDS, primero debe completar estas dos tareas.

Temas

- Tarea 1: suscribirse a Db2 en AWS Marketplace
- Tarea 2: registre su suscripción con IBM

Tarea 1: suscribirse a Db2 en AWS Marketplace

Para utilizar la licencia de Db2 con AWS Marketplace, debe tener una suscrición a AWS Marketplace activa para Db2. Como las suscripciones están asociadas a una edición de IBM Db2 específica, debe suscribirse a Db2 en AWS Marketplace para cada edición de Db2 que desee utilizar: edición avanzada de IBM Db2, edición estándar de IBM Db2. Para obtener información sobre suscripciones

de AWS Marketplace, consulte Saas usage-based subscriptions en la AWS Marketplace Buyer Guide.

Le recomendamos que se suscriba a Db2 en AWS Marketplace antes de empezar a crear una instancia de base de datos.

Tarea 2: registre su suscripción con IBM

Tras suscribirse a Db2 en AWS Marketplace, complete el registro de su pedido de IBM desde la página de AWS Marketplace correspondiente al tipo de suscripción a Db2 que haya elegido. En la página de AWS Marketplace, elija Ver las opciones de compra y, a continuación, elija Configurar la cuenta. Puede registrarse con su cuenta de IBM existente o creando una cuenta de IBM gratuita.

Obtención de una oferta privada

Puede solicitar una oferta privada de AWS Marketplace para Db2 de IBM. Para obtener más información, consulte Private offers en la Guía del comprador de AWS Marketplace.

> **Note**
>
> Si es usted usuario de AWS Organizations y ha recibido una oferta privada que se ha enviado a sus cuentas de pagador y de afiliado, siga el procedimiento que se indica a continuación para suscribirse a Db2 directamente en cada cuenta de su organización.

Obtención de una oferta privada de Db2

1. Una vez enviada la oferta privada, conéctese a la consola de AWS Marketplace.
2. Abra el correo electrónico que contiene un enlace a una oferta privada de Db2.
3. Siga el enlace para acceder directamente a la oferta privada.

   > **Note**
   >
   > Si sigue este enlace antes de iniciar sesión en la cuenta correcta, aparecerá el error Página no encontrada (404).

4. Revise los términos y condiciones.
5. Elija Aceptar condiciones.

> **Note**
>
> Si no se acepta una oferta privada de AWS Marketplace, las tarifas de servicio de Db2 de AWS Marketplace se seguirán facturando a la tarifa por hora pública.

6. Para comprobar los detalles de la oferta, seleccione Mostrar detalles en el listado de productos.

Tras completar el procedimiento, puede crear su instancia de base de datos siguiendo los pasos que se indican en the section called “Creación de una instancia de base de datos”. En la AWS Management Console, en Licencia, asegúrese de elegir A través de AWS Marketplace.

Cambio entre licencias de Db2

Puede cambiar de entre licencias de Db2 en RDS para Db2. Por ejemplo, puede empezar con Traiga su propia licencia y, a continuación, cambiar a la licencia de Db2 a través de AWS Marketplace.

> **Important**
>
> Si desea cambiar a una licencia de Db2 a través de AWS Marketplace, asegúrese de tener una suscripción de AWS Marketplace activa para la edición de IBM Db2 que desee utilizar. Si no la tiene, primero suscríbase a Db2 en AWS Marketplace para esa edición de Db2 y, a continuación, complete el procedimiento de restauración.

Consola

Cambio entre licencias de Db2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Automated backups (Copias de seguridad automatizadas).

   Las copias de seguridad automatizadas se muestran en la pestaña Current Region (Región actual).
3. Elija la instancia de base de datos que quiere restaurar.
4. Para Actions (Acciones), elija Restore to point in time (Restaurar a un momento dado).

   Aparecerá la ventana Restore to point in time (Restaurar a un momento dado).

5. Elija Latest restorable time (Última hora de restauración) para restaurar a la última hora posible o elija Custom (Personalizar) para elegir una hora.

   Si elige Personalizar, escriba la fecha y hora en la que quiere restaurar la instancia.

   > **Note**
   >
   > Las horas se muestran en su zona horaria local, que se indica mediante una diferencia de la hora universal coordinada (UTC). Por ejemplo, UTC-5 es la hora estándar del Este/horario de verano central.

6. Para el motor de base de datos, elija la licencia de Db2 que desee utilizar.
7. En Identificador de instancias de bases de datos, escriba el nombre la instancia de bases de datos restaurada de destino. El nombre debe ser único.
8. Elija otras opciones según sea necesario, como la clase de instancia de base de datos, el almacenamiento y si quiere utilizar el escalado automático de almacenamiento.

   Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.
9. Elija Restore to point in time (Restaurar a un momento dado).

Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

AWS CLI

Para cambiar entre licencias de Db2, utilice el comando restore-db-instance-to-point-in-time. El siguiente ejemplo restaura la última versión de un momento específico, establece el motor de base de datos en IBM Db2 Advanced Edition y ajusta el modelo de licencia de Db2 a través de AWS Marketplace.

Puede especificar otras opciones. Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

Example

Para Linux, macOS o Unix:

```
aws rds restore-db-instance-to-point-in-time \
```

```
    --source-db-instance-identifier my_source_db_instance \
    --target-db-instance-identifier my_target_db_instance \
    --use-latest-restorable-time \
    --engine db2-ae \
    --license-model marketplace-license
```

Para Windows:

```
aws rds restore-db-instance-to-point-in-time ^
    --source-db-instance-identifier my_source_db_instance ^
    --target-db-instance-identifier my_target_db_instance ^
    --use-latest-restorable-time ^
    --engine db2-ae ^
    --license-model marketplace-license
```

Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

API de RDS

Para cambiar de entre licencias de Db2, llame a la operación `RestoreDBInstanceToPointInTime` de la API de Amazon RDS con los siguientes parámetros:

- `SourceDBInstanceIdentifier`
- `TargetDBInstanceIdentifier`
- `RestoreTime`
- `Engine`
- `LicenseModel`

Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Amazon RDS para clases de instancia de Db2

La capacidad de cómputo y de memoria de la instancia de base de datos se determina mediante su clase de instancia. La clase de instancia de base de datos que necesita depende de la potencia de procesamiento y de los requisitos de memoria.

Clases de instancia admitidas de RDS para Db2

Las clases de instancia admitidas de Amazon RDS para Db2 son un subconjunto de las clases de instancia de base de datos de Amazon RDS. Para ver la lista completa de las clases de instancia de Amazon RDS, consulte Clases de instancia de base de datos de .

Temas

- Clases de instancia de RDS para Db2 admitidas para Db2 Standard Edition
- Clases de instancia de RDS para Db2 admitidas para Db2 Advanced Edition

Clases de instancia de RDS para Db2 admitidas para Db2 Standard Edition

En la tabla siguiente, se muestran todas las clases de instancia compatibles con la Db2 Standard Edition de la base de datos de Db2 versión 11.5.9.0. Estas clases de instancias están disponibles para traiga su propia licencia (BYOL) y licencia de Db2 a través de AWS Marketplace.

Tipo de clase de instancia	Clase de instancia
Clases de instancia de uso general con procesadores Intel Xeon Scalable de tercera generación, almacenamiento SSD y optimización de red	db.m6idn.large–db.m6idn.8xlarge
Clases de instancia de uso general con procesadores basados en procesadores Intel Xeon Scalable de tercera generación	db.m6in.large–db.m6in.8xlarge
Clases de instancia de uso general	db.m7i.large–db.m7i.8xlarge db.m6i.large–db.m6i.8xlarge
Clases de instancia optimizada para memoria con SSD local basado en NVMe y con procesadores Intel Xeon Scalable de tercera generación	db.x2iedn.xlarge
Clases de instancia optimizada para memoria con procesadores Intel Xeon Scalable de tercera generación	db.r6idn.large–db.r6idn.4xlarge db.r6in.large–db.r6in.4xlarge
Clases de instancia optimizadas para memoria	db.r7i.large–db.r7i.8xlarge

Tipo de clase de instancia	Clase de instancia
	db.r6i.large–db.r6i.4xlarge
Clases de instancia de rendimiento con ráfagas	db.t3.small–db.t3.2xlarge

Clases de instancia de RDS para Db2 admitidas para Db2 Advanced Edition

En la tabla siguiente, se muestran todas las clases de instancia compatibles con la Db2 Advanced Edition de la base de datos de Db2 versión 11.5.9.0. Estas clases de instancias están disponibles para traiga su propia licencia (BYOL) y licencia de Db2 a través de AWS Marketplace.

Tipo de clase de instancia	Clase de instancia
Clases de instancia de uso general con procesadores Intel Xeon Scalable de tercera generación, almacenamiento SSD y optimización de red	db.m6idn.large–db.m6idn.32xlarge
Clases de instancia de uso general con procesadores basados en procesadores Intel Xeon Scalable de tercera generación	db.m6in.large–db.m6in.32xlarge
Clases de instancia de uso general	db.m6i.large–db.m7i.48xlarge db.m7i.large–db.m7i.48xlarge
Clases de instancia optimizada para memoria con SSD local basado en NVMe y con procesadores Intel Xeon Scalable de tercera generación	db.x2iedn.xlarge–db.x2iedn.32xlarge
Clases de instancia optimizada para memoria con procesadores Intel Xeon Scalable de tercera generación	db.r6idn.large–db.r6idn.32xlarge db.r6in.8xlarge–db.r6in.32xlarge
Clases de instancia optimizadas para memoria	db.r6i.large–db.r7i.48xlarge db.r7i.large–db.r7i.48xlarge

Tipo de clase de instancia	Clase de instancia
Clases de instancia de rendimiento con ráfagas	db.t3.small–db.t3.2xlarge

Roles predeterminados de Amazon RDS para Db2

RDS para Db2 añade los seis siguientes roles y se los otorga al `master_user_role` con la opción `ADMIN`. Cuando se aprovisiona la base de datos, RDS para Db2 concede `master_user_role` al usuario maestro. El usuario maestro, a su vez, puede conceder estos roles a otros usuarios, grupos o roles con instrucciones `GRANT` nativas conectándose a la base de datos.

- DBA: RDS para Db2 crea este rol vacío con autorización de `DATAACCESS`. El usuario maestro puede agregar más autorizaciones o privilegios a este rol y, a continuación, conceder el rol a otros usuarios, grupos o roles.
- DBA_RESTRICTED: RDS para Db2 crea este rol vacío. El usuario maestro puede agregar privilegios a este rol y, a continuación, conceder el rol a otros usuarios, grupos o roles.
- DEVELOPER: RDS para Db2 crea este rol vacío con autorización de `DATAACCESS`. El usuario maestro puede agregar más autorizaciones o privilegios a este rol y, a continuación, conceder el rol a otros usuarios, grupos o roles.
- ROLE_NULLID_PACKAGES: RDS para Db2 otorga privilegios de `EXECUTE` a este rol en los paquetes `ALL NULLID` que estaban enlazados a Db2 cuando se ejecutó `CREATE DATABASE`.
- ROLE_PROCEDURES: RDS para Db2 otorga privilegios `EXECUTE` a este rol en todos los procedimientos de `SYSIBM`.
- ROLE_TABLESPACES: RDS para Db2 otorga privilegios `USAGE` a los espacios de tabla creados por el comando `CREATE DATABASE`.

Parámetros de Amazon RDS para Db2

Amazon RDS para Db2 utiliza tres tipos de parámetros: parámetros de configuración del administrador de bases de datos, variables de registro y parámetros de configuración de bases de datos. Puede administrar los dos primeros tipos mediante grupos de parámetros y el último tipo mediante el procedimiento almacenado rdsadmin.update_db_param.

De manera predeterminada, una instancia de base de datos de RDS para Db2 usa un grupo de parámetros de base de datos específico de una base de datos y una instancia de base de datos

Db2. Este grupo de parámetros contiene parámetros para el motor de base de datos IBM Db2, específicamente los parámetros de configuración del administrador de bases de datos y variables de registro. Para obtener más información sobre el trabajo con grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

Los parámetros de configuración de RDS para Db2 se configuran en los valores predeterminados del motor de almacenamiento que ha seleccionado. Para obtener más información sobre los parámetros Db2, consulte Db2 database configuration parameters en la documentación de IBM Db2.

Temas

- Visualización de los parámetros en los grupos de parámetros
- Visualización de todos los parámetros con los comandos de Db2
- Modificación de los parámetros en grupos de parámetros
- Modificación de parámetros de configuración de la base de datos con comandos de Db2

Visualización de los parámetros en los grupos de parámetros

Los parámetros de configuración del administrador de bases de datos y las variables de registro se establecen en grupos de parámetros. Puede ver los parámetros de configuración del administrador de bases de datos y las variables de registro de una versión específica de Db2 mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para ver los valores de los parámetros de un grupo de parámetros de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

   Los grupos de parámetros de base de datos aparecen en una lista.
3. Seleccione el nombre del grupo de parámetros para ver su lista de parámetros.

AWS CLI

Puede ver los parámetros de configuración del administrador de bases de datos y las variables de registro de una versión de Db2 ejecutando el comando describe-engine-default-parameters. Especifique uno de los siguientes valores para la opción `--db-parameter-group-family`:

- db2-ae-11.5
- db2-se-11.5

Por ejemplo, para ver los parámetros de Db2 Standard Edition 11.5, ejecute el siguiente comando:

```
aws rds describe-engine-default-parameters --db-parameter-group-family db2-se-11.5
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
{
    "EngineDefaults": {
        "Parameters": [
            {
                "ParameterName": "agent_stack_sz",
                "ParameterValue": "1024",
                "Description": "You can use this parameter to determine the amount of
 memory that is allocated by Db2 for each agent thread stack.",
                "Source": "engine-default",
                "ApplyType": "static",
                "DataType": "integer",
                "AllowedValues": "256-32768",
                "IsModifiable": false
            },
            {
                "ParameterName": "agentpri",
                "ParameterValue": "-1",
                "Description": "This parameter controls the priority given to all
 agents and to other database manager instance processes and threads by the operating
 system scheduler. This priority determines how CPU time is allocated to the database
 manager processes, agents, and threads relative to other processes and threads running
 on the machine.",
                "Source": "engine-default",
                "ApplyType": "static",
                "DataType": "integer",
                "AllowedValues": "1-99",
                "IsModifiable": false
            },
            ...
        ]
    }
}
```

Para enumerar solo los parámetros modificables de Db2 Standard Edition 11.5, ejecute el siguiente comando.

Para Linux, macOS o Unix:

```
aws rds describe-engine-default-parameters \
    --db-parameter-group-family db2-se-11.5 \
    --query 'EngineDefaults.Parameters[?IsModifiable==`true`].
{ParameterName:ParameterName, DefaultValue:ParameterValue}'
```

Para Windows:

```
aws rds describe-engine-default-parameters ^
    --db-parameter-group-family db2-se-11.5 ^
    --query 'EngineDefaults.Parameters[?IsModifiable==`true`].
{ParameterName:ParameterName, DefaultValue:ParameterValue}'
```

API de RDS

Para ver los valores de los parámetros de un grupo de parámetros de base de datos, utilice la operación `DescribeDBParameters` con el siguiente parámetro obligatorio.

- `DBParameterGroupName`

Visualización de todos los parámetros con los comandos de Db2

Puede ver los ajustes de los parámetros de configuración del administrador de bases de datos, los parámetros de configuración de la base de datos y las variables de registro mediante los comandos de Db2.

Visualización de la configuración

1. Conexión a su base de datos Db2. En el siguiente ejemplo, sustituya *database_name*, *master_username* y *master_password* por su propia información.

   ```
   db2 "connect to database_name user master_username using master_password"
   ```

2. Busque la versión de Db2 compatible.

```
db2 "select service_level, fixpack_num from table(sysproc.env_get_inst_info()) as
 instanceinfo"
```

3. Vea los parámetros de una versión específica de Db2.

   - Para ver los parámetros de configuración del administrador de bases de datos, ejecute el siguiente comando:

     ```
     db2 "select cast(substr(name,1,24) as varchar(24)) as name, case
         when value_flags = 'NONE' then '' else value_flags end flags,
         cast(substr(value,1,64) as varchar(64)) as current_value
         from sysibmadm.dbmcfg
         order by name asc with UR"
     ```

   - Vea los parámetros de configuración del administrador de bases de datos ejecutando el siguiente comando:

     ```
     db2 "select cast(substr(name,1,24) as varchar(24)) as name, case
         when value_flags = 'NONE' then '' else value_flags end flags,
         cast(substr(value,1,64) as varchar(64)) as current_value
         from table(db_get_cfg(null)) order by name asc, member asc with UR"
     ```

   - Vea las variables de registro configuradas actualmente ejecutando el siguiente comando:

     ```
     db2 "select cast(substr(reg_var_name,1,50) as varchar(50)) as reg_var_name,
         cast(substr(reg_var_value,1,50) as varchar(50)) as reg_var_value,
         level from table(env_get_reg_variables(null))
         order by reg_var_name,member with UR"
     ```

Modificación de los parámetros en grupos de parámetros

Puede modificar los parámetros de configuración del administrador de bases de datos y las variables de registro en grupos de parámetros personalizados mediante la AWS Management Console, la AWS CLI o la API de RDS. Para obtener más información, consulte Grupos de parámetros de base de datos para instancias de Amazon RDS.

Consola

Modificación de parámetros de configuración del administrador de bases de datos y variables de registro

1. Cree un grupo de parámetros personalizado. Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Modifique los parámetros en ese grupo de parámetros personalizado. Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

AWS CLI

Modificación de parámetros de configuración del administrador de bases de datos y variables de registro

1. Cree un grupo de parámetros personalizado ejecutando el comando create-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: un nombre para el grupo de parámetros que se está creando.
   - `--db-parameter-group-family`: la edición y la versión principal del motor de Db2. Valores válidos: `db2-se-11.5`, `db2-ae-11.5`.
   - `--description`: la descripción para este grupo de parámetros.

   Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Modifique los parámetros del grupo de parámetros personalizado que creó ejecutando el comando modify-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: el nombre del grupo de parámetros creado.
   - `--parameters`: una matriz de los nombres de parámetros, valores y métodos de aplicación para la actualización del parámetro.

Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

API de RDS

Modificación de parámetros de configuración del administrador de bases de datos y variables de registro

1. Cree un grupo de parámetros de base de datos personalizado con la operación CreateDBParameterGroup.

   Incluya los siguientes parámetros obligatorios:

   - `DBParameterGroupName`
   - `DBParameterGroupFamily`
   - `Description`

   Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Modifique los parámetros del grupo de parámetros personalizado que creó mediante la operación ModifyDBParameterGroup.

   Incluya los siguientes parámetros obligatorios:

   - `DBParameterGroupName`
   - `Parameters`

   Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Modificación de parámetros de configuración de la base de datos con comandos de Db2

Puede modificar parámetros de configuración de la base de datos con comandos de Db2.

Modificación de parámetros de configuración de la base de datos

1. Conéctese a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Cambie los parámetros de configuración de la base de datos mediante una llamada al procedimiento almacenado `rdsadmin.update_db_param`. Para obtener más información, consulte rdsadmin.update_db_param.

```
db2 "call rdsadmin.update_db_param(
    'database_name',
    'parameter_to_modify',
    'changed_value')"
```

Intercalación EBCDIC para bases de datos Db2 en Amazon RDS

Amazon RDS para Db2 admite la intercalación EBCDIC para las bases de datos Db2. Solo puede especificar una secuencia de intercalación EBCDIC para una base de datos al crear la base de datos mediante el procedimiento almacenado the section called “rdsadmin.create_database” de Amazon RDS.

Al crear una instancia de base de datos de RDS para Db2 mediante la AWS Management Console, AWS CLI o la API de RDS, puede especificar un nombre de base de datos. Si especifica un nombre de base de datos, Amazon RDS crea una base de datos con la intercalación predeterminada de `SYSTEM`. Si necesita crear una base de datos con la intercalación EBCDIC, no especifique un nombre de base de datos al crear una instancia de base de datos.

La intercalación de una base de datos en RDS para Db2 se establece en el momento de la creación y es inmutable.

Para crear una base de datos Db2 con intercalación EBCDIC

1. Si no tiene una instancia de base de datos de RDS para Db2, cree una instancia de base de datos pero no especifique un nombre de base de datos. Puede crear una instancia de base de datos mediante la AWS Management Console, la AWS CLI o la API de RDS. Para obtener más información, consulte Creación de una instancia de base de datos.

2. Cree una base de datos de Db2 y establezca la opción de intercalación en un valor EBCDIC mediante una llamada al procedimiento almacenado `rdsadmin.create_database`. Para obtener más información, consulte rdsadmin.create_database.

> **Important**
>
> Después de crear una base de datos mediante el procedimiento almacenado, no puede cambiar la secuencia de intercalación. Si desea que una base de datos utilice una secuencia de intercalación diferente, elimine la base de datos mediante una llamada al procedimiento almacenado the section called “rdsadmin.drop_database”. A continuación, cree una base de datos con la secuencia de intercalación requerida.

Zona horaria local para instancias de base de datos de Amazon RDS para Db2

La zona horaria de una instancia de base de datos de Amazon RDS en la que se ejecuta Db2 se define de forma predeterminada. El valor predeterminado es la Hora Universal Coordinada (UTC). Para que coincida con la zona horaria de sus aplicaciones, en su lugar puede definir la zona horaria de su instancia de base de datos en una hora local.

La zona horaria se define al crear inicialmente la instancia de base de datos. Puede crear su instancia de base de datos utilizando la AWS Management Console, la API de RDS o la AWS CLI. Para obtener más información, consulte Creación de una instancia de base de datos.

Si su instancia de base de datos forma parte de una implementación multi-AZ, al conmutar por error, su zona horaria seguirá siendo la zona horaria local que definió.

Puede restaurar la instancia de base de datos a un punto temporal que especifique. La hora aparece en la zona horaria local. Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Definir la zona horaria local en su instancia de base de datos tiene las siguientes limitaciones:

- No puede modificar la zona horaria de una instancia de base de datos de Amazon RDS para Db2 existente.
- No puede restaurar una instantánea a partir de una instancia de base de datos de una zona horaria en una instancia de base de datos de una zona horaria diferente.

- Es recomendable que no restaure un archivo de copia de seguridad de una zona horaria en una zona horaria diferente. Si restaura un archivo de copia de seguridad de una zona horaria en otra, debe auditar las consultas y las aplicaciones para comprobar los efectos del cambio de zona horaria.

Zonas horarias disponibles

Puede utilizar los siguientes valores para el ajuste de la zona horaria.

Zona	Time zone (Zona horarioa)
África	África/Casablanca, África/El Cairo, África/Harare, África/Lagos, África/Luanda, África/Monrovia, África/Nairobi, África/Trípoli, África/Windhoek
América	América/Araguaína, América/Argentina/Buenos_Aires, América/Asunción, América/Bogotá, América/Caracas, América/Chicago, América/Chihuahua, América/Cuiaba, América/Denver, América/Detroit, América/Fortaleza, América/Godthab, América/Guatemala, América/Halifax, América/Lima, América/Los_Ángeles, América/Manaos, América/Matamoros, América/Ciudad_de_México, América/Monterrey, América/Montevideo, América/Nueva_York, América/Phoenix, América/Santiago, América/São_Paulo, América/Tijuana, América/Toronto
Asia	Asia/Amán, Asia/Asjabad, Asia/Bagdad, Asia/Bakú, Asia/Bangkok, Asia/Beirut, Asia/Calcuta, Asia/Daca, Asia/Damasco, Asia/Ereván, Asia/Hong_Kong, Asia/Irkutsk, Asia/Jerusalén, Asia/Kabul, Asia/Karachi, Asia/Katmandú, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Magadán, Asia/Manila, Asia/Mascate, Asia/Novosibirsk, Asia/Rangún, Asia/Riad, Asia/Seúl, Asia/Shanghái, Asia/Singapur, Asia/Taipéi, Asia/Teherán, Asia/Tokio, Asia/Ulán_Bator, Asia/Vladivostok, Asia/Yakarta, Asia/Yakutsk
Atlántico	Atlántico/Azores, Atlántico/Cabo_Verde
Australia	Australia/Adelaida, Australia/Brisbane, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/Lord_Howe, Australia/Perth, Australia/Sídney
Brasil	Brasil/DeNoronha, Brasil/Este

Zona	Time zone (Zona horarioa)
Canadá	Canadá/Terranova, Canadá/Saskatchewan
etc	Etc/GMT-3
Europa	Europa/Ámsterdam, Europa/Atenas, Europa/Berlín, Europa/Dublín, Europa/Helsinki, Europa/Kaliningrado, Europa/Londres, Europa/Madrid, Europa/Moscú, Europa/París, Europa/Praga, Europa/Roma, Europa/Sarajevo, Europa/Estocolmo
Pacífico	Pacífico/Apia, Pacífico/Auckland, Pacífico/Chatham, Pacífico/Fiyi, Pacífico/Guam, Pacífico/Honolulu, Pacífico/Kiritimati, Pacífico/Marquesas, Pacífico/Samoa, Pacífico/Tongatapu, Pacífico/Wake
EE. UU.	EE. UU./Alaska, EE. UU./Central, EE. UU./Indiana-Este, EE. UU./Este, EE. UU./Pacífico
UTC	UTC

Requisitos previos para crear una instancia de base de datos de Amazon RDS para Db2

Estos son los requisitos previos para crear una instancia de base de datos.

Temas

- Cuenta de administrador
- Consideraciones adicionales

Cuenta de administrador

Cuando se crea una instancia de base de datos, debe designar una cuenta de administrador para la instancia. Amazon RDS concede autoridad `DBADM` a esta cuenta de administrador de base de datos local.

La cuenta de administrador tiene las siguientes características, capacidades y limitaciones:

- Es un usuario local y no un Cuenta de AWS.
- No tiene autoridades a nivel de instancia de Db2, como `SYSADM`, `SYSMAINT` o `SYSCTRL`.
- No se puede detener ni iniciar una instancia de Db2.
- No se puede eliminar una base de datos Db2 si especificó el nombre al crear la instancia de base de datos.
- Tiene acceso completo a la base de datos Db2, incluidas las tablas y vistas del catálogo.
- Puede crear usuarios y grupos locales mediante procedimientos almacenados de Amazon RDS.
- Puede conceder y revocar autoridades y privilegios.

La cuenta de administrador puede realizar las siguientes tareas:

- Crear, modificar o eliminar instancias de base de datos.
- Crear instantáneas de bases de datos.
- Iniciar una restauración a un momento dado
- Crear copias de seguridad automatizadas de instantáneas de bases de datos.
- Crear copias de seguridad manuales de instantáneas de bases de datos.
- Utilizar otras características de Amazon RDS.

Consideraciones adicionales

Antes de crear una instancia de base de datos, tenga en cuenta lo siguiente:

- Cada instancia de base de datos de Amazon RDS para Db2 puede alojar hasta 50 bases de datos Db2. Para obtener más información, consulte Varias bases de datos en una instancia de base de datos de Amazon RDS para Db2.
- Initial database name (Nombre inicial de la base de datos)
  - Si no proporciona un nombre al crear una instancia de base de datos, Amazon RDS no crea una base de datos.
  - No proporcione un nombre de base de datos en las siguientes circunstancias:
    - Desea modificar el parámetro `db2_compatibility_vector`. Para obtener más información, consulte Establecimiento del parámetro db2_compatibility_vector.
- En el modelo traiga su propia licencia (BYOL), primero debe crear un grupo de parámetros personalizado que contenga su IBM Customer ID y su IBM Site ID. Para obtener más información, consulte Traiga su propia licencia para Db2.
- En la licencia Db2 a través del modelo AWS Marketplace, necesita una suscripción de AWS Marketplace activa para la edición de IBM Db2 concreta que quiera usar. Si aún no tiene una, suscríbase a Db2 en AWS Marketplace para la edición IBM Db2 que desee utilizar. Para obtener más información, consulte Licencia de Db2 a través de AWS Marketplace.

Varias bases de datos en una instancia de base de datos de Amazon RDS para Db2

Puede crear varias bases de datos en una única instancia de base de datos de RDS para Db2 llamando al procedimiento almacenado rdsadmin.create_database. Una única instancia de base de datos de RDS para Db2 está limitada a 50 bases de datos. Este número incluye las bases de datos en estado activado y desactivado.

> **Note**
>
> Si crea varias bases de datos en una instancia de base de datos de RDS para Db2 creada antes del 15 de noviembre de 2024, debe reiniciar la instancia de base de datos para permitir la compatibilidad con varias bases de datos.

Cuando cree bases de datos, Amazon RDS las activa de manera predeterminada. Para optimizar los recursos de memoria, puede desactivar las bases de datos que utilice con poca frecuencia y, posteriormente, activarlas cuando sea necesario. Para obtener más información, consulte the section called “Desactivación de una base de datos” y the section called “Activación de una base de datos”.

El número de bases de datos activadas en una instancia de base de datos depende de los recursos de memoria disponibles en el servidor. Los recursos de memoria se diferencian según la clase de instancia de base de datos y la cantidad de memoria configurada para la base de datos. Para obtener información acerca de las clases de instancia de base de datos, consulte the section called “Clases de instancia de base de datos”. Para obtener más información sobre cómo actualizar la memoria de una base de datos de RDS para Db2, consulte the section called “rdsadmin.update_db_param”.

Le recomendamos que elija una clase de instancia de base de datos con 2 GB de memoria para las tareas comunes de una base de datos, los requisitos del sistema operativo y otras tareas de automatización de Amazon RDS, como las copias de seguridad. Para obtener más información sobre el cambio de clase de instancias de bases de datos, consulte the section called “Modificación de una instancia de base de datos”.

Además, IBM recomienda contar con un mínimo de 1 GB de memoria para cada base de datos activa. Para obtener más información, consulte los requisitos de disco y memoria en la documentación de IBM.

Puede calcular el número máximo de bases de datos activas que puede tener una instancia de base de datos con la siguiente fórmula:

```
Active database limit = (total server memory - 2 GB) / 1 GB
```

El siguiente ejemplo muestra el número máximo de bases de datos activas para una instancia de base de datos con una clase de instancia de base de datos db.m6i.xlarge:

```
Active database limit = (total server memory - 2 GB) / 1 GB
                      = (16 GB - 2 GB) / 1 GB
                      = 14 databases
```

Si una base de datos activa se bloquea, cuando Amazon RDS la recupera vuelve a activarla. En algunos casos, como cuando se modifica una clase de instancia de base de datos a una configuración de memoria inferior, es posible que no haya suficiente memoria para activar todas las bases de datos de la instancia de base de datos. En esos casos, Amazon RDS activa las bases de datos en el orden en que se crearon.

> **Note**
>
> Las bases de datos que Amazon RDS no pueda activar por falta de memoria permanecen desactivadas.

Conexión a la instancia de base de datos de Db2

Cuando Amazon RDS haya aprovisionado su instancia de base de datos de Amazon RDS para Db2, puede usar cualquier aplicación cliente de SQL estándar para conectarse a la instancia de base de datos. Como Amazon RDS es un servicio administrado, no puede iniciar sesión como `SYSADM`, `SYSCTRL`, `SECADM` ni`SYSMAINT`.

Puede conectarse a una instancia de base de datos que ejecute el motor de base de datos IBM Db2mediante IBM Db2 CLP, IBM CLPPlus, DBeaver o IBM Db2 Data Management Console.

> **Note**
>
> La conexión a una base de datos Db2 se puede producir con errores si la instancia de base de datos de RDS para Db2 no tiene memoria suficiente. Para obtener más información, consulte the section called “Error de conexión a la base”.

Temas

- Búsqueda del punto de conexión de la instancia de base de datos de Amazon RDS para Db2
- Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 CLP
- Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM CLPPlus
- Conexión a la instancia de base de datos de Amazon RDS para Db2 con DBeaver
- Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 Data Management Console
- Consideraciones sobre grupos de seguridad con Amazon RDS para Db2

Búsqueda del punto de conexión de la instancia de base de datos de Amazon RDS para Db2

Cada instancia de base de datos de Amazon RDS contiene un punto de enlace y cada punto de enlace contiene el nombre DNS y el número de puerto para la instancia de base de datos. Para conectarse a su instancia de base de datos de Amazon RDS para Db2 con una aplicación cliente SQL, necesita el nombre de DNS y el número de puerto para la instancia de base de datos.

Puede encontrar los puntos de enlace para una instancia de base de datos mediante la AWS Management Console o la AWS CLI.

Consola

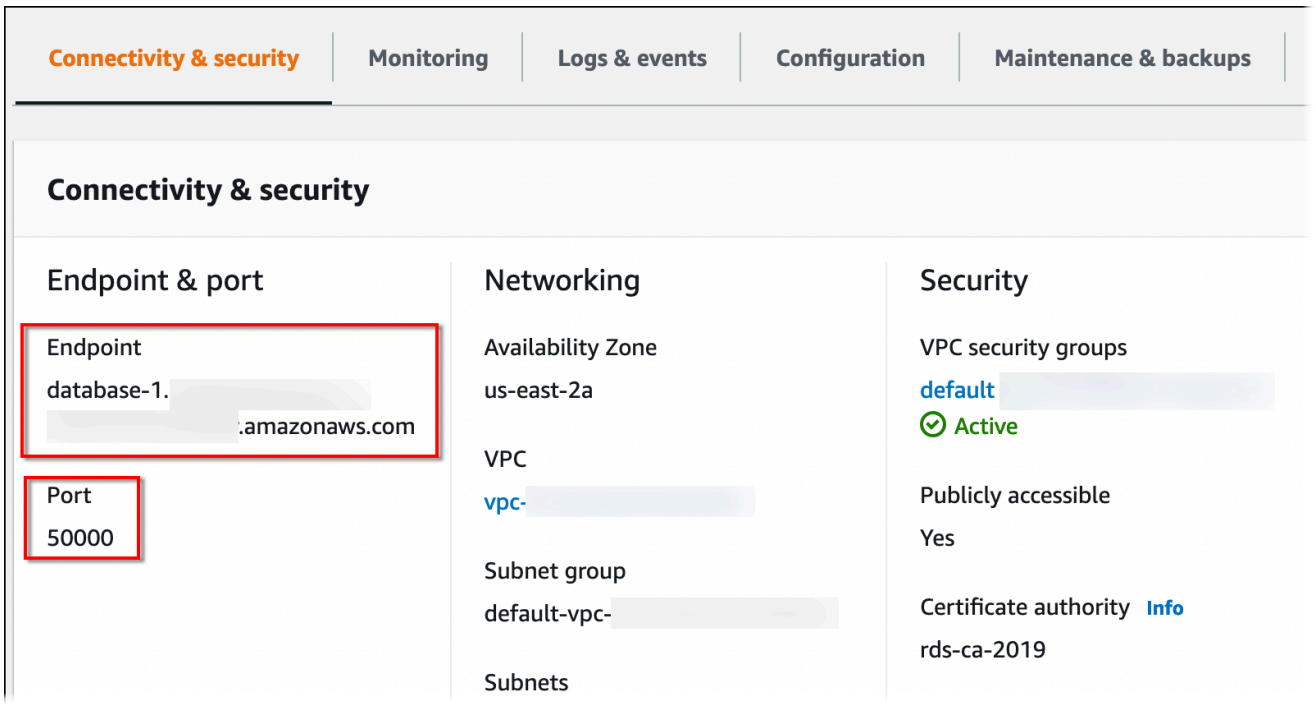
Para encontrar el punto de conexión de una instancia de base de datos de RDS para Db2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola, elija la Región de AWS de la instancia de base de datos.
3. Busque el nombre DNS y el número de puerto para su instancia de base de datos de RDS para Db2.

    a. Elija Databases (Bases de datos) para ver una lista de las instancias de base de datos.

    b. Seleccione el nombre de la instancia de base de datos de RDS para Db2 para mostrar los detalles de la instancia.

    c. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



AWS CLI

Para encontrar el punto de conexión de una instancia de base de datos de RDS para Db2, ejecute el comando describe-db-instances. En el ejemplo siguiente, sustituya *database-1* por el nombre de su instancia de base de datos.

Para Linux, macOS o:Unix

```
aws rds describe-db-instances \
    --db-instance-identifier database-1 \
    --query 'DBInstances[].
{DBInstanceIdentifier:DBInstanceIdentifier,DBName:DBName,Endpoint:Endpoint}' \
    --output json
```

En:Windows

```
aws rds describe-db-instances ^
    --db-instance-identifier database-1 ^
    --query 'DBInstances[].
{DBInstanceIdentifier:DBInstanceIdentifier,DBName:DBName,Endpoint:Endpoint}' ^
    --output json
```

El resultado de este comando debería ser similar al siguiente ejemplo. La línea `Address` en la salida contiene el nombre DNS.

```
[
    {
        "DBInstanceIdentifier": "database-1",
        "DBName": "DB2DB",
        "Endpoint": {
            "Address": "database-1.123456789012.us-east-2.amazonaws.com",
            "Port": 50000,
            "HostedZoneId": "Z2OC4A7DETW6VH"
        }
    }
]
```

Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 CLP

Puede utilizar una utilidad de línea de comandos como IBM Db2 CLP para conectarse a instancias de base de datos de Amazon RDS para Db2. Esta utilidad forma parte de IBM Data Server Runtime Client. Para descargar el cliente desde IBM Fix Central, consulte IBM Data Server Client Packages Version 11.5 Mod 8 Fix Pack 0 en el servicio de soporte de IBM.

Temas

- Terminología
- Instalación del cliente
- Conexión a una instancia de base de datos
- Solución de problemas de conexiones a la instancia de base de datos de RDS para Db2

Terminología

Los siguientes términos ayudan a explicar los comandos que se utilizan al conectarse a la instancia de base de datos de RDS para Db2.

catalog tcpip node

> Este comando registra un nodo de base de datos remoto con un cliente Db2 local, lo que hace que la aplicación cliente pueda acceder al nodo. Para catalogar un nodo, debe proporcionar información como el nombre de host del servidor, el número de puerto y el protocolo de comunicación. A partir de ahí, el nodo catalogado representa un servidor de destino en el que residen una o más bases de datos remotas. Para obtener más información, consulte Comando CATALOG TCPIP/TCPIP4/TCPIP6 NODE en la documentación de IBM Db2.

catalog database

> Este comando registra una base de datos remota con un cliente Db2 local, lo que hace que la aplicación cliente pueda acceder a la base de datos. Para catalogar una base de datos, debe proporcionar información como el alias de la base de datos, el nodo en el que reside y el tipo de autenticación necesario para conectarse a la base de datos. Para obtener más información, consulte Comando CATALOG DATABASE en la documentación de IBM Db2.

Instalación del cliente

Después de downloading the package for Linux, instale el cliente con privilegios de administrador o raíz.

> **Note**
>
> Para instalar el cliente en AIX o Windows, siga el mismo procedimiento pero modifique los comandos para su sistema operativo.

Para instalar el cliente en Linux

1. Ejecute **`./db2_install -f sysreq`** y elija **`yes`** para aceptar la licencia.
2. Elija la ubicación para instalar el cliente.
3. Ejecute **`clientInstallDir/instance/db2icrt -s client`** ***`instance_name`***. Sustituya *`instance_name`* por un usuario de sistema operativo válido en Linux. En Linux, el nombre de la instancia de base de datos de Db2 está vinculado al nombre de usuario del sistema operativo.

   Este comando crea un directorio **`sqllib`** en el directorio principal del usuario designado en Linux.

Conexión a una instancia de base de datos

Para conectarse a una instancia de base de datos de RDS para Db2, necesita su nombre DNS y el número de puerto. Para obtener información sobre cómo encontrarlos, consulte Búsqueda del punto de conexión. También debe conocer el nombre de la base de datos, el nombre de usuario maestro y la contraseña maestra que definió al crear la instancia de base de datos de RDS para Db2. Para obtener más información sobre cómo encontrarlos, consulte Creación de una instancia de base de datos.

Para conectarse a una instancia de base de datos de RDS para Db2 con IBM Db2 CLP

1. Inicie sesión con el nombre de usuario que especificó durante la instalación del cliente IBM Db2 CLP.
2. Catalogue su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`node_name`*, *`dns_name`* y *`port`* por el nombre del nodo del catálogo local, el nombre de DNS de la instancia de base de datos y el número de puerto.

   ```
   db2 catalog TCPIP node node_name remote dns_name server port
   ```

   Ejemplo

```
db2 catalog TCPIP node remnode remote database-1.123456789012.us-
east-1.amazonaws.com server 50000
```

3. Catalogación de la base de datos `rdsadmin` y su base de datos. Esto le permitirá conectarse a la base de datos `rdsadmin` para realizar algunas tareas administrativas mediante los procedimientos almacenados de Amazon RDS. Para obtener más información, consulte Administración de la instancia de base de datos de RDS para Db2.

   En el siguiente ejemplo, sustituya *`database_alias`*, *`node_name`* y *`database_name`* por los alias de esta base de datos, el nombre del nodo definido en el paso anterior y el nombre de la base de datos. `server_encrypt` cifra el nombre de usuario y la contraseña a través de la red.

```
db2 catalog database rdsadmin [ as database_alias ] at node node_name
 authentication server_encrypt

db2 catalog database database_name [ as database_alias ] at node node_name
 authentication server_encrypt
```

   Ejemplo

```
db2 catalog database rdsadmin at node remnode authentication server_encrypt

db2 catalog database testdb as rdsdb2 at node remnode authentication server_encrypt
```

4. Conexión a su base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`rds_database_alias`*, *`master_username`* y *`master_password`* por el nombre de la base de datos, el nombre de usuario maestro y la contraseña maestra de su instancia de base de datos de RDS para Db2.

```
db2 connect to rds_database_alias user master_username using master_password
```

   El resultado de este comando debería ser similar al siguiente ejemplo:

```
Database Connection Information

    Database server        = DB2/LINUXX8664 11.5.9.0
    SQL authorization ID   = ADMIN
    Local database alias   = TESTDB
```

5. Ejecución de consultas y visualización de resultados. El siguiente ejemplo muestra una instrucción SQL que selecciona la base de datos que ha creado.

```
db2 "select current server from sysibm.dual"
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
1
    ------------------
    TESTDB

    1 record(s) selected.
```

Solución de problemas de conexiones a la instancia de base de datos de RDS para Db2

Si recibe el siguiente error `NULLID`, eso normalmente indica que las versiones del cliente y del servidor de RDS para Db2 no coinciden. Para ver las versiones del cliente de Db2 compatibles, consulte Combinaciones compatibles de clientes, controladores y niveles de servidor en la documentación de IBM Db2.

```
db2 "select * from syscat.tables"
SQL0805N Package "NULLID.SQLC2O29 0X4141414141454A69" was not found.
SQLSTATE=51002
```

Tras recibir este error, debe vincular los paquetes de su antiguo cliente de Db2 a una versión de servidor de Db2 compatible con RDS para Db2.

Para vincular paquetes de un cliente de Db2 anterior a un servidor de Db2 más reciente

1. Localice los archivos de la vinculación en la máquina cliente. Normalmente, estos archivos se encuentran en el directorio bnd de la ruta de instalación del cliente de Db2 y tienen la extensión .bnd.
2. Conexión al servidor Db2. En el ejemplo siguiente, sustituya *database_name* por el nombre de su servidor Db2. Sustituya *master_username* y *master_password* por su información. Este usuario tiene autoridad `DBADM`.

```
db2 connect to database_name user master_username using master_password
```

3. Ejecute el comando `bind` para vincular los paquetes.

   a. Navegue hasta el directorio donde se encuentran los archivos de vinculación en la máquina cliente.

   b. Ejecute el comando `bind` para cada archivo.

      Se requieren las siguientes opciones:

      - `blocking all`: vincula todos los paquetes del archivo de vinculación en una sola solicitud de base de datos.
      - `grant public`: otorga permiso a `public` para ejecutar el paquete.
      - `sqlerror continue`: especifica que el proceso `bind` continúa incluso si se producen errores.

      Para obtener más información sobre el comando `bind`, consulte Comando BIND en la documentación de IBM Db2.

4. Compruebe que la vinculación se ha realizado correctamente consultando la vista del catálogo `syscat.package` o comprobando el mensaje devuelto tras el comando `bind`.

Para obtener más información, consulte DB2 v11.5 Bind File and Package Name List en el servicio de soporte de IBM.

Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM CLPPlus

Puede utilizar una utilidad como IBM CLPPlus para conectarse a una instancia de base de datos de Amazon RDS para Db2. Esta utilidad forma parte de IBM Data Server Runtime Client. Para descargar el cliente desde IBM Fix Central, consulte IBM Data Server Client Packages Version 11.5 Mod 8 Fix Pack 0 en el servicio de soporte de IBM.

> **Important**
>
> Le recomendamos que ejecute IBM CLPPlus en un sistema operativo que admita interfaces gráficas de usuario como macOS, Windows o Linux con un equipo de sobremesa. Si ejecuta Linux headless, utilice el switch -nw con comandos CLPPlus.

Temas

- Instalación del cliente
- Conexión a una instancia de base de datos

Instalación del cliente

Tras descargar el paquete para Linux, instale el cliente.

> **Note**
>
> Para instalar el cliente en AIX o Windows, siga el mismo procedimiento pero modifique los comandos para su sistema operativo.

Para instalar el cliente en Linux

1. Ejecute **`./db2_install`**.
2. Ejecute **`clientInstallDir/instance/db2icrt -s client`** ***`instance_name`***. Sustituya *`instance_name`* por un usuario de sistema operativo válido en Linux. En Linux, el nombre de la instancia de base de datos de Db2 está vinculado al nombre de usuario del sistema operativo.

   Este comando crea un directorio **`sqllib`** en el directorio principal del usuario designado en Linux.

Conexión a una instancia de base de datos

Para conectarse a una instancia de base de datos de RDS para Db2, necesita su nombre DNS y el número de puerto. Para obtener información sobre cómo encontrarlos, consulte Búsqueda del punto de conexión. También debe conocer el nombre de la base de datos, el nombre de usuario maestro

y la contraseña maestra que definió al crear la instancia de base de datos de RDS para Db2. Para obtener más información sobre cómo encontrarlos, consulte Creación de una instancia de base de datos.

Para conectarse a una instancia de base de datos de RDS para Db2 con IBM CLPPlus

1. Revise la sintaxis del comando. En el siguiente ejemplo, sustituya *clientDir* por la ubicación en la que está instalado el cliente.

```
cd clientDir/bin
    ./clpplus -h
```

2. Configure su servidor Db2. En el siguiente ejemplo, sustituya *dsn_name*, *database_name*, *endpoint* y *port* por el nombre de DSN, el nombre de la base de datos, el punto de conexión y el puerto de su instancia de base de datos de RDS para Db2. Para obtener más información, consulte Búsqueda del punto de conexión de la instancia de base de datos de Amazon RDS para Db2.

```
db2cli writecfg add -dsn dsn_name -database database_name -host endpoint -port port
 -parameter "Authentication=SERVER_ENCRYPT"
```

3. Conéctese a una instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *master_username* y *dsn_name* por el nombre de usuario maestro y el nombre de DSN.

```
./clpplus -nw master_username@dsn_name
```

4. Se abrirá una ventana de Java Shell. Introduzca la contraseña maestra para su instancia de base de datos de RDS para Db2.

> **Note**
>
> Si no se abre una ventana Java Shell, ejecute **`./clpplus -nw`** para usar la misma ventana de línea de comandos.

```
Enter password: *********
```

Se realizará una conexión y se producirá un resultado similar al del siguiente ejemplo:

```
Database Connection Information :
---------------------------------
Hostname = database-1.abcdefghij.us-east-1.rds.amazonaws.com
Database server = DB2/LINUXX8664  SQL110590
SQL authorization ID = admin
Local database alias = DB2DB
Port = 50000
```

5. Ejecución de consultas y visualización de resultados. El siguiente ejemplo muestra una instrucción SQL que selecciona la base de datos que ha creado.

```
SQL > select current server from sysibm.dual;
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
1
    --------------------
    DB2DB
    SQL>
```

Conexión a la instancia de base de datos de Amazon RDS para Db2 con DBeaver

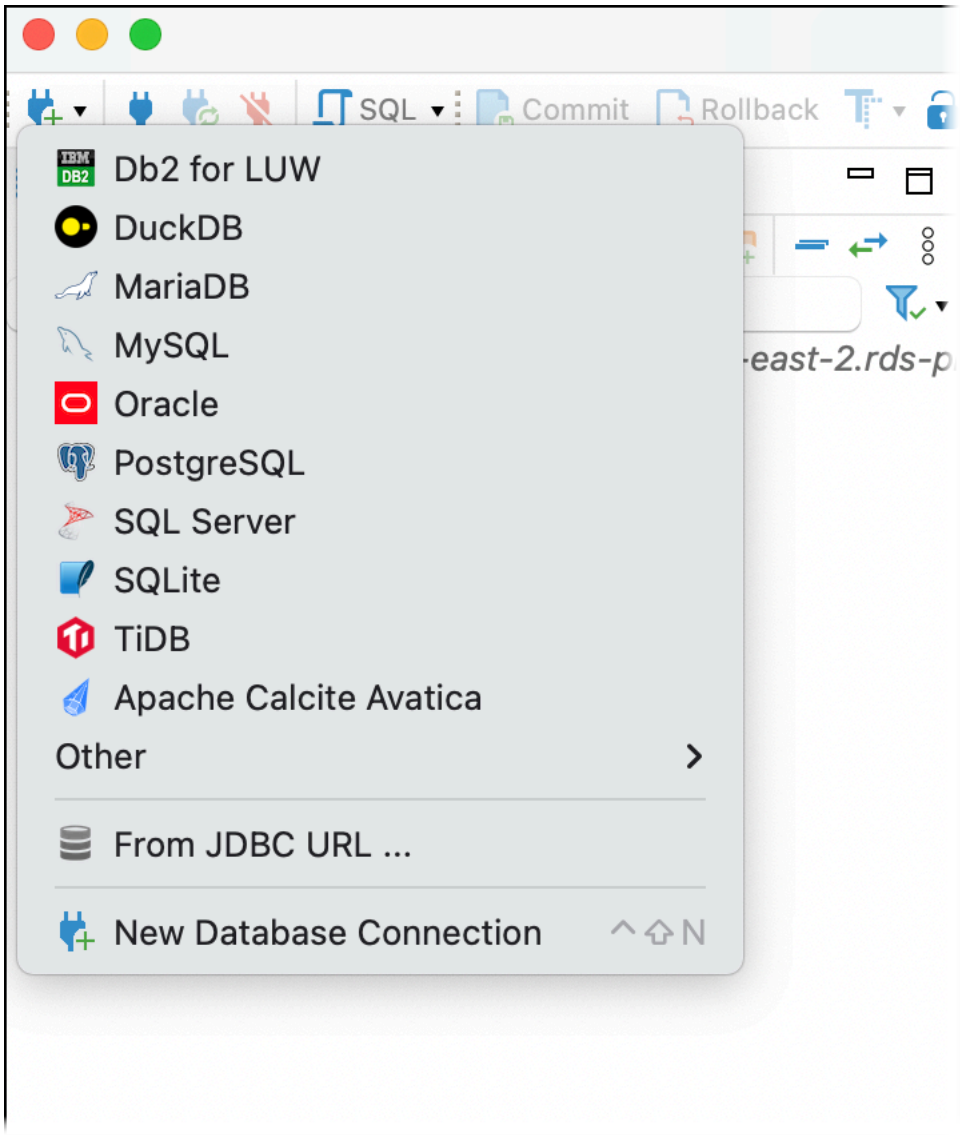
Puede utilizar herramientas de terceros, por ejemplo, DBeaver, para conectarse a instancias de base de datos de Amazon RDS para Db2. Para descargar esta utilidad, consulte Comunidad DBeaver.

Para conectarse a una instancia de base de datos de RDS para Db2, necesita su nombre DNS y el número de puerto. Para obtener información sobre cómo encontrarlos, consulte Búsqueda del punto de conexión. También debe conocer el nombre de la base de datos, el nombre de usuario maestro y la contraseña maestra que definió al crear la instancia de base de datos de RDS para Db2. Para obtener más información sobre cómo encontrarlos, consulte Creación de una instancia de base de datos.

Para conectarse a una instancia de base de datos de RDS para Db2 con DBeaver

1. Inicie DBeaver.

2. Elija el icono de Nueva conexión en la barra de herramientas y, a continuación, elija Db2 para LUW.



3. En la ventana Conexión a una base de datos, proporcione información sobre su instancia de base de datos de RDS para Db2.

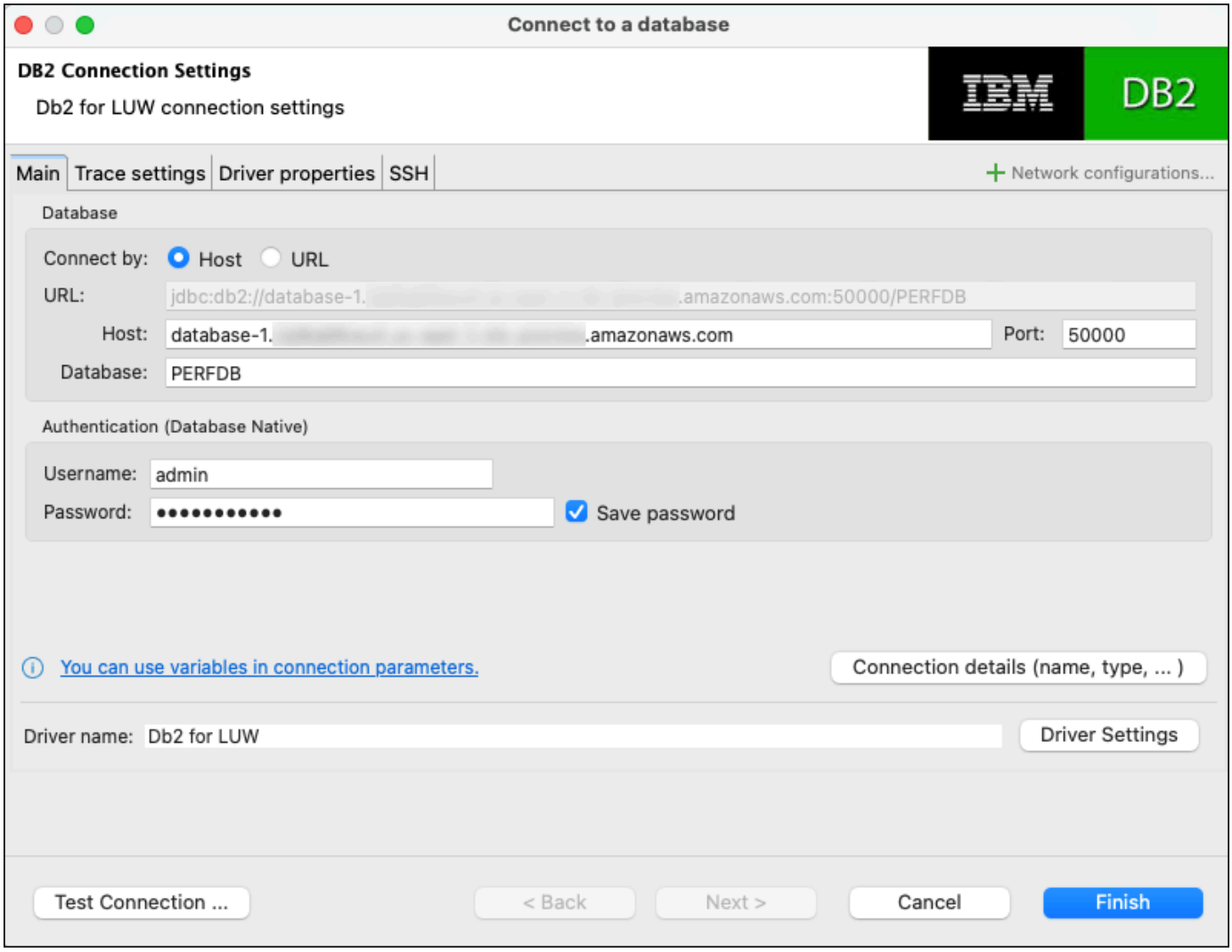
   a. Introduzca la información siguiente:

      - En Nombre del host, escriba el nombre DNS de la instancia de base de datos.
      - En Puerto, escriba el número de puerto de la instancia de base de datos.
      - En Base de datos, escriba el nombre de la base de datos.
      - En Username (Nombre de usuario), escriba el nombre del administrador de base de datos para la instancia de base de datos.

- En Contraseña, escriba la contraseña del administrador de base de datos para la instancia de base de datos.

b. Seleccione Guardar contraseña.

c. Seleccione Configuración del controlador.



4. En la ventana Editar controlador, especifique propiedades de seguridad adicionales.

a. Seleccione la pestaña Propiedades del controlador.

b. Agregue dos Propiedades de usuario.

i. Abra el menú contextual (con el botón derecho del ratón) y, a continuación, seleccione Agregar nueva propiedad.

ii. En Nombre de la propiedad, ponga encryptionAlgorithm y seleccione Aceptar.

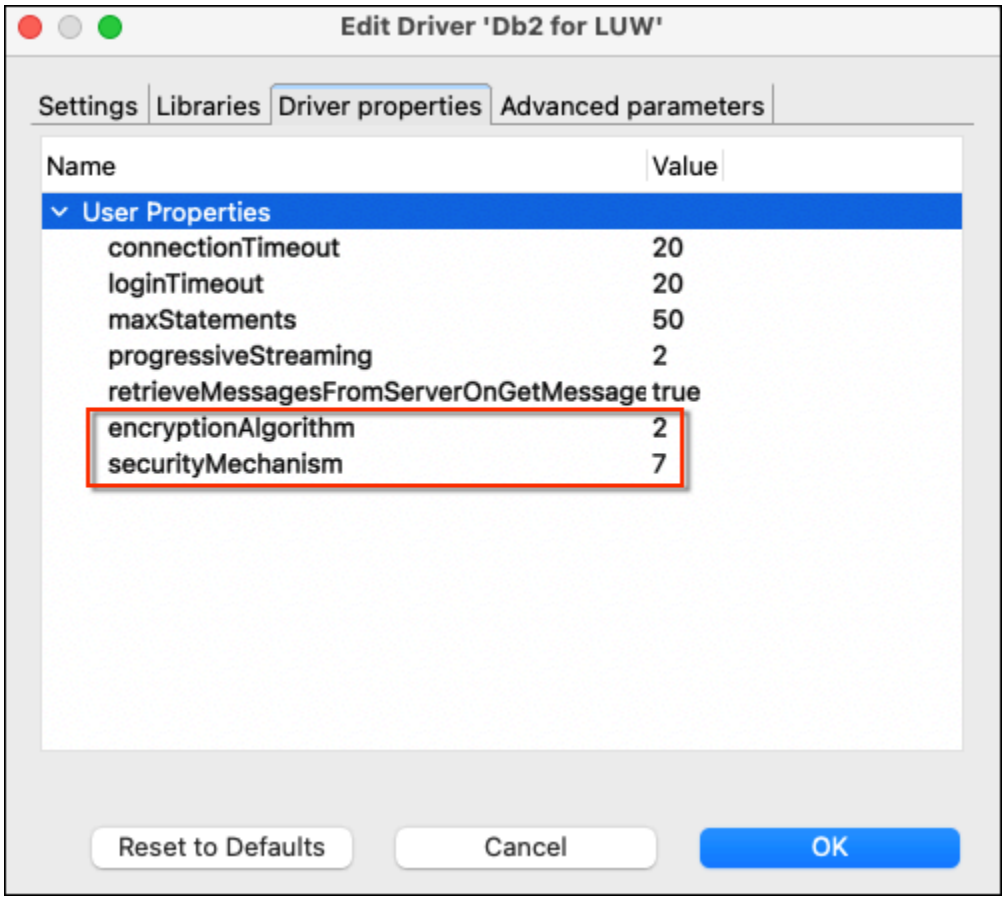
iii. Con la fila encryptionAlgorithm seleccionada, elija la columna Valor y añada 2.

iv. Abra el menú contextual (con el botón derecho del ratón) y, a continuación, seleccione Agregar nueva propiedad.

v. En Nombre de propiedad, ponga securityMechanism y seleccione Aceptar.

vi. Con la fila securityMechanism seleccionada, elija la columna Valor y añada 7.

c. Seleccione Aceptar.

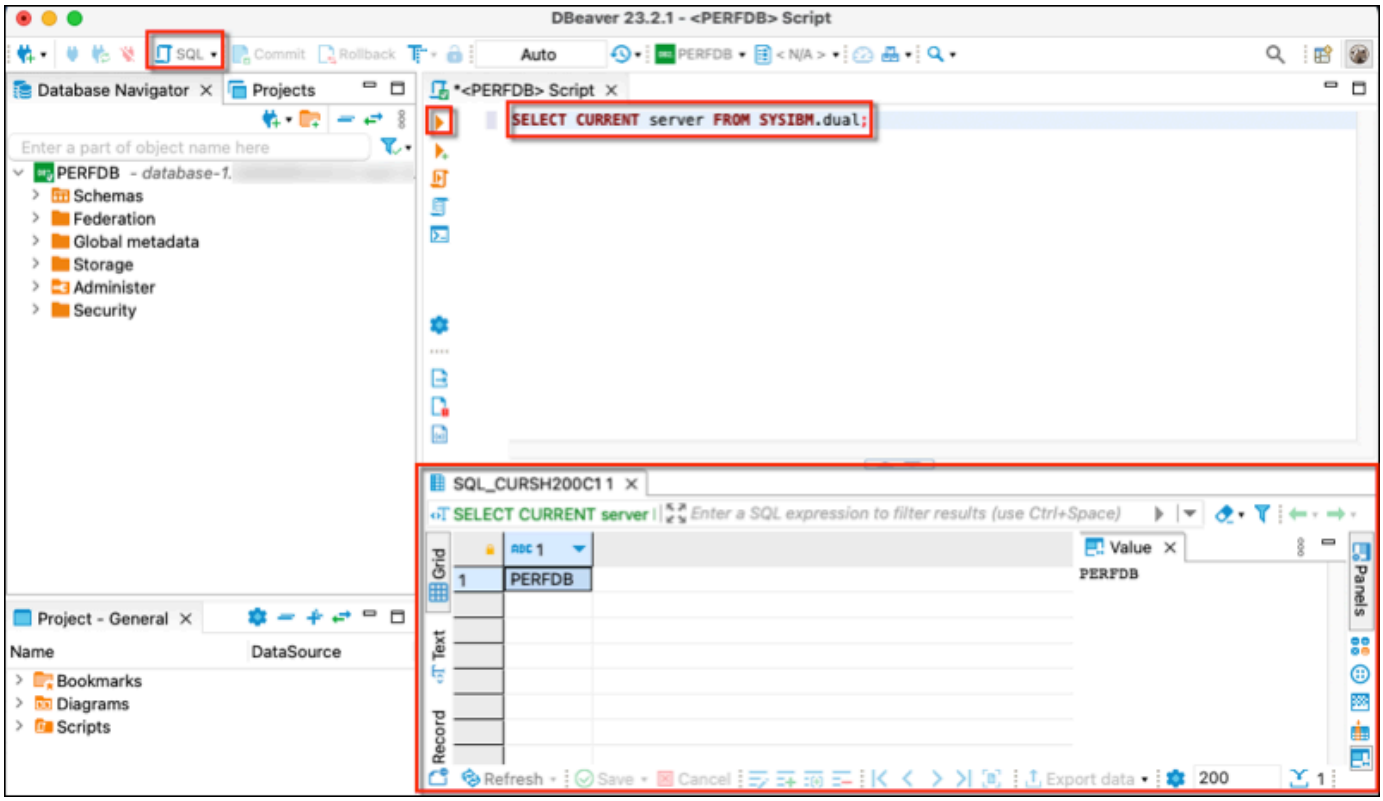


5. En la ventana Conectarse a una base de datos, seleccione Probar conexión. Si no tiene un controlador DB2 JBDC instalado en su ordenador, el controlador se descargará automáticamente.
6. Seleccione Aceptar.
7. Seleccione Finalizar.
8. En la pestaña Navegación de base de datos, elija el nombre de la base de datos. Ahora puede explorar objetos.

Ahora lo tiene todo listo para ejecutar comandos SQL.

Para ejecutar comandos SQL y ver los resultados

1. En el menú superior, elija SQL. Esto abre un panel de scripts SQL.
2. En el panel Script, introduzca un comando SQL.
3. Para ejecutar el comando, pulse el botón Ejecutar consulta SQL.
4. En el panel de resultados de SQL, consulte los resultados de sus consultas SQL.



Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 Data Management Console

Puede conectarse a una instancia de base de datos de Amazon RDS para Db2 con IBM Db2 Data Management Console. IBM Db2 Data Management Console puede administrar y monitorear varias instancias de base de datos de RDS para Db2.

> **Note**
>
> Debe tener un equipo con Amazon EC2 Linux o Windows que esté en la misma VPC y el mismo grupo de seguridad que la instancia de base de datos de RDS para Db2. La VPC y el

grupo de seguridad controlan la conexión a la instancia de base de datos a través de la red interna.

IBM Db2 Data Management Console requiere una base de datos del repositorio de Db2 para almacenar los metadatos y las métricas de rendimiento, pero no puede crear automáticamente una base de datos de repositorio de RDS para Db2. En cambio, primero debe crear una base de datos del repositorio para supervisar una o varias instancias de base de datos de RDS para Db2. A continuación, puede instalar IBM Db2 Data Management Console y conectarse a la instancia de base de datos de RDS para Db2 con IBM Db2 Data Management Console.

Temas

- Paso 1: creación de una base de datos del repositorio para supervisar instancias de base de datos
- Paso 2: instalación y configuración de IBM Db2 Data Management Console
- Paso 3: configuración de la base de datos del repositorio y conexión a las instancias de base de datos de RDS para Db2
- Uso de IBM Db2 Data Management Console

Paso 1: creación de una base de datos del repositorio para supervisar instancias de base de datos

Puede utilizar una instancia de base de datos RDS para Db2 existente del tamaño adecuado como repositorio para que IBM Db2 Data Management Console monitorice otras instancias de base de datos de RDS para Db2. Sin embargo, dado que el usuario administrador no tiene la autoridad SYSCTRL para crear grupos de búferes y espacios de tabla, no se puede utilizar la creación de repositorios de IBM Db2 Data Management Console para crear una base de datos de repositorios. En su lugar, debe crear una base de datos del repositorio. Esta base de datos del repositorio supervisa las instancias de base de datos de RDS para Db2.

Puede crear una base de datos del repositorio de dos maneras diferentes. Puede crear una base de datos de RDS para Db2 y, a continuación, crear manualmente un grupo de búferes, un espacio de tablas de usuario y un espacio de tablas temporal del sistema. O bien, puede crear una instancia de Amazon EC2 independiente para alojar una base de datos del repositorio de IBM Db2 Data Management Console.

Temas

- Creación manual de un grupo de búferes, un espacio de tablas de usuario y un espacio de tablas temporal del sistema
- Creación de una instancia de Amazon EC2 para alojar un repositorio de IBM Db2 Data Management Console

Creación manual de un grupo de búferes, un espacio de tablas de usuario y un espacio de tablas temporal del sistema

Creación de un grupo de búferes, un espacio de tablas de usuario y un espacio de tablas temporal del sistema

1. Conéctese a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 connect to rdsadmin user master_username using master_password
   ```

2. Cree un grupo de búferes para IBM Db2 Data Management Console. En el siguiente ejemplo, sustituya *`database_name`* por el nombre del repositorio que ha creado para que IBM Db2 Data Management Console monitorice sus instancias de base de datos RDS para Db2.

   ```
   db2 "call rdsadmin.create_bufferpool('database_name',
        'BP4CONSOLE', 1000, 'Y', 'Y', 32768)"
   ```

3. Cree un espacio de tablas de usuario para IBM Db2 Data Management Console. En el siguiente ejemplo, sustituya *`database_name`* por el nombre del repositorio que ha creado para que IBM Db2 Data Management Console monitorice sus instancias de base de datos RDS para Db2.

   ```
   db2 "call rdsadmin.create_tablespace('database_name',
        'TS4CONSOLE', 'BP4CONSOLE', 32768)"
   ```

4. Cree un espacio de tablas temporal del sistema para IBM Db2 Data Management Console. En el siguiente ejemplo, sustituya *`database_name`* por el nombre del repositorio que ha creado para que IBM Db2 Data Management Console monitorice sus instancias de base de datos RDS para Db2.

   ```
   db2 "call rdsadmin.create_tablespace('database_name',
       'TS4CONSOLE_TEMP', 'BP4CONSOLE', 32768, 0, 0, 'S')"
   ```

Ya tiene todo listo para instalar IBM Db2 Data Management Console. Para obtener más información sobre la instalación y la configuración, consulte Paso 2: instalación y configuración de IBM Db2 Data Management Console.

Creación de una instancia de Amazon EC2 para alojar un repositorio de IBM Db2 Data Management Console

Puede crear una instancia de Amazon Elastic Compute Cloud (Amazon EC2) independiente para alojar un repositorio de IBM Db2 Data Management Console. Para obtener información sobre cómo crear una instancia de Amazon EC2, consulte Tutorial: Introducción a las instancias Linux de Amazon EC2 en la Guía de usuario de Amazon EC2.

Paso 2: instalación y configuración de IBM Db2 Data Management Console

Tras crear un grupo de búferes, un espacio de tablas de usuario y un espacio de tablas temporal del sistema, tendrá todo listo para instalar y configurar IBM Db2 Data Management Console.

> **Important**
>
> Debe tener un equipo con Amazon EC2 Linux o Windows que esté en la misma VPC y el mismo grupo de seguridad que la instancia de base de datos de RDS para Db2. La VPC y el grupo de seguridad controlan la conexión a la instancia de base de datos a través de la red interna. Además, ya debe haber creado una base de datos del repositorio para IBM Db2 Data Management Console.

Instalación y configuración de IBM Db2 Data Management Console

1. Descargue IBM Db2 Data Management Console en IBM Db2 Data Management Console Version 3.1x releases en el sitio web de soporte de IBM.
2. Instale IBM Db2 Data Management Console.
3. Abra IBM Db2 Data Management Console y utilice la dirección IP del equipo con Amazon EC2 y el número de puerto que utilizó para la conexión HTTP o HTTPS a la instancia de Amazon EC2. Por ejemplo, utilice `http://xx.xx.xx.xx:11080` o `https://xx.xx.xx.xx.11081`. Sustituya *`xx.xx.xx.xx`* por la dirección IP del equipo con Amazon EC2. `11080` y `11081` son los puertos predeterminados para las conexiones HTTP y HTTPS.
4. (Opcional) Si desea usar el puerto 80 o 443 en la instancia de Amazon EC2, puede usar Apache httpd o un servidor HTTP de Nginx para enviar mediante proxy el puerto de IBM Db2 Data

Management Console a los puertos 80 o 443. Para obtener más información, consulte Apache HTTP Server Project y el sitio web de nginx.

Para permitir la conexión a IBM Db2 Data Management Console, debe editar las reglas de entrada del grupo de seguridad. Si usa un proxy, cambie el puerto 80 o 443 de TCP/IP para redirigirlo a los puertos de IBM Db2 Data Management Console. Si no usa un proxy, cambie el puerto 80 o 443 de TCP/IP por los puertos predeterminados 11080 (HTTP) o 11081 (HTTPS).

Ahora puede iniciar sesión en IBM Db2 Data Management Console para configurar la base de datos del repositorio y conectarse a las instancias de base de datos de RDS para Db2. Para obtener más información, consulte Configuración de la base de datos del repositorio y conexión a las instancias de base de datos.

Paso 3: configuración de la base de datos del repositorio y conexión a las instancias de base de datos de RDS para Db2

Cuando se conecte a la base de datos del repositorio por primera vez, IBM Db2 Data Management Console configurará automáticamente el repositorio. Una vez configurada la base de datos del repositorio, puede añadir conexiones de base de datos a IBM Db2 Data Management Console.

Para conectarse a una instancia de base de datos de RDS para Db2, necesita su nombre DNS y el número de puerto. Para obtener información sobre cómo encontrarlos, consulte Búsqueda del punto de conexión. También debe conocer el nombre de la base de datos, el nombre de usuario maestro y la contraseña maestra que definió al crear la instancia de base de datos de RDS para Db2. Para obtener más información sobre cómo encontrarlos, consulte Creación de una instancia de base de datos. Si se conecta a través de Internet, permita que el tráfico llegue al puerto de la base de datos. Para obtener más información, consulte Creación de una instancia de base de datos.

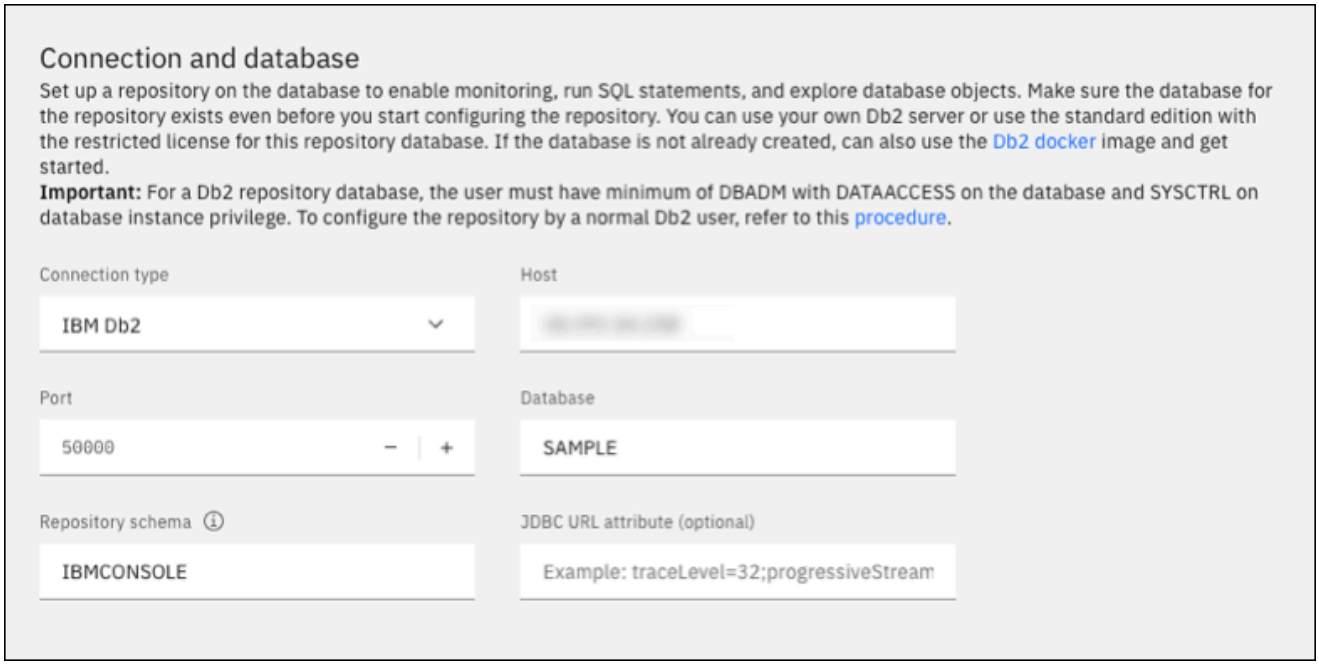
Para conectarse a instancias de base de datos de RDS para Db2 con IBM Db2 Data Management Console

1. Inicie sesión en IBM Db2 Data Management Console con las credenciales que ha configurado durante la instalación.
2. Configure el repositorio.

    a. En la sección Conexión y base de datos, introduzca la siguiente información para su instancia de base de datos de RDS para Db2:

        • En Nombre del host, escriba el nombre DNS de la instancia de base de datos.

- En Puerto, escriba el número de puerto de la instancia de base de datos.
- En Base de datos, escriba el nombre de la base de datos.



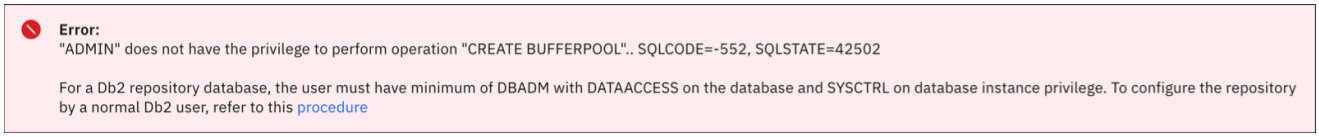
b. En la sección Seguridad y credenciales, introduzca la siguiente información para su instancia de base de datos de RDS para Db2:

- En Tipo de seguridad, elija Usuario y contraseña cifrados.
- En Username (Nombre de usuario), escriba el nombre del administrador de base de datos para la instancia de base de datos.
- En Contraseña, escriba la contraseña del administrador de base de datos para la instancia de base de datos.

c. Elija Test Connection (Probar conexión).

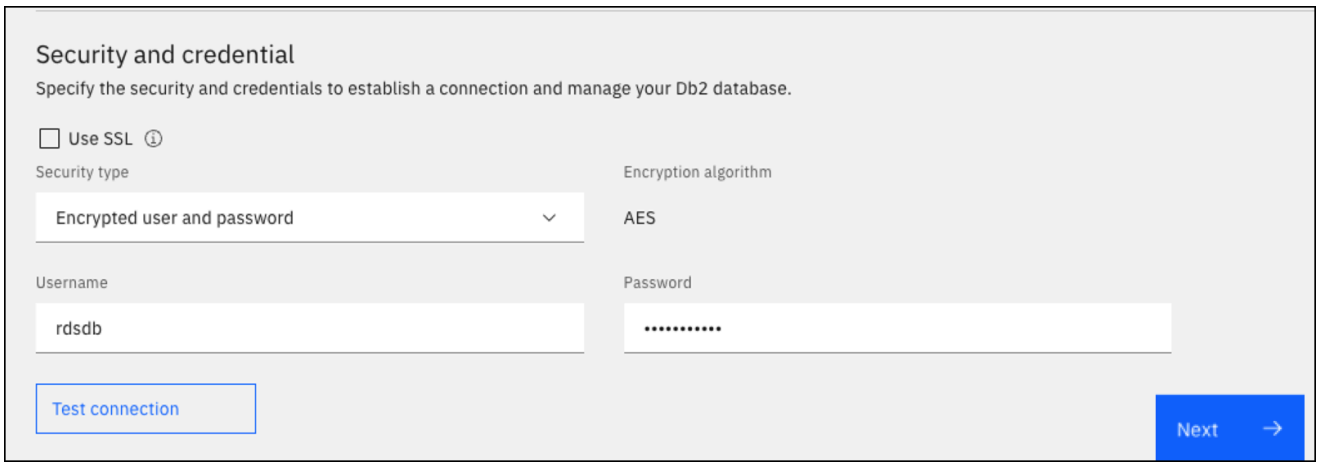
> **Note**
>
> Si la conexión no se realiza correctamente, confirme que el puerto de la base de datos esté abierto según las reglas de entrada del grupo de seguridad. Para obtener más información, consulte Consideraciones sobre grupos de seguridad con Amazon RDS para Db2.

Si no ha creado manualmente un grupo de búferes, un espacio de tabla de usuario ni un espacio de tabla temporal del sistema en RDS para Db2, es posible que aparezca el siguiente mensaje de error:



Asegúrese de haber creado una tabla de búfer, un espacio de tablas y objetos para un que un repositorio IBM Db2 Data Management Console monitorice su instancia de base de datos de RDS para Db2. También puede utilizar una instancia de base de datos de Db2 de Amazon EC2 para alojar un repositorio de IBM Db2 Data Management Console con el fin de supervisar la instancia de base de datos de RDS para Db2. Para obtener más información, consulte Paso 1: creación de una base de datos del repositorio para supervisar instancias de base de datos.

d. Tras probar satisfactoriamente su conexión, seleccione Siguiente.



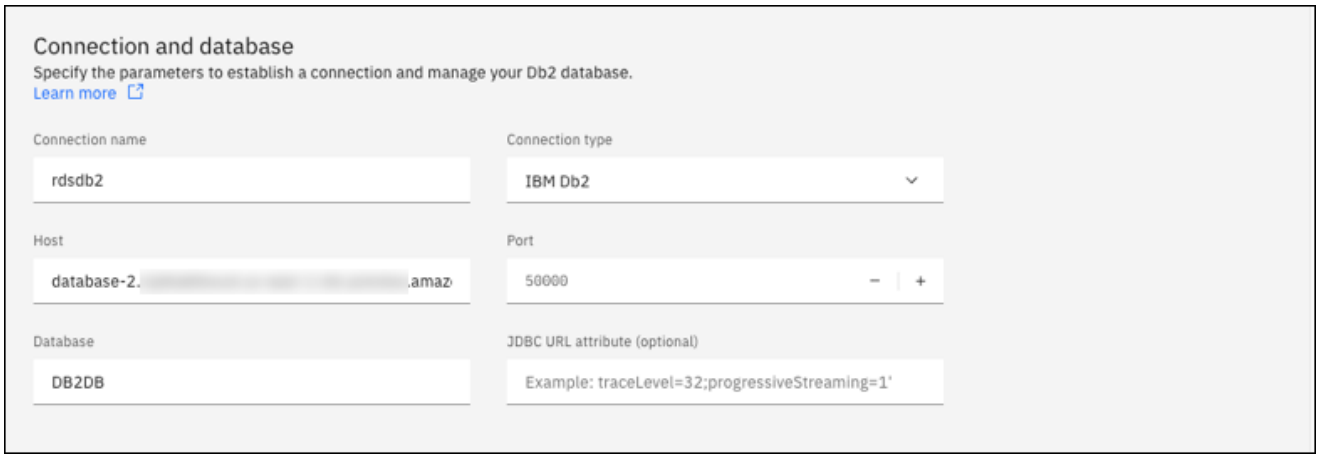
Si IBM Db2 Data Management Console encuentra el grupo de búferes, el espacio de tabla de usuario y el espacio de tabla temporal del sistema en la instancia de base de datos de RDS para Db2, IBM Db2 Data Management Console configurará automáticamente la base de datos del repositorio. Si usa la instancia de Db2 en la instancia de Amazon EC2 como base de datos del repositorio, IBM Db2 Data Management Console creará automáticamente el grupo de búferes y otros objetos.

3. En la ventana de Configurar inscripción al monitor de eventos de estadísticas, seleccione Siguiente.

4. (Opcional) Agregue una nueva conexión. Si desea utilizar una instancia de base de datos de RDS para Db2 diferente para la administración y la monitorización, agregue una conexión a una instancia de base de datos de RDS para Db2 que no sea de repositorio.

   a. En la sección Conexión y base de datos, introduzca la siguiente información para que la instancia de base de datos de RDS para Db2 la utilice en la administración y la monitorización:

      - En Nombre de la conexión, introduzca el identificador de la base de datos de Db2.
      - En Nombre del host, escriba el nombre DNS de la instancia de base de datos.
      - En Puerto, escriba el número de puerto de la instancia de base de datos.
      - En Base de datos, escriba el nombre de la base de datos.



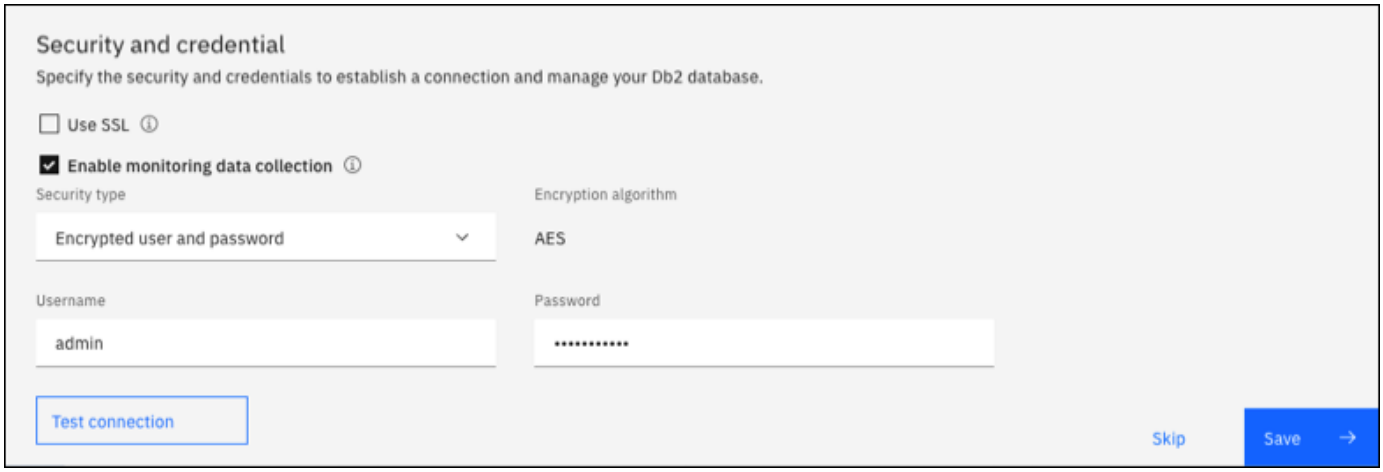
   b. En la sección Seguridad y credenciales, seleccione Habilitar la recopilación de datos de monitorización.

   c. Escriba la siguiente información para la instancia de base de datos de RDS para Db2:

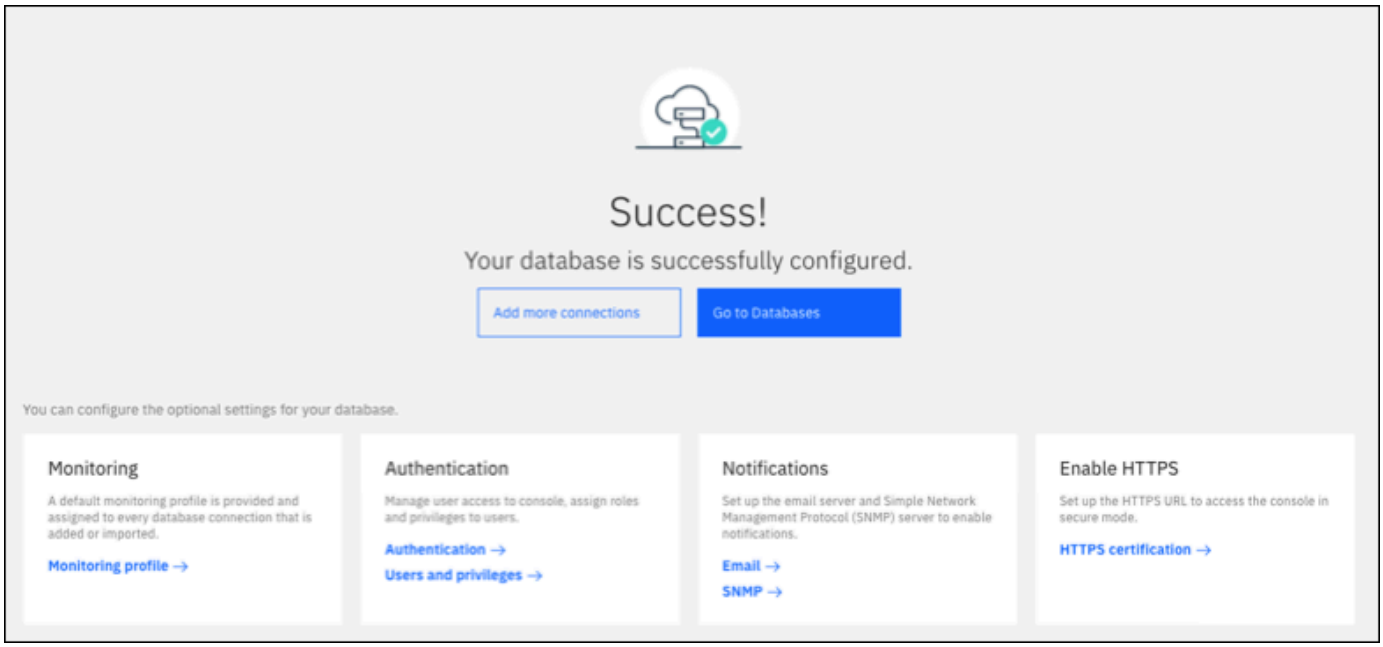
      - En Username (Nombre de usuario), escriba el nombre del administrador de base de datos para la instancia de base de datos.
      - En Contraseña, escriba la contraseña del administrador de base de datos para la instancia de base de datos.

   d. Elija Test Connection (Probar conexión).

   e. Tras probar satisfactoriamente su conexión, seleccione Guardar.



Una vez agregada la conexión, aparecerá una ventana similar a la siguiente. Esta ventana indica que la base de datos se ha configurado correctamente.



5. Seleccione Ir a bases de datos. Aparecerá una ventana de bases de datos similar a la que se muestra a continuación. Esta ventana es un panel que muestra las métricas, los estados y las conexiones.



Ya puede comenzar a utilizar IBM Db2 Data Management Console.

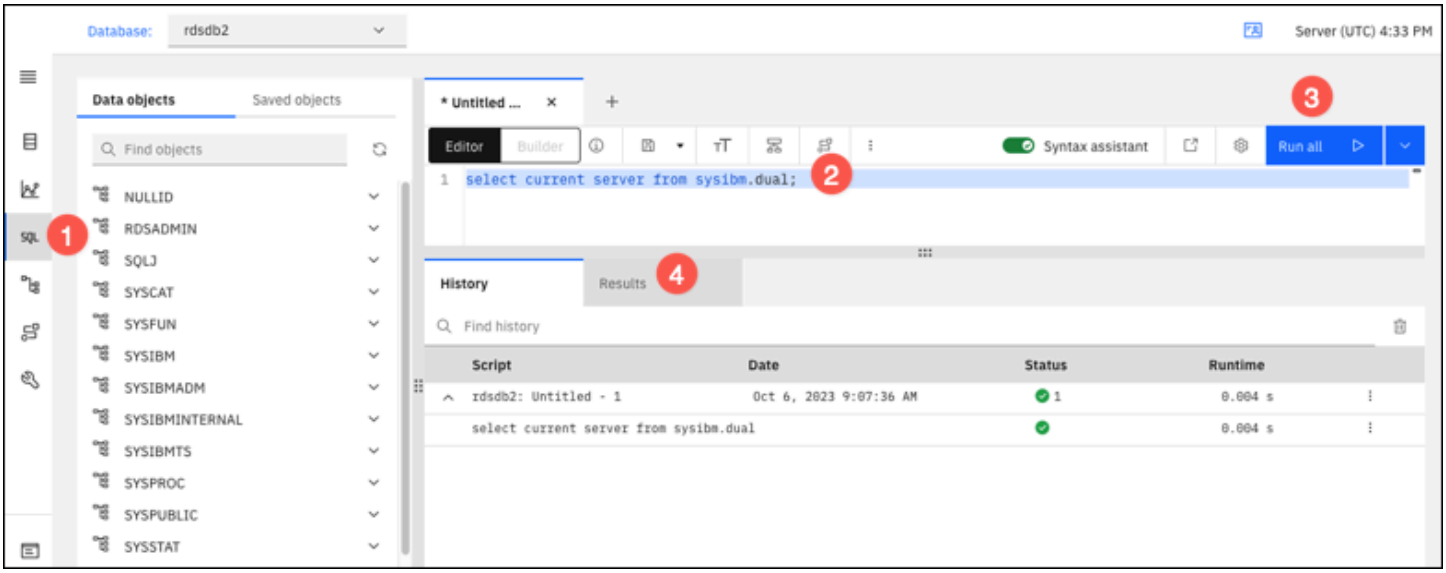
Uso de IBM Db2 Data Management Console

Puede utilizar IBM Db2 Data Management Console para realizar los siguientes tipos de tareas:

- Administrar varias instancias de base de datos de RDS para Db2.
- Ejecutar comandos SQL.
- Explorar, crear o cambiar los datos y los objetos de la base de datos.
- Crear instrucciones `EXPLAIN PLAN` en SQL.
- Ajustar consultas.

Para ejecutar comandos SQL y ver los resultados

1. En la barra de navegación, seleccione SQL.
2. Introduzca un comando SQL.
3. Seleccione Ejecutar todo.
4. Para ver los resultados, seleccione la pestaña Resultados.



Consideraciones sobre grupos de seguridad con Amazon RDS para Db2

Para poder conectarse a la instancia de base de datos de Amazon RDS para Db2, esta debe estar asociada a un grupo de seguridad que contenga las direcciones IP y la configuración de red necesarias. La instancia de base de datos de RDS para Db2 puede utilizar el grupo de seguridad predeterminado. Si se asignó un grupo de seguridad no configurado predeterminado cuando se creó la instancia de base de datos de RDS para Db2, el firewall evitará las conexiones a Internet. Para obtener información acerca de la creación de grupos de seguridad nuevos, consulte Control de acceso con grupos de seguridad.

Después de crear el nuevo grupo de seguridad, modifique la instancia de base de datos para asociarla al grupo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Puede mejorar la seguridad utilizando SSL para cifrar conexiones a su instancia de base de datos. Para obtener más información, consulte Uso de SSL con una instancia de base de datos de Amazon RDS para Db2.

Protección de conexiones de instancias de bases de datos de Amazon RDS para Db2

Amazon RDS para Db2 admite formas de mejorar la seguridad de sus instancias de base de datos de RDS para Db2.

Temas

- Uso de SSL con una instancia de base de datos de Amazon RDS para Db2
- Uso de la autenticación de Kerberos para Amazon RDS para Db2

Uso de SSL con una instancia de base de datos de Amazon RDS para Db2

SSL es un protocolo estándar del sector que se utiliza para proteger las conexiones de red entre el cliente y el servidor. Después de la versión 3.0 de SSL, el nombre se cambió a TLS, pero a menudo nos referimos al protocolo como SSL. Amazon RDS admite el cifrado SSL para las instancias de bases de datos de Amazon RDS para Db2. Con SSL/TLS puede cifrar una conexión entre el cliente de la aplicación y la instancia de base de datos de RDS para Db2. La compatibilidad con SSL/TLS está disponible en todas las Regiones de AWS para RDS para Db2.

A fin de habilitar el cifrado SSL/TLS para una instancia de base de datos de RDS para Db2, agregue la opción Db2 SSL al grupo de parámetros asociado a la instancia de base de datos. Amazon RDS utiliza un segundo puerto, según lo requiera Db2, para las conexiones SSL/TLS. Esto permite que se produzca la comunicación cifrada de SSL y de texto sin cifrar al mismo tiempo entre una instancia de base de datos y un cliente Db2. Por ejemplo, es posible utilizar el puerto con la comunicación de texto sin cifrar para ponerse en contacto con otros recursos dentro de una VPC mientras se utiliza el puerto con comunicación cifrada SSL para ponerse en contacto con recursos situados fuera de la VPC.

Temas

- Crear una conexión SSL/TLS
- Conexión a su servidor de bases de datos Db2

Crear una conexión SSL/TLS

Para crear una conexión SSL/TLS, elija una autoridad de certificación (CA), descargue un paquete de certificados para todas las Regiones de AWS y agregue parámetros a un grupo de parámetros personalizado.

Paso 1: elegir una CA y descargar un certificado

Elija una autoridad de certificación (CA) y descargue un paquete de certificados para todas las Regiones de AWS. Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Paso 2: actualizar los parámetros de un grupo de parámetros personalizado

> **Important**
>
> Si utiliza el modelo traiga su propia licencia (BYOL) para RDS para Db2, modifique el grupo de parámetros personalizado que creó para su IBM Customer ID y su IBM Site ID. Si utiliza un modelo de licencia diferente para RDS para Db2, siga el procedimiento para agregar parámetros a un grupo de parámetros personalizado. Para obtener más información, consulte Opciones de licencias de Amazon RDS para Db2.

No puede modificar los grupos de parámetros predeterminados de las instancias de base de datos de RDS para Db2. Por lo tanto, debe crear un grupo de parámetros personalizado, modificarlo y asociarlo a las instancias de base de datos de RDS para Db2. Para obtener información acerca de los grupos de parámetros, consulte Grupos de parámetros de base de datos para instancias de Amazon RDS.

Utilice la configuración de parámetros en la tabla siguiente.

Parámetro	Valor
`DB2COMM`	`TCPIP,SSL` o `SSL`
`SSL_SVCENAME`	`<any port number except the number used for the non-SSL port>`

Para actualizar los parámetros de un grupo de parámetros personalizado

1. Cree un grupo de parámetros personalizado ejecutando el comando create-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: un nombre para el grupo de parámetros que se está creando.
   - `--db-parameter-group-family`: la edición y la versión principal del motor de Db2. Valores válidos: `db2-se-11-5`, `db2-ae-11.5`.
   - `--description`: la descripción para este grupo de parámetros.

   Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Modifique los parámetros del grupo de parámetros personalizado que creó ejecutando el comando modify-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: el nombre del grupo de parámetros creado.
   - `--parameters`: una matriz de los nombres de parámetros, valores y métodos de aplicación para la actualización del parámetro.

   Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.
3. Asocie el grupo de parámetros a la instancia de base de datos de RDS para Db2. Para obtener más información, consulte Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS.

Conexión a su servidor de bases de datos Db2

Las instrucciones para conectarse al servidor de bases de datos Db2 son específicas del lenguaje.

Java

Para conectarse a su servidor de bases de datos Db2 mediante Java

1. Descargue el controlador JDBC. Para obtener más información, consulte DB2 JDBC Driver Versions and Downloads en el servicio de asistencia de IBM.
2. Cree un archivo de script de shell con el siguiente contenido. Este script agrega todos los certificados del paquete a un Java KeyStore.

> **Important**
>
> Compruebe que `keytool` exista en la ruta del script para que el script pueda localizarlo. Si utiliza un cliente de Db2, puede localizar el `keytool` en `~sqlib/java/jdk64/jre/bin`.

```
#!/bin/bash
PEM_FILE=$1
PASSWORD=$2
KEYSTORE=$3
# number of certs in the PEM file
CERTS=$(grep 'END CERTIFICATE' $PEM_FILE| wc -l)
for N in $(seq 0 $(($CERTS - 1))); do
    ALIAS="${PEM_FILE%.*}-$N"
    cat $PEM_FILE |
    awk "n==$N { print }; /END CERTIFICATE/ { n++ }" |
    keytool -noprompt -import -trustcacerts -alias $ALIAS -keystore $KEYSTORE -
storepass $PASSWORD
done
```

3. Para ejecutar el script de shell e importar el archivo PEM con el paquete de certificados en un Java KeyStore, ejecute el siguiente comando. Sustituya *`shell_file_name.sh`* por el nombre del archivo de script de shell y *`password`* por la contraseña de su Java KeyStore.

```
./shell_file_name.sh global-bundle.pem password trustore.jks
```

4. Para comprobar la conexión a su servidor Db2, ejecute el siguiente comando. Sustituya los siguientes marcadores de posición del ejemplo por la información de la instancia de base de datos de RDS para Db2.

- *ip_address*: la dirección IP del punto de conexión de la instancia de base de datos.
- *port*: número de puerto de la conexión SSL. Puede ser cualquier número de puerto, excepto el número que se utiliza para el puerto que no es SSL.
- *database_name*: el nombre de la base de datos en su instancia de base de datos.
- *master_username*: el nombre de usuario maestro para la instancia de base de datos.
- *master_password*: la contraseña maestra de la instancia de base de datos.

```
export trustStorePassword=MyPassword
java -cp ~/dsdriver/jdbc_sqlj_driver/linuxamd64/db2jcc4.jar \
com.ibm.db2.jcc.DB2Jcc -url \
"jdbc:db2://ip_address:port/database_name:\
sslConnection=true;sslTrustStoreLocation=\
~/truststore.jks;\
sslTrustStorePassword=${trustStorePassword};\
sslVersion=TLSv1.2;\
encryptionAlgorithm=2;\
securityMechanism=7;" \
-user master_username -password master_password
```

Node.js

Para conectarse a su servidor de bases de datos Db2 mediante Node.js

1. Instale el controlador node-ibm_db. Para obtener más información, consulte Installing the node-ibm_db driver on Linux and UNIX systems en la documentación de IBM Db2.
2. Cree un archivo JavaScript basado en el siguiente contenido. Sustituya los siguientes marcadores de posición del ejemplo por la información de la instancia de base de datos de RDS para Db2.

   - *ip_address*: la dirección IP del punto de conexión de la instancia de base de datos.
   - *master_username*: el nombre de usuario maestro para la instancia de base de datos.
   - *master_password*: la contraseña maestra de la instancia de base de datos.
   - *database_name*: el nombre de la base de datos en su instancia de base de datos.
   - *port*: número de puerto de la conexión SSL. Puede ser cualquier número de puerto, excepto el número que se utiliza para el puerto que no es SSL.

```
var ibmdb = require("ibm_db");
const hostname = "ip_address";
const username = "master_username";
const password = "master_password";
const database = "database_name";
const port = "port";
const certPath = "/root/qa-bundle.pem";
ibmdb.open("DRIVER={DB2};DATABASE=" + database + ";HOSTNAME=" +
 hostname + ";UID=" + username + ";PWD=" + password + ";PORT=" + port +
 ";PROTOCOL=TCPIP;SECURITY=SSL;SSLServerCertificate=" + certPath + ";", function
 (err, conn){
 if (err) return console.log(err);
 conn.close(function () {
 console.log('done');
 });
});
```

3. Para ejecutar el archivo JavaScript ejecute el siguiente comando:

```
node ssl-test.js
```

Python

Para conectarse a su servidor de bases de datos Db2 mediante Python

1. Cree un archivo Python con el siguiente contenido. Sustituya los siguientes marcadores de posición del ejemplo por la información de la instancia de base de datos de RDS para Db2.

   - *port*: número de puerto de la conexión SSL. Puede ser cualquier número de puerto, excepto el número que se utiliza para el puerto que no es SSL.
   - *master_username*: el nombre de usuario maestro para la instancia de base de datos.
   - *master_password*: la contraseña maestra de la instancia de base de datos.
   - *database_name*: el nombre de la base de datos en su instancia de base de datos.
   - *ip_address*: la dirección IP del punto de conexión de la instancia de base de datos.

```
import click
import ibm_db
```

```
import sys

port = port;
master_user_id = "master_username" # Master id used to create your DB instance
master_password = "master_password" # Master password used to create your DB
 instance
db_name = "database_name" # If not given "db-name'
vpc_customer_private_ip = "ip_address" # Hosts end points - Customer private IP
 Addressicert_path = "/root/ssl/global-bundle.pem" # cert path

@click.command()
@click.option("--path", help="certificate path")
def db2_connect(path):

    try:
        conn =
 ibm_db.connect(f"DATABASE={db_name};HOSTNAME={vpc_customer_private_ip};PORT={port};

 PROTOCOL=TCPIP;UID={master_user_id};PWD={master_password};SECURITY=ssl;SSLServerCertifi
 "", "")
        try:
            ibm_db.exec_immediate(conn, 'create table tablename (a int);')
            print("Query executed successfully")
        except Exception as e:
            print(e)
        finally:
            ibm_db.close(conn)
            sys.exit(1)
    except Exception as ex:
        print("Trying to connect...")

if __name__ == "__main__":
    db2_connect()
```

2. Cree el siguiente script de shell, que ejecuta el archivo Python que ha creado. Reemplace *python_file_name.py* por el nombre de su archivo de script Python.

```
#!/bin/bash
PEM_FILE=$1
# number of certs in the PEM file
CERTS=$(grep 'END CERTIFICATE' $PEM_FILE| wc -l)

for N in $(seq 0 $(($CERTS - 1))); do
```

```
    ALIAS="${PEM_FILE%.*}-$N"
    cert=`cat $PEM_FILE | awk "n==$N { print }; /END CERTIFICATE/ { n++ }"`
    cat $PEM_FILE | awk "n==$N { print }; /END CERTIFICATE/ { n++ }" >
 $ALIAS.pem
    python3 <python_file_name.py> --path $ALIAS.pem
    output=`echo $?`
    if [ $output == 1 ]; then
        break
    fi
done
```

3. Para importar el archivo PEM con el paquete de certificados y ejecutar el script de shell, ejecute el siguiente comando. Sustituya *shell_file_name.sh* por el nombre de su archivo de script de shell.

```
./shell_file_name.sh global-bundle.pem
```

Uso de la autenticación de Kerberos para Amazon RDS para Db2

Puede usar la autenticación de Kerberos para autenticar a los usuarios cuando se conecten a su instancia de base de datos de Amazon RDS para Db2. La instancia de base de datos funciona con AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) para habilitar la autenticación de Kerberos. Cuando los usuarios se autentican con una instancia de base de datos de RDS para Db2 unida al dominio de confianza, las solicitudes de autenticación se reenvían al directorio que se ha creado con AWS Directory Service. Para obtener más información, consulte What is AWS Directory Service? ¿Qué es AWS Directory Service? en la Guía de administración de AWS Directory Service.

Primero, cree un directorio de AWS Managed Microsoft AD para almacenar las credenciales de usuario. A continuación, agregue el dominio y demás información del directorio AWS Managed Microsoft AD a la instancia de base de datos de RDS para Db2. Cuando los usuarios se autentican con la instancia de base de datos de RDS para Db2, las solicitudes de autenticación se reenvían al directorio AWS Managed Microsoft AD.

Mantener todas las credenciales en el mismo directorio puede ahorrarle tiempo y esfuerzo. Con este método, dispone de un lugar centralizado para almacenar y administrar credenciales de numerosas instancias de bases de datos. El uso de un directorio también puede mejorar su perfil de seguridad general.

Para obtener información sobe la autenticación de Kerberos, consulte los siguientes temas.

Temas

- Configuración de la autenticación de Kerberos para instancias de base de datos de Amazon RDS para Db2
- Conexión a Amazon RDS para Db2 con autenticación de Kerberos

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de RDS para Db2 con autenticación de Kerberos, consulte Regiones y motores de base de datos admitidos para autenticación de Kerberos en Amazon RDS.

> **Note**
>
> La autenticación de Kerberos no es compatible con las clases de instancia de base de datos que están en desuso para las instancias de base de datos de RDS para Db2. Para obtener más información, consulte Amazon RDS para clases de instancia de Db2.

Información general sobre la autenticación de Kerberos para instancias de base de datos de RDS para Db2

Para configurar la autenticación de Kerberos para una instancia de base de datos de RDS para Db2, complete los siguientes pasos generales, que se describen con más detalle más adelante:

1. Utilice AWS Managed Microsoft AD para crear un directorio de AWS Managed Microsoft AD. Puede utilizar la AWS Management Console, la AWS Command Line Interface (AWS CLI) o AWS Directory Service para crear el directorio. Para obtener más información, consulte Eliminar su directorio AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
2. Cree un rol de AWS Identity and Access Management (IAM) que utilice la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. El rol de IAM permite a Amazon RDS realizar llamadas al directorio.

   Para que el rol de IAM permita el acceso, el punto de conexión AWS Security Token Service (AWS STS) debe activarse en la Región de AWS correcta para su Cuenta de AWS. Los puntos de

conexión de AWS STS están activos de forma predeterminada en todas las Regiones de AWS y puede usarlos sin ninguna acción posterior. Para obtener más información, consulte Activación y desactivación de AWS STS en una región de Región de AWS en la Guía del usuario de IAM.

3. Cree o modifique una instancia de base de datos de RDS para Db2 desde la AWS Management Console, la AWS CLI o la API de RDS utilizando uno de los siguientes métodos:
   - Cree una nueva instancia de base de datos de RDS para Db2 utilizando la consola, el comando create-db-instance o la operación de la API CreateDBInstance. Para ver instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Modifique una instancia de base de datos de RDS para Db2 existente mediante la consola, el comando modify-db-instance o la operación de la API ModifyDBInstance. Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.
   - Restaure una instancia de base de datos de RDS para Db2 a partir de una instantánea de base de datos utilizando la consola, el comando restore-db-instance-from-db-snapshot o la operación de la API RestoreDBInstanceFromDBSnapshot. Para obtener instrucciones, consulte Restauración a una instancia de base de datos.
   - Restaure una instancia de base de datos de RDS para Db2 en un momento dado utilizando la consola, el comando restore-db-instance-to-point-in-time o la operación de la API RestoreDBInstanceToPointInTime. Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

   Puede localizar la instancia de base de datos en la misma Amazon Virtual Private Cloud (VPC) que el directorio o en una Cuenta de AWS o VPC diferente. Cuando cree o modifique la instancia de base de datos de RDS para Db2, realice las siguientes tareas:
   - Proporcione el identificador de dominio (identificador `d-*`) que se generó cuando creó el directorio.
   - Proporcione el nombre del rol de IAM que ha creado.
   - Verifique que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico de entrada del grupo de seguridad del directorio.
4. Configure el cliente de Db2 y verifique que el tráfico puede fluir entre el host cliente y AWS Directory Service para los puertos siguientes:
   - TCP/UDP puerto 53 – DNS
   - TCP 88 – autenticación de Kerberos
   - TCP 389 — LDAP
   - TCP 464 – autenticación de Kerberos

Administración de una instancia de base de datos en un dominio

Puede usar la AWS Management Console, la AWS CLI o la API de RDS para administrar la instancia de base de datos y la relación con su Microsoft Active Directory. Puede, por ejemplo, puede asociar un Active Directory para habilitar la autenticación de Kerberos. También puede eliminar la asociación para que un Active Directory deshabilite la autenticación de Kerberos. También puede mover una instancia de base de datos para que sea autenticada externamente por un Microsoft Active Directory a otro.

Por ejemplo, al ejecutar el comando modify-db-instance de la CLI, puede llevar a cabo las siguientes acciones:

- Vuelva a intentar habilitar la autenticación de Kerberos en una pertenencia que haya dado un error especificando el ID de directorio de la pertenencia actual para la opción `--domain`.
- Deshabilite la autenticación de Kerberos en una instancia de base de datos especificando `none` para la opción `--domain`.
- Trasladar una instancia de base de datos de un dominio a otro especificando el identificador de dominio del nuevo dominio para la opción `--domain`.

Descripción de la pertenencia a los dominios

Una vez que haya creado o modificado una instancia de base de datos, esta se convierte en miembro del dominio. Puede ver el estado de la suscripción al dominio en la consola o ejecutando el comando describe-db-instances de la CLI. El estado de la instancia de base de datos puede ser uno de los siguientes:

- `kerberos-enabled`: la instancia de base de datos tiene habilitada la autenticación de Kerberos.
- `enabling-kerberos`: AWS está en proceso de habilitar la autenticación de Kerberos en esta instancia de base de datos.
- `pending-enable-kerberos`: la habilitación de la autenticación de Kerberos está pendiente en esta instancia de base de datos.
- `pending-maintenance-enable-kerberos`: AWS intentará habilitar la autenticación de Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `pending-disable-kerberos`: la deshabilitación de la autenticación de Kerberos está pendiente en esta instancia de base de datos.

- `pending-maintenance-disable-kerberos`: AWS intentará desactivar la autenticación de Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `enable-kerberos-failed`: un problema de configuración ha impedido que AWS habilite la autenticación de Kerberos en la instancia de base de datos. Corrija el problema de configuración antes de volver a ejecutar el comando para modificar la instancia de base de datos.
- `disabling-kerberos`: AWS está en proceso de desactivar la autenticación de Kerberos en esta instancia de base de datos.

Una solicitud para habilitar la autenticación de Kerberos puede generar un error a causa de un problema de conectividad de la red o de un rol de IAM incorrecto. En algunos casos, el intento de habilitar la autenticación de Kerberos podría fallar al crear o modificar una instancia de base de datos. Si esto ocurre, asegúrese de que está utilizando el rol de IAM correcto y, a continuación modifique la instancia de base de datos para unirse al dominio.

Configuración de la autenticación de Kerberos para instancias de base de datos de Amazon RDS para Db2

Utilice AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) para configurar la autenticación de Kerberos de una instancia de base de datos de RDS para Db2. Para configurar la autenticación de Kerberos, siga estos pasos:

Temas

- Paso 1: crear un directorio con AWS Managed Microsoft AD
- Paso 2: crear un rol de IAM para que Amazon RDS pueda acceder a AWS Directory Service
- Paso 3: crear y configurar usuarios
- Paso 4: crear un grupo de administración de RDS para Db2 en AWS Managed Microsoft AD
- Paso 5: crear o modificar una instancia de base de datos de RDS para Db2
- Paso 6: configurar un cliente Db2

Paso 1: crear un directorio con AWS Managed Microsoft AD

AWS Directory Service crea un Active Directory totalmente administrado en Nube de AWS. Al crear un directorio de AWS Managed Microsoft AD, AWS Directory Service crea dos controladores de dominio y servidores DNS para usted. Los servidores de directorios se crean en diferentes subredes

de una VPC. Esta redundancia ayuda a garantizar que su directorio permanezca accesible incluso si ocurre un fallo.

Cuando crea un directorio de AWS Managed Microsoft AD, AWS Directory Service realiza en su nombre las siguientes tareas:

- Configura un Active Directory dentro de la VPC.
- Crea una cuenta de administrador del directorio con el nombre de usuario `Admin` y la contraseña especificada. Esta cuenta le permite administrar el directorio.

  > **Important**
  >
  > Asegúrese de guardar esta contraseña. AWS Directory Service no almacena esta contraseña y no se puede recuperar ni restablecer.

- Crea un grupo de seguridad para los controladores del directorio. El grupo de seguridad debe permitir la comunicación con la instancia de base de datos de RDS para Db2.

Al lanzar AWS Directory Service for Microsoft Active Directory, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa, que tiene el nombre de NetBIOS que introdujo al crear el directorio, se encuentra en la raíz del dominio. La raíz del dominio es propiedad de AWS, que también se encarga de su administración.

La cuenta `Admin` que se creó con el directorio de AWS Managed Microsoft AD dispone de permisos para realizar las actividades administrativas más habituales para la unidad organizativa:

- Crear, actualizar o eliminar usuarios.
- Añadir recursos a su dominio, como servidores de archivos o de impresión y, a continuación, asignar permisos para esos recursos a usuarios dentro de la unidad organizativa.
- Crear unidades organizativas y contenedores adicionales.
- Delegar autoridad.
- Restaurar objetos eliminados de la papelera de reciclaje de Active Directory.
- Ejecute Active Directory y los módulos del Servicio de nombres de dominio (DNS) para Windows PowerShell en el AWS Directory Service.

La cuenta `Admin` también tiene derechos para realizar las siguientes actividades en todo el dominio:

- Administrar configuraciones DNS (agregar, quitar o actualizar registros, zonas y programas de envío).
- Ver logs de eventos DNS.
- Ver logs de eventos de seguridad.

Para crear un directorio con AWS Managed Microsoft AD

1. Inicie sesión en AWS Management Console y abra la consola de AWS Directory Service en https://console.aws.amazon.com/directoryservicev2/.
2. Elija Configurar directorio.
3. Elija AWS Managed Microsoft AD. AWS Managed Microsoft AD es la única opción que se admite actualmente para usar con Amazon RDS.
4. Elija Siguiente.
5. En la página Enter directory information (Especifique la información del directorio), facilite la siguiente información:

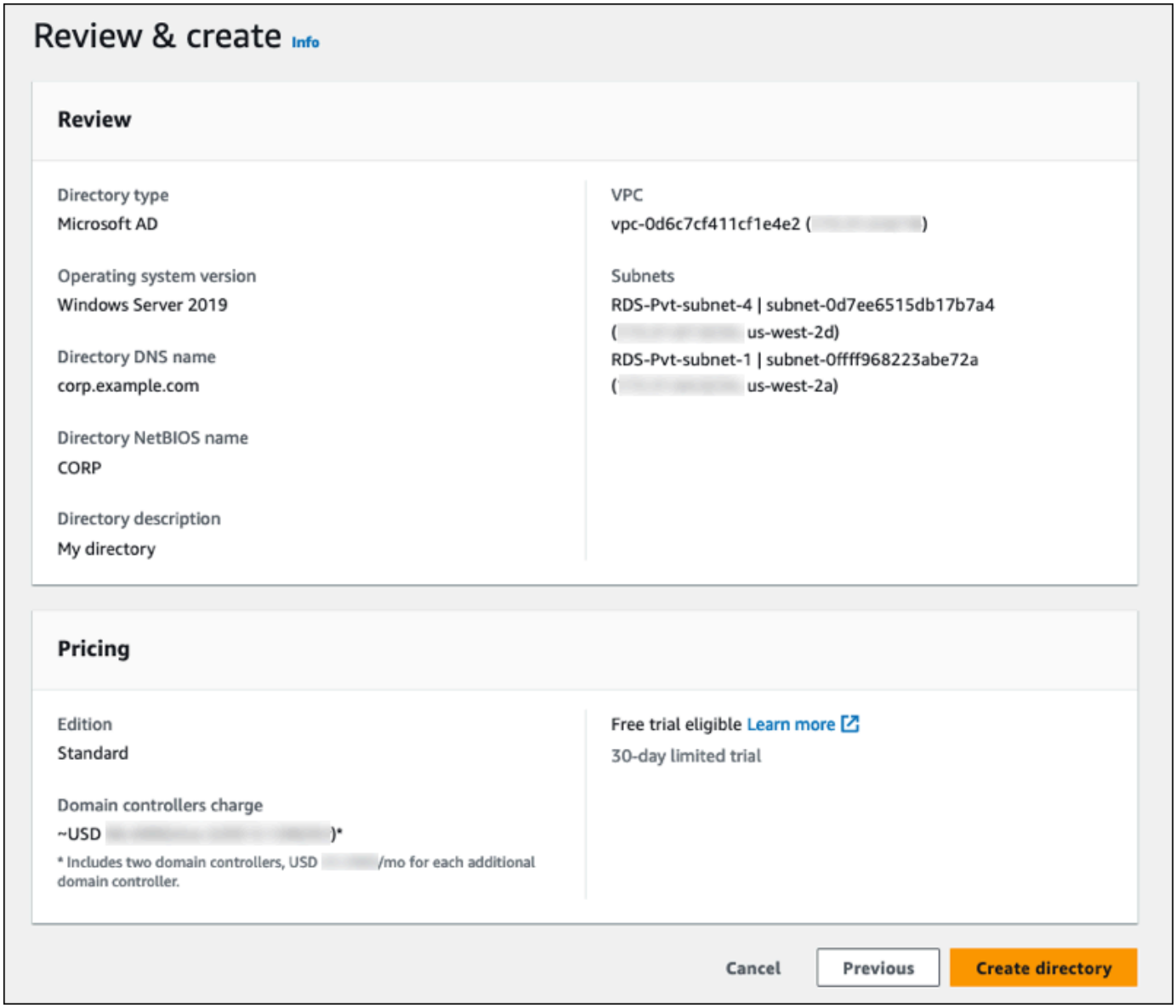
   - Edición: elija la edición que se adapte a sus necesidades.
   - Nombre de DNS del directorio: el nombre completo del directorio, como por ejemplo `corp.example.com`.
   - Nombre de NetBIOS del directorio: un nombre abreviado del directorio opcional, como `CORP`.
   - Descripción del directorio: una descripción opcional para el directorio.
   - Contraseña de administrador: la contraseña del administrador del directorio. Al crear el directorio, se crea también una cuenta de administrador con el nombre de usuario `Admin` y esta contraseña.

     La contraseña del administrador del directorio no puede contener la palabra "admin".
     La contraseña distingue entre mayúsculas y minúsculas y debe tener un mínimo de 864 caracteres y un máximo de 64. También debe contener al menos un carácter de tres de las siguientes categorías:

     - Letras minúsculas (a–z)
     - Letras mayúsculas (A–Z)
     - Números (0–9)
     - Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
     - Confirmar contraseña: vuelva a escribir la contraseña del administrador.

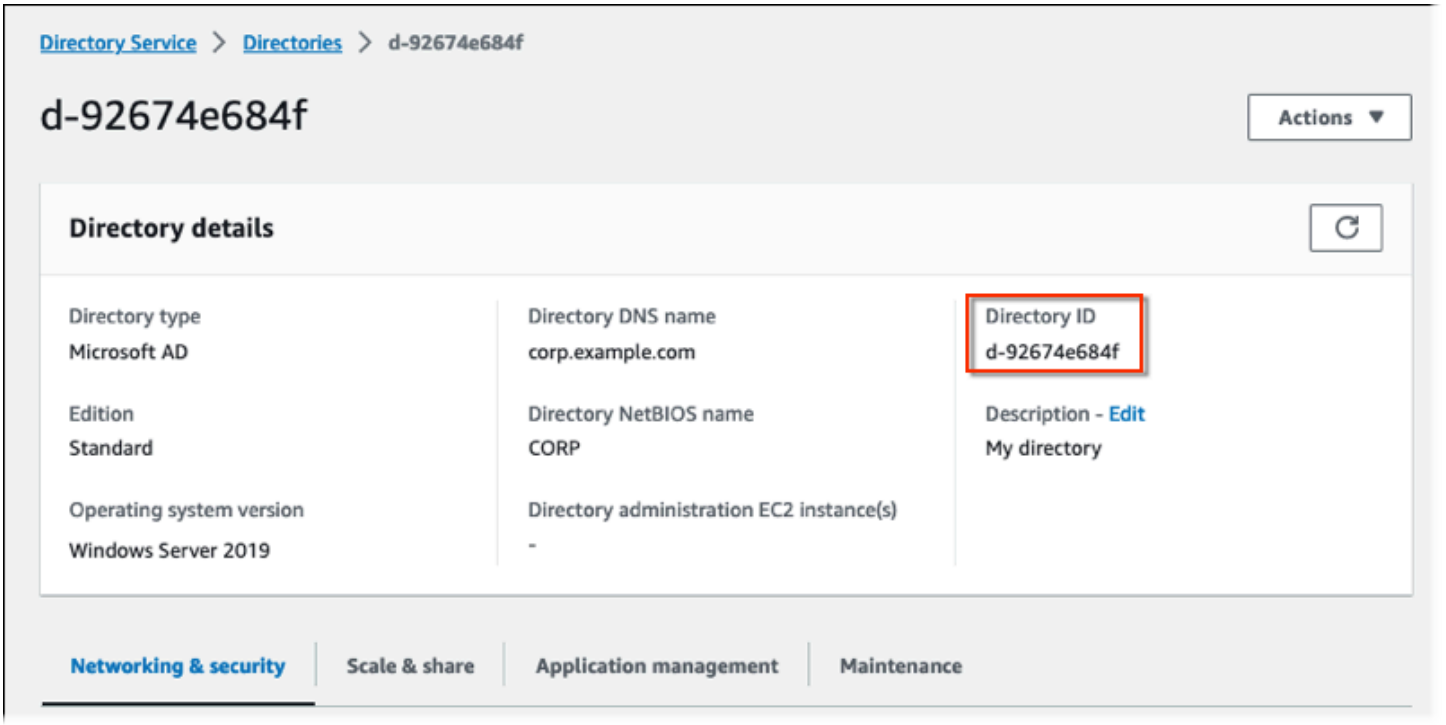
> **Important**
>
> Asegúrese de guardar esta contraseña. AWS Directory Service no almacena esta contraseña y no se puede recuperar ni restablecer.

6. Elija Siguiente.
7. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la información siguiente:
   - VPC: elija la VPC del directorio. Puede crear la instancia de base de datos de RDS para Db2 en esta misma VPC o en una VPC diferente.
   - Subredes: elija las subredes de los servidores del directorio. Las dos subredes deben estar en diferentes zonas de disponibilidad.
8. Elija Siguiente.
9. Revise la información del directorio. Si es necesario realizar algún cambio, seleccione Previous (Anterior) y realizar los cambios. Cuando la información sea correcta, seleccione Create directory (Crear directorio).



La creación del directorio tarda varios minutos. Cuando se haya creado correctamente, el valor de Status (Estado) cambiará a Active (Activo).

Para ver información acerca de su directorio, seleccione el ID del directorio en ID de directorio. Anote el valor de Directory ID (ID de directorio). Necesita este valor cuando cree o modifique su instancia de base de datos de RDS para Db2.



Paso 2: crear un rol de IAM para que Amazon RDS pueda acceder a AWS Directory Service

Para que Amazon RDS llame a AWS Directory Service en su nombre, su cuenta de Cuenta de AWS precisa un rol de IAM que utilice la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. Este rol permite a Amazon RDS realizar llamadas a AWS Directory Service.

Cuando se crea una instancia de base de datos con la AWS Management Console y la cuenta de usuario de la consola tiene el permiso `iam:CreateRole`, la consola crea automáticamente el rol de IAM necesario. En este caso, el nombre del rol es `rds-directoryservice-kerberos-access-role`. De no ser así, debe crear el rol de IAM manualmente. Cuando cree este rol de IAM, elija `Directory Service` y asocie la política administrada de AWS `AmazonRDSDirectoryServiceAccess` a este.

A fin de obtener más información acerca de la creación de roles de IAM para un servicio, consulte Creación de un rol para delegar permisos a un servicio de AWS en la guía del usuario de IAM.

> **Note**
>
> El rol de IAM utilizado para la autenticación de Windows para RDS para Microsoft SQL Server no se puede usar en RDS para Db2.

Como alternativa al uso de la política administrada de `AmazonRDSDirectoryServiceAccess`, puede crear políticas con los permisos necesarios. En este caso, el rol de IAM debe tener la siguiente política de confianza de IAM:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El rol debe también tener la siguiente política de rol de IAM:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
```

```
  ]
}
```

Paso 3: crear y configurar usuarios

Puede utilizar la herramienta Active Directory Users and Computers para crear usuarios. Esta es una de las herramientas de Active Directory Domain Services y Active Directory Lightweight Directory Services. Para obtener más información, consulte Agregar usuarios y equipos al dominio de Active Directory en la documentación de Microsoft. En este caso, los usuarios son individuos u otras entidades, como sus equipos, que forman parte del dominio y cuyas identidades se mantienen en el directorio.

Para crear usuarios en un directorio de AWS Directory Service, debe estar conectado a una instancia de Amazon EC2 basada en Windows que sea miembro del directorio de AWS Directory Service. Al mismo tiempo, debe estar registrado como usuario con privilegios para crear usuarios. Para obtener más información, consulte Crear un usuario en la Guía de administración de AWS Directory Service.

Paso 4: crear un grupo de administración de RDS para Db2 en AWS Managed Microsoft AD

RDS para Db2 no admite la autenticación de Kerberos del usuario maestro ni de los dos usuarios reservados de Amazon RDS `rdsdb` y `rdsadmin`. En su lugar, debe crear un nuevo grupo llamado `masterdba` en AWS Managed Microsoft AD. Para obtener más información, consulte Crear una cuenta de grupo en Active Directory en la documentación de Microsoft. Todos los usuarios que agregue a este grupo tendrán privilegios de usuario maestro.

Una vez habilitada la autenticación de Kerberos, el usuario maestro pierde el rol `masterdba`. Como resultado, el usuario maestro no podrá acceder a la pertenencia al grupo de usuarios local de la instancia a menos que deshabilite la autenticación de Kerberos. Para seguir utilizando el usuario maestro con contraseña de inicio de sesión, cree un usuario en AWS Managed Microsoft AD con el mismo nombre que el usuario maestro. Luego, agregue los usuarios al grupo `masterdba`.

Paso 5: crear o modificar una instancia de base de datos de RDS para Db2

Cree o modifique una instancia de base de datos de RDS para Db2 para usarla con su directorio. Puede utilizar la AWS Management Console, la AWS CLI o la API de RDS para asociar una instancia de base de datos con un directorio. Puedes hacerlo de una de las siguientes formas:

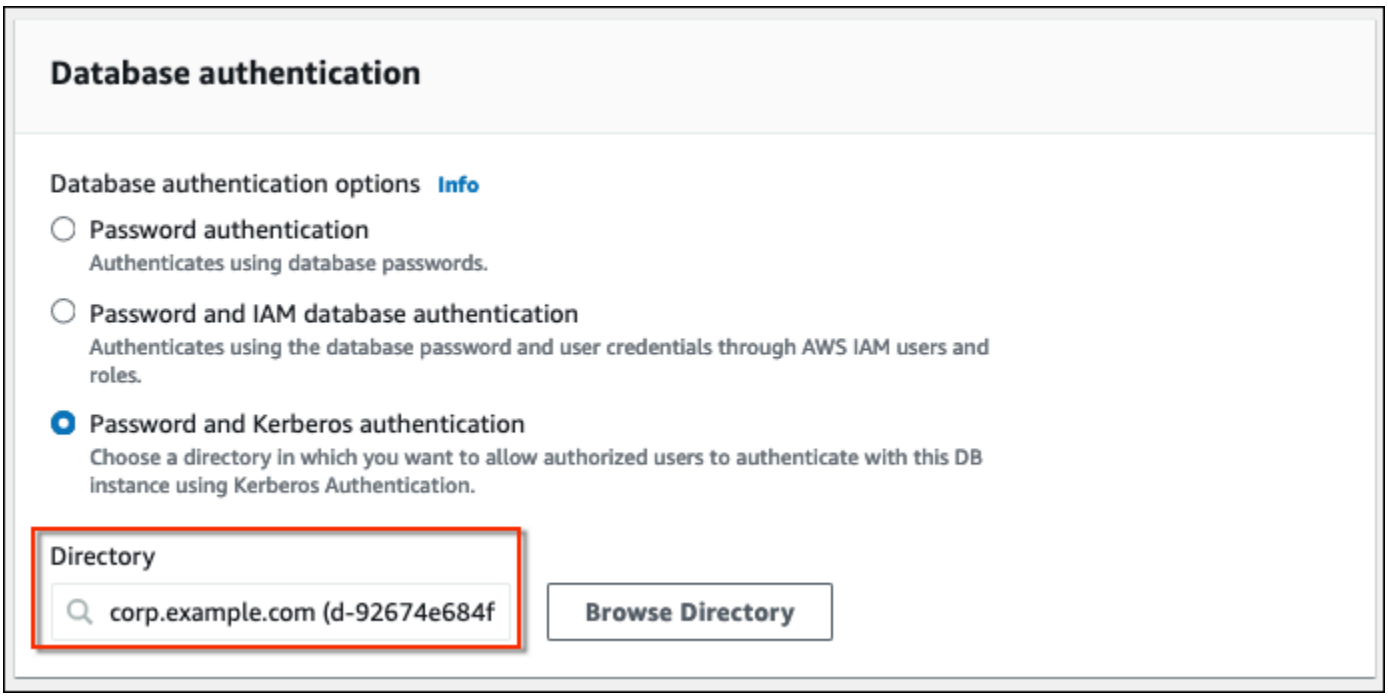
- Cree una nueva instancia de base de datos de RDS para Db2 utilizando la consola, el comando create-db-instance o la operación de la API CreateDBInstance. Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.

- Modifique una instancia de base de datos de RDS para Db2 existente utilizando la consola, el comando modify-db-instance o la operación de la API ModifyDBInstance. Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Restaure una instancia de base de datos de RDS para Db2 a partir de una instantánea de base de datos utilizando la consola, el comando restore-db-instance-from-db-snapshot o la operación de la API RestoreDBInstanceFromDBSnapshot. Para obtener instrucciones, consulte Restauración a una instancia de base de datos.
- Restaure una instancia de base de datos de RDS para Db2 en un momento dado utilizando la consola, el comando restore-db-instance-to-point-in-time o la operación de la API RestoreDBInstanceToPointInTime. Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

La autenticación de Kerberos solo es compatible con instancias de base de datos de RDS para Db2 en una VPC. La instancia de DB puede estar en la misma VPC que el directorio o en una VPC diferente. La instancia de base de datos debe usar un grupo de seguridad que permita el ingreso y la salida dentro de la VPC del directorio, de modo que la instancia de base de datos pueda comunicarse con el directorio.

Consola

Si utiliza la consola para crear, modificar o restaurar una instancia de base de datos, elija Contraseña y autenticación de Kerberos en la sección Autenticación de base de datos. Luego, elija Browse Directory (Examinar directorio). Seleccione el directorio o elija Crear un nuevo directorio para utilizar Directory Service.



AWS CLI

Cuando utilice la AWS CLI, se necesitan los siguientes parámetros para que la instancia de base de datos pueda usar el directorio que ha creado:

- Para el parámetro `--domain`, utilice el identificador de dominio (identificador "`d-*`") que se generó cuando creó el directorio.
- Para el parámetro `--domain-iam-role-name`, utilice el rol que creó que usa la política `AmazonRDSDirectoryServiceAccess` de IAM administrada.

El siguiente comando de la CLI modifica una instancia de base de datos para usar un directorio. Sustituya los siguientes valores de muestra en el ejemplo por los suyos:

- *`db_instance_name`*: el nombre de su instancia de base de datos de RDS para Db2.
- *`directory_id`*: el ID del directorio AWS Directory Service for Microsoft Active Directory que ha creado.
- *`role_name`*: el nombre del rol de IAM que ha creado.

```
aws rds modify-db-instance --db-instance-identifier db_instance_name --domain
 d-directory_id --domain-iam-role-name role_name
```

> **Important**
>
> Si modifica una instancia de base de datos para habilitar la autenticación de Kerberos, reinicie la instancia de base de datos después de realizar el cambio.

Paso 6: configurar un cliente Db2

Para configurar un cliente Db2

1. Cree un archivo /etc/krb5.conf (o equivalente) para apuntar al dominio.

   > **Note**
   >
   > Para los sistemas operativos Windows, cree un archivo C:\windows\krb5.ini.

2. Verifique que el tráfico puede fluir entre el host cliente y AWS Directory Service. Use una utilidad de red como, por ejemplo, Netcat para las siguientes tareas:

   a. Verificar el tráfico sobre DNS para el puerto 53.

   b. Verificar el tráfico sobre TCP/UDP para el puerto 53 y para Kerberos, lo que incluye los puertos 88 y 464 para AWS Directory Service.

3. Verifique que el tráfico puede fluir entre el host cliente y la instancia de base de datos sobre el puerto de base de datos. Puede usar el comando db2 para conectarse a la base de datos y acceder a ella.

El ejemplo siguiente es el contenido del archivo /etc/krb5.conf para AWS Managed Microsoft AD:

```
[libdefaults]
default_realm = EXAMPLE.COM
[realms]
EXAMPLE.COM = {
kdc = example.com
admin_server = example.com
}
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

Conexión a Amazon RDS para Db2 con autenticación de Kerberos

Utilice el siguiente procedimiento para conectarse a una instancia de base de datos de Amazon RDS para Db2 con autenticación de Kerberos.

Para conectarse a RDS para Db2 con autenticación de Kerberos

1. En el símbolo del sistema, ejecute el siguiente comando. En el ejemplo siguiente, sustituya *username* por el nombre de su usuario Microsoft Active Directory.

   ```
   kinit username
   ```

2. Si la instancia de base de datos de RDS para Db2 utiliza una VPC accesible públicamente, ponga una dirección IP privada para su punto de conexión de instancia de base de datos en su archivo `/etc/hosts` en el cliente EC2. El siguiente ejemplo obtiene la dirección IP y, a continuación, la agrega al archivo `/etc/hosts`.

   ```
   % dig +short Db2-endpoint.AWS-Region.rds.amazonaws.com
   ;; Truncated, retrying in TCP mode.
   ec2-34-210-197-118.AWS-Region.compute.amazonaws.com.
   34.210.197.118

   % echo "34.210.197.118  Db2-endpoint.AWS-Region.rds.amazonaws.com" >> /etc/hosts
   ```

3. Utilice el siguiente comando para iniciar sesión en una instancia de base de datos de RDS para Db2 que esté asociada a Active Directory. Sustituya *database_name* por el nombre de la base de datos de RDS para Db2.

   ```
   db2 connect to database_name
   ```

Administración de la instancia de base de datos de Amazon RDS para Db2

Este tema abarca las tareas de administración comunes que se realizan con una instancia de base de datos de Amazon RDS para Db2. Algunas tareas son las mismas para todas las instancias de base de datos de Amazon RDS. Otras tareas son específicas de RDS para Db2.

Las siguientes tareas son comunes para todas las bases de datos de RDS. También hay tareas específicas de RDS para Db2, como la conexión a una base de datos de RDS para Db2 con un cliente SQL estándar.

Área de la tarea	Documentación relacionada
Clases de instancias, almacenamiento y PIOPS Si está creando una instancia de producción, aprenda cómo funcionan las clases de instancia, los tipos de almacenamiento y las IOPS provisionadas en Amazon RDS.	Clases de instancia de base de datos de Tipos de almacenamiento de Amazon RDS
Implementaciones Multi-AZ Una instancia de base de datos de producción debe usar implementaciones Multi-AZ. Las implementaciones Multi-AZ proporcionan unos niveles superiores de disponibilidad, durabilidad de los datos y tolerancia a errores para las instancias de base de datos.	Configuración y administración de una implementación multi-AZ para Amazon RDS
Amazon VPC Si su Cuenta de AWS tiene una nube privada virtual (VPC) predeterminada, la instancia de base de datos se creará automáticamente dentro de la VPC predeterminada. Si su cuenta no tiene una VPC predeterminada y desea que la instancia de base de datos esté en una VPC, debe crear los grupos de VPC y de subredes antes de crear la instancia de base de datos.	Uso de una instancia de base de datos en una VPC

Área de la tarea	Documentación relacionada
Grupos de seguridad De forma predeterminada, las instancias de base de datos utilizan un firewall que impide el acceso. Asegúrese de crear un grupo de seguridad con las direcciones IP y la configuración de red correctas para acceder a la instancia de base de datos.	Control de acceso con grupos de seguridad
Grupos de parámetros Como su instancia de base de datos de RDS para Db2 requiere que añada los parámetros `rds.ibm_customer_id` y `rds.ibm_site_id` , cree un grupo de parámetros antes de crear la instancia de base de datos. Si su instancia de base de datos requiere otros parámetros de base de datos concretos, añádalos también a este grupo de parámetros antes de crear la instancia de base de datos.	Adición de ID de IBM a un grupo de parámetros para instancias de base de datos de RDS para Db2 Grupos de parámetros para Amazon RDS
Grupos de opciones Si la instancia de base de datos requiere opciones de base de datos concretas, cree un grupo de opciones antes de crear la instancia de base de datos.	Opciones de instancias de base de datos de Amazon RDS para Db2
Conexión a la instancia de base de datos Después de crear un grupo de seguridad y de asociarlo a una instancia de base de datos, puede conectarse a la instancia de base de datos usando cualquier aplicación cliente estándar de SQL, como IBM Db2 CLP.	Conexión a la instancia de base de datos de Db2
Copia de seguridad y restauración Puede configurar su instancia de base de datos para que realice copias de seguridad del almacenamiento automatizadas o tomar instantáneas manuales y restaurar después las instancias a partir de las copias de seguridad o las instantáneas.	Copia de seguridad, restauración y exportación de datos

Área de la tarea	Documentación relacionada
Supervisión Puede supervisar una instancia de base de datos de RDS para Db2 con IBM Db2 Data Management Console. También puede monitorizar una instancia de base de datos de RDS para Db2 utilizando las métricas, los eventos y la monitoriz ación avanzada de CloudWatch Amazon RDS.	Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 Data Management Console Consulta de métricas en la consola de Amazon RDS Consulta de eventos de Amazon RDS Supervisión de las métricas del sistema operativo con Supervisión mejorada
Archivos de registro Puede obtener acceso a los archivos de log de la instancia de base de datos de RDS para Db2.	Supervisión de archivos de registro de Amazon RDS

Temas

- Realización de tareas comunes del sistema para instancias de base de datos de Amazon RDS para Db2
- Ejecución de tareas comunes de base de datos para instancias de base de datos de Amazon RDS para Db2

Realización de tareas comunes del sistema para instancias de base de datos de Amazon RDS para Db2

Puede realizar ciertas tareas comunes de administrador de bases de datos relacionadas con el sistema en las instancias de base de datos de Amazon RDS que ejecuten Db2. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de bases de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Para obtener información sobre cómo conceder y revocar privilegios y cómo conectarse a la base de datos remota de RDS for Db2, consulte los temas siguientes.

Temas

- Concesión y revocación de privilegios de RDS para Db2
- Asociación a la instancia de base de datos RDS para Db2 remota

Creación de un punto de conexión de base de datos personalizado

Al migrar a Amazon RDS para Db2, puede utilizar direcciones URL de punto de conexión de base de datos personalizadas para minimizar los cambios en la aplicación. Por ejemplo, si utiliza `db2.example.com` como registro DNS actual, puede añadirlo a Amazon Route 53. En Route 53, puede usar zonas alojadas privadas para asignar el punto de conexión de su base de datos de DNS actual a un punto de conexión de base de datos de RDS para Db2. Para añadir un registro `A` o `CNAME` personalizado para un punto de conexión de base de datos de Amazon RDS, consulte Registro y administración de dominios mediante Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

> **Note**
>
> Si no puede transferir su dominio a Route 53, puede usar su proveedor de DNS para crear un registro `CNAME` para la URL del punto de conexión de la base de datos de RDS para Db2. Consulte la documentación de su proveedor de DNS.

Concesión y revocación de privilegios de RDS para Db2

Los usuarios obtienen acceso a las bases de datos al pertenecer a grupos asociados a las bases de datos.

Utilice los siguientes procedimientos para conceder y revocar privilegios para controlar el acceso a la base de datos.

Estos procedimientos utilizan IBM Db2 CLP en un equipo local para conectarse a una instancia de base de datos de RDS para Db2. Asegúrese de catalogar el nodo TCP/IP y la base de datos para conectarse a la instancia de base de datos de RDS para Db2 que se ejecuta en su equipo local. Para obtener más información, consulte Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 CLP.

Temas

- Concesión a un usuario de acceso a su base de datos
- Cambio de la contraseña de un usuario
- Agregar grupos a un usuario
- Eliminación de grupos de un usuario
- Eliminación de un usuario
- Mostrar usuarios
- Creación de un rol
- Concesión de un rol
- Revocación de un rol
- Descarte de un rol
- Concesión de autorización a la base de datos
- Revocación de la autorización de una base de datos

Concesión a un usuario de acceso a su base de datos

Para conceder a un usuario acceso a su base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 connect to rdsadmin user master_username using master_password
   ```

   El resultado de este comando debería ser similar al siguiente ejemplo:

   ```
   Database Connection Information

   Database server        = DB2/LINUXX8664 11.5.8.0
   SQL authorization ID   = ADMIN
   Local database alias   = RDSADMIN
   ```

2. Agregue un usuario a su lista de autorización llamando a `rdsadmin.add_user`. Para obtener más información, consulte rdsadmin.add_user.

   ```
   db2 "call rdsadmin.add_user(
   ```

```
    'username',
    'password',
    'group_name,group_name')"
```

3. (Opcional) Agregue grupos adicionales al usuario llamando a `rdsadmin.add_groups`. Para obtener más información, consulte rdsadmin.add_groups.

```
db2 "call rdsadmin.add_groups(
    'username',
    'group_name,group_name')"
```

4. Confirme las autoridades que están disponibles para el usuario. En el siguiente ejemplo, sustituya *rds_database_alias*, *master_user* y *master_password* por su propia información. Además, sustituya *username* por el nombre de usuario del usuario.

```
db2 terminate
db2 connect to rds_database_alias user master_user using master_password
db2 "SELECT SUBSTR(AUTHORITY,1,20) AUTHORITY, D_USER, D_GROUP, D_PUBLIC
       FROM TABLE (SYSPROC.AUTH_LIST_AUTHORITIES_FOR_AUTHID ('username', 'U') ) AS
 T
       ORDER BY AUTHORITY"
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
AUTHORITY            D_USER D_GROUP D_PUBLIC
-------------------- ------ ------- --------
ACCESSCTRL           N      N       N
BINDADD              N      N       N
CONNECT              N      N       N
CREATETAB            N      N       N
CREATE_EXTERNAL_ROUT N      N       N
CREATE_NOT_FENCED_RO N      N       N
CREATE_SECURE_OBJECT N      N       N
DATAACCESS           N      N       N
DBADM                N      N       N
EXPLAIN              N      N       N
IMPLICIT_SCHEMA      N      N       N
LOAD                 N      N       N
QUIESCE_CONNECT      N      N       N
SECADM               N      N       N
SQLADM               N      N       N
SYSADM               *      N       *
```

```
SYSCTRL              *       N       *
SYSMAINT             *       N       *
SYSMON               *       N       *
WLMADM               N       N       N
```

5. Otorgue los roles ROLE_NULLID_PACKAGES, ROLE_TABLESPACES y ROLE_PROCEDURES de RDS para Db2 al grupo al que agregó el usuario. Para obtener más información, consulte Roles predeterminados de Amazon RDS para Db2.

> **Note**
>
> Creamos instancias de base de datos RDS para Db2 en modo RESTRICTIVE. Por lo tanto, los roles ROLE_NULLID_PACKAGES, ROLE_TABLESPACES y ROLE_PROCEDURES de RDS para Db2 otorgan privilegios de ejecución en paquetes NULLID para IBM Db2 CLP y Dynamic SQL. Estas funciones también otorgan privilegios de usuario en los espacios de tabla.

a. Conexión a su base de datos Db2. En el siguiente ejemplo, sustituya *database_name*, *master_user* y *master_password* por su propia información.

```
db2 connect to database_name user master_user using master_password
```

b. Otorgue el rol ROLE_NULLED_PACKAGES a un grupo. En el siguiente ejemplo, reemplace *group_name* por el nombre del grupo al que quiera agregar el rol.

```
db2 "grant role ROLE_NULLID_PACKAGES to group group_name"
```

c. Otorgue el rol ROLE_TABLESPACES al mismo grupo. En el siguiente ejemplo, reemplace *group_name* por el nombre del grupo al que quiera agregar el rol.

```
db2 "grant role ROLE_TABLESPACES to group group_name"
```

d. Otorgue el rol ROLE_PROCEDURES al mismo grupo. En el siguiente ejemplo, reemplace *group_name* por el nombre del grupo al que quiera agregar el rol.

```
db2 "grant role ROLE_PROCEDURES to group group_name"
```

6. Otorgue las autoridades `connect`, `bindadd`, `createtab` y `IMPLICIT_SCHEMA` al grupo al que agregó el usuario. En el siguiente ejemplo, reemplace *`group_name`* por el nombre del segundo grupo al que haya agregado el usuario.

```
db2 "grant usage on workload SYSDEFAULTUSERWORKLOAD to public"
db2 "grant connect, bindadd, createtab, implicit_schema on database to
 group group_name"
```

7. Repita los pasos 4 al 6 para cada grupo adicional al que haya agregado el usuario.
8. Pruebe el acceso del usuario conectándose como usuario, creando una tabla, insertando valores en la tabla y devolviendo los datos de la tabla. En el siguiente ejemplo, sustituya *`rds_database_alias`*, *`username`* y *`password`* por el nombre de la base de datos y el nombre de usuario y la contraseña del usuario.

```
db2 connect to rds_database_alias user username using password
db2 "create table t1(c1 int not null)"
db2 "insert into t1 values (1),(2),(3),(4)"
db2 "select * from t1"
```

Cambio de la contraseña de un usuario

Para cambiar la contraseña de un usuario

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Cambie la contraseña llamando a `rdsadmin.change_password`. Para obtener más información, consulte rdsadmin.change_password.

```
db2 "call rdsadmin.change_password(
    'username',
    'new_password')"
```

Agregar grupos a un usuario

Para agregar grupos a un usuario

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Agregue grupos a un usuario mediante una llamada a `rdsadmin.add_groups`. Para obtener más información, consulte rdsadmin.add_groups.

```
db2 "call rdsadmin.add_groups(
    'username',
    'group_name,group_name')"
```

Eliminación de grupos de un usuario

Para eliminar grupos de un usuario

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Elimine grupos llamando a `rdsadmin.remove_groups`. Para obtener más información, consulte rdsadmin.remove_groups.

```
db2 "call rdsadmin.remove_groups(
    'username',
    'group_name,group_name')"
```

Eliminación de un usuario

Para eliminar un usuario de la lista de autorizaciones

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 connect to rdsadmin user master_username using master_password
   ```

2. Elimine un usuario de la lista de autorización llamando a `rdsadmin.remove_user`. Para obtener más información, consulte rdsadmin.remove_user.

   ```
   db2 "call rdsadmin.remove_user('username')"
   ```

Mostrar usuarios

Para mostrar los usuarios en una lista de autorización, llame al procedimiento almacenado `rdsadmin.list_users`. Para obtener más información, consulte rdsadmin.list_users.

```
db2 "call rdsadmin.list_users()"
```

Creación de un rol

Puede utilizar el procedimiento almacenado rdsadmin.create_role para crear un rol.

Para crear un rol

1. Conéctese a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su información.

   ```
   db2 connect to rdsadmin user master_username using master_password
   ```

2. Configure Db2 para generar contenido.

   ```
   db2 set serveroutput on
   ```

3. Crear un rol. Para obtener más información, consulte the section called “rdsadmin.create_role”.

   ```
   db2 "call rdsadmin.create_role(
   ```

```
    'database_name',
    'role_name')"
```

4. Configure Db2 para que no genere contenido.

```
db2 set serveroutput off
```

Concesión de un rol

Puede usar el procedimiento almacenado rdsadmin.grant_role para asignar un rol a un rol, usuario o grupo.

Asignación de un rol

1. Conéctese a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Configure Db2 para generar contenido.

```
db2 set serveroutput on
```

3. Asigne un rol. Para obtener más información, consulte the section called “rdsadmin.grant_role”.

```
db2 "call rdsadmin.grant_role(
    'database_name',
    'role_name',
    'grantee',
    'admin_option')"
```

4. Configure Db2 para que no genere contenido.

```
db2 set serveroutput off
```

Revocación de un rol

Puede usar el procedimiento almacenado rdsadmin.revoke_role para revocar un rol a un rol, usuario o grupo.

Revocación de un rol

1. Conéctese a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Revoque un rol. Para obtener más información, consulte the section called "rdsadmin.revoke_role".

```
db2 "call rdsadmin.revoke_role(
    ?,
    'database_name',
    'role_name',
    'grantee')"
```

Descarte de un rol

Puede utilizar el procedimiento ??? almacenado para descartar un rol.

Descarte de un rol

1. Conéctese a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Descartar un rol. Para obtener más información, consulte ???.

```
db2 "call rdsadmin.drop_role(
    ?,
    'database_name',
    'role_name')"
```

Concesión de autorización a la base de datos

El usuario maestro, que tiene la autorización `DBADM`, puede conceder autorización `DBADM`, `ACCESSCTRL` o `DATAACCESS` a un rol, usuario o grupo.

Para conceder autorización a la base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Conceda acceso a un usuario llamando a `rdsadmin.dbadm_grant`. Para obtener más información, consulte rdsadmin.dbadm_grant.

```
db2 "call rdsadmin.dbadm_grant(
    ?,
    'database_name,
    'authorization',
    'grantee')"
```

Ejemplo de caso de uso

El siguiente procedimiento le mostrará cómo crear un rol, conceder la autorización `DBADM` al rol, asignar el rol a un usuario y conceder el rol a un grupo.

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Cree un rol llamado `PROD_ROLE` para una base de datos llamada `TESTDB`. Para obtener más información, consulte rdsadmin.create_role.

```
db2 "call rdsadmin.create_role(
    'TESTDB',
    'PROD_ROLE')"
```

3. Asigne el rol a un usuario llamado `PROD_USER`. El `PROD_USER` recibe la autorización de administrador para asignar roles. Para obtener más información, consulte rdsadmin.grant_role.

```
db2 "call rdsadmin.grant_role(
```

```
    ?,
    'TESTDB',
    'PROD_ROLE',
    'USER PROD_USER',
    'Y')"
```

4. (Opcional) Proporcione autorizaciones o privilegios adicionales. En el siguiente ejemplo, se concede la autorización DBADM a un rol llamado PROD_ROLE para una base de datos llamada FUNDPROD. Para obtener más información, consulte rdsadmin.dbadm_grant.

```
db2 "call rdsadmin.dbadm_grant(
    ?,
    'FUNDPROD',
    'DBADM',
    'ROLE PROD_ROLE')"
```

5. Finalice la sesión.

```
db2 terminate
```

6. Conéctese a la base de datos TESTDB con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *master_username* y *master_password* por su propia información.

```
db2 connect to TESTDB user master_username using master_password
```

7. Agregue más autorizaciones al rol.

```
db2 "grant connect, implicit_schema on database to role PROD_ROLE"
```

8. Otorgue el rol PROD_ROLE a un grupo.

```
db2 "grant role PROD_ROLE to group PRODGRP"
```

Los usuarios que pertenecen al grupo PRODGRP ahora pueden realizar acciones como conectarse a la base de datos de TESTDB, crear tablas o crear esquemas.

Revocación de la autorización de una base de datos

El usuario maestro, que tiene la autorización DBADM, puede revocar la autorización DBADM, ACCESSCTRL o DATAACCESS a un rol, usuario o grupo.

Para revocar una autorización de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Revoque el acceso de los usuarios llamando a `rdsadmin.dbadm_revoke`. Para obtener más información, consulte rdsadmin.dbadm_revoke.

```
db2 "call rdsadmin.dbadm_revoke(
    ?,
    'database_name',
    'authorization',
    'grantee')"
```

Asociación a la instancia de base de datos RDS para Db2 remota

Siga los pasos que se indican a continuación para asociar a la instancia remota de base de datos remota de RDS para Db2 y ejecute operaciones `get snapshot`.

Para asociar a la instancia de base de datos RDS para Db2 remota

1. Ejecute una sesión IBM Db2 CLP en el cliente. Para obtener información sobre la catalogación de la instancia de base de datos y la base de datos de RDS para Db2, consulte Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 CLP. Tome nota del nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2.
2. Asocie la instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`node_name`*, *`master_username`* y *`master_password`* por el nombre del nodo TCPIP que haya catalogado y el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2.

```
db2 attach to node_name user master_username using master_password
```

Tras la asociación a la instancia de base de datos remota de RDS para Db2, puede ejecutar los siguientes comandos y otros comandos `get snapshot`. Para obtener más información, consulte Comando GET SNAPSHOT en la documentación de IBM Db2.

```
db2 list applications
db2 get snapshot for all databases
db2 get snapshot for database manager
db2 get snapshot for all applications
```

Ejecución de tareas comunes de base de datos para instancias de base de datos de Amazon RDS para Db2

Puede realizar ciertas tareas comunes de DBA relacionadas con las bases de datos en las instancias de base de datos de Amazon RDS para Db2. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. Además, el usuario maestro no puede ejecutar comandos o utilidades que lo requieran las autoridades `SYSADM`, `SYSMAINT` o `SYSCTRL`.

Para obtener información sobre las tareas comunes de los grupos de búferes, las bases de datos y los espacios de tablas, consulte los siguientes temas.

Temas

- Tareas comunes para grupos de búferes
- Tareas comunes para bases de datos
- Tareas comunes para espacios de tablas

Tareas comunes para grupos de búferes

Puede crear, modificar o eliminar grupos de búferes para una base de datos de RDS para Db2. Crear, modificar o eliminar grupos de búferes requiere una autoridad `SYSADM` o `SYSCTRL` de nivel superior, algo que no está disponible para el usuario maestro. En su lugar, utilice procedimientos almacenados de Amazon RDS.

También puede vaciar los grupos de búferes.

Temas

- Creación de un grupo de búferes

- Modificación de un grupo de búferes
- Eliminación de un grupo de búferes
- Vaciado de los grupos de búferes

Creación de un grupo de búferes

Para crear un grupo de búferes para las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.create_bufferpool`. Para obtener más información, consulte Instrucción CREATE BUFFERPOOL en la documentación de IBM Db2.

Para crear un grupo de búferes

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. Cree un grupo de búferes mediante una llamada a `rdsadmin.create_bufferpool`. Para obtener más información, consulte rdsadmin.create_bufferpool.

   ```
   db2 "call rdsadmin.create_bufferpool(
       'database_name',
       'buffer_pool_name',
       buffer_pool_size,
       'immediate',
       'automatic',
       page_size,
       number_block_pages,
       block_size)"
   ```

Modificación de un grupo de búferes

Para modificar un grupo de búferes para las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.alter_bufferpool`. Para obtener más información, consulte Instrucción ALTER BUFFERPOOL en la documentación de IBM Db2.

Para modificar un grupo de búferes

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Modifique un conjunto de búferes mediante una llamada a `rdsadmin.alter_bufferpool`. Para obtener más información, consulte rdsadmin.alter_bufferpool.

```
db2 "call rdsadmin.alter_bufferpool(
    'database_name',
    'buffer_pool_name',
    buffer_pool_size,
    'immediate',
    'automatic',
    change_number_blocks,
    number_block_pages,
    block_size)"
```

Eliminación de un grupo de búferes

Para eliminar un grupo de búferes para las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.drop_bufferpool`. Para obtener más información, consulte Eliminación de grupos de búferes en la documentación de IBM Db2.

> **Important**
>
> Asegúrese de que no haya ningún espacio de tabla asignado al grupo de búferes que desee eliminar.

Para eliminar un grupo de búferes

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Elimine un grupo de búferes llamando a `rdsadmin.drop_bufferpool`. Para obtener más información, consulte rdsadmin.drop_bufferpool.

```
db2 "call rdsadmin.drop_bufferpool(
    'database_name',
    'buffer_pool_name')"
```

Vaciado de los grupos de búferes

Puede vaciar los grupos de búferes para forzar un punto de control de modo que RDS para Db2 escriba las páginas desde la memoria en el almacenamiento.

> **Note**
>
> No es necesario vaciar los grupos de búferes. Db2 escribe los registros de forma sincrónica antes de confirmar las transacciones. Es posible que las páginas sucias sigan en un grupo de búferes, pero Db2 las escribe en el almacenamiento de forma asíncrona. Incluso aunque el sistema se cierre inesperadamente, al reiniciar la base de datos, Db2 realiza automáticamente una recuperación tras el error. Durante la recuperación tras el error, Db2 escribe los cambios confirmados en la base de datos o revierte los cambios de las transacciones no confirmadas.

Para vaciar los grupos de búferes

1. Conéctese a su base de datos Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *rds_database_alias*, *master_username* y *master_password* por su propia información.

```
db2 connect to rds_database_alias user master_username using master_password
```

2. Vacíe los grupos de búferes.

```
db2 flush bufferpools all
```

Tareas comunes para bases de datos

Puede crear, eliminar o restaurar bases de datos en su instancia de base de datos de RDS para Db2. Crear, eliminar o restaurar bases de datos requiere una autoridad `SYSADM` de nivel superior, algo que no está disponible para el usuario maestro. En su lugar, utilice procedimientos almacenados de Amazon RDS.

También puede realizar tareas de administración habituales, como la monitorización, el mantenimiento y la recopilación de información sobre sus bases de datos.

Temas

- Creación de una base de datos
- Configuración de los ajustes para una base de datos
- Modificación de los parámetros en una base de datos
- Configuración de la retención de registros
- Enumeración de la información de registro
- Desactivación de una base de datos
- Activación de una base de datos
- Reactivación de una base de datos
- Eliminación de una base de datos
- Restauración de una base de datos
- Enumeración de bases de datos
- Recopilación de información sobre las bases de datos
- Forzado a las aplicaciones a salir de bases de datos
- Generación de informes de rendimiento

Creación de una base de datos

Para crear una base de datos en su instancia de base de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.create_database`. Para obtener más información, consulte Comando CREATE DATABASE en la documentación de IBM Db2.

> **Note**
>
> Si tiene previsto modificar el parámetro `db2_compatibility_vector`, modifíquelo antes de crear una base de datos. Para obtener más información, consulte Establecimiento del parámetro db2_compatibility_vector.

Para crear una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. Cree una base de datos llamando a `rdsadmin.create_database`. Para obtener más información, consulte rdsadmin.create_database.

   ```
   db2 "call rdsadmin.create_database('database_name')"
   ```

3. (Opcional) Cree bases de datos adicionales llamando a `rdsadmin.create_database` para cada base de datos que desee crear. Cada instancia de base de datos de Db2 puede contener hasta 50 bases de datos. Para obtener más información, consulte rdsadmin.create_database.

   ```
   db2 "call rdsadmin.create_database('database_name')"
   ```

4. (Opcional) Confirme que la base de datos se haya creado mediante uno de estos métodos:

   - Llamar a `rdsadmin.list_databases`. Para obtener más información, consulte rdsadmin.list_databases.
   - Ejecute los siguientes comandos SQL:

     ```
     db2 "select varchar(r.task_type,25) as task_type, r.database_name,
         varchar(r.lifecycle,15) as lifecycle, r.created_at, r.database_name,
         varchar(bson_to_json(task_input_params),256) as input_params,
         varchar(r.task_output,1024) as task_output
         from table(rdsadmin.get_task_status(null,null,'create_database'))
         as r order by created_at desc"
     ```

Configuración de los ajustes para una base de datos

A fin de configurar los ajustes de una base de datos en su instancia de base de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.set_configuration`. Por ejemplo, puede configurar el número de búferes o manipuladores de búferes que se van a crear durante una operación de restauración.

Configuración de los ajustes de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. (Opcional) Compruebe cuál es la configuración actual llamando a `rdsadmin.show_configuration`. Para obtener más información, consulte the section called “rdsadmin.show_configuration”.

   ```
   db2 "call rdsadmin.show_configuration('name')"
   ```

3. Configure los ajustes de la base de datos llamando a `rdsadmin.set_configuration`. Para obtener más información, consulte the section called “rdsadmin.set_configuration”.

   ```
   db2 "call rdsadmin.set_configuration(
       'name',
       'value')"
   ```

Modificación de los parámetros en una base de datos

Amazon RDS para Db2 utiliza tres tipos de parámetros: parámetros de configuración del administrador de bases de datos, variables de registro y parámetros de configuración de bases de datos. Puede actualizar los dos primeros tipos mediante grupos de parámetros, y el último tipo mediante el procedimiento almacenado rdsadmin.update_db_param.

> **Note**
>
> Solo puede modificar los valores de los parámetros existentes. No se pueden añadir parámetros nuevos que no sean compatibles en RDS para Db2.

Para obtener más información sobre estos parámetros y sobre cómo modificar sus valores, consulte the section called “Parámetros de Db2”.

Configuración de la retención de registros

Para configurar el tiempo que Amazon RDS retiene los archivos de registro de las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.set_archive_log_retention`.

Configuración de la retención de registros de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. (Opcional) Compruebe cuál es la configuración actual de retención de registros llamando a `rdsadmin.show_archive_log_retention`. Para obtener más información, consulte the section called “rdsadmin.show_archive_log_retention”.

   ```
   db2 "call rdsadmin.show_archive_log_retention(
       ?,
       'database_name')"
   ```

3. Configure la retención de registros para la base de datos llamando a `rdsadmin.set_archive_log_retention`. Para obtener más información, consulte the section called “rdsadmin.set_archive_log_retention”.

   ```
   db2 "call rdsadmin.set_archive_log_retention(
       ?,
       'database_name',
       'archive_log_retention_hours')"
   ```

Enumeración de la información de registro

Para obtener detalles sobre los archivos de registro de archivo, incluidos detalles como el tamaño total de almacenamiento utilizado, llame al procedimiento almacenado `rdsadmin.list_archive_log_information`.

Enumeración de la información de registro de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Llame a `rdsadmin.list_archive_log_information` para devolver una lista de la información de los archivos de registro. Para obtener más información, consulte ???.

```
db2 "call rdsadmin.list_archive_log_information(
    ?,
    'database_name')"
```

Desactivación de una base de datos

Para desactivar una base de datos en la instancia de base de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.deactivate_database`.

Cuando cree una base de datos en su instancia de bases de datos de RDS para Db2, Amazon RDS la activa de manera predeterminada. Puede desactivar las bases de datos que utilice con poca frecuencia para conservar los recursos de memoria.

Desactivación de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Desactive una base de datos llamando a `rdsadmin.deactivate_database`. Para obtener más información, consulte ???.

```
db2 "call rdsadmin.deactivate_database(
    ?,
    'database_name')"
```

Activación de una base de datos

Para activar una base de datos en una instancia de base de datos de RDS para Db2 independiente, llame al procedimiento almacenado `rdsadmin.activate_database`.

Cuando cree una base de datos en su instancia de bases de datos de RDS para Db2, Amazon RDS la activa de manera predeterminada. Puede desactivar las bases de datos que utilice con poca frecuencia para conservar los recursos de memoria y, posteriormente, activar una base de datos desactivada.

Activación de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. Active una base de datos llamando a `rdsadmin.activate_database`. Para obtener más información, consulte ???.

   ```
   db2 "call rdsadmin.activate_database(
       ?,
       'database_name')"
   ```

Reactivación de una base de datos

Para reactivar una base de datos, llame al procedimiento almacenado `rdsadmin.reactivate_database`. Después de realizar cambios en las configuraciones de las bases de datos, es posible que necesite reactivar una base de datos en una instancia de base de datos de RDS para Db2. Para determinar si necesita reactivar una base de datos, conéctese a la base de datos y ejecute `db2 get db cfg show detail`.

También puede llamar a este procedimiento almacenado para reactivar una base de datos en una instancia de base de datos RDS para Db2 independiente después de realizar cambios en las configuraciones de la base de datos. O bien, puede reactivar una base de datos en una instancia de base de datos RDS para Db2 independiente llamando primero al procedimiento almacenado `rdsadmin.deactivate_database` y, a continuación, al procedimiento almacenado

`rdsadmin.activate_database`. Para obtener más información, consulte Desactivación de una base de datos y Activación de una base de datos.

Reactivación de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Reactive una base de datos llamando a `rdsadmin.reactivate_database`. Para obtener más información, consulte ???.

```
db2 "call rdsadmin.reactivate_database(
    ?,
    'database_name')"
```

Eliminación de una base de datos

Para eliminar una base de datos de su instancia de base de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.drop_database`. Para obtener más información, consulte Dropping databases en la documentación de IBM Db2.

> **Note**
>
> Solo puede eliminar una base de datos llamando al procedimiento almacenado si se cumplen las siguientes condiciones: Para obtener más información, consulte the section called “Notas de uso” para `rdsadmin.drop_database`.

Eliminación de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Elimine una base de datos llamando a `rdsadmin.drop_database`. Para obtener más información, consulte rdsadmin.drop_database.

```
db2 "call rdsadmin.drop_database('database_name')"
```

Restauración de una base de datos

Para mover una base de datos de un bucket de Amazon S3 a su instancia de bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.restore_database`. Para obtener más información, consulte Comando RESTORE DATABASE en la documentación de IBM Db2.

Para restaurar una base de datos de

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. (Opcional) Compruebe cuál es la configuración actual para optimizar la operación de restauración llamando a `rdsadmin.show_configuration`. Para obtener más información, consulte the section called “rdsadmin.show_configuration”.

```
db2 "call rdsadmin.show_configuration('name')"
```

3. Configure los ajustes para optimizar la operación de restauración llamando a `rdsadmin.set_configuration`. Establecer estos valores de forma explícita puede mejorar el rendimiento al restaurar bases de datos con grandes volúmenes de datos. Para obtener más información, consulte the section called “rdsadmin.set_configuration”.

```
db2 "call rdsadmin.set_configuration(
    'name',
    'value')"
```

4. Restaure la base de datos llamando a `rdsadmin.restore_database`. Para obtener más información, consulte the section called “rdsadmin.restore_database”.

```
db2 "call rdsadmin.restore_database(
    ?,
```

```
    'database_name',
    's3_bucket_name',
    's3_prefix',
    restore_timestamp,
    'backup_type')"
```

5. (Opcional) Confirme que la base de datos se ha restaurado llamando a `rdsadmin.list_databases` y comprobando que la base de datos restaurada aparece en la lista. Para obtener más información, consulte rdsadmin.list_databases.
6. Ponga la base de datos de nuevo en línea y aplique registros de transacciones adicionales llamando a `rdsadmin.rollforward_database`. Para obtener más información, consulte the section called “rdsadmin.rollforward_database”.

```
db2 "call rdsadmin.rollforward_database(
    ?,
    'database_name',
    's3_bucket_name',
    s3_prefix,
    'rollforward_to_option',
    'complete_rollforward')"
```

7. Si ha configurado `complete_rollforward` como `FALSE` en el paso anterior, lo último que debe hacer para volver a poner la base de datos en línea es llamar a `rdsadmin.complete_rollforward`. Para obtener más información, consulte the section called “rdsadmin.complete_rollforward”.

```
db2 "call rdsadmin.complete_rollforward(
    ?,
    'database_name')"
```

Enumeración de bases de datos

Puede enumerar todas las bases de datos que se ejecutan en Amazon RDS para Db2 llamando a la función definida por el usuario `rdsadmin.list_databases`.

Enumeración de sus bases de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Haga una lista de sus bases de datos llamando a `rdsadmin.list_databases`. Para obtener más información, consulte rdsadmin.list_databases.

```
db2 "select * from table(rdsadmin.list_databases())"
```

Recopilación de información sobre las bases de datos

Para recopilar información sobre una base de datos en una instancia de base de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.db2pd_command`. Esta información puede ayudarle a supervisar sus bases de datos o a solucionar problemas.

Recopilación de información sobre una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *master_username* y *master_password* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Recopile información sobre la base de datos llamando a `rdsadmin.db2pd_command`. Para obtener más información, consulte rdsadmin.db2pd_command.

```
db2 "call rdsadmin.db2pd_command('db2pd_cmd')"
```

Forzado a las aplicaciones a salir de bases de datos

Para obligar a las aplicaciones a salir de una base de datos en la instancia de base de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.force_application`. Antes de realizar el mantenimiento de las bases de datos, saque las aplicaciones de sus bases de datos.

Forzado a las aplicaciones a salir de una base de datos

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *master_username* y *master_password* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Fuerce a las aplicaciones a salir de una base de datos llamando a `rdsadmin.force_application`. Para obtener más información, consulte rdsadmin.force_application.

```
db2 "call rdsadmin.force_application(
    ?,
    'applications')"
```

Generación de informes de rendimiento

Puede generar informes de rendimiento con un procedimiento o un script. Para obtener información sobre el uso de un procedimiento, consulte DBSUMMARY procedure - Generate a summary report of system and application performance metrics en la documentación de IBM Db2.

Db2 incluye un archivo `db2mon.sh` en su directorio `~sqllib/sample/perf`. La ejecución del script produce un amplio informe de métricas de SQL de bajo costo. Para descargar el archivo `db2mon.sh` y los archivos de script relacionados, consulte el directorio perf del repositorio de GitHub de IBM db2-samples.

Para generar informes de rendimiento con el script

1. Conéctese a su base de datos Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

2. Cree un grupo de búferes denominado `db2monbp` con un tamaño de página de 4096 mediante una llamada a `rdsadmin.create_bufferpool`. Para obtener más información, consulte rdsadmin.create_bufferpool.

```
db2 "call rdsadmin.create_bufferpool('database_name','db2monbp',4096)"
```

3. Cree un espacio de tablas temporal con el nombre `db2montmptbsp` que utilice el grupo de búferes `db2monbp` mediante una llamada a `rdsadmin.create_tablespace`. Para obtener más información, consulte rdsadmin.create_tablespace.

```
db2 "call rdsadmin.create_tablespace('database_name',\
    'db2montmptbsp','db2monbp',4096,1000,100,'T')"
```

4. Abra el script `db2mon.sh` y modifique la línea sobre la conexión a una base de datos.

   a. Elimine la siguiente línea.

   ```
   db2 -v connect to $dbName
   ```

   b. Sustituya la línea del paso anterior por la línea siguiente. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2.

   ```
   db2 -v connect to $dbName user master_username using master_password
   ```

   c. Elimine las siguientes líneas.

   ```
   db2 -v create bufferpool db2monbp

   db2 -v create user temporary tablespace db2montmptbsp bufferpool db2monbp

   db2 -v drop tablespace db2montmptbsp

   db2 -v drop bufferpool db2monbp
   ```

5. Ejecute el script `db2mon.sh` para generar un informe a intervalos específicos. En el siguiente ejemplo, sustituya *`absolute_path`* por la ruta completa al archivo de script, *`rds_database_alias`* con el nombre de su base de datos, y sustituya *`seconds`* por el número de segundos (0 a 3600) entre la generación de informes.

   ```
   absolute_path/db2mon.sh rds_database_alias seconds | tee -a db2mon.out
   ```

   Ejemplos

   El siguiente ejemplo muestra que el archivo de script se encuentra en el directorio `perf`, situado bajo el directorio home.

   ```
   /home/db2inst1/sqllib/samples/perf/db2mon.sh rds_database_alias seconds | tee -a
    db2mon.out
   ```

6. Elimine el grupo de búferes y el espacio de tabla que se han creado para el archivo `db2mon.sh`. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. Sustituya *`database_name`* por el nombre de su base de datos. Para obtener más información, consulte rdsadmin.drop_tablespace y rdsadmin.drop_bufferpool.

```
db2 connect to rdsadmin user master_username using master_password

db2 "call rdsadmin.drop_tablespace('database_name','db2montmptbsp')"

db2 "call rdsadmin.drop_bufferpool('database_name','db2monbp')"
```

Administrar el almacenamiento

Db2 utiliza el almacenamiento automático para administrar el almacenamiento físico de los objetos de las bases de datos, como tablas, índices y archivos temporales. En lugar de asignar manualmente el espacio de almacenamiento y realizar un seguimiento de las rutas de almacenamiento que se utilizan, el almacenamiento automático permite al sistema Db2 crear y administrar las rutas de almacenamiento según sea necesario. Esto puede simplificar la administración de las bases de datos Db2 y reducir la probabilidad de problemas debidos a errores humanos. Para obtener más información, consulte Almacenamiento automático en la documentación de IBM Db2.

Con RDS para Db2, puede aumentar dinámicamente el tamaño del almacenamiento mediante la expansión automática de los volúmenes lógicos y el sistema de archivos. Para obtener más información, consulte Uso de almacenamiento para instancias de base de datos de Amazon RDS.

Tareas comunes para espacios de tablas

Puede crear, modificar, cambiar de nombre o eliminar espacios de tabla para una base de datos de RDS para Db2. Crear, modificar, cambiar de nombre o eliminar espacios de tabla requiere una autoridad `SYSADM` de nivel superior, que no está disponible para el usuario principal. En su lugar, utilice procedimientos almacenados de Amazon RDS.

Temas

- Creación de un espacio de tabla
- Modificación de un espacio de tabla
- Cambio de nombre de un espacio de tabla

- Eliminación de un espacio de tabla
- Comprobación del estado de un espacio de tabla
- Devolución de información detallada sobre espacios de tabla
- Mostrar el estado y el grupo de almacenamiento de un espacio de tabla
- Mostrar los espacios de tabla de una tabla
- Mostrar los contenedores de espacio de tabla

Creación de un espacio de tabla

Para crear un espacio de tabla para las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.create_tablespace`. Para obtener más información, consulte Instrucción CREATE TABLESPACE en la documentación de IBM Db2.

> **Important**
>
> Para crear un espacio de tabla, debe tener un grupo de búferes del mismo tamaño de página para asociarlo al espacio de tablas. Para obtener más información, consulte Tareas comunes para grupos de búferes.

Para crear un espacio de tabla

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. Cree un espacio de tablas llamando a `rdsadmin.create_tablespace`. Para obtener más información, consulte rdsadmin.create_tablespace.

   ```
   db2 "call rdsadmin.create_tablespace(
       'database_name',
       'tablespace_name',
       'buffer_pool_name',
       tablespace_initial_size,
       tablespace_increase_size,
   ```

```
    'tablespace_type')"
```

Modificación de un espacio de tabla

Para modificar un espacio de tabla para las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.alter_tablespace`. Puede utilizar este procedimiento almacenado para cambiar el grupo de búferes de un espacio de tabla, reducir el límite máximo o poner un espacio de tabla en línea. Para obtener más información, consulte Instrucción ALTER TABLESPACE en la documentación de IBM Db2.

Para modificar un espacio de tabla

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 "connect to rdsadmin user master_username using master_password"
   ```

2. Modifique un espacio de tabla llamando a `rdsadmin.alter_tablespace`. Para obtener más información, consulte rdsadmin.alter_tablespace.

   ```
   db2 "call rdsadmin.alter_tablespace(
       'database_name',
       'tablespace_name',
       'buffer_pool_name',
       buffer_pool_size,
       tablespace_increase_size,
       'max_size', 'reduce_max',
       'reduce_stop',
       'reduce_value',
       'lower_high_water',
       'lower_high_water_stop',
       'switch_online')"
   ```

Cambio de nombre de un espacio de tabla

Para cambiar el nombre de un espacio de tabla para las bases de datos de RDS para Db2, llame al procedimiento `rdsadmin.rename_tablespace` almacenado. Para obtener más información, consulte Instrucción RENAME TABLESPACE en la documentación de IBM Db2.

Cambio de nombre de un espacio de tabla

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Cambie el nombre de un espacio de tabla llamando a `rdsadmin.rename_tablespace`. Para obtener más información, incluidas las restricciones sobre el nombre de un espacio de tabla, consulte rdsadmin.rename_tablespace.

```
db2 "call rdsadmin.rename_tablespace(
    'database_name',
    'source_tablespace_name',
    'target_tablespace_name')"
```

Eliminación de un espacio de tabla

Para eliminar un espacio de tabla para las bases de datos de RDS para Db2, llame al procedimiento almacenado `rdsadmin.drop_tablespace`. Antes de borrar un espacio de tabla, coloque primero todos los objetos del espacio de tablas, como tablas, índices u objetos grandes (LOB). Para obtener más información, consulte Eliminación de espacios de tabla en la documentación de IBM Db2.

Para eliminar un espacio de tabla

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

```
db2 "connect to rdsadmin user master_username using master_password"
```

2. Elimine un espacio de tabla llamando a `rdsadmin.drop_tablespace`. Para obtener más información, consulte rdsadmin.drop_tablespace.

```
db2 "call rdsadmin.drop_tablespace(
    'database_name',
    'tablespace_name')"
```

Comprobación del estado de un espacio de tabla

Puede comprobar el estado de un espacio de tabla con la función `cast`.

Para comprobar del estado de un espacio de tabla

1. Conéctese a su base de datos Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`rds_database_alias`*, *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 connect to rds_database_alias user master_username using master_password
   ```

2. Devolver un resultado resumido.

   Para obtener un resultado resumido:

   ```
   db2 "select cast(tbsp_id as smallint) as tbsp_id,
   cast(tbsp_name as varchar(35)) as tbsp_name,
   cast(tbsp_type as varchar(3)) as tbsp_type,
   cast(tbsp_state as varchar(10)) as state,
   cast(tbsp_content_type as varchar(8)) as contents from
    table(mon_get_tablespace(null,-1)) order by tbsp_id"
   ```

Devolución de información detallada sobre espacios de tabla

Puede devolver información sobre un espacio de tabla para un miembro o para todos los miembros mediante la función `cast`.

Para devolver información detallada sobre espacios de tabla

1. Conéctese a su base de datos Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`rds_database_alias`*, *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 connect to rds_database_alias user master_username using master_password
   ```

2. Devuelve los detalles de todos los espacios de tabla de la base de datos de un miembro o de todos los miembros.

   Para un miembro:

```
db2 "select cast(member as smallint) as member,
cast(tbsp_id as smallint) as tbsp_id,
cast(tbsp_name as varchar(35)) as tbsp_name,
cast(tbsp_type as varchar(3)) as tbsp_type,
cast(tbsp_state as varchar(10)) as state,
cast(tbsp_content_type as varchar(8)) as contents,
cast(tbsp_total_pages as integer) as total_pages,
cast(tbsp_used_pages as integer) as used_pages,
cast(tbsp_free_pages as integer) as free_pages,
cast(tbsp_page_top as integer) as page_hwm,
cast(tbsp_page_size as integer) as page_sz,
cast(tbsp_extent_size as smallint) as extent_sz,
cast(tbsp_prefetch_size as smallint) as prefetch_sz,
cast(tbsp_initial_size as integer) as initial_size,
cast(tbsp_increase_size_percent as smallint) as increase_pct,
cast(storage_group_name as varchar(12)) as stogroup from
 table(mon_get_tablespace(null,-1)) order by member, tbsp_id "
```

Para todos los miembros:

```
db2 "select cast(member as smallint) as member
cast(tbsp_id as smallint) as tbsp_id,
cast(tbsp_name as varchar(35)) as tbsp_name,
cast(tbsp_type as varchar(3)) as tbsp_type,
cast(tbsp_state as varchar(10)) as state,
cast(tbsp_content_type as varchar(8)) as contents,
cast(tbsp_total_pages as integer) as total_pages,
cast(tbsp_used_pages as integer) as used_pages,
cast(tbsp_free_pages as integer) as free_pages,
cast(tbsp_page_top as integer) as page_hwm,
cast(tbsp_page_size as integer) as page_sz,
cast(tbsp_extent_size as smallint) as extent_sz,
cast(tbsp_prefetch_size as smallint) as prefetch_sz,
cast(tbsp_initial_size as integer) as initial_size,
cast(tbsp_increase_size_percent as smallint) as increase_pct,
cast(storage_group_name as varchar(12)) as stogroup from
 table(mon_get_tablespace(null,-2)) order by member, tbsp_id "
```

Mostrar el estado y el grupo de almacenamiento de un espacio de tabla

Puede enumerar el estado y el grupo de almacenamiento de un espacio de tabla mediante la ejecución de una instrucción de SQL.

Para enumerar el estado y el grupo de almacenamiento de un espacio de tabla, ejecute la siguiente instrucción SQL:

```
db2 "SELECT varchar(tbsp_name, 30) as tbsp_name,
                  varchar(TBSP_STATE, 30) state,
                  tbsp_type,
                  varchar(storage_group_name,30) storage_group
FROM TABLE(MON_GET_TABLESPACE('',-2)) AS t"
```

Mostrar los espacios de tabla de una tabla

Puede enumerar los espacios de tabla de una tabla ejecutando una instrucción de SQL.

Para mostrar los espacios de tabla de una tabla, ejecute la siguiente instrucción SQL. En el siguiente ejemplo, sustituya *SCHEMA_NAME* y *TABLE_NAME* por los nombres del esquema y la tabla:

```
db2 "SELECT
   VARCHAR(SD.TBSPACE,30) AS DATA_SPACE,
   VARCHAR(SL.TBSPACE,30) AS LONG_SPACE,
   VARCHAR(SI.TBSPACE,30) AS INDEX_SPACE
 FROM
   SYSCAT.DATAPARTITIONS P
   JOIN SYSCAT.TABLESPACES SD ON SD.TBSPACEID = P.TBSPACEID
   LEFT JOIN SYSCAT.TABLESPACES SL ON SL.TBSPACEID = P.LONG_TBSPACEID
   LEFT JOIN SYSCAT.TABLESPACES SI ON SI.TBSPACEID = P.INDEX_TBSPACEID
 WHERE
    TABSCHEMA = 'SCHEMA_NAME'
 AND TABNAME   = 'TABLE_NAME'"
```

Mostrar los contenedores de espacio de tabla

Puede enumerar todos los contenedores de espacios de tablas o contenedores de espacios de tabla específicos mediante el comando `cast`.

Para enumerar los contenedores de espacios de tabla de un espacio de tabla

1. Conéctese a su base de datos Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *rds_database_alias*, *master_username* y *master_password* por su propia información:

```
db2 connect to rds_database_alias user master_username using master_password
```

2. Devuelve una lista de todos los contenedores de espacios de tabla de la base de datos o de contenedores de espacios de tabla específicos.

   Para todos los contenedores de espacios de tabla:

```
db2 "select cast(member as smallint) as member,
cast(tbsp_name as varchar(35)) as tbsp_name,
cast(container_id as smallint) as id,
cast(container_name as varchar(60)) as container_path, container_type as type from
 table(mon_get_container(null,-2)) order by member,tbsp_id,container_id"
```

   Para contenedores de espacios de tabla específicos:

```
db2 "select cast(member as smallint) as member,
cast(tbsp_name as varchar(35)) as tbsp_name,
cast(container_id as smallint) as id,
cast(container_name as varchar(60)) as container_path, container_type as type from
 table(mon_get_container('TBSP_1',-2)) order by member, tbsp_id,container_id"
```

Integración de una instancia de base de datos de Amazon RDS para Db2 con Amazon S3

Puede transferir archivos entre una instancia de base de datos de Amazon RDS para Db2 y un bucket de Amazon Simple Storage Service (Amazon S3) con los procedimientos almacenados de Amazon RDS. Para obtener más información, consulte Referencia de procedimientos almacenados de Amazon RDS para Db2.

> **Note**
>
> Su instancia de base de datos y el bucket de Amazon S3 deben estar en la misma Región de AWS.

Para que RDS para Db2 se integre con Amazon S3, su instancia de base de datos debe tener acceso a un bucket Amazon S3 donde resida su RDS para Db2. Si no dispone de un bucket de S3, cree un bucket.

Temas

- Paso 1: Crear una política de IAM
- Paso 2: crear un rol de IAM y asociar la política de IAM
- Paso 3: agregar su rol de IAM a su instancia de base de datos de RDS para Db2

Paso 1: Crear una política de IAM

En este paso, cree una política AWS Identity and Access Management (IAM) con los permisos necesarios para transferir archivos del bucket de Amazon S3 a la instancia de base de datos de RDS. En este paso, también se asume que ya ha creado un bucket de S3. Para obtener más información, consulte Crear un bucket en la Guía del usuario de Amazon S3.

Antes de crear la política, anote la siguiente información:

- El nombre de recurso de Amazon (ARN) del bucket
- El ARN para su clave de AWS Key Management Service (AWS KMS), si el bucket utiliza el cifrado SSE-KMS o SSE-S3.

Cree una política de IAM que incluya los siguientes permisos:

```
"kms:GenerateDataKey",
"kms:Decrypt",
"s3:PutObject",
"s3:GetObject",
"s3:AbortMultipartUpload",
"s3:ListBucket",
"s3:DeleteObject",
"s3:GetObjectVersion",
"s3:ListMultipartUploadParts"
```

Puede crear una política de IAM mediante la AWS Management Console o la AWS Command Line Interface (AWS CLI).

Consola

Para crear una política de IAM que permita a Amazon RDS acceder a un bucket de Amazon S3

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Crear política y, a continuación, elija JSON.
4. Agregue acciones por servicio. Para transferir archivos desde un bucket de Amazon S3 a Amazon RDS, debe seleccionar los permisos del bucket y los permisos de objeto.
5. Expanda Resources (Recursos). Debe especificar los recursos del bucket y del objeto.
6. Elija Siguiente.
7. Escriba un nombre para la política en Nombre de la política.
8. (Opcional) En Description (Descripción), escriba una descripción para esta política.
9. Seleccione Crear política.

AWS CLI

Para crear una política de IAM que permita a Amazon RDS acceder a un bucket de Amazon S3

1. Ejecute el comando create-policy. En el siguiente ejemplo, sustituya *iam_policy_name* y *s3_bucket_name* por un nombre para su política de IAM y el nombre del bucket de Amazon S3 en el que resida su base de datos de RDS para Db2.

Para Linux, macOS o Unix:

```
aws iam create-policy \
    --policy-name iam_policy_name \
    --policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt",
            "s3:PutObject",
            "s3:GetObject",
            "s3:AbortMultipartUpload",
            "s3:ListBucket",
            "s3:DeleteObject",
            "s3:GetObjectVersion",
            "s3:ListMultipartUploadParts"
          ],
          "Resource": [
            "arn:aws:s3:::s3_bucket_name/*",
            "arn:aws:s3:::s3_bucket_name"
          ]
        }
      ]
    }'
```

Para Windows:

```
aws iam create-policy ^
    --policy-name iam_policy_name ^
    --policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:AbortMultipartUpload",
              "s3:ListBucket",
```

```
            "s3:DeleteObject",
            "s3:GetObjectVersion",
            "s3:ListMultipartUploadParts"
          ],
          "Resource": [
            "arn:aws:s3:::s3_bucket_name/*",
            "arn:aws:s3:::s3_bucket_name"
          ]
        }
      ]
    }'
```

2. Después de crear la política, apunte el ARN de la política. Necesita el ARN para Paso 2: crear un rol de IAM y asociar la política de IAM.

Para obtener más información acerca de cómo crear una política de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Paso 2: crear un rol de IAM y asociar la política de IAM

En este paso se supone que se ha creado la política de IAM en Paso 1: Crear una política de IAM. En este paso, creará un rol de IAM para la instancia de base de datos de RDS para Db2 y, a continuación, asociará la política de IAM al rol.

Puede crear un rol de IAM a su instancia de base de datos mediante la AWS Management Console o la AWS CLI.

Consola

Para crear un rol de IAM y asociarle la política de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Creación de rol.
4. En Tipo de entidad de confianza, elija Servicio de AWS.
5. Para el Servicio o caso de uso, seleccione RDS y, a continuación, seleccione RDS: Agregar rol a la base de datos.
6. Elija Siguiente.

7. Para Políticas de permisos, busque y seleccione el nombre de la política de IAM que creó.
8. Elija Siguiente.
9. En Nombre de rol, ingrese un nombre de rol.
10. (Opcional) En Descripción, ingrese una descripción para el nuevo rol.
11. Elija Creación de rol.

AWS CLI

Para crear un rol de IAM y asociarle la política de IAM

1. Ejecute el comando create-role. En el siguiente ejemplo, sustituya *iam_role_name* por un nombre para su rol de IAM.

   Para Linux, macOS o Unix:

```
aws iam create-role \
    --role-name iam_role_name \
    --assume-role-policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "rds.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }'
```

   Para Windows:

```
aws iam create-role ^
    --role-name iam_role_name ^
    --assume-role-policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
```

```
            "Service": "rds.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }'
```

2. Después de crear el rol, anote el ARN del rol. Necesita el ARN para Paso 3: agregar su rol de IAM a su instancia de base de datos de RDS para Db2.
3. Ejecute el comando attach-role-policy. En el siguiente ejemplo, sustituya *iam_policy_arn* por el ARN de la política de IAM que creó en Paso 1: Crear una política de IAM. Reemplace *iam_role_name* por el nombre del rol de IAM que acaba de crear.

   Para Linux, macOS o Unix:

   ```
   aws iam attach-role-policy \
      --policy-arn iam_policy_arn \
      --role-name iam_role_name
   ```

   Para Windows:

   ```
   aws iam attach-role-policy ^
      --policy-arn iam_policy_arn ^
      --role-name iam_role_name
   ```

Para obtener más información, vea Crear un rol para delegar permisos a un usuario de IAM en Guía del usuario de IAM.

Paso 3: agregar su rol de IAM a su instancia de base de datos de RDS para Db2

En este paso, agregará su rol de IAM a su instancia de base de datos de RDS para Db2 Tenga en cuenta los siguientes requisitos:

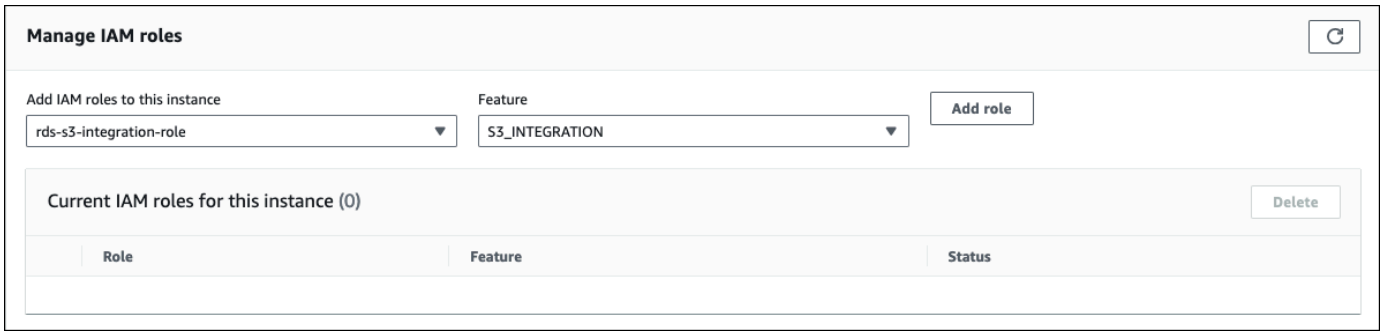
- Debe tener acceso a un rol de IAM con la política de permisos de Amazon S3 requerida adjunta.
- Solo puede asociar un rol de IAM a su instancia de base de datos de RDS para Db2 cada vez.
- Su instancia de base de datos de RDS para Db2 debe tener el estado Disponible.

Puede añadir un rol de IAM a su instancia de base de datos mediante la AWS Management Console o la AWS CLI.

Consola

Para añadir un rol de IAM a su instancia de base de datos de RDS para Db2

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el nombre de la instancia de base de datos de RDS para Db2.
4. En la pestaña Connectivity & Security (Conectividad y seguridad), desplácese hacia abajo hasta la sección Manage IAM roles (Administrar roles de IAM) de la parte inferior de la página.
5. En Añadir roles de IAM a esta instancia, elija el rol que creó en Paso 2: crear un rol de IAM y asociar la política de IAM.
6. En Feature (Característica), elija S3_INTEGRATION.
7. Seleccione Add role (Añadir rol).



AWS CLI

Para añadir un rol de IAM a su instancia de base de datos de RDS para Db2, ejecute el comando add-role-to-db-instance. En el ejemplo siguiente, sustituya *db_instance_name* e *iam_role_arn* por el nombre de la instancia de base de datos y el ARN del rol de IAM que creó en Paso 2: crear un rol de IAM y asociar la política de IAM.

Para Linux, macOS o Unix:

```
aws rds add-role-to-db-instance \
    --db-instance-identifier db_instance_name \
    --feature-name S3_INTEGRATION \
```

```
    --role-arn iam_role_arn \
```

Para Windows:

```
aws rds add-role-to-db-instance ^
    --db-instance-identifier db_instance_name ^
    --feature-name S3_INTEGRATION ^
    --role-arn iam_role_arn ^
```

Para confirmar que el rol se agregó correctamente a su instancia de base de datos de RDS para Db2, ejecute el comando describe-db-instances. En el siguiente ejemplo, sustituya *db_instance_name* por el nombre de la instancia de base de datos.

Para Linux, macOS o Unix:

```
aws rds describe-db-instances \
    --filters "Name=db-instance-id,Values=db_instance_name" \
    --query 'DBInstances[].AssociatedRoles'
```

Para Windows:

```
aws rds describe-db-instances ^
    --filters "Name=db-instance-id,Values=db_instance_name" ^
    --query 'DBInstances[].AssociatedRoles'
```

El resultado de este comando debería ser similar al siguiente ejemplo:

```
[
    [
        {
            "RoleArn": "arn:aws:iam::0123456789012:role/rds-db2-s3-role",
            "FeatureName": "S3_INTEGRATION",
            "Status": "ACTIVE"
        }
    ]
]
```

Migración de datos a Amazon RDS para Db2

Puede migrar bases de datos de Db2 autoadministradas a Amazon RDS para Db2 mediante AWS o herramientas nativas de Db2.

Para obtener información sobre cómo migrar una base de datos de Db2 a Amazon RDS para Db2 mediante los servicios de AWS, consulte Uso de servicios de AWS para migrar datos de Db2 a Amazon RDS para Db2.

Para obtener información sobre cómo migrar una base de datos de Db2 a Amazon RDS para Db2 mediante las herramientas nativas de Db2, consulte Uso de herramientas nativas de Db2 para migrar datos de Db2 a Amazon RDS para Db2.

Uso de servicios de AWS para migrar datos de Db2 a Amazon RDS para Db2

En Amazon RDS, hay varias formas de migrar datos de una base de datos de Db2 a Amazon RDS para Db2. Puede realizar una migración puntual de su base de datos Db2 desde entornos Linux, AIX o Windows a Amazon RDS para Db2. Para minimizar el tiempo de inactividad, puede realizar una migración con un tiempo de inactividad prácticamente nulo. Puede migrar sus datos guardándolos en Amazon S3 y cargándolos tabla por tabla en su base de datos de Db2. También puede realizar una migración sincrónica a través de la replicación o usar AWS Database Migration Service.

En el caso de las migraciones puntuales para bases de datos Db2 basadas en Linux, Amazon RDS solo admite copias de seguridad en línea y sin conexión. Amazon RDS no admite copias de seguridad Delta ni incrementales. En el caso de las migraciones con un tiempo de inactividad prácticamente nulo para bases de datos Db2 basadas en Linux, Amazon RDS requiere copias de seguridad en línea. Le recomendamos que utilice copias de seguridad en línea para las migraciones con un tiempo de inactividad prácticamente nulo y copias de seguridad sin conexión para las migraciones que puedan gestionar tiempo de inactividad.

Temas

- Migración de Linux a Linux de Amazon RDS para Db2
- Migración de Linux a Linux con un tiempo de inactividad prácticamente nulo para Amazon RDS para Db2
- Migración de forma sincrónica de Linux a Linux de Amazon RDS para Db2
- Migración de AIX o Windows a Linux de Amazon RDS para Db2

- Migración de datos de Db2 mediante Amazon S3 a Amazon RDS para Db2
- Migración a Amazon RDS para Db2 con AWS Database Migration Service (AWS DMS)

Migración de Linux a Linux de Amazon RDS para Db2

Con este enfoque de migración, realiza copias de seguridad de su base de datos de Db2 autoadministrada en un bucket de Amazon S3. Luego, utilice los procedimientos almacenados de Amazon RDS para restaurar la base de datos Db2 en una instancia de base de datos de Amazon RDS para Db2. Para obtener más información sobre cómo usar Amazon S3, consulte Integración de una instancia de base de datos de Amazon RDS para Db2 con Amazon S3.

La herramienta de copia de seguridad y restauración de RDS para Db2 sigue las rutas de actualización y las restricciones admitidas por IBM Db2. Para obtener más información, consulte Supported upgrade paths for Db2 servers y Upgrade restrictions for Db2 servers en la documentación de IBM Db2.

Temas

- Limitaciones y recomendaciones para el uso de la restauración nativa
- Copia de seguridad de la base de datos en Amazon S3
- Creación de un grupo de almacenamiento automático predeterminado
- Restauración de la base de datos Db2

Limitaciones y recomendaciones para el uso de la restauración nativa

Las siguientes limitaciones y recomendaciones se aplican al uso de la restauración nativa:

- Amazon RDS solo admite la migración de versiones de Db2 en las instalaciones que coincidan con las versiones admitidas de RDS para Db2. Para obtener más información acerca de las versiones admitidas, consulte Versiones secundarias de Db2 compatibles en Amazon RDS.
- Amazon RDS solo admite copias de seguridad en línea y sin conexión para la restauración nativa. Amazon RDS no admite copias de seguridad Delta ni incrementales.
- No se puede restaurar desde un bucket de Amazon S3 en una Región de AWS que no coincida con la región en la que está ubicada la instancia de base de datos de RDS para Db2.
- Amazon S3 limita el tamaño de los archivos que se cargan en un bucket de Amazon S3 a 5 TB. Si un archivo de copia de seguridad de una base de datos supera los 5 TB, divida el archivo de copia de seguridad en archivos más pequeños.

- Amazon RDS no admite rutinas externas no restringidas, ni restauraciones incrementales ni restauraciones Delta.
- No puede restaurar desde una base de datos de origen cifrada, pero puede restaurar a una instancia de base de datos de Amazon RDS cifrada.

Al restaurar la base de datos, la copia de seguridad se copia y, a continuación, se extrae en la instancia de base de datos de RDS para Db2. Le recomendamos que aprovisione un espacio de almacenamiento para la instancia de base de datos de RDS para Db2 que sea igual o mayor que la suma del tamaño de la copia de seguridad, más el tamaño de la base de datos original en el disco.

El tamaño máximo de la base de datos restaurada es el tamaño máximo admitido menos el tamaño de la copia de seguridad. Por ejemplo, si el tamaño máximo de la base de datos admitido es 64 TiB y el tamaño de la copia de seguridad es 30 TiB, el tamaño máximo de la base de datos restaurada será de 34 TiB.

```
64 TiB - 30 TiB = 34 TiB
```

Copia de seguridad de la base de datos en Amazon S3

Para hacer una copia de seguridad de la base de datos en Amazon S3, necesita los siguientes componentes AWS:

- Un bucket de Amazon S3 para almacenar los archivos de la copia de seguridad: cargue los archivos de copia de seguridad que desee migrar a Amazon RDS. Le recomendamos que utilice copias de seguridad sin conexión para las migraciones que puedan gestionar tiempo de inactividad. Si ya tiene un bucket de S3, puede utilizar ese bucket. Si no tiene un bucket de S3, consulte Crear un bucket en la Guía de usuario de Amazon S3.

  > **Note**
  >
  > Si su base de datos es grande y tardaría mucho en transferirse a un bucket de S3, puede solicitar un dispositivo AWS Snow Family y solicitar a AWS que realice la copia de seguridad. Tras copiar los archivos al dispositivo y devolverlos al equipo de Snow Family, el equipo transferirá las copias de seguridad de las imágenes a su bucket de S3. Para obtener más información, consulte la Documentación de AWS Snow Family.

- Un rol de IAM para acceder al bucket de S3: si ya tiene un rol de IAM, puede usar ese rol. Si no dispone de un rol, consulte Paso 2: crear un rol de IAM y asociar la política de IAM.

- Una política de IAM con relaciones de confianza y permisos asociados a su rol de IAM: para obtener más información, consulte Paso 1: Crear una política de IAM.
- El rol de IAM agregado a su instancia de base de datos de RDS para Db2: para obtener más información, consulte Paso 3: agregar su rol de IAM a su instancia de base de datos de RDS para Db2.

Creación de un grupo de almacenamiento automático predeterminado

La base de datos de origen debe tener un grupo de almacenamiento automático predeterminado. Si la base de datos no dispone de un grupo de almacenamiento automático predeterminado, debe crear uno.

Creación de un grupo de almacenamiento automático predeterminado

1. Conéctese a su base de datos de origen. En el siguiente ejemplo, sustituya *source_database* por el nombre de su base de datos.

```
db2 connect to source_database
```

2. Cree un grupo de almacenamiento automático y configúrelo como predeterminado. En el siguiente ejemplo, sustituya *storage_path* por la ruta absoluta en la que se encuentre el grupo de almacenamiento.

```
db2 "create stogroup IBMSTOGROUP ON storage_path set as default"
```

3. Finalice los procesos de backend.

```
db2 terminate
```

4. Desactive la base de datos y detenga todos los servicios de la base de datos. En el siguiente ejemplo, sustituya *source_database* por el nombre de la base de datos para la que ha creado el grupo de almacenamiento.

```
db2 deactivate db source_database
```

5. Haga una copia de seguridad de la base de datos. En el siguiente ejemplo, sustituya *source_database* por el nombre de la base de datos para la que ha creado el grupo de almacenamiento. Sustituya *file_system_path* por la ruta absoluta donde desee hacer la copia de seguridad de la base de datos.

```
db2 backup database source_database to file_system_path
```

Restauración de la base de datos Db2

Tras hacer una copia de seguridad de su base de datos en Amazon S3 y crear un grupo de almacenamiento automático, ya puede restaurar la base de datos Db2 a la instancia de base de datos de RDS para Db2.

Para restaurar la base de datos Db2 en la instancia de base de datos de RDS para Db2

1. Conéctese a una instancia de base de datos de RDS para Db2. Para obtener más información, consulte Conexión a la instancia de base de datos de Db2.
2. (Opcional) Para asegurarse de que la base de datos está configurada con los ajustes óptimos para la operación de restauración, puede llamar a the section called “rdsadmin.show_configuration” para comprobar los valores de `RESTORE_DATABASE_PARALLELISM` y `RESTORE_DATABASE_NUM_BUFFERS`. Llame a the section called “rdsadmin.set_configuration” para cambiar estos valores, según sea necesario. Establecer estos valores de forma explícita puede mejorar el rendimiento al restaurar bases de datos con grandes volúmenes de datos.
3. Restaure la base de datos mediante una llamada a `rdsadmin.restore_database`. Para obtener más información, consulte rdsadmin.restore_database.

Migración de Linux a Linux con un tiempo de inactividad prácticamente nulo para Amazon RDS para Db2

Con este enfoque de migración, migra una base de datos Db2 basada en Linux desde una base de datos Db2 autoadministrada (origen) hasta Amazon RDS para Db2. Este enfoque se traduce en una interrupción o tiempo de inactividad mínimos o nulos para la aplicación o los usuarios. Este enfoque hace copias de seguridad de la base de datos y las restaura mediante la reproducción de registros, lo que ayuda a evitar interrupciones en las operaciones en curso y proporciona una alta disponibilidad de la base de datos.

Para lograr una migración con un tiempo de inactividad prácticamente nulo, RDS para Db2 implementa la restauración con reproducción de registros. Este enfoque realiza una copia de seguridad de su base de datos Db2 autoadministrada basada en Linux y la restaura en el servidor de

RDS para Db2. Con los procedimientos almacenados de Amazon RDS, puede aplicar los registros de transacciones subsiguientes para actualizar la base de datos.

Temas

- Limitaciones y recomendaciones de migración con un tiempo de inactividad prácticamente nulo
- Copia de seguridad de la base de datos en Amazon S3
- Creación de un grupo de almacenamiento automático predeterminado
- Migración de su base de datos de Db2

Limitaciones y recomendaciones de migración con un tiempo de inactividad prácticamente nulo

Las siguientes limitaciones y recomendaciones se aplican al uso de la migración con un tiempo de inactividad casi nulo:

- Amazon RDS requiere una copia de seguridad en línea para las migraciones con un tiempo de inactividad prácticamente nulo. Esto se debe a que Amazon RDS mantiene su base de datos en un estado pendiente de avance de transacciones mientras carga los registros de transacciones archivados. Para obtener más información, consulte the section called “Migración de su base de datos de Db2”.
- No se puede restaurar desde un bucket de Amazon S3 en una Región de AWS que no coincida con la región en la que está ubicada la instancia de base de datos de RDS para Db2.
- Amazon S3 limita el tamaño de los archivos cargados en un bucket de S3 a 5 TB. Si un archivo de copia de seguridad de una base de datos supera los 5 TB, divida el archivo de copia de seguridad en archivos más pequeños.
- Amazon RDS no admite rutinas externas no restringidas, ni restauraciones incrementales ni restauraciones Delta.
- No puede restaurar desde una base de datos de origen cifrada, pero puede restaurar a una instancia de base de datos de Amazon RDS cifrada.

Al restaurar la base de datos, Amazon RDS copia la copia de seguridad y la extrae en su instancia de base de datos de RDS para Db2. Le recomendamos que aprovisione un espacio de almacenamiento para la instancia de base de datos de RDS para Db2 que sea igual o mayor que la suma del tamaño de la copia de seguridad, más el tamaño de la base de datos original en el disco.

El tamaño máximo de la base de datos restaurada es el tamaño máximo admitido menos el tamaño de la copia de seguridad. Por ejemplo, si el tamaño máximo de la base de datos admitido es 64 TiB

y el tamaño de la copia de seguridad es 30 TiB, el tamaño máximo de la base de datos restaurada será de 34 TiB.

```
64 TiB - 30 TiB = 34 TiB
```

Copia de seguridad de la base de datos en Amazon S3

Para hacer una copia de seguridad de la base de datos en Amazon S3, necesita los siguientes componentes AWS:

- Un bucket de Amazon S3 para almacenar los archivos de la copia de seguridad: cargue los archivos de copia de seguridad que desee migrar a Amazon RDS. Amazon RDS requiere una copia de seguridad en línea para las migraciones con un tiempo de inactividad prácticamente nulo. Si ya tiene un bucket de S3, puede utilizar ese bucket. Si no tiene un bucket de S3, consulte Crear un bucket en la Guía de usuario de Amazon S3.

  > **Note**
  >
  > Si su base de datos es grande y tardaría mucho en transferirse a un bucket de S3, puede solicitar un dispositivo AWS Snow Family y solicitar a AWS que realice la copia de seguridad. Tras copiar los archivos al dispositivo y devolverlos al equipo de Snow Family, el equipo transferirá las copias de seguridad de las imágenes a su bucket de S3. Para obtener más información, consulte la Documentación de AWS Snow Family.

- Un rol de IAM para acceder al bucket de S3: si ya tiene un rol AWS Identity and Access Management (de IAM), puede usar ese rol. Si no dispone de un rol, consulte Paso 2: crear un rol de IAM y asociar la política de IAM.
- Una política de IAM con relaciones de confianza y permisos asociados a su rol de IAM: para obtener más información, consulte Paso 1: Crear una política de IAM.
- El rol de IAM agregado a su instancia de base de datos de RDS para Db2: para obtener más información, consulte Paso 3: agregar su rol de IAM a su instancia de base de datos de RDS para Db2.

Creación de un grupo de almacenamiento automático predeterminado

La base de datos de origen debe tener un grupo de almacenamiento automático predeterminado. Si la base de datos no dispone de un grupo de almacenamiento automático predeterminado, debe crear uno.

Creación de un grupo de almacenamiento automático predeterminado

1. Conéctese a su base de datos de origen. En el siguiente ejemplo, sustituya *source_database* por el nombre de su base de datos.

```
db2 connect to source_database
```

2. Cree un grupo de almacenamiento automático y configúrelo como predeterminado. En el siguiente ejemplo, sustituya *storage_path* por la ruta absoluta en la que se encuentre el grupo de almacenamiento.

```
db2 "create stogroup IBMSTOGROUP ON storage_path set as default"
```

3. Finalice los procesos de backend.

```
db2 terminate
```

Migración de su base de datos de Db2

Tras hacer una copia de seguridad de su base de datos en Amazon S3 y crear un grupo de almacenamiento automático, estará listo para migrar la base de datos Db2 a la instancia de base de datos de RDS para Db2.

Para realizar una migración con un tiempo de inactividad prácticamente nulo

1. Realice una copia de seguridad en línea de la base de datos de origen. Para obtener más información, consulte Comando BACKUP DATABASE en la documentación de IBM Db2.
2. Copie la copia de seguridad de la base de datos en un bucket de Amazon S3. Para obtener más información acerca del uso de Amazon S3, consulte la Guía del usuario de Amazon Simple Storage Service.
3. Conéctese al servidor `rdsadmin` con el *master_username* y la *master_password* de su instancia de base de datos de RDS para Db2.

```
db2 connect to rdsadmin user master_username using master_password
```

4. (Opcional) Para asegurarse de que la base de datos está configurada con los ajustes óptimos para la operación de restauración, puede llamar a the section called “rdsadmin.show_configuration” para comprobar los valores de

`RESTORE_DATABASE_PARALLELISM` y `RESTORE_DATABASE_NUM_BUFFERS`. Llame a the section called “rdsadmin.set_configuration” para cambiar estos valores, según sea necesario. Establecer estos valores de forma explícita puede mejorar el rendimiento al restaurar bases de datos con grandes volúmenes de datos.

5. Para restaurar la copia de seguridad en el servidor de RDS para Db2, llame a `rdsadmin.restore_database`. Establece `backup_type` en `ONLINE`. Para obtener más información, consulte rdsadmin.restore_database.
6. Copie los registros de archivo desde el servidor de origen en el bucket de S3. Para obtener más información, consulte Archive logging en la documentación de IBM Db2.
7. Aplique los registros de archivo tantas veces como sea necesario llamando a `rdsadmin.rollforward_database`. Configure `complete_rollforward` en `FALSE` para mantener la base de datos en el estado `ROLL-FORWARD PENDING`. Para obtener más información, consulte rdsadmin.rollforward_database.
8. Después de aplicar todos los registros de archivo, llame a `rdsadmin.complete_rollforward` para poner la base de datos en línea. Para obtener más información, consulte rdsadmin.complete_rollforward.
9. Cambie las conexiones de las aplicaciones al servidor de RDS para Db2 actualizando los puntos de conexión de la aplicación para la base de datos o actualizando los puntos de conexión de DNS para redirigir el tráfico al servidor de RDS para Db2. También puede utilizar la característica de redireccionamiento automático de clientes de Db2 en su base de datos de Db2 autoadministrada con el punto de conexión de base de datos de RDS para Db2. Para obtener más información, consulte la Automatic client reroute description and setup en la documentación de IBM Db2.
10. (Opcional) Cierre la base de datos de origen.

Migración de forma sincrónica de Linux a Linux de Amazon RDS para Db2

Con este enfoque de migración, puede configurar la replicación entre su base de datos Db2 autoadministrada y su instancia de base de datos de Amazon RDS para Db2. Los cambios realizados en la base de datos autoadministrada se replican en la instancia de base de datos de RDS para Db2 prácticamente en tiempo real. Este enfoque puede proporcionar una disponibilidad continua y minimizar el tiempo de inactividad durante el proceso de migración.

Migración de AIX o Windows a Linux de Amazon RDS para Db2

Con este enfoque de migración, utiliza herramientas nativas de Db2 para hacer copias de seguridad de su base de datos de Db2 autoadministrada en un bucket de Amazon S3. Las herramientas nativas de Db2 incluyen la utilidad `export`, el comando del sistema `db2move` o el comando del sistema `db2look`. La base de datos Db2 puede administrarse de forma automática o en Amazon Elastic Compute Cloud (Amazon EC2). Puede trasladar datos desde su sistema AIX o Windows a su bucket de Amazon S3. A continuación, utilice un cliente de Db2 para cargar los datos directamente desde el bucket de S3 a su base de datos de Amazon RDS para Db2. El tiempo de inactividad depende del tamaño de la base de datos. Para obtener más información sobre cómo usar Amazon S3, consulte Integración de una instancia de base de datos de Amazon RDS para Db2 con Amazon S3.

Para migrar la base de datos Db2 a RDS para Db2

1. Prepárese para realizar una copia de seguridad de la base de datos. Configure una cantidad de almacenamiento suficiente para guardar la copia de seguridad en su sistema Db2 autoadministrado.
2. Haga una copia de seguridad de su base de datos.
    a. Ejecute el comando del sistema db2look para extraer el archivo de lenguaje de definición de datos (DDL) de todos los objetos.
    b. Ejecute la utilidad de exportación de Db2, el comando del sistema db2move o una instrucción CREATE EXTERNAL TABLE para descargar los datos de la tabla Db2 y almacenarlos en su sistema Db2.
3. Traslade su copia de seguridad a un bucket de Amazon S3. Para obtener más información, consulte Integración de una instancia de base de datos de Amazon RDS para Db2 con Amazon S3.

    > **Note**
    >
    > Si su base de datos es grande y tardaría mucho en transferirse a un bucket de S3, puede solicitar un dispositivo AWS Snow Family y solicitar a AWS que realice la copia de seguridad. Tras copiar los archivos al dispositivo y devolverlos al equipo de Snow Family, el equipo transferirá las copias de seguridad de las imágenes a su bucket de S3. Para obtener más información, consulte la Documentación de AWS Snow Family.

4. Utilice un cliente de Db2 para cargar los datos directamente desde el bucket de S3 a su base de datos de RDS para Db2. Para obtener más información, consulte Migración con Amazon S3.

Migración de datos de Db2 mediante Amazon S3 a Amazon RDS para Db2

Con este enfoque de migración, primero debe guardar datos desde una sola tabla en un archivo de datos que debe colocar en un bucket de Amazon S3. A continuación, utilice el comando LOAD para cargar los datos de ese archivo de datos en una tabla de la base de datos de Amazon RDS para Db2. Para obtener más información sobre cómo usar Amazon S3, consulte Integración de una instancia de base de datos de Amazon RDS para Db2 con Amazon S3.

Temas

- Guardado de datos en Amazon S3
- Carga de datos en tablas de RDS para Db2

Guardado de datos en Amazon S3

Para guardar datos de una sola tabla en Amazon S3, emplee una utilidad de base de datos para extraer los datos del sistema de administración de bases de datos (DBMS) en un archivo CSV. A continuación, cargue el archivo de datos en Amazon S3.

Para almacenar archivos de datos en Amazon S3, necesita los siguientes componentes de:AWS

- Un bucket de Amazon S3 para almacenar los archivos de copia de seguridad: si ya tiene un bucket de S3, puede utilizar ese bucket. Si no tiene un bucket de S3, consulte Crear un bucket en la Guía de usuario de Amazon S3.
- Un rol de IAM para acceder al bucket de S3: si ya tiene un rol de IAM, puede usar ese rol. Si no dispone de un rol, consulte Paso 2: crear un rol de IAM y asociar la política de IAM.
- Una política de IAM con relaciones de confianza y permisos asociados a su rol de IAM: para obtener más información, consulte Paso 1: Crear una política de IAM.
- El rol de IAM agregado a su instancia de base de datos de RDS para Db2: para obtener más información, consulte Paso 3: agregar su rol de IAM a su instancia de base de datos de RDS para Db2.

Carga de datos en tablas de RDS para Db2

Tras guardar los archivos de datos en Amazon S3, puede cargar los datos de estos archivos en tablas individuales de su instancia de base de datos de RDS para Db2.

Carga de datos de la tabla de Db2 en la tabla de base de datos de RDS para Db2

1. Conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

   ```
   db2 connect to rdsadmin user master_username using master_password
   ```

2. Catalogue un alias de acceso al almacenamiento que apunte al bucket de Amazon S3 donde se almacenan los archivos guardados. Anote el nombre de este alias para utilizarlo en el paso siguiente. Solo necesita realizar este paso una vez si tiene pensado cargar varias tablas de archivos de datos almacenados en el mismo bucket de Amazon S3.

   En el siguiente ejemplo, se cataloga un alias denominado *`my_s3_alias`* que concede acceso a un usuario llamado *`jorge_souza`* a un bucket denominado *`amzn-s3-demo-bucket`*.

   ```
   db2 "call rdsadmin.catalog_storage_access(?, 'my_s3_alias', 'amzn-s3-demo-bucket',
    'USER', 'jorge_souza')"
   ```

   Para obtener más información acerca de este procedimiento, consulte the section called “rdsadmin.catalog_storage_access”.

3. Ejecute el comando `LOAD` con el alias de acceso al almacenamiento que apunta a su bucket de Amazon S3.

   > **Note**
   >
   > Si el comando `LOAD` devuelve un error, es posible que deba crear un punto de conexión de puerta de enlace de VPC para Amazon S3 y agregar reglas de salida al grupo de seguridad. Para obtener más información, consulte the section called “Error de E/S de archivos”.

   En el siguiente ejemplo, se cargan los datos de un archivo de datos denominado *`my_s3_datafile.csv`* en una tabla denominada *`my_db2_table.`* En el ejemplo, se supone que el archivo de datos está en el bucket de Amazon S3 al que apunta el alias denominado *`my_s3_alias`*.

```
db2 "load from db2remote://my_s3_alias//my_s3_datafile.csv of DEL insert
 into my_db2_table";
```

En el siguiente ejemplo, se cargan LOB de un archivo de datos denominado *my_table1_export.ixf* en una tabla denominada *my_db2_table*. En el ejemplo, se supone que el archivo de datos está en el bucket de Amazon S3 al que apunta el alias denominado *my_s3_alias*.

```
db2 "call sysproc.admin_cmd('load from
 "db2remote://my_s3_alias//my_table1_export.ixf" of ixf
        lobs from "db2remote://my_s3_alias//" xml from "db2remote://my_s3_alias//"
        modified by lobsinfile implicitlyhiddeninclude identityoverride
 generatedoverride periodoverride transactionidoverride
        messages on server
        replace into "my_schema"."my_db2_table"
                                nonrecoverable
        indexing mode incremental allow no access')"
```

Repita este paso para cada archivo de datos del bucket de Amazon S3 que desee cargar en una tabla de la instancia de base de datos de RDS para Db2.

Para obtener más información sobre el comando LOAD, consulte LOAD command.

Migración a Amazon RDS para Db2 con AWS Database Migration Service (AWS DMS)

Puede usar AWS DMS para migraciones únicas y, a continuación, sincronizar desde Db2 en Linux, Unix (como AIX) y Windows a Amazon RDS para Db2. Para obtener más información, consulte ¿Qué es AWS Database Migration Service?.

Uso de herramientas nativas de Db2 para migrar datos de Db2 a Amazon RDS para Db2

Puede emplear varias herramientas, utilidades y comandos nativos de Db2 para trasladar datos directamente de una base de datos de Db2 a una base de datos de Amazon RDS para Db2. Para utilizar estas herramientas nativas de Db2, debe poder conectar su equipo cliente a una instancia de

base de datos de RDS para Db2. Para obtener más información, consulte Conexión de una máquina cliente a una instancia de base de datos de Amazon RDS para Db2.

> **Note**
>
> Otra forma de trasladar los datos consiste en guardarlos primero en un bucket de Amazon S3 y, a continuación, utilizar el comando `LOAD` para transferir esos datos a una tabla de base de datos de RDS para Db2. Este método proporciona el mejor rendimiento al migrar una gran cantidad de datos, gracias a la buena conectividad de red entre RDS para Db2 y S3. Para obtener más información, consulte the section called “Migración con Amazon S3”.

Nombre de la herramienta	Caso de uso	Limitaciones
db2look	Copia de metadatos desde una base de datos Db2 autoadministrada hasta una base de datos de Amazon RDS para Db2	• Debe modificar la sintaxis para crear grupos de búferes, crear espacios de tabla y crear roles para que coincida con la sintaxis utilizada por Procedimientos almacenados de RDS para Db2.
Comando de la IMPORT	Migración de tablas pequeñas y tablas con objetos grandes (LOB) de un equipo cliente a la instancia de base de datos RDS para Db2.	• Más lento que la utilidad `LOAD` debido a las operaciones de registro `INSERT` y `DELETE`. • Rendimiento deficiente con un ancho de banda de la red limitado.
Utilidad INGEST	Transmite continuamente datos desde archivos y canalizaciones sin objetos grandes (LOB) desde el equipo cliente hasta la instancia de base de datos de	• No se pueden transmiti r archivos de datos que contengan LOB. En su lugar, utilice el comando `IMPORT`.

Nombre de la herramienta	Caso de uso	Limitaciones
	RDS para Db2. Es compatible con las operaciones `INSERT` y `MERGE`.	• Se requiere conectividad entre la base de datos Db2 autoadministrada y la base de datos de RDS para Db2.
Comando de la INSERT	Copia de datos en tablas pequeñas desde una base de datos Db2 autoadministrada hasta una base de datos de Amazon RDS para Db2	• Se requiere conectividad entre la base de datos Db2 autoadministrada y la base de datos de RDS para Db2. • Rendimiento deficiente con un ancho de banda de la red limitado.
Comando de la LOAD CLIENT	Migración de tablas pequeñas sin objetos grandes (LOB) de un equipo cliente a la instancia de base de datos RDS para Db2.	• No se pueden migrar archivos de datos que contengan LOB. En su lugar, utilice el comando `IMPORT`. • Rendimiento deficiente con un ancho de banda de la red limitado.

Conexión de una máquina cliente a una instancia de base de datos de Amazon RDS para Db2

Para utilizar cualquiera de las herramientas nativas de Db2 para mover datos desde una base de datos de Db2 hasta una base de datos de Amazon RDS para Db2, primero debe conectar la máquina cliente a una instancia de base de datos de RDS para Db2.

La máquina cliente puede ser cualquiera de las siguientes:

- Una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en Linux, Windows o macOS. Esta instancia debe estar en la misma nube privada virtual (VPC) que la instancia de base de datos de RDS para Db2, AWS Cloud9 o AWS CloudShell.

- Una instancia Db2 autoadministrada en una instancia de Amazon EC2. Las instancias deben estar en la misma VPC.
- Una instancia Db2 autoadministrada en una instancia de Amazon EC2. Las instancias pueden estar en diferentes VPC si ha habilitado el emparejamiento de VPC. Para obtener más información, consulte Crear una conexión de emparejamiento de VPC en la Guía de emparejamiento de Amazon Virtual Private Cloud.
- Una máquina local que ejecute Linux, Windows o macOS en un entorno autoadministrado. Debe tener conectividad pública a RDS para Db2 o habilitar la conectividad VPN entre instancias de Db2 autoadministradas y AWS.

Para conectar su máquina cliente a su instancia de base de datos de RDS para Db2, inicie sesión en su máquina cliente con IBM Db2 Data Management Console. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS y IBM Db2 Data Management Console.

Puede usar AWS Database Migration Service (AWS DMS) para ejecutar consultas en la base de datos, ejecutar un plan de ejecución de SQL y monitorizar la base de datos. Para obtener más información, consulte ¿Qué es el Database Migration Service de AWS? en la Guía del usuario de AWS Database Migration Service.

Tras conectar correctamente la máquina cliente a la instancia de base de datos de RDS para Db2, estará preparado para utilizar cualquier herramienta nativa de Db2 para copiar datos. Para obtener más información, consulte Uso de herramientas nativas de Db2 para migrar datos de Db2 a Amazon RDS para Db2.

Copia de metadatos de bases de datos de Db2 a Amazon RDS para Db2 con db2look

`db2look` es una herramienta nativa de Db2 que extrae archivos, objetos, autorizaciones, configuraciones, WLM y diseños de bases de datos del lenguaje de definición de datos (DDL). Puede utilizar `db2look` para copiar metadatos de bases de datos desde una base de datos Db2 autoadministrada a una base de datos de Amazon RDS para Db2. Para obtener más información, consulte Mimicking databases using db2look en la documentación de IBM Db2.

Para copiar los metadatos de la base de datos

1. Ejecute la herramienta `db2look` en su sistema Db2 autoadministrado para extraer el archivo DDL. En el ejemplo siguiente, sustituya *`database_name`* por el nombre de su base de datos Db2.

```
db2look -d database_name -e -l -a -f -wlm -cor -createdb -printdbcfg -o db2look.sql
```

2. Si su máquina cliente tiene acceso a la base de datos de origen (Db2 autoadministrada) y a la instancia de base de datos de RDS para Db2, puede crear el archivo `db2look.sql` en la máquina cliente asociándolo directamente a la instancia remota. A continuación, catalogue la instancia de Db2 remota y autoadministrada.

   a. Catalogue el nodo. En el siguiente ejemplo, sustituya *dns_ip_address* y *port* por el nombre DNS o la dirección IP y el número de puerto de la base de datos Db2 autoadministrada.

   ```
   db2 catalog tcpip node srcnode REMOTE dns_ip_address server port
   ```

   b. Catalogue la base de datos. En el siguiente ejemplo, sustituya *source_database_name* y *source_database_alias* por el nombre de la base de datos Db2 autoadministrada y el alias que desee utilizar para esta base de datos.

   ```
   db2 catalog database source_database_name as source_database_alias at node
    srcnode \
       authentication server_encrypt
   ```

   c. Asocie a la base de datos de origen. En el siguiente ejemplo, sustituya *source_database_alias*, *user_id* y *user_password* por el alias que creó en el paso anterior y el ID de usuario y la contraseña de la base de datos Db2 autoadministrada.

   ```
   db2look -d source_database_alias -i user_id -w user_password -e -l -a -f -wlm \
       -cor -createdb -printdbcfg -o db2look.sql
   ```

3. Si no puede acceder a la base de datos Db2 autoadministrada de forma remota desde el equipo cliente, copie el archivo `db2look.sql` en el equipo cliente. A continuación, catalogue su instancia de base de datos de RDS para Db2.

   a. Catalogue el nodo. En el siguiente ejemplo, sustituya *dns_ip_address* y *port* por el nombre DNS o la dirección IP y el número de puerto de la instancia de la base de datos de RDS para Db2.

   ```
   db2 catalog tcpip node remnode REMOTE dns_ip_address server port
   ```

b. Catalogue la base de datos. En el siguiente ejemplo, sustituya *rds_database_name* y *rds_database_alias* por el nombre de la base de datos de RDS para Db2 y el alias que desee utilizar para esta base de datos.

```
db2 catalog database rds_database_name as rds_database_alias at node remnode \
    authentication server_encrypt
```

c. Catalogue la base de datos de administración que administra RDS para Db2. No puede utilizar esta base de datos para almacenar datos.

```
db2 catalog database rdsadmin as rdsadmin at node remnode authentication
 server_encrypt
```

4. Cree grupos de búferes y espacios de tablas. El administrador no tiene privilegios para crear grupos de búferes ni espacios de tabla. Sin embargo, puede utilizar los procedimientos almacenados de Amazon RDS para crearlos.

a. Busque los nombres y las definiciones de los grupos de búferes y los espacios de tabla en el archivo `db2look.sql`.

b. Conéctese a Amazon RDS con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *master_username* y *master_password* por su propia información.

```
db2 connect to rdsadmin user master_username using master_password
```

c. Cree un grupo de búferes mediante una llamada a `rdsadmin.create_bufferpool`. Para obtener más información, consulte rdsadmin.create_bufferpool.

```
db2 "call rdsadmin.create_bufferpool(
    'database_name',
    'buffer_pool_name',
    buffer_pool_size,
    'immediate',
    'automatic',
    page_size,
    number_block_pages,
    block_size)"
```

d. Cree un espacio de tablas llamando a `rdsadmin.create_tablespace`. Para obtener más información, consulte rdsadmin.create_tablespace.

```
db2 "call rdsadmin.create_tablespace(
    'database_name',
    'tablespace_name',
    'buffer_pool_name',
    tablespace_initial_size,
    tablespace_increase_size,
    'tablespace_type')"
```

e. Repita los pasos c o d para cada grupo de búferes o espacio de tabla adicional que quiera agregar.

f. Termine la conexión.

```
db2 terminate
```

5. Cree tablas y objetos.

a. Conéctese a su base de datos de RDS para Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *rds_database_name*, *master_username* y *master_password* por su propia información.

```
db2 connect to rds_database_name user master_username using master_password
```

b. Ejecute el archivo `db2look.sql`.

```
db2 -tvf db2look.sql
```

c. Termine la conexión.

```
db2 terminate
```

Importación de datos desde un equipo cliente a Amazon RDS para Db2 con el comando IMPORT

Puede utilizar el comando `IMPORT` desde un equipo cliente para importar los datos al servidor de Amazon RDS for Db2.

> **Important**
>
> El método del comando `IMPORT` es útil para migrar tablas pequeñas y tablas que incluyan objetos grandes (LOB). El comando `IMPORT` es más lento que la utilidad `LOAD` debido a las operaciones de registro `INSERT` y `DELETE`. Si el ancho de banda de la red entre el equipo cliente y RDS para Db2 es limitado, le recomendamos que utilice un enfoque de migración diferente. Para obtener más información, consulte Uso de herramientas nativas de Db2 para migrar datos de Db2 a Amazon RDS para Db2.

Para importar datos al servidor de RDS para Db2

1. Inicie sesión en su equipo cliente con IBM Db2 Data Management Console. Para obtener más información, consulte Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 Data Management Console.
2. Catalogue la base de datos de RDS para Db2 en el equipo cliente.

   a. Catalogue el nodo. En el siguiente ejemplo, sustituya *dns_ip_address* y *port* por el nombre DNS o la dirección IP y el número de puerto de la base de datos Db2 autoadministrada.

   ```
   db2 catalog tcpip node srcnode REMOTE dns_ip_address server port
   ```

   b. Catalogue la base de datos. En el siguiente ejemplo, sustituya *source_database_name* y *source_database_alias* por el nombre de la base de datos Db2 autoadministrada y el alias que desee utilizar para esta base de datos.

   ```
   db2 catalog database source_database_name as source_database_alias at node
    srcnode \
       authentication server_encrypt
   ```

3. Asocie a la base de datos de origen. En el siguiente ejemplo, sustituya *source_database_alias*, *user_id* y *user_password* por el alias que creó en el paso anterior y el ID de usuario y la contraseña de la base de datos Db2 autoadministrada.

   ```
   db2look -d source_database_alias -i user_id -w user_password -e -l -a -f -wlm \
       -cor -createdb -printdbcfg -o db2look.sql
   ```

4. Genere el archivo de datos mediante el comando `EXPORT` en su sistema Db2 autoadministrado. En el siguiente ejemplo, sustituya el *`directory`* por el directorio de la máquina cliente en el que se encuentra el archivo de datos. Sustituya *`file_name`* y *`table_name`* por el nombre del archivo de datos y el nombre de la tabla.

```
db2 "export to /directory/file_name.txt of del lobs to /directory/lobs/ \
    modified by coldel\| select * from table_name"
```

5. Conéctese a su base de datos de RDS para Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`rds_database_alias`*, *`master_username`* y *`master_password`* por su propia información.

```
db2 connect to rds_database_alias user master_username using master_password
```

6. Utilice el comando `IMPORT` para importar datos desde un archivo del equipo cliente a la base de datos remota de RDS para Db2. Para obtener más información, consulte Comando IMPORT en la documentación de IBM Db2. En el siguiente ejemplo, sustituya el *`directory`* y el *`file_name`* por el directorio del equipo cliente en el que se encuentra el archivo de datos y el nombre del archivo de datos. Sustituya *`SCHEMA_NAME`* y *`TABLE_NAME`* por los nombres de su esquema y su tabla.

```
db2 "IMPORT from /directory/file_name.tbl OF DEL LOBS FROM /directory/lobs/ \
    modified by coldel\| replace into SCHEMA_NAME.TABLE_NAME"
```

7. Termine la conexión.

```
db2 terminate
```

Importación de datos desde un equipo cliente a Amazon RDS para Db2 con el comando LOAD

Puede utilizar el comando `LOAD CLIENT` para cargar datos de un archivo en una máquina cliente en el servidor de RDS para Db2. Como no existe conectividad SSH con el servidor de RDS para Db2, puede usar el comando `LOAD CLIENT` en su servidor Db2 autoadministrado o en su equipo cliente de Db2.

> **Important**
>
> El método del comando `LOAD CLIENT` es útil para migrar tablas pequeñas. Si el ancho de banda de la red entre el cliente y RDS para Db2 es limitado, le recomendamos que utilice un enfoque de migración diferente. Para obtener más información, consulte Uso de herramientas nativas de Db2 para migrar datos de Db2 a Amazon RDS para Db2.
> Si el archivo de datos incluye referencias a nombres de archivos de objetos grandes, el comando `LOAD` no funcionará porque los objetos grandes (LOB) deben residir en el servidor de Db2. Si intenta cargar los LOB del equipo cliente al servidor de RDS para Db2, recibirá un error de tipo SQL3025N. En su lugar, utilice el comando IMPORT.

Para cargar datos en el servidor de RDS para Db2

1. Inicie sesión en su equipo cliente con IBM Db2 Data Management Console. Para obtener más información, consulte Conexión a la instancia de base de datos de Amazon RDS para Db2 con IBM Db2 Data Management Console.
2. Catalogue la base de datos de RDS para Db2 en el equipo cliente.

   a. Catalogue el nodo. En el siguiente ejemplo, sustituya *dns_ip_address* y *port* por el nombre DNS o la dirección IP y el número de puerto de la base de datos Db2 autoadministrada.

   ```
   db2 catalog tcpip node srcnode REMOTE dns_ip_address server port
   ```

   b. Catalogue la base de datos. En el siguiente ejemplo, sustituya *source_database_name* y *source_database_alias* por el nombre de la base de datos Db2 autoadministrada y el alias que desee utilizar para esta base de datos.

   ```
   db2 catalog database source_database_name as source_database_alias at node
    srcnode \
       authentication server_encrypt
   ```

3. Asocie a la base de datos de origen. En el siguiente ejemplo, sustituya *source_database_alias*, *user_id* y *user_password* por el alias que creó en el paso anterior y el ID de usuario y la contraseña de la base de datos Db2 autoadministrada.

   ```
   db2look -d source_database_alias -i user_id -w user_password -e -l -a -f -wlm \
   ```

```
    -cor -createdb -printdbcfg -o db2look.sql
```

4. Genere el archivo de datos mediante el comando EXPORT en su sistema Db2 autoadministrado. En el siguiente ejemplo, sustituya el *directory* por el directorio de la máquina cliente en el que se encuentra el archivo de datos. Sustituya *file_name* y *TABLE_NAME* por el nombre del archivo de datos y el nombre de la tabla.

```
db2 "export to /directory/file_name.txt of del modified by coldel\| \
    select * from TPCH.TABLE_NAME"
```

5. Conéctese a su base de datos de RDS para Db2 con el nombre de usuario y la contraseña maestros de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *rds_database_alias*, *master_username* y *master_password* por su propia información.

```
db2 connect to rds_database_alias user master_username using master_password
```

6. Utilice el comando LOAD para cargar datos desde un archivo del equipo cliente a la base de datos remota de RDS para Db2. Para obtener más información, consulte Comando LOAD en la documentación de IBM Db2. En el siguiente ejemplo, sustituya el *directory* por el directorio de la máquina cliente en el que se encuentra el archivo de datos. Sustituya *file_name* y *TABLE_NAME* por el nombre del archivo de datos y el nombre de la tabla.

```
db2 "LOAD CLIENT from /directory/file_name.txt \
    modified by coldel\| replace into TPCH.TABLE_NAME \
    nonrecoverable without prompting"
```

7. Termine la conexión.

```
db2 terminate
```

Importación de datos desde Db2 a Amazon RDS para Db2 con el comando INSERT

Puede utilizar el comando INSERT desde un servidor Db2 autoadministrado para insertar los datos en una base de datos de Amazon RDS para Db2. Con este enfoque de migración, se utiliza un alias para la instancia de base de datos remota de RDS para Db2. Su base de datos Db2 autoadministrada (origen) debe poder conectarse a la base de datos de RDS para Db2 (destino).

> **Important**
>
> El método del comando `INSERT` es útil para migrar tablas pequeñas. Si el ancho de banda de la red entre la base de datos de Db2 autoadministrada y la base de datos de RDS para Db2 es limitado, le recomendamos que utilice un enfoque de migración diferente. Para obtener más información, consulte Uso de herramientas nativas de Db2 para migrar datos de Db2 a Amazon RDS para Db2.

Para copiar datos desde una base de datos Db2 autoadministrada hasta una base de datos de Amazon RDS para Db2

1. Catalogue la instancia de base de datos de RDS para Db2 en la instancia de Db2 autoadministrada.

   a. Catalogue el nodo. En el siguiente ejemplo, sustituya *dns_ip_address* y *port* por el nombre DNS o la dirección IP y el número de puerto de la base de datos Db2 autoadministrada.

   ```
   db2 catalog tcpip node remnode REMOTE dns_ip_address SERVER port
   ```

   b. Catalogue la base de datos. En el siguiente ejemplo, sustituya *rds_database_name* por el nombre de la base de datos de la instancia de base de datos de RDS para Db2.

   ```
   db2 catalog database rds_database_name as remdb at node remnode \
       authentication server_encrypt
   ```

2. Habilite la federación en la instancia de Db2 autoadministrada. En el siguiente ejemplo, sustituya *source_database_name* por el nombre de la base de datos de la instancia de Db2 autoadministrada.

   ```
   db2 update dbm cfg using FEDERATED YES source_database_name
   ```

3. Cree tablas en la instancia de base de datos de RDS para Db2.

   a. Catalogue el nodo. En el siguiente ejemplo, sustituya *dns_ip_address* y *port* por el nombre DNS o la dirección IP y el número de puerto de la base de datos Db2 autoadministrada.

```
db2 catalog tcpip node srcnode REMOTE dns_ip_address server port
```

b. Catalogue la base de datos. En el siguiente ejemplo, sustituya *source_database_name* y *source_database_alias* por el nombre de la base de datos Db2 autoadministrada y el alias que desee utilizar para esta base de datos.

```
db2 catalog database source_database_name as source_database_alias at node
 srcnode \
    authentication server_encrypt
```

4. Asocie a la base de datos de origen. En el siguiente ejemplo, sustituya *source_database_alias*, *user_id* y *user_password* por el alias que creó en el paso anterior y el ID de usuario y la contraseña de la base de datos Db2 autoadministrada.

```
db2look -d source_database_alias -i user_id -w user_password -e -l -a -f -wlm \
    -cor -createdb -printdbcfg -o db2look.sql
```

5. Configure la federación y cree un alias para la tabla de bases de datos de RDS para Db2 en la instancia de Db2 autoadministrada.

a. Conexión a la base de datos local. En el siguiente ejemplo, sustituya *source_database_name* por el nombre de la base de datos de su instancia de Db2 autoadministrada.

```
db2 connect to source_database_name
```

b. Cree un encapsulador para acceder a los orígenes de datos de Db2.

```
db2 create wrapper drda
```

c. Defina un origen de datos en una base de datos federada. En el siguiente ejemplo, sustituya *admin* y *admin_password* por las credenciales de su instancia de Db2 autoadministrada. Sustituya *rds_database_name* por el nombre de la base de datos de la instancia de base de datos de RDS para Db2.

```
db2 "create server rdsdb2 type DB2/LUW version '11.5.9.0' \
    wrapper drda authorization "admin" password "admin_password" \
    options( dbname 'rds_database_name', node 'remnode')"
```

d. Asigne los usuarios en las dos bases de datos. En el siguiente ejemplo, sustituya *master_username* y *master_password* por las credenciales de su instancia de RDS para Db2 autoadministrada.

```
db2 "create user mapping for user server rdsdb2 \
    options (REMOTE_AUTHID 'master_username', REMOTE_PASSWORD
 'master_password')"
```

e. Compruebe la conexión al servidor de RDS para Db2.

```
db2 set passthru rdsdb2
```

f. Cree un alias para la tabla en la base de datos remota de RDS para Db2. En el siguiente ejemplo, sustituya *NICKNAME* y *TABLE_NAME* por un alias para la tabla y el nombre de la tabla.

```
db2 create nickname REMOTE.NICKNAME for RDSDB2.TABLE_NAME.NICKNAME
```

6. Inserte los datos en la tabla de la base de datos remota de RDS para Db2. Utilice el apodo en una instrucción `select` de la tabla local de la instancia de Db2 autoadministrada. En el siguiente ejemplo, sustituya *NICKNAME* y *TABLE_NAME* por un alias para la tabla y el nombre de la tabla.

```
db2 "INSERT into REMOTE.NICKNAME select * from RDS2DB2.TABLE_NAME.NICKNAME"
```

Importación de datos desde Db2 a Amazon RDS para Db2 con la utilidad INGEST

Puede utilizar la utilidad `INGEST` para transmitir datos de forma continua desde archivos y canalizaciones de un equipo cliente a una instancia de base de datos de Amazon RDS para Db2 de destino. La utilidad `INGEST` es compatible con las operaciones `INSERT` y `MERGE`. Para obtener más información, consulte Ingest utility en la documentación de IBM Db2.

Como la utilidad `INGEST` admite alias, puede utilizarla para transferir datos de una base de datos de Db2 autoadministrada a una base de datos de RDS para Db2. Este enfoque funciona siempre que exista conectividad de red entre las dos bases de datos.

> **Important**
>
> La utilidad `INGEST` no admite objetos grandes (LOB). En su lugar, utilice el comando `IMPORT`.

Para utilizar la característica `RESTARTABLE` de la utilidad `INGEST`, ejecute el siguiente comando en la base de datos de RDS para Db2.

```
db2 "call sysproc.sysinstallobjects('INGEST','C',NULL,NULL)"
```

Federación de Amazon RDS para Db2

Puede usar su base de datos de Amazon RDS para Db2 como base de datos federada. Tras configurar la federación de RDS para Db2, podrá acceder a los datos de varias bases de datos de su base de datos de RDS para Db2 y consultarlos. La federación evita tener que migrar datos a su base de datos de RDS para Db2 o consolidar los datos en una única base de datos.

Al utilizar la base de datos de RDS para Db2 como base de datos federada, puede seguir accediendo a todas las características de RDS para Db2 y aprovechar varios Servicios de AWS, al mismo tiempo que mantiene los datos en distintas bases de datos. Puede configurar tanto una federación homogénea, que conecta diferentes bases de datos del mismo tipo, como una federación heterogénea, que conecta diferentes bases de datos de diferentes tipos.

Primero debe conectar la base de datos de Db2 de RDS para Db2 a bases de datos remotas. A continuación, puede ejecutar consultas en todas las bases de datos conectadas. Por ejemplo, puede ejecutar una instrucción JOIN de SQL que combine las tablas de su base de datos de RDS para Db2 con las tablas de una base de datos remota de Db2 en z/OS.

Temas

- Federación homogénea
- Federación heterogénea

Federación homogénea

Puede configurar una federación homogénea entre su base de datos de RDS para Db2 y la siguiente familia de productos de Db2:

- Db2 para Linux, UNIX y Windows (LUW)
- Db2 iSeries
- Db2 para z/OS

La federación homogénea de RDS para Db2 no admite las siguientes acciones:

- Ejecución de comandos `CATALOG` para configurar un directorio de nodos y una base de datos remota en una base de datos de host de RDS para Db2
- Configuración del equilibrio de carga de trabajo (WLB) al federarse a Db2 en z/OS

- Configuración del archivo de configuración del controlador del servidor de datos de IBM (`db2dsdriver.cfg`)

La federación homogénea de RDS para Db2 tiene los siguientes requisitos:

- Debe crear el contenedor DRDA en el modo `UNFENCED`. Si no lo hace, la federación no funcionará en RDS para Db2.
- Debe permitir que el tráfico entrante y saliente de su base de datos de host de RDS para Db2 llegue a sus bases de datos de host remotas. Para obtener más información, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

Temas

- Paso 1: creación de un contenedor de DRDA y un servidor federado
- Paso 2: creación de un mapeo de usuario
- Paso 3: comprobación de la conexión

Paso 1: creación de un contenedor de DRDA y un servidor federado

Para una federación homogénea, cree un contenedor DRDA y un servidor federado. La conexión al host remoto utiliza `HOST`, `PORT` y `DBNAME`.

Elija uno de los siguientes métodos según el tipo de base de datos de Db2 remota:

- Base de datos Db2 para Linux, UNIX y Windows (LUX): ejecute los siguientes comandos de SQL. En el siguiente ejemplo, sustituya *`server_name`* por el nombre del servidor que utilizará para la federación. Sustituya *`db2_version`* por la versión de la base de datos de Db2 remota. Sustituya *`username`* y *`password`* por las credenciales de la base de datos remota de Db2 a la que desee conectarse. Sustituya *`db_name`*, *`dns_name`* y *`port`* por los valores correspondientes para la base de datos de Db2 remota a la que desee conectarse.

```
create wrapper drda options(DB2_FENCED 'N');
create server server_name type DB2/LUW wrapper drda version 'db2_version'
 authorization "master_username" password "master_password" options (add DBNAME
 'db_name',add HOST 'dns_name',add PORT 'port');
```

  Ejemplo

```
create wrapper drda options(DB2_FENCED 'N');
create server SERVER1 type DB2/LUW wrapper drda version '11.5' authorization
 "sysuser" password "******" options (add DBNAME 'TESTDB2',add HOST
 'ip-123-45-67-899.us-west-1.compute.internal',add PORT '25010');
```

- Db2 iSeries: ejecute los siguientes comandos de SQL. En el siguiente ejemplo, sustituya *wrapper_name* y *library_name* por un nombre para el contenedor DRDA y el archivo de biblioteca del contenedor. Sustituya *server_name* por el nombre del servidor que usará para la federación. Sustituya *db2_version* por la versión de la base de datos de Db2 remota. Sustituya *username* y *password* por las credenciales de la base de datos remota de Db2 a la que desee conectarse. Sustituya *dns_name*, *port* y *db_name* por los valores correspondientes para la base de datos de Db2 remota a la que desee conectarse.

  ```
  create wrapper wrapper_name library 'library name' options(DB2_FENCED 'N');
  create server server_name type db2/mvs version db2_version wrapper wrapper_name
   authorization "sername" password "password" options (HOST 'dns_name', PORT 'port',
   DBNAME 'db_name');
  ```

  Ejemplo

  ```
  create wrapper WRAPPER1 library 'libdb2drda.so' options(DB2_FENCED 'N');
  create server SERVER1 type db2/mvs version 11 wrapper WRAPPER1 authorization
   "sysuser" password "******" options (HOST 'test1.123.com', PORT '446', DBNAME
   'STLEC1');
  ```

- Db2 para z/OS: ejecute los siguientes comandos de SQL. En el siguiente ejemplo, sustituya *wrapper_name* y *library_name* por un nombre para el contenedor DRDA y el archivo de biblioteca del contenedor. Sustituya *server_name* por el nombre del servidor que usará para la federación. Sustituya *db2_version* por la versión de la base de datos de Db2 remota. Sustituya *username* y *password* por las credenciales de la base de datos remota de Db2 a la que desee conectarse. Sustituya *dns_name*, *port* y *db_name* por los valores correspondientes para la base de datos de Db2 remota a la que desee conectarse.

  ```
  create wrapper wrapper_name library 'library_name' options(DB2_FENCED 'N');
  create server server_name type db2/mvs version db2_version wrapper wrapper_name
   authorization "username" password "password" options (HOST 'dns_name', PORT 'port',
   DBNAME 'db_name');
  ```

Ejemplo

```
create wrapper WRAPPER1 library 'libdb2drda.so' OPTIONS(DB2_FENCED 'N');
create server SERVER1 type db2/mvs version 11 wrapper WRAPPER1 authorization
 "sysuser" password "******" options (HOST 'test1.123.com', PORT '446', DBNAME
 'STLEC1');
```

Paso 2: creación de un mapeo de usuario

Cree un mapeo de usuario para asociar su servidor federado a su servidor de origen de datos ejecutando el siguiente comando de SQL. En el siguiente ejemplo, sustituya *server_name* por el nombre del servidor remoto en el que desee realizar las operaciones. Este es el servidor que creó en el paso 1. Sustituya *username* y *password* por sus credenciales para este servidor remoto.

```
create user mapping for user server server_name options (REMOTE_AUTHID 'username',
 REMOTE_PASSWORD 'password');
```

Para obtener más información, consulte User mappings en la documentación de IBM Db2.

Paso 3: comprobación de la conexión

Compruebe la conexión para confirmar que la configuración de la federación se ha realizado correctamente. Abra una sesión para enviar comandos de SQL nativos a su origen de datos remoto mediante el comando SET PASSTHRU y, a continuación, cree una tabla en el servidor de datos remoto.

1. Abra y cierre una sesión para enviar SQL a un origen de datos. En el siguiente ejemplo, sustituya *server_name* por el nombre del servidor que creó para la federación en el paso 1.

   ```
   set passthru server_name;
   ```

2. Cree una nueva tabla. En el siguiente ejemplo, sustituya *column_name*, *data_type* y *value* por los elementos correspondientes de la tabla.

   ```
   create table table_name
    ( column_name data_type(value), column_name data_type(value);
   ```

Para obtener más información, consulte CREATE TABLE statement en la documentación de IBM Db2.

3. Cree un índice, inserte los valores de las filas en la tabla y restablezca la conexión. Al restablecer la conexión, se pierde la conexión, pero se conservan los procesos de backend. En el siguiente ejemplo, sustituya *index_name*, *table_name*, *column_name* y *columnx_value* por su información.

```
create index index_name on table_name(column_name);
insert into table_name values(column1_value,column2_value,column3_value);
insert into table_name values(column1_value,column2_value,column3_value);
set passthru reset;

connect reset;
```

4. Conéctese a su base de datos de Db2 remota, cree un apodo para su servidor remoto y realice operaciones. Cuando haya terminado de acceder a los datos de la base de datos remota de Db2, restablezca y, a continuación, finalice la conexión. En el ejemplo siguiente, sustituya *database_name* por el nombre de su base de datos de Db2 remota. Sustituya *nickname* por un nombre. Sustituya *server_name* y *table_name* por el nombre del servidor remoto y la tabla de ese servidor en los que quiera realizar operaciones. Sustituya *username* por la información de su servidor remoto. Sustituya *sql_command* por la operación que se va a realizar en el servidor remoto.

```
connect to database_name;
create nickname nickname for server_name."username"."table_name";
select sql_command from nickname;
connect reset;
terminate;
```

Ejemplo

El siguiente ejemplo crea una sesión de transferencia para permitir las operaciones en el servidor federado de `testdb10`.

Después, crea la tabla `t1` con tres columnas con distintos tipos de datos.

A continuación, el ejemplo crea el índice `i1_t1` en tres columnas de la tabla `t1`. Después, inserta dos filas con los valores de estas tres columnas y, a continuación, se desconecta.

Por último, el ejemplo se conecta a la base de datos remota de Db2 `testdb2` y se crea un apodo para la tabla `t1` en el servidor federado `testdb10`. Crea el apodo con el nombre de usuario `TESTUSER` de ese origen de datos. Un comando de SQL genera todos los datos de la tabla `t1`. El ejemplo desconecta y finaliza la sesión.

```
set passthru testdbl0;

create table t1 ( c1 decimal(13,0), c2 char(200), c3 int);

create index i1_t1 on t1(c3);
insert into t1 values(1,'Test',1);
insert into t1 values(2,'Test 2',2);
connect reset;

connect to testdb2;
create nickname remote_t1 for testdbl0."TESTUSER"."T1";
select * from remote_t1;
connect reset;
terminate;
```

Federación heterogénea

Puede configurar una federación heterogénea entre la base de datos de RDS para Db2 y otros orígenes de datos, como Oracle y Microsoft SQL Server. Para obtener una lista completa de los orígenes de datos compatibles con Db2 LUW, consulte Data Source Support Matrix of Federation Bundled in Db2 LUW V11.5 el sitio de soporte de IBM.

La federación heterogénea de RDS para Db2 no admite los siguientes elementos:

- Contenedores nativos para los demás orígenes de datos
- Contenedores JDBC para los demás orígenes de datos
- Federación a orígenes de datos de Sybase, Informix y Teradata, porque estos orígenes de datos requieren la instalación del software cliente en RDS para Db2

La federación heterogénea de RDS para Db2 tiene los siguientes requisitos:

- RDS para Db2 solo admite el método de contenedor de ODBC.

- Si crea una definición explícita de un contenedor, debe establecer la opción `DB2_FENCED` en `'N'`. Para obtener una lista de las opciones de contenedor válidas para ODBC, consulte ODBC options en la documentación de IBM Db2.
- Debe permitir que el tráfico entrante y saliente de su base de datos de host de RDS para Db2 llegue a su base de datos de host remota. Para obtener más información, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

Para obtener información sobre la federación a Oracle, consulte How to query Oracle by using Db2 Federation and the ODBC driver? en el sitio de soporte de IBM.

Para obtener información sobre los orígenes de datos compatibles con la federación, consulte Data Source Support Matrix of Federation Bundled in Db2 LUW V11.5 el sitio de soporte de IBM.

Temas

- Paso 1: creación de un contenedor de ODBC
- Paso 2: creación de un servidor federado
- Paso 3: creación de un mapeo de usuario
- Paso 4: comprobación de la conexión

Paso 1: creación de un contenedor de ODBC

Cree un contenedor ejecutando el siguiente comando:

```
db2 "create wrapper odbc options( module '/home/rdsdb/sqllib/federation/odbc/lib/
libodbc.so')"
```

Paso 2: creación de un servidor federado

Cree un servidor federado ejecutando el siguiente comando. En el siguiente ejemplo, sustituya *`server_name`* por el nombre del servidor que utilizará para la federación. Sustituya *`wrapper_type`* por el contenedor apropiado. Sustituya *`db_version`* por la versión de la base de datos remota. Sustituya *`dns_name`*, *`port`* y *`db_name`* por los valores correspondientes para la base de datos remota a la que desee conectarse.

```
db2 "create server server_name type wrapper_type version db_version options (HOST
 'dns_name', PORT 'port', SERVICE_NAME 'service_name')“
```

Para obtener información sobre los tipos de contenedores, consulte Data Source Support Matrix of Federation Bundled in Db2 LUW V11.5 el sitio de soporte de IBM.

Ejemplo

El siguiente ejemplo crea un servidor federado para una base de datos de Oracle remota.

```
db2 "create server server1 type oracle_odbc version 12.1 options (HOST
 'test1.amazon.com', PORT '1521', SERVICE_NAME 'pdborcl.amazon.com')“
```

Paso 3: creación de un mapeo de usuario

Cree un mapeo de usuario para asociar su servidor federado a su servidor de origen de datos ejecutando el siguiente comando de SQL. En el siguiente ejemplo, sustituya *server_name* por el nombre del servidor remoto en el que desee realizar las operaciones. Este es el servidor que creó en el paso 2. Sustituya *username* y *password* por sus credenciales para este servidor remoto.

```
create user mapping for user server server_name options (REMOTE_AUTHID 'username',
 REMOTE_PASSWORD 'password');
```

Para obtener más información, consulte User mappings en la documentación de IBM Db2.

Paso 4: comprobación de la conexión

Compruebe la conexión para confirmar que la configuración de la federación se ha realizado correctamente. Abra una sesión para enviar comandos de SQL nativos a su origen de datos remoto mediante el comando SET PASSTHRU y, a continuación, cree una tabla en el servidor de datos remoto.

1. Abra y cierre una sesión para enviar SQL a un origen de datos. En el siguiente ejemplo, sustituya *server_name* por el nombre del servidor que creó para la federación en el paso 2.

   ```
   set passthru server_name;
   ```

2. Cree una nueva tabla. En el siguiente ejemplo, sustituya *column_name*, *data_type* y *value* por los elementos correspondientes de la tabla.

   ```
   create table table_name
    ( column_name data_type(value), column_name data_type(value);
   ```

Para obtener más información, consulte CREATE TABLE statement en la documentación de IBM Db2.

3. Cree un índice, inserte los valores de las filas en la tabla y restablezca la conexión. Al restablecer la conexión, se pierde la conexión, pero se conservan los procesos de backend. En el siguiente ejemplo, sustituya *index_name*, *table_name*, *column_name* y *columnx_value* por su información.

```
create index index_name on table_name(column_name);
insert into table_name values(column1_value,column2_value,column3_value);
insert into table_name values(column1_value,column2_value,column3_value);
set passthru reset;

connect reset;
```

4. Conéctese a su base de datos de Db2 remota, cree un apodo para su servidor remoto y realice operaciones. Cuando haya terminado de acceder a los datos de la base de datos remota de Db2, restablezca y, a continuación, finalice la conexión. En el ejemplo siguiente, sustituya *database_name* por el nombre de su base de datos de Db2 remota. Sustituya *nickname* por un nombre. Sustituya *server_name* y *table_name* por el nombre del servidor remoto y la tabla de ese servidor en los que quiera realizar operaciones. Sustituya *username* por la información de su servidor remoto. Sustituya *sql_command* por la operación que se va a realizar en el servidor remoto.

```
connect to database_name;
create nickname nickname for server_name."username"."table_name";
select sql_command from nickname;
connect reset;
terminate;
```

Ejemplo

El siguiente ejemplo crea una sesión de transferencia para permitir las operaciones en el servidor federado de `testdb10`.

Después, crea la tabla `t1` con tres columnas con distintos tipos de datos.

A continuación, el ejemplo crea el índice `i1_t1` en tres columnas de la tabla `t1`. Después, inserta dos filas con los valores de estas tres columnas y, a continuación, se desconecta.

Por último, el ejemplo se conecta a la base de datos remota de Db2 `testdb2` y se crea un apodo para la tabla `t1` en el servidor federado `testdb10`. Crea el apodo con el nombre de usuario TESTUSER de ese origen de datos. Un comando de SQL genera todos los datos de la tabla `t1`. El ejemplo desconecta y finaliza la sesión.

```
set passthru testdbl0;

create table t1 ( c1 decimal(13,0), c2 char(200), c3 int);

create index i1_t1 on t1(c3);
insert into t1 values(1,'Test',1);
insert into t1 values(2,'Test 2',2);
connect reset;

connect to testdb2;
create nickname remote_t1 for testdbl0."TESTUSER"."T1";
select * from remote_t1;
connect reset;
terminate;
```

Trabajo con las réplicas de Amazon RDS para Db2

Para configurar la replicación entre instancias de base de datos de RDS para Db2, puede crear bases de datos de réplica. Para obtener un resumen de las diferencias entre las réplicas de RDS para Db2 y otros motores de base de datos, consulte Diferencias entre réplicas de lectura para motores de base de datos.

Una base de datos de réplica de Db2 es una copia física de la base de datos principal. Una réplica de Db2 en modo de espera se denomina réplica en espera. Db2 no permite lecturas ni escrituras en una réplica, pero puede promocionar una réplica para que sea de escritura. La réplica promocionada tiene los datos replicados hasta el momento en que se realizó la solicitud para promocionarla. RDS para Db2 utiliza la recuperación ante desastres de alta disponibilidad (HADR) de Db2 para la replicación. Para obtener más información, consulte High availability disaster recovery (HADR) en la documentación de IBM Db2.

Réplicas en espera

Al crear o modificar una réplica de Db2, puede colocarla en modo en espera. Para las réplicas en espera, la variable de entorno `DB2_HADR_ROS` de Db2 se establece en `OFF` para que la base de datos de la réplica no acepte conexiones de usuarios. El uso principal de las réplicas en espera es la recuperación ante desastres entre regiones.

Una réplica en espera no puede servir una carga de trabajo de solo lectura. La réplica en espera no tiene registros de archivo.

Puede crear hasta tres réplicas a partir de una instancia de base de datos de origen.

Activaciones de base de datos

HADR de Db2 se configura en la base de datos. Después de crear réplicas, HADR se establece para todas las bases de datos Db2, incluida `rdsadmin`, que RDS administra de forma completa. Antes de crear réplicas de Db2, debe activar explícitamente todas las bases de datos. De lo contrario, no se realizará la creación de réplicas y Amazon RDS emitirá un evento. Después de que una instancia de base de datos tenga una o más réplicas, no puede activar ni desactivar ninguna base de datos en la instancia de base de datos mediante los procedimientos almacenados `rdsadmin.activate_database` o `rdsadmin.deactivate_database`. No obstante, puede llamar al procedimiento almacenado `rdsadmin.reactivate_database` para reactivar las bases de datos. Para obtener más información, consulte Administración de bases de datos.

Configuraciones de HADR

Puede ver todas las configuraciones de HADR para una base de datos si se conecta a ella y ejecuta `db2 get db cfg`.

Retención de registros de archivo

Amazon RDS purga los registros de una instancia de base de datos principal después de que se cumplan las siguientes condiciones:

- Los registros tienen al menos dos horas de antigüedad.
- Ha transcurrido la configuración de horas de retención de registros de archivo.
- Los registros de archivo se han replicado correctamente en todas las instancias de base de datos de réplica. Esta condición se aplica tanto a instancias de base de datos en la misma Región de AWS como a instancias de base de datos entre regiones.

Para obtener información acerca de cómo configurar las horas de retención del registro de archivo, consulte rdsadmin.set_archive_log_retention.

Amazon RDS comprueba y limpia cada base de datos individualmente. Si una base de datos pierde la conexión HADR o si la información sobre la conexión no está disponible, Amazon RDS omite la base de datos y no purga los registros de archivo.

Interrupciones durante la replicación de Db2

Cuando crea una réplica, Amazon RDS toma una instantánea de base de datos de la instancia de base de datos de origen y comienza la replicación. Cuando comienza la operación de instantánea de base de datos, la instancia de base de datos de origen experimenta una suspensión de E/S muy breve. La suspensión de E/S suele durar un segundo. No obstante, si la instancia de base de datos de origen es una implementación multi-AZ, la instancia de base de datos de origen no experimenta ninguna suspensión de E/S. Esto se debe a que, con las implementaciones multi-AZ, la instantánea se toma de la instancia de base de datos secundaria.

La instantánea de base de datos se convierte en la réplica de Db2. Amazon RDS establece los parámetros y permisos necesarios para la base de datos de origen y la réplica sin interrumpir el servicio. Del mismo modo, si elimina una réplica, no se produce ninguna interrupción.

Requisitos y consideraciones sobre réplicas de RDS para Db2

Antes de crear una réplica de Db2, familiarícese con los siguientes requisitos y consideraciones.

Requisitos de versión y licencia para réplicas de RDS para Db2

Antes de crear una réplica de RDS para Db2, consulte la siguiente información:

- Tanto la edición avanzada (AE) de Db2 como la estándar (SE) pueden crear réplicas en espera tanto para el modelo “traiga su propia licencia (BYOL)” como para el modelo de licencia Db2 a través del modelo AWS Marketplace.
- Debe especificar un grupo de parámetros personalizados para la réplica de lectura. Para las réplicas que utilizan el modelo BYOL, este grupo de parámetros personalizado debe incluir IBM Site ID e IBM Customer ID. Puede especificar este grupo de parámetros personalizado para la réplica de lectura mediante la AWS Management Console, la AWS CLI o la API de RDS. Para obtener más información, consulte ID de IBM para Traiga su propia licencia para Db2.
- Para las réplicas en espera, el recuento de vCPU es dos, independientemente del tamaño de la instancia de base de datos. Los siguientes elementos describen las diferencias entre los tipos de licencia de RDS para Db2:
  - Para el modelo BYOL, las configuraciones de AWS License Manager muestran que las instancias de base de datos de RDS para Db2 utilizan dos vCPU.
  - Para la licencia de Db2 a través del modelo AWS Marketplace, las facturas reflejan los costos de licencia para dos vCPU.
- Todas las versiones 11.5 de Db2 admiten instancias de base de datos de réplica. Las réplicas de Db2 admiten actualizaciones de versión secundaria.

Consideraciones sobre la copia de seguridad y la restauración para réplicas de RDS para Db2

Antes de crear una réplica de RDS para Db2, tenga en cuenta los siguientes elementos:

- Para crear instantáneas de réplicas de RDS para Db2 o activar copias de seguridad automáticas, asegúrese de configurar el período de retención de copias de seguridad manualmente. Las copias de seguridad automáticas no están activadas de forma predeterminada.
- Cuando se restaura una copia de seguridad de réplicas, esta se restaura a la hora de la base de datos, no a la hora en que se realizó la copia de seguridad. El tiempo de base de datos se refiere a la última hora de la transacción aplicada de los datos de la copia de seguridad. La diferencia es

significativa, porque una réplica puede tener un retardo de minutos u horas con respecto a la base de datos principal. Cuando hay varias bases de datos, RDS para Db2 utiliza la hora más antigua de la base de datos.

Para averiguar la diferencia, ejecute el comando describe-db-snapshots de AWS CLI o llame a la operación DescribeDBSnapshots de la API de RDS. Compare el valor `SnapshotDatabaseTime` con el valor `OriginalSnapshotCreateTime`. El valor `SnapshotDatabaseTime` es la hora de la base de datos de la copia de seguridad de la réplica. El valor `OriginalSnapshotCreateTime` es la última transacción aplicada en la base de datos principal.

Consideraciones sobre la replicación para réplicas de RDS para Db2

Antes de crear una réplica de RDS para Db2, tenga en cuenta los siguientes elementos:

- La replicación utiliza HADR de Db2 para todas las bases de datos de la instancia de base de datos de RDS para Db2.
- La replicación no admite el comando `LOAD`. Si ejecuta el comando `LOAD` desde la instancia de base de datos de origen, recibirá datos incoherentes.
- RDS para Db2 no replica los siguientes elementos:
  - Acceso al almacenamiento. Tenga en cuenta los datos, como las tablas externas, que dependen del acceso al almacenamiento.
  - LOB no en línea.
  - Binarios de procedimientos almacenados externos (en C o Java).
- Para las réplicas en espera, RDS para Db2 replica los siguientes elementos:
  - Usuarios locales, excepto los usuarios maestros
  - Parámetros de configuración de base de datos

Otros aspectos para las réplicas de RDS para Db2

Antes de crear una réplica de RDS para Db2, tenga en cuenta los siguientes elementos:

- RDS para Db2 replica las configuraciones de base de datos en las réplicas. Cuando RDS para Db2 promociona una réplica, desactiva y activa cada base de datos.
- RDS para Db2 replica los usuarios locales, pero no el usuario maestro, en las réplicas. Puede modificar el usuario maestro en la réplica. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

- Todas las bases de datos deben encontrarse en estado activo. Para obtener información sobre cómo activar bases de datos, consulte Administración de bases de datos.
- Todos los procedimientos almacenados para crear, eliminar, restaurar o hacer avanzar bases de datos deben completarse antes de crear una réplica. Para obtener información sobre estos procedimientos almacenados, consulte Administración de bases de datos.
- Cuando se crea la réplica, Amazon RDS establece el parámetro de base de datos `blocknonlogged` para todas las bases de datos de la instancia de base de datos de origen en `YES`. Cuando la réplica de origen se convierte en una instancia independiente de nuevo, Amazon RDS vuelve a establecer el valor en `NO`. Para obtener más información, consulte blocknonlogged - Block creation of tables that allow non-logged activity configuration parameter en la documentación de IBM Db2.
- Cuando se crea la réplica, Amazon RDS establece el parámetro de base de datos `logindexbuild` para todas las bases de datos de la instancia de base de datos de origen en `YES`. Cuando la réplica de origen se convierte en una instancia independiente de nuevo, Amazon RDS vuelve a establecer el valor en `NO`. Para obtener más información, consulte logindexbuild - Log index pages created configuration parameter en la documentación de IBM Db2.

Preparación para crear una réplica de RDS para Db2

Antes de empezar a utilizar la réplica, realice las siguientes tareas:

Tareas

- Habilitar copias de seguridad automáticas
- Planificación de los recursos de computación y almacenamiento
- Preparación de bases de datos

Habilitar copias de seguridad automáticas

Para que una instancia de base de datos pueda servir como instancia de base de datos de origen, debe habilitar las copias de seguridad automáticas en la instancia de base de datos de origen. Para obtener información sobre cómo realizar este procedimiento, consulte Habilitar las copias de seguridad automatizadas.

Planificación de los recursos de computación y almacenamiento

Asegúrese de que la instancia de base de datos de origen y sus réplicas tengan el tamaño adecuado, en términos de informática y almacenamiento, para adaptarse a su carga operativa. Si una réplica llega a su capacidad en materia de recursos de cómputo, de red o de almacenamiento, dejará de recibir o aplicar los cambios desde su origen. RDS para Db2 no interviene para mitigar el retardo elevado de réplicas entre una instancia de base de datos de origen y las réplicas. Puede modificar los recursos de CPU y almacenamiento de una réplica independientemente de su origen y otras réplicas.

Preparación de bases de datos

Antes de crear la réplica, asegúrese de que la instancia de base de datos contiene todas las bases de datos que desea que estén presentes en la instancia de base de datos. Después de crear la réplica, no puede crear, eliminar ni restaurar de forma nativa una base de datos en la instancia de base de datos. No se realizará ninguna llamada a los procedimientos almacenados rdsadmin.create_database, rdsadmin.drop_database o rdsadmin.restore_database.

Además, asegúrese de que todas las bases de datos de la instancia de base de datos se encuentren en estado activo. De lo contrario, no se realizará la creación de la réplica. Para obtener información sobre cómo activar bases de datos, consulte Administración de bases de datos.

Creación de una réplica de RDS para Db2 en modo de espera

Puede crear una réplica en modo de espera mediante la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Creación de una réplica en espera a partir de una instancia de base de datos de RDS para Db2 de origen

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija la instancia de base de datos RDS para Db2 que desea utilizar como origen de una réplica en espera.
4. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).

5. En Modo de réplica, elija En espera.
6. Elija los ajustes que desee usar. En DB instance identifier (Identificador de instancias de bases de datos), escriba un nombre para la réplica de lectura. Ajuste otros valores como considere necesario.
7. En Regiones, elija la Región de AWS donde se iniciará la réplica en espera.
8. Elija el tamaño de la instancia y el tipo de almacenamiento. Es recomendable usar la misma clase de instancia de base de datos y el mismo tipo de almacenamiento que la instancia de base de datos de origen para la réplica de lectura.
9. En Implementación multi-AZ, elija Crear una instancia en espera para crear una réplica en espera en otra zona de disponibilidad para admitir la conmutación por error de la réplica en espera.
10. Elija los demás ajustes que desee usar.
11. Elija Create replica (Crear réplica).

En la página Bases de datos, la réplica en espera tiene el rol Réplica.

AWS CLI

Para crear una réplica de Db2 en modo de espera, establezca `--replica-mode` en `mounted` en el comando create-db-instance-read-replica de la AWS CLI.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier my_read_replica \
    --source-db-instance-identifier my_db_instance \
    --replica-mode mounted
```

Para Windows:

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier my_read_replica ^
    --source-db-instance-identifier my_db_instance ^
    --replica-mode mounted
```

API de RDS

Para crear una réplica de Db2 en modo de espera, especifique `ReplicaMode=mounted` en la operación CreateDBInstanceReadReplica de la API de RDS.

Trabajo con copias de seguridad de réplicas de RDS para Db2

Puede crear y restaurar copias de seguridad de una réplica de RDS para Db2. RDS para Db2 admite tanto copias de seguridad automáticas como instantáneas manuales. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos. En las secciones siguientes se describen las diferencias clave entre la administración de copias de seguridad de una base de datos principal y una réplica de RDS para Db2.

Temas

- Activación de copias de seguridad de réplicas de RDS para Db2
- Restauración de una copia de seguridad de réplicas de RDS para Db2

Activación de copias de seguridad de réplicas de RDS para Db2

Una réplica de RDS para Db2 no tiene activadas las copias de seguridad automáticas de forma predeterminada. Para activar las copias de seguridad automáticas, establezca el periodo de retención de copia de seguridad en un valor positivo distinto de cero.

Consola

Desactivación de las copias de seguridad automatizadas inmediatamente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, seleccione la instancia de base de datos que desee modificar.
3. Elija Modify.
4. En Periodo de retención de copia de seguridad, elija un valor positivo distinto de cero, por ejemplo, tres días.
5. Elija Continue.
6. Seleccione Apply immediately (Aplicar inmediatamente).

7. Elija Modificar la instancia de base de datos para guardar los cambios y habilitar las copias de seguridad automatizadas.

AWS CLI

Para activar las copias de seguridad automáticas, utilice el comando modify-db-instance de la AWS CLI.

Incluya los siguientes parámetros:

- `--db-instance-identifier`
- `--backup-retention-period`
- `--apply-immediately` o `--no-apply-immediately`

En el ejemplo siguiente se activan las copias de seguridad automáticas mediante el establecimiento del periodo de retención de copias de seguridad en tres días. Los cambios se aplican inmediatamente.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my_db_instance  \
    --backup-retention-period 3 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my_db_instance  ^
    --backup-retention-period 3 ^
    --apply-immediately
```

API de RDS

Para activar las copias de seguridad automáticas, utilice la operación ModifyDBInstance de la API de RDS con los siguientes parámetros obligatorios:

- `DBInstanceIdentifier`
- `BackupRetentionPeriod`

Restauración de una copia de seguridad de réplicas de RDS para Db2

Puede restaurar una copia de seguridad de una réplica de RDS para Db2 del mismo modo que restaura una copia de seguridad de la base de datos principal. Para obtener más información, consulte los temas siguientes:

- Restauración a una instancia de base de datos
- Restauración de una instancia de base de datos a un momento especificado para Amazon RDS

La consideración principal a la hora de restaurar una copia de seguridad de réplicas es determinar el punto en el tiempo en el que se va a restaurar. El tiempo de base de datos se refiere a la última hora de la transacción aplicada de los datos de la copia de seguridad. Cuando restaura una copia de seguridad de réplicas, se restaura la hora de la base de datos, no la hora en que se realizó la copia de seguridad. La diferencia es significativa porque una réplica puede tener un retardo de minutos u horas con respecto a la base de datos principal. Por lo tanto, la hora de la base de datos de una copia de seguridad de réplica y el momento en el que se restaura pueden ser mucho anteriores a la hora de creación de la copia de seguridad.

Para averiguar la diferencia entre la hora de la base de datos y la hora de creación, ejecute el comando describe-db-snapshots de AWS CLI o llame a la operación DescribeDBSnapshots de la API de RDS. Compare los valores `SnapshotDatabaseTime` y `OriginalSnapshotCreateTime`. El valor `SnapshotDatabaseTime` es la hora más antigua de la base de datos entre todas las bases de datos de la copia de seguridad de la réplica. El valor `OriginalSnapshotCreateTime` es la última transacción aplicada en la base de datos principal. Tenga en cuenta que los retardos de replicación pueden ser diferentes para varias bases de datos y la hora de la base de datos podría estar entre estas dos horas.

El siguiente ejemplo de la AWS CLI muestra la diferencia entre las dos horas:

```
aws rds describe-db-snapshots \
    --db-instance-identifier my_db2_replica
    --db-snapshot-identifier my_replica_snapshot

{
    "DBSnapshots": [
```

```
        {
            "DBSnapshotIdentifier": "my_replica_snapshot",
            "DBInstanceIdentifier": "my_db2_replica",
            "SnapshotDatabaseTime": "2022-07-26T17:49:44Z",
            ...
            "OriginalSnapshotCreateTime": "2021-07-26T19:49:44Z"
        }
    ]
}
```

Solución de problemas de replicación de RDS para Db2

En este contenido se describen los posibles problemas de replicación de RDS para Db2 y las soluciones.

Temas

- Supervisión del retardo de replicación de Db2
- Errores de replicación de Db2

Supervisión del retardo de replicación de Db2

Para supervisar el retraso de replicación en Amazon CloudWatch, consulte la métrica `ReplicaLag` de Amazon RDS. Para obtener información sobre el retardo de replicación, consulte Monitoreo de la replicación de lectura y Métricas de Amazon CloudWatch para Amazon RDS.

En el caso de una réplica en espera, si el tiempo de retardo es demasiado largo, consulte la tabla `MON_GET_HADR` para conocer el estado de la instancia de base de datos de origen. No consulte la instancia de base de datos de réplica, ya que las instancias de base de datos de réplica no aceptan conexiones de usuario.

Errores de replicación de Db2

La replicación de Db2 puede encontrarse en estado de error por varios motivos. Supervise los eventos y el estado de la instancia de base de datos para asegurarse de que la instancia de base de datos se está replicando. Para confirmar que la instancia de base de datos se está replicando, consulte los registros de diagnóstico de la réplica en la consola de Amazon RDS. En los registros, busque errores en los mensajes de HADR. Compare el número de secuencia del registro con el número de secuencia principal. Para obtener más información, consulte Archivos de registro de base de datos de Amazon RDS para Db2.

Opciones de instancias de base de datos de Amazon RDS para Db2

A continuación, encontrará opciones o características adicionales que están disponibles para las instancias de Amazon RDS que ejecutan el motor de base de datos Db2. Para activar estas opciones, puede añadirlas a un grupo de opciones personalizado y, a continuación, asociar el grupo de opciones a la instancia de base de datos. Para obtener más información acerca de cómo trabajar con grupos de opciones, consulte Trabajo con grupos de opciones.

Amazon RDS admite las siguientes opciones para Db2:

Opción	ID de la opción
Registro de auditoría de Db2	`DB2_AUDIT`

Registro de auditoría de Db2

Con el registro de auditoría de Db2, Amazon RDS registra la actividad de la base de datos, lo que incluye a los usuarios que inician sesión en la base de datos y las consultas ejecutadas en esta. RDS carga los registros de auditoría completados en su bucket de Amazon S3 mediante el rol de AWS Identity and Access Management (IAM) que usted proporciona.

Temas

- Configuración del registro de auditoría de Db2
- Administración del registro de auditoría de Db2
- Visualización de registros de auditoría
- Solución de problemas en el registro de auditoría de Db2

Configuración del registro de auditoría de Db2

Para habilitar el registro de auditoría en una base de datos de Amazon RDS para Db2, active la opción `DB2_AUDIT` en la instancia de base de datos de Amazon RDS para Db2. Luego, configure una política de auditoría para habilitar la característica en la base de datos específica. Para habilitar la opción en la instancia de base de datos de RDS para Db2, debe configurar los ajustes de la opción `DB2_AUDIT`. Para ello, debe proporcionar los nombres de recursos de Amazon (ARN) para su bucket de Amazon S3 y el rol de IAM con permisos para acceder a su bucket.

Para configurar el registro de auditoría de Db2 para una base de datos de RDS para Db2, siga estos pasos.

Temas

- Paso 1: Crear un bucket de Amazon S3
- Paso 2: Crear una política de IAM
- Paso 3: Crear un rol de IAM y asociar la política de IAM
- Paso 4: Configurar un grupo de opciones para el registro de auditoría de Db2
- Paso 5: Configurar la política de auditoría
- Paso 6: Comprobar la configuración de la auditoría

Paso 1: Crear un bucket de Amazon S3

Si aún no lo ha hecho, cree un bucket de Amazon S3 en el que Amazon RDS pueda cargar los archivos de registro de auditoría de la base de datos de RDS para Db2. Se aplican las siguientes restricciones al bucket de S3 que usa como destino para los archivos de auditoría:

- Debería estar en la misma Región de AWS que su instancia de base de datos de RDS para Db2.
- No debe estar abierto al público.
- El propietario del bucket también debe ser el propietario del rol de IAM.

Para aprender a crear un bucket de Amazon S3, consulte Crear un bucket en la Guía de usuario Amazon S3.

Tras habilitar el registro de auditoría, Amazon RDS envía automáticamente los registros de la instancia de base de datos a las siguientes ubicaciones:

- Registros en el nivel de instancia de base de datos: *bucket_name*`/db2-audit-logs/`*dbi_resource_id*`/`*date_time_utc*`/`
- Registros en el nivel de base de datos: *bucket_name*`/db2-audit-logs/`*dbi_resource_id*`/`*date_time_utc*`/`*db_name*`/`

Apunte el nombre de recurso de Amazon (ARN) del bucket. Esta información será necesaria para completar los pasos siguientes.

Paso 2: Crear una política de IAM

Cree una política de IAM con los permisos necesarios para transferir archivos de registro de auditoría desde su instancia de base de datos a su bucket de Amazon S3. En este paso, se da por sentado que ya tiene un bucket de S3.

Antes de crear la política, obtenga la siguiente información:

- El ARN de su bucket.
- El ARN para su clave de AWS Key Management Service (AWS KMS), si el bucket utiliza el cifrado SSE-KMS.

Cree una política de IAM que incluya los siguientes permisos:

```
"s3:ListBucket",
 "s3:GetBucketAcl",
 "s3:GetBucketLocation",
 "s3:PutObject",
 "s3:ListMultipartUploadParts",
 "s3:AbortMultipartUpload",
 "s3:ListAllMyBuckets"
```

> **Note**
>
> Amazon RDS necesita la acción `s3:ListAllMyBuckets` internamente para verificar que la misma Cuenta de AWS tenga el bucket S3 y la instancia de base de datos de RDS para Db2.

Si el bucket usa el cifrado SSE-KMS, incluya también los siguientes permisos para el rol de IAM y la clave de AWS KMS.

Incluya los permisos siguientes a la política para el rol de IAM.

```
"kms:GenerateDataKey",
 "kms:Decrypt"
```

Incluya los permisos siguientes a la política de claves de la clave de AWS KMS. Reemplace *111122223333* por el número de cuenta y *AR0A123456789EXAMPLE* por el nombre del rol de IAM.

```
{
  "Sid": "Allow RDS role to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:sts::111122223333:assumed-role/AR0A123456789EXAMPLE/RDS-Db2Audit",
      "arn:aws:iam::111122223333:role/AR0A123456789EXAMPLE"
    ]
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

Puede crear una política de IAM mediante la AWS Management Console o la AWS Command Line Interface (AWS CLI).

Consola

Para crear una política de IAM que permita a Amazon RDS acceder a un bucket de Amazon S3

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Crear política y, a continuación, elija JSON.
4. En Agregar acciones, filtre por S3. Agregue el acceso ListBucket, GetBucketAcl y GetBucketLocation.
5. En Agregar un recurso, seleccione Agregar. En Tipo de recurso, elija bucket e introduzca el nombre del bucket. Luego, elija Agregar recurso.
6. Elija Agregar nueva instrucción.
7. En Agregar acciones, filtre por S3. Agregue el acceso PutObject, ListMultipartUploadParts y AbortMultipartUpload.
8. En Agregar un recurso, seleccione Agregar. En Tipo de recurso, elija objeto e introduzca *your bucket name/**. Luego, elija Agregar recurso.
9. Elija Agregar nueva instrucción.
10. En Agregar acciones, filtre por S3. Agregue el acceso ListAllMyBuckets.
11. En Agregar un recurso, seleccione Agregar. Para Tipo de recurso, elija Todos los recursos. Luego, elija Agregar recurso.
12. Si utiliza sus propias claves de KMS para cifrar los datos:
    1. Elija Agregar nueva instrucción.
    2. En Agregar acciones, filtre por KMS. Agregue el acceso GenerateDataKey y Decrypt.
    3. En Agregar un recurso, seleccione Agregar. Para Tipo de recurso, elija Todos los recursos. Luego, elija Agregar recurso.
13. Elija Siguiente.
14. Escriba un nombre para la política en Nombre de la política.
15. (Opcional) En Description (Descripción), escriba una descripción para esta política.
16. Seleccione Crear política.

AWS CLI

Para crear una política de IAM que permita a Amazon RDS acceder a un bucket de Amazon S3

1. Ejecute el comando create-policy. En el siguiente ejemplo, sustituya *iam_policy_name* y *amzn-s3-demo-bucket* por un nombre para su política de IAM y por el nombre de su bucket de Amazon S3 de destino.

   Para Linux, macOS o Unix:

```
aws iam create-policy \
    --policy-name iam_policy_name \
    --policy-document '{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "Statement1",
                "Effect": "Allow",
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetBucketLocation"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket"
                ]
            },
            {
                "Sid": "Statement2",
                "Effect": "Allow",
                "Action": [
                    "s3:PutObject",
                    "s3:ListMultipartUploadParts",
                    "s3:AbortMultipartUpload"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket/*"
                ]
            },
            {
                "Sid": "Statement3",
                "Effect": "Allow",
                "Action": [
```

```
                    "s3:ListAllMyBuckets"
                ],
                "Resource": [
                    "*"
                ]
            },
            {
                "Sid": "Statement4",
                "Effect": "Allow",
                "Action": [
                    "kms:GenerateDataKey",
                    "kms:Decrypt"
                ],
                "Resource": [
                    "*"
                ]
            }
        ]
  }'
```

Para Windows:

```
aws iam create-policy ^
    --policy-name iam_policy_name ^
    --policy-document '{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "Statement1",
                "Effect": "Allow",
                "Action": [
                    "s3:ListBucket",
                    "s3:GetBucketAcl",
                    "s3:GetBucketLocation"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket"
                ]
            },
            {
                "Sid": "Statement2",
                "Effect": "Allow",
                "Action": [
```

```
                    "s3:PutObject",
                    "s3:ListMultipartUploadParts",
                    "s3:AbortMultipartUpload"
                ],
                "Resource": [
                    "arn:aws:s3:::amzn-s3-demo-bucket/*"
                ]
            },
            {
                "Sid": "Statement3",
                "Effect": "Allow",
                "Action": [
                    "s3:ListAllMyBuckets"
                ],
                "Resource": [
                    "*"
                ]
            },
            {
                "Sid": "Statement4",
                "Effect": "Allow",
                "Action": [
                    "kms:GenerateDataKey",
                    "kms:Decrypt"
                ],
                "Resource": [
                    "*"
                ]
            }
        ]
}'
```

2. Después de crear la política, apunte el ARN de la política. Necesita el ARN para Paso 3: Crear un rol de IAM y asociar la política de IAM.

Para obtener más información acerca de cómo crear una política de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Paso 3: Crear un rol de IAM y asociar la política de IAM

En este paso, se da por sentado que ha creado la política de IAM en Paso 2: Crear una política de IAM. En este paso, creará un rol de IAM para la instancia de base de datos de RDS para Db2 y, a continuación, asociará la política de IAM al rol.

Puede crear un rol de IAM a su instancia de base de datos mediante la consola o la AWS CLI.

Consola

Para crear un rol de IAM y asociarle la política de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.
4. En Tipo de entidad de confianza, elija Servicio de AWS.
5. Para el Servicio o caso de uso, seleccione RDS y, a continuación, seleccione RDS: Agregar rol a la base de datos.
6. Elija Siguiente.
7. Para Políticas de permisos, busque y seleccione el nombre de la política de IAM que creó.
8. Elija Siguiente.
9. En Nombre de rol, ingrese un nombre de rol.
10. (Opcional) En Descripción, ingrese una descripción para el nuevo rol.
11. Seleccione Crear rol.

AWS CLI

Para crear un rol de IAM y asociarle la política de IAM

1. Ejecute el comando create-role. En el siguiente ejemplo, sustituya *iam_role_name* por un nombre para su rol de IAM.

   Para Linux, macOS o Unix:

```
aws iam create-role \
    --role-name iam_role_name \
    --assume-role-policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
```

```
            "Service": "rds.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }'
```

Para Windows:

```
aws iam create-role ^
    --role-name iam_role_name ^
    --assume-role-policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "Service": "rds.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }'
```

2. Después de crear el rol, anote el ARN del rol. Necesitará este ARN en el siguiente paso (Paso 4: Configurar un grupo de opciones para el registro de auditoría de Db2).
3. Ejecute el comando attach-role-policy. En el siguiente ejemplo, sustituya *iam_policy_arn* por el ARN de la política de IAM que creó en Paso 2: Crear una política de IAM. Reemplace *iam_role_name* por el nombre del rol de IAM que acaba de crear.

   Para Linux, macOS o Unix:

   ```
   aws iam attach-role-policy \
      --policy-arn iam_policy_arn \
      --role-name iam_role_name
   ```

   Para Windows:

   ```
   aws iam attach-role-policy ^
      --policy-arn iam_policy_arn ^
      --role-name iam_role_name
   ```

Para obtener más información, vea Crear un rol para delegar permisos a un usuario de IAM en Guía del usuario de IAM.

Paso 4: Configurar un grupo de opciones para el registro de auditoría de Db2

El proceso de incorporación de la opción del registro de auditoría de Db2 a una instancia de base de datos de RDS para Db2 es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada y configure todas las opciones necesarias.
3. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir la opción del registro de auditoría de Db2, no es necesario reiniciar la instancia de base de datos. En cuanto el grupo de opciones esté activo, podrá crear auditorías y almacenar registros de auditoría en su bucket de S3.

Para añadir y configurar el registro de auditoría de Db2 en el grupo de opciones de una instancia de base de datos

1. Elija una de las siguientes opciones:
   - Use un grupo de opciones existente.
   - Cree un grupo de opciones de base de datos personalizado y utilice ese grupo. Para obtener más información, consulte Creación de un grupo de opciones.
2. Agregue la opción DB2_AUDIT al grupo de opciones y configure las opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
   - En IAM_ROLE_ARN, escriba el ARN para el rol de IAM que creó en the section called “Creación de un rol de IAM y asociación de la política de IAM”.
   - Para S3_BUCKET_ARN, introduzca el ARN del bucket de S3 que se utilizará en los registros de auditoría de Db2. El bucket debe estar en la misma región que la instancia de base de datos de RDS para Db2. La política asociada al rol de IAM que haya introducido debe permitir las operaciones necesarias en este recurso.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente. Elija una de las siguientes opciones:

- Si está creando una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia.
- En una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Paso 5: Configurar la política de auditoría

A fin de configurar la política de auditoría para su base de datos de RDS para Db2, conéctese a la base de datos de `rdsadmin` con el nombre de usuario y la contraseña principales de su instancia de base de datos de RDS para Db2. Luego, llame al procedimiento almacenado `rdsadmin.configure_db_audit` con el nombre de base de datos de su base de datos y con los valores de parámetro aplicables.

El siguiente ejemplo se conecta a la base de datos y configura una política de auditoría para `testdb` con las categorías AUDIT, CHECKING, OBJMAINT, SECMAINT, SYSADMIN, y VALIDATE. El valor de estado `BOTH` registra los éxitos y los errores, y el `ERROR TYPE` es `NORMAL` de manera predeterminada. Para obtener más información sobre el uso de este procedimiento almacenado, consulte the section called “rdsadmin.configure_db_audit”.

```
db2 "connect to rdsadmin user master_user using master_password"
db2 "call rdsadmin.configure_db_audit('testdb', 'ALL', 'BOTH', ?)"
```

Paso 6: Comprobar la configuración de la auditoría

Para asegurarse de que la política de auditoría está configurada correctamente, compruebe el estado de la configuración de auditoría.

Para comprobar la configuración, conéctese a la base de datos `rdsadmin` con el nombre de usuario y la contraseña principales de su instancia de base de datos de RDS para Db2. Luego, ejecute la siguiente instrucción SQL con el nombre de base de datos de su base de datos. En el siguiente ejemplo, el nombre de base de datos es *testdb*.

```
db2 "select task_id, task_type, database_name, lifecycle,
    varchar(bson_to_json(task_input_params), 500) as task_params,
    cast(task_output as varchar(500)) as task_output
    from table(rdsadmin.get_task_status(null,'testdb','CONFIGURE_DB_AUDIT'))"
```

```
Sample Output

TASK_ID              TASK_TYPE            DATABASE_NAME       LIFECYCLE
-------------------- -------------------- --------------- -------------
                   2  CONFIGURE_DB_AUDIT            DB2DB       SUCCESS

... continued ...
TASK_PARAMS
------------------------------------------------------------
{ "AUDIT_CATEGORY" : "ALL", "CATEGORY_SETTING" : "BOTH" }

... continued ...
                                          TASK_OUTPUT
-------------------------------------------------------
2023-12-22T20:27:03.029Z Task execution has started.

2023-12-22T20:27:04.285Z Task execution has completed successfully.
```

Administración del registro de auditoría de Db2

Tras configurar el registro de auditoría de Db2, puede modificar la política de auditoría de una base de datos específica o deshabilitar el registro de auditoría en el nivel de base de datos o de toda la instancia de base de datos. También puede cambiar el bucket de Amazon S3 en el que se cargan los archivos de registro.

Temas

- Modificación de una política de auditoría de Db2
- Modificación de la ubicación de los archivos de registro
- Deshabilitación del registro de auditoría de Db2

Modificación de una política de auditoría de Db2

Para modificar la política de auditoría de una base de datos RDS para Db2 específica, ejecute el procedimiento almacenado `rdsadmin.configure_db_audit`. Con este procedimiento almacenado, puede cambiar las categorías, los ajustes de las categorías y la configuración de los tipos de error de la política de auditoría. Para obtener más información, consulte the section called “rdsadmin.configure_db_audit”.

Modificación de la ubicación de los archivos de registro

Para cambiar el bucket de Amazon S3 en el que se cargan los archivos de registro, lleve a cabo una de las siguientes acciones:

- Modificar el grupo de opciones actual asociado a su instancia de base de datos de RDS para Db2: actualice la configuración de `S3_BUCKET_ARN` para la opción `DB2_AUDIT` de modo que apunte al nuevo bucket. Además, actualice la política de IAM asociada al rol de IAM especificado en la configuración de `IAM_ROLE_ARN` del grupo de opciones asociado. Esta política de IAM debe darle a su nuevo bucket los permisos de acceso necesarios. Para obtener más información acerca de los permisos necesarios en la política de IAM, consulte Creación de una política de IAM.
- Asociar la instancia de base de datos de RDS para Db2 a un grupo de opciones diferente: modifique la instancia de base de datos para cambiar el grupo de opciones asociado. Asegúrese de que el nuevo grupo de opciones esté configurado con los ajustes `S3_BUCKET_ARN` y `IAM_ROLE_ARN` correctos. Para obtener información acerca de cómo configurar estos ajustes para la opción `DB2_AUDIT`, consulte Configurar un grupo de opciones.

Al modificar el grupo de opciones, debe aplicar los cambios inmediatamente. Para obtener más información, consulte the section called “Modificación de una instancia de base de datos”.

Deshabilitación del registro de auditoría de Db2

Para deshabilitar el registro de auditoría de Db2, realice una de las siguientes acciones:

- Deshabilitar el registro de auditoría para la instancia de base de datos de RDS para Db2: modifique su instancia de base de datos y elimine el grupo de opciones que contiene la opción `DB2_AUDIT`. Para obtener más información, consulte the section called “Modificación de una instancia de base de datos”.
- Deshabilitar el registro de auditoría para una base de datos específica: detenga el registro de auditoría y elimine la política de auditoría llamando a `rdsadmin.disable_db_audit` con el nombre de base de datos de su base de datos. Para obtener más información, consulte the section called “rdsadmin.disable_db_audit”.

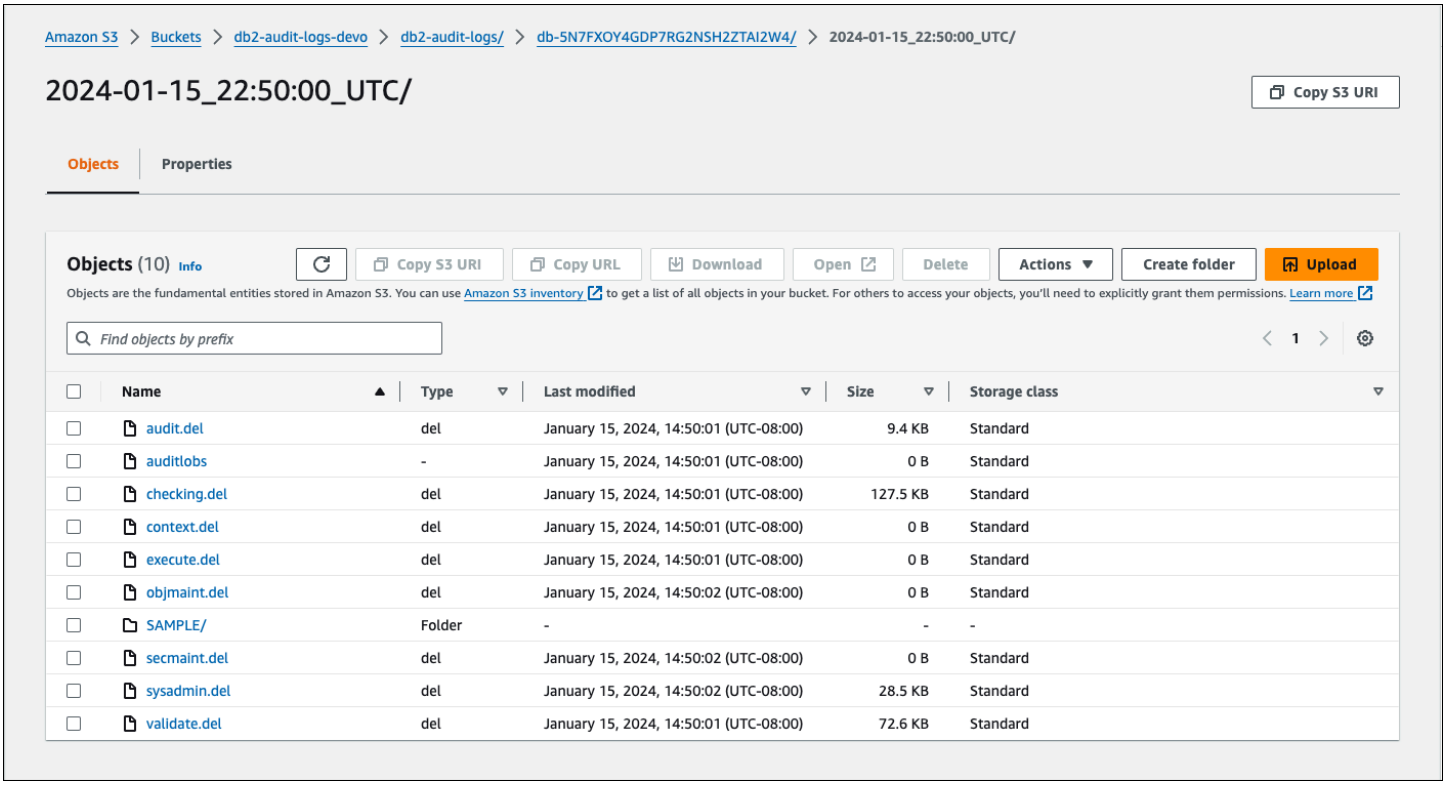
```
db2 "call rdsadmin.disable_db_audit(
    'db_name',
    ?)"
```

Visualización de registros de auditoría

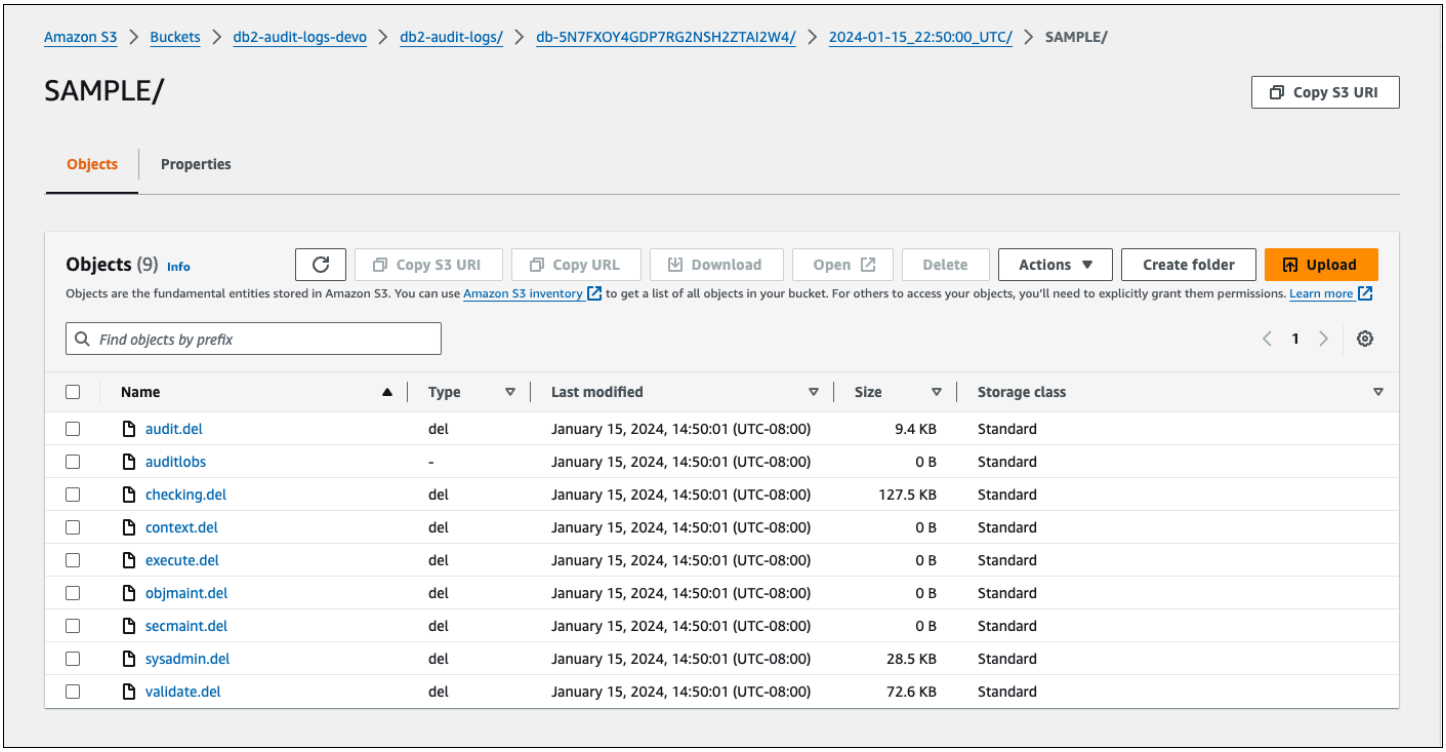
Tras habilitar el registro de auditoría de Db2, espere al menos una hora antes de ver los datos de auditoría en su bucket de Amazon S3. Amazon RDS envía automáticamente los registros desde su instancia de base de datos de RDS para Db2 a las siguientes ubicaciones:

- Registros en el nivel de instancia de base de datos: *bucket_name*/db2-audit-logs/*dbi_resource_id*/*date_time_utc*/
- Registros en el nivel de base de datos: *bucket_name*/db2-audit-logs/*dbi_resource_id*/*date_time_utc*/*db_name*/

En la siguiente captura de pantalla de ejemplo de la consola Amazon S3, se muestra una lista de carpetas para los archivos de registro en el nivel de instancia de base de datos de RDS para Db2.



La siguiente captura de pantalla de ejemplo de la consola de Amazon S3 muestra los archivos de registro en el nivel de base de datos para la instancia de base de datos de RDS para Db2.



Solución de problemas en el registro de auditoría de Db2

Utilice la siguiente información para solucionar problemas comunes con el registro de auditoría de Db2.

No se puede configurar la política de auditoría

Si, al llamar al procedimiento almacenado `rdsadmin.configure_db_audit`, se produce un error, es posible que el grupo de opciones que contiene la opción `DB2_AUDIT` no esté asociado a la instancia de base de datos de RDS para Db2. Modifique la instancia de base de datos para añadir el grupo de opciones y llame de nuevo al procedimiento almacenado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

No hay datos en el bucket de Amazon S3

Si faltan datos de registro en el bucket de Amazon S3, compruebe lo siguiente:

- El bucket de Amazon S3 debe estar en la misma región que la instancia de base de datos de RDS para Db2.
- El rol que especificó en la configuración de la opción `IAM_ROLE_ARN` debe estar configurado con los permisos necesarios para cargar registros en su bucket de Amazon S3. Para obtener más información, consulte Creación de una política de IAM.

- Los ARN de la configuración de las opciones `IAM_ROLE_ARN` y `S3_BUCKET_ARN` deben ser los correctos en el grupo de opciones asociado a su instancia de base de datos de RDS para Db2. Para obtener más información, consulte Configurar un grupo de opciones.

Para verificar el estado de la tarea de la configuración de registro de auditoría, conéctese a la base de datos y ejecute una instrucción SQL. Para obtener más información, consulte Comprobar la configuración de la auditoría.

También puede comprobar los eventos para obtener más información sobre por qué faltan registros. Para obtener información sobre cómo ver eventos, consulte the section called “Visualización de los registros, los eventos y los flujos en la consola de Amazon RDS”.

Procedimientos almacenados externos de Amazon RDS para Db2

Puede crear rutinas externas y registrarlas en sus bases de datos de Amazon RDS para Db2 como procedimientos almacenados externos. Actualmente, RDS para Db2 solo admite rutinas basadas en Java para procedimientos almacenados externos.

Procedimientos almacenados externos basados en Java

Los procedimientos almacenados externos basados en Java son rutinas Java externas que se registran en la base de datos de RDS para Db2 como procedimientos almacenados externos.

Temas

- Limitaciones de los procedimientos almacenados externos basados en Java
- Configuración de procedimientos almacenados externos basados en Java

Limitaciones de los procedimientos almacenados externos basados en Java

Antes de desarrollar su rutina externa, tenga en cuenta las siguientes limitaciones y restricciones.

Para crear su rutina externa, asegúrese de utilizar el kit de desarrollo de Java (JDK) proporcionado por Db2. Para obtener más información, consulte Java software support for Db2 database products.

Su programa Java solo puede crear archivos en el directorio `/tmp` y Amazon RDS no permite habilitar permisos ejecutables ni permisos de definición de ID de usuario (SUID) en estos archivos. Su programa Java tampoco puede usar llamadas al sistema de sockets ni las siguientes llamadas al sistema:

- _sysctl
- acct
- afs_syscall
- bpf
- capset
- chown
- chroot
- create_module

- delete_module
- fanotify_init
- fanotify_mark
- finit_module
- fsconfig
- fsopen
- fspick
- get_kernel_syms
- getpmsg
- init_module
- mount
- move_mount
- nfsservctl
- open_by_handle_at
- open_tree
- pivot_root
- putpmsg
- query_module
- quotactl
- reboot
- security
- setdomainname
- setfsuid
- sethostname
- sysfs
- tuxcall
- umount2
- uselib
- ustat

- vhangup
- vserver

Para conocer las restricciones adicionales en las rutinas externas de Db2, consulte Restrictions on external routines en la documentación de IBM Db2.

Configuración de procedimientos almacenados externos basados en Java

Para configurar un procedimiento almacenado externo, cree un archivo .jar con su rutina externa, instálelo en la base de datos de RDS para Db2 y, a continuación, regístrelo como procedimiento almacenado externo.

Temas

- Paso 1: habilite los procedimientos almacenados externos
- Paso 2: instale el archivo .jar con la rutina externa
- Paso 3: registre el procedimiento almacenado externo
- Paso 4: valide el procedimiento almacenado externo

Paso 1: habilite los procedimientos almacenados externos

Para habilitar los procedimientos almacenados externos, establezca el parámetro `db2_alternate_authz_behaviour` en uno de los valores siguientes en un grupo de parámetros personalizado asociado a la instancia de base de datos:

- `EXTERNAL_ROUTINE_DBADM`: concede de forma implícita a cualquier usuario, grupo o rol con autoridad `DBADM` el permiso `CREATE_EXTERNAL_ROUTINE`.
- `EXTERNAL_ROUTINE_DBAUTH`: permite a un usuario con autoridad `DBADM` conceder el permiso `CREATE_EXTERNAL_ROUTINE` a cualquier usuario, grupo o rol. En este caso, no se concede implícitamente este permiso a ningún usuario, grupo o rol, ni siquiera a un usuario con autoridad `DBADM`.

Para obtener más información sobre esta configuración, consulte GRANT (database authorities) statement en la documentación de IBM Db2.

Puede crear y modificar una instancia de base de datos mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS.

Consola

Configuración del parámetro db2_alternate_authz_behaviour en un grupo de parámetros personalizado

1. Si desea utilizar un grupo de parámetros de base de datos personalizado diferente al que está utilizando su instancia de base de datos, cree un nuevo grupo de parámetros de base de datos. Si utiliza el modelo Traiga su propia licencia (BYOL), asegúrese de que el nuevo grupo de parámetros personalizados incluya los ID de IBM. Para obtener información acerca de estos ID, consulte the section called “ID de IBM para Traiga su propia licencia para Db2”. Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Establezca el valor del parámetro `db2_alternate_authz_behaviour` en su grupo de parámetros personalizados. Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

AWS CLI

Configuración del parámetro db2_alternate_authz_behaviour en un grupo de parámetros personalizado

1. Si desea utilizar un grupo de parámetros de base de datos personalizado diferente al que está utilizando su instancia de base de datos, cree un grupo de parámetros personalizado ejecutando el comando create-db-parameter-group. Si utiliza el modelo Traiga su propia licencia (BYOL), asegúrese de que el nuevo grupo de parámetros personalizados incluya los ID de IBM. Para obtener información acerca de estos ID, consulte the section called “ID de IBM para Traiga su propia licencia para Db2”.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: un nombre para el grupo de parámetros que se está creando.
   - `--db-parameter-group-family`: la edición y la versión principal del motor de Db2. Los valores válidos son `db2-se-11.5` y `db2-ae-11.5`.
   - `--description`: la descripción para este grupo de parámetros.

Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.

En el siguiente ejemplo, se muestra cómo crear un grupo de parámetros personalizado denominado `MY_EXT_SP_PARAM_GROUP` para la familia de grupos de parámetros `db2-se-11.5`.

Para Linux, macOS o:Unix

```
aws rds create-db-parameter-group \
--region us-east-1 \
--db-parameter-group-name MY_EXT_SP_PARAM_GROUP \
--db-parameter-group-family db2-se-11.5 \
--description "test db2 external routines"
```

En:Windows

```
aws rds create-db-parameter-group ^
--region us-east-1 ^
--db-parameter-group-name MY_EXT_SP_PARAM_GROUP ^
--db-parameter-group-family db2-se-11.5 ^
--description "test db2 external routines"
```

2. Modifique el parámetro `db2_alternate_authz_behaviour` en su grupo de parámetros personalizados ejecutando el comando modify-db-parameter-group.

   Incluya las siguientes opciones obligatorias:

   - `--db-parameter-group-name`: el nombre del grupo de parámetros creado.
   - `--parameters`: una matriz de los nombres de parámetros, valores y métodos de aplicación para la actualización del parámetro.

   Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

   En el siguiente ejemplo, se muestra cómo modificar el grupo de parámetros `MY_EXT_SP_PARAM_GROUP` configurando el valor de `db2_alternate_authz_behaviour` en `EXTERNAL_ROUTINE_DBADM`.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name MY_EXT_SP_PARAM_GROUP \
    --parameters
 "ParameterName='db2_alternate_authz_behaviour',ParameterValue='EXTERNAL_ROUTINE_DBADM',App
```

En:Windows

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name MY_EXT_SP_PARAM_GROUP ^
    --parameters
 "ParameterName='db2_alternate_authz_behaviour',ParameterValue='EXTERNAL_ROUTINE_DBADM',App
```

API de RDS

Configuración del parámetro db2_alternate_authz_behaviour en un grupo de parámetros personalizado

1. Si desea utilizar un grupo de parámetros de base de datos personalizado diferente del que utiliza su instancia de base de datos, cree un nuevo grupo de parámetros de base de datos mediante la operación CreateDBParameterGroup de la API de Amazon RDS. Si utiliza el modelo Traiga su propia licencia (BYOL), asegúrese de que el nuevo grupo de parámetros personalizados incluya los ID de IBM Db2. Para obtener información acerca de estos ID, consulte the section called “ID de IBM para Traiga su propia licencia para Db2”.

   Incluya los siguientes parámetros obligatorios:

   - `DBParameterGroupName`
   - `DBParameterGroupFamily`
   - `Description`

   Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.
2. Modifique el parámetro `db2_alternate_authz_behaviour` del grupo de parámetros personalizado que creó mediante la operación ModifyDBParameterGroup de la API de RDS.

Incluya los siguientes parámetros obligatorios:

- `DBParameterGroupName`
- `Parameters`

Para obtener más información acerca de cómo modificar un grupo de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Paso 2: instale el archivo .jar con la rutina externa

Tras crear la rutina de Java, cree el archivo .jar y, a continuación, ejecute `db2 "call sqlj.install_jar('file:`*`file_path`*`',`*`jar_ID`*`)"` para instalarlo en la base de datos de RDS para Db2.

En el siguiente ejemplo, se muestra cómo crear una rutina de Java e instalarla en una base de datos de RDS para Db2. En el ejemplo, se incluye un código de ejemplo para una rutina sencilla que puede utilizar para probar el proceso. En este ejemplo, se da por supuesto lo siguiente:

- El código Java se compila en un servidor en el que está instalado Db2. Se trata de una práctica recomendada, ya que si no se compila con el JDK proporcionado por IBM, se pueden producir errores sin ninguna explicación.
- El servidor tiene la base de datos de RDS para Db2 catalogada localmente.

Si desea probar el proceso con el siguiente código de ejemplo, cópielo y guárdelo en un archivo denominado `MYJAVASP.java`.

```
import java.sql.*;
public class MYJAVASP
{
public static void my_JAVASP (String inparam) throws SQLException, Exception
{
try
{
// Obtain the calling context's connection details.
Connection myConn = DriverManager.getConnection("jdbc:default:connection");
String myQuery = "INSERT INTO TEST.TEST_TABLE VALUES (?, CURRENT DATE)";
PreparedStatement myStmt = myConn.prepareStatement(myQuery);
myStmt.setString(1, inparam);
```

```
myStmt.executeUpdate();
}
catch (SQLException sql_ex)
{
throw sql_ex;
}
catch (Exception ex)
{
throw ex;
}
}
```

El siguiente comando compila la rutina de Java.

```
~/sqllib/java/jdk64/bin/javac MYJAVASP.java
```

El siguiente comando crea el archivo .jar.

```
~/sqllib/java/jdk64/bin/jar cvf MYJAVASP.jar MYJAVASP.class
```

Los siguientes comandos se conectan a la base de datos denominada `MY_DB2_DATABASE` e instalan el archivo .jar.

```
db2 "connect to MY_DB2_DATABASE user master_username using master_password"

db2 "call sqlj.install_jar('file:/tmp/MYJAVASP.jar','MYJAVASP')"
db2 "call sqlj.refresh_classes()"
```

Paso 3: registre el procedimiento almacenado externo

Tras instalar el archivo .jar en la base de datos de RDS para Db2, regístrelo como procedimiento almacenado ejecutando el comando `db2 CREATE PROCEDURE` o `db2 REPLACE PROCEDURE`.

El siguiente ejemplo muestra cómo conectarse a la base de datos y registrar la rutina de Java creada en el paso anterior como un procedimiento almacenado.

```
db2 "connect to MY_DB2_DATABASE user master_username using master_password"

create procedure TESTSP.MYJAVASP (in input char(6))
specific myjavasp
dynamic result sets 0
```

```
deterministic
language java
parameter style java
no dbinfo
fenced
threadsafe
modifies sql data
program type sub
external name 'MYJAVASP!my_JAVASP';
```

Paso 4: valide el procedimiento almacenado externo

Utilice los siguientes pasos para probar el procedimiento almacenado externo de ejemplo que se registró en el paso anterior.

Validación del procedimiento almacenado externo

1. Cree una tabla como `TEST.TEST_TABLE` en el siguiente ejemplo.

   ```
   db2 "create table TEST.TEST_TABLE(C1 char(6), C2 date)"
   ```

2. Llame al nuevo procedimiento almacenado externo. La llamada devuelve un estado de `0`.

   ```
   db2 "call TESTSP.MYJAVASP('test')"
   Return Status = 0
   ```

3. Consulte la tabla que creó en el paso 1 para comprobar los resultados de la llamada al procedimiento almacenado.

   ```
   db2 "SELECT * from TEST.TEST_TABLE"
   ```

   La consulta produce una salida similar a la del ejemplo siguiente:

   ```
   C1     C2
   ------ ----------
   test   02/05/2024
   ```

Problemas conocidos y limitaciones para Amazon RDS para Db2

Los siguientes elementos son problemas y limitaciones conocidos para trabajar con Amazon RDS para Db2:

Temas

- Limitación de autenticación
- Rutinas no restringidas
- Espacios de tablas de almacenamiento no automáticos durante la migración
- Establecimiento del parámetro db2_compatibility_vector
- Migración de bases de datos que contienen paquetes NO VÁLIDOS

Limitación de autenticación

Amazon RDS establece `db2auth` en `JCC_ENFORCE_SECMEC` de manera predeterminada. Sin embargo, si no quiere aplicar el cifrado de los identificadores de usuario y contraseñas a través de la red, puede anular esta configuración cambiando el parámetro `db2auth` a `CLEAR_TEXT` dentro del grupo de parámetros. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Rutinas no restringidas

RDS para Db2 no admite la creación de rutinas no restringidas ni la migración de estas rutinas mediante la creación de copias de seguridad y la restauración de los datos. Para comprobar si la base de datos contiene rutinas no restringidas, ejecute el siguiente comando de SQL:

```
SELECT 'COUNT:' || count(*) FROM SYSCAT.ROUTINES where fenced='N' and routineschema not
 in ('SQLJ','SYSCAT','SYSFUN','SYSIBM','SYSIBMADM','SYSPROC','SYSTOOLS')
```

Espacios de tablas de almacenamiento no automáticos durante la migración

RDS para Db2 no admite la creación de nuevos espacios de tablas de almacenamiento no automáticos. Al utilizar la restauración nativa para una migración única de la base de datos, RDS para Db2 convierte automáticamente los espacios de tabla de almacenamiento no automáticos en

espacios automáticos y, a continuación, restaura la base de datos en RDS para Db2. Para obtener información sobre las migraciones únicas, consulte Migración de Linux a Linux de Amazon RDS para Db2y Migración de AIX o Windows a Linux de Amazon RDS para Db2.

Establecimiento del parámetro db2_compatibility_vector

Con Amazon RDS, puede crear una base de datos inicial al crear la instancia de base de datos y, a continuación, modificar los parámetros de un grupo de parámetros asociado. Sin embargo, en el caso de Db2, si desea establecer el parámetro `db2_compatibility_vector` en un grupo de parámetros, primero debe modificar el parámetro en un grupo de parámetros personalizado, crear la instancia de base de datos sin una base de datos y, a continuación, crear una base de datos mediante el procedimiento `rdsadmin.create_database` almacenado.

Establecimiento del parámetro **`db2_compatibility_vector`**

1. Cree un grupo de parámetros personalizado. (No puede modificar parámetros en un grupo de parámetros predeterminado).
2. Modifique el parámetro.
3. Cree una instancia de base de datos.
4. Cree una base de datos mediante el procedimiento `rdsadmin.create_database` almacenado.
5. Asocie el grupo de parámetros a la instancia de base de datos que contiene la base de datos.

Migración de bases de datos que contienen paquetes NO VÁLIDOS

Si migra las bases de datos de Db2 que contienen paquetes `INVALID` a RDS para Db2 mediante el comando `RESTORE`, es posible que se produzcan problemas al empezar a utilizar las bases de datos. Los paquetes `INVALID` pueden provocar problemas debido a la configuración de autorización del usuario de la instancia de base de datos `rdsdb` y a la retirada de la autorización de `PUBLIC`. Los paquetes de `INVALID` provocan el error de los siguientes comandos:

- `db2updv115`
- `db2 "call SYSPROC.ADMIN_REVALIDATE_DB_OBJECTS()"`

Antes de migrar la base de datos con el comando `RESTORE`, asegúrese de que la base de datos no contenga paquetes `INVALID` ejecutando el siguiente comando:

```
db2 "select count(*) from sysibm.sysroutines where valid = 'N'"
```

Si el comando devuelve un recuento superior a cero, ejecute el siguiente comando:

```
db2 "call SYSPROC.ADMIN_REVALIDATE_DB_OBJECTS()"
```

Después, ejecute el comando anterior para confirmar que la base de datos ya no contiene paquetes `INVALID`.

```
db2 "select count(*) from sysibm.sysroutines where valid = 'N'"
```

Ahora estará listo para hacer una copia de seguridad de la base de datos y restaurarla en la instancia de base de datos de RDS para Db2.

Referencia de procedimientos almacenados de Amazon RDS para Db2

Para administrar sus instancias de base de datos de Amazon RDS para Db2 ejecutando el motor Db2, llame a los procedimientos almacenados integrados.

Procedimiento almacenado	Categoría	Descripción
???	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.activate_database` para activar una base de datos en una instancia de base de datos independiente de RDS para Db2.
the section called “rdsadmin.add_groups”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.add_groups` para agregar uno o más grupos a un usuario para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.add_user”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.add_user` para agregar un usuario a una lista de autorización para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.alter_bufferpool”	Grupos de búferes	Utilice el procedimiento almacenado `rdsadmin.alter_bufferpool` para modificar un grupo de búferes para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.alter_tablespace”	Espacios de tabla	Utilice el procedimiento almacenado `rdsadmin.alter_tablespace` para modificar un espacio de tabla para una base

Procedimiento almacenado	Categoría	Descripción
		de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.catalog_storage_access”	Acceso al almacenamiento	Utilice el procedimiento almacenado `rdsadmin.catalog_storage_access` para catalogar un alias de almacenamiento para acceder a un bucket de Amazon S3 con archivos de datos de Db2 para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.change_password”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.change_password` para cambiar la contraseña de usuario de una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.complete_rollforward”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.complete_rollforward` para poner en línea una base de datos en una instancia de RDS para Db2 desde un estado `ROLL-FORWARD PENDING` . Se produce un estado `ROLL-FORWARD PENDING` cuando se llama a the section called “rdsadmin.rollforward_database” pero se establece el parámetro `complete_rollforward` en `FALSE`.
the section called “rdsadmin.configure_db_audit”	Políticas de auditoría	Utilice el procedimiento almacenado `rdsadmin.configure_db_audit` para modificar una política de auditoría para una base de datos en una instancia de base de datos de RDS para Db2. Si no existe ninguna política de auditoría, al ejecutar este procedimiento almacenado se crea una política de auditoría.

Procedimiento almacenado	Categoría	Descripción
the section called “rdsadmin.create_bufferpool”	Grupos de búferes	Utilice el procedimiento almacenado `rdsadmin.create_bufferpool` para crear un grupo de búferes para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.create_database”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.create_database` para crear una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.create_role”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.create_role` para crear un rol y asociarlo a una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.create_tablespace”	Espacios de tabla	Utilice el procedimiento almacenado `rdsadmin.create_tablespace` para crear un espacio de tabla para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.db2pd_command”	Bases de datos	Utilice el procedimiento `rdsadmin.db2pd_command` almacenado para recopilar información sobre una base de datos en una instancia de base de datos de RDS para Db2. Esta información puede ayudar a supervisar y solucionar problemas de bases de datos en RDS para Db2.

Procedimiento almacenado	Categoría	Descripción
the section called “rdsadmin.dbadm_grant”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.dbadm_grant` para conceder uno o más tipos de autorización (`DBADM`, `ACCESSCTRL` o `DATAACCESS`) a uno o más roles, usuarios o grupos de una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.dbadm_revoke”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.dbadm_revoke` para revocar uno o más tipos de autorización (`DBADM`, `ACCESSCTRL` o `DATAACCESS`) de uno o más roles, usuarios o grupos para una base de datos en una instancia de base de datos de RDS para Db2.
???	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.deactivate_database` para desactivar una base de datos en una instancia de base de datos de RDS para Db2. Puede desactivar las bases de datos para conservar los recursos de memoria.
the section called “rdsadmin.disable_db_audit”	Políticas de auditoría	Utilice el procedimiento almacenado `rdsadmin.disable_db_audit` para detener el registro de auditorías y eliminar una política de auditoría de una base de datos en una instancia de base de datos de RDS para Db2.

Procedimiento almacenado	Categoría	Descripción
the section called “rdsadmin.drop_bufferpool”	Grupos de búferes	Utilice el procedimiento almacenado `rdsadmin.drop_bufferpool` para descartar un grupo de búferes para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.drop_database”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.drop_database` para descartar una base de datos de una instancia de base de datos de RDS para Db2.
???	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.drop_role` para eliminar un rol de una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.drop_tablespace”	Espacios de tabla	Utilice el procedimiento almacenado `rdsadmin.drop_tablespace` para descartar un espacio de tabla de una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.force_application”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.force_application` para forzar a las aplicaciones a salir de una base de datos en una instancia de base de datos de RDS para Db2 para realizar tareas de mantenimiento.

Procedimiento almacenado	Categoría	Descripción
the section called “rdsadmin.grant_role”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.grant_role` para asignar un rol a un rol, usuario o grupo del beneficiario en una base de datos en una instancia de base de datos de RDS para Db2. También puede utilizar este procedimiento almacenado para conceder al rol del beneficiario la autorización `DBADM` para asignar roles.
???	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.list_archive_log_information` para devolver información sobre los registros de archivo de una base de datos en una instancia de base de datos de RDS para Db2. Esta información incluye detalles como el tamaño y la fecha de creación de los archivos de registro individuales, y el almacenamiento total utilizado por los archivos de registro de archivo.
the section called “rdsadmin.list_users”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.list_users` para devolver una lista de usuarios en una lista de autorizaciones para una base de datos en una instancia de base de datos de RDS para Db2.

Procedimiento almacenado	Categoría	Descripción
???	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.reactivate_database` para reactivar una base de datos en una instancia de base de datos de RDS para Db2 después de realizar cambios en la configuración de la base de datos. Para una base de datos en una instancia de base de datos independiente, puede utilizar este procedimiento almacenado o el procedimiento almacenado ???.
the section called “rdsadmin.remove_groups”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.remove_groups` para eliminar uno o más grupos de un usuario para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.remove_user”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.remove_user` para eliminar un usuario de una lista de autorización para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.rename_tablespace”	Espacios de tabla	Utilice el procedimiento almacenado `rdsadmin.rename_tablespace` para renombrar un espacio de tabla para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.restore_database”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.restore_database` para restaurar una base de datos en una instancia de base de datos de RDS para Db2 de un bucket de Amazon S3.

Procedimiento almacenado	Categoría	Descripción
the section called “rdsadmin.revoke_role”	Concesión y revocación de privilegios	Utilice el procedimiento almacenado `rdsadmin.revoke_role` para revocar un rol de un rol, usuario o grupo del beneficiario en una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.rollforward_database”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.rollforward_database` para poner en línea una base de datos en una instancia de base de datos de RDS para Db2 y aplicar los registros de transacciones después de restaurar una base de datos en una instancia de base de datos de RDS para Db2 mediante una llamada a the section called “rdsadmin.restore_database”.
the section called “rdsadmin.set_archive_log_retention”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.set_archive_log_retention` para configurar durante cuánto tiempo se retendrán los archivos de registro de una base de datos en una instancia de base de datos de RDS para Db2. También puede usar este procedimiento almacenado para deshabilitar la retención del registro de archivos.
the section called “rdsadmin.set_configuration”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.set_configuration` para configurar determinadas opciones para una base de datos en una instancia de base de datos de RDS para Db2.

Procedimiento almacenado	Categoría	Descripción
the section called “rdsadmin.show_archive_log_retention”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.show_archive_log_retention` para devolver la configuración actual de retención del registro de archivos de una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.show_configuration”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.show_configuration` para devolver una o más configuraciones modificables para una base de datos en una instancia de base de datos de RDS para Db2.
the section called “rdsadmin.uncatalog_storage_access”	Acceso al almacenamiento	Utilice el procedimiento `rdsadmin.uncatalog_storage_access` almacenado para eliminar un alias de almacenamiento para acceder a un bucket de Amazon S3 con archivos de datos de Db2.
the section called “rdsadmin.update_db_param”	Bases de datos	Utilice el procedimiento almacenado `rdsadmin.update_db_param` para actualizar los parámetros de base de datos para una base de datos en una instancia de base de datos de RDS para Db2.

Temas

- Consideraciones sobre los procedimientos almacenados de Amazon RDS para Db2
- Concesión y revocación de privilegios
- Procedimientos almacenados para políticas de auditoría de RDS para Db2
- Procedimientos almacenados de grupos de búferes de RDS para Db2
- Administración de bases de datos
- Procedimientos almacenados de acceso al almacenamiento de RDS para Db2

- Procedimientos almacenados de espacios de tablas de RDS para Db2

Consideraciones sobre los procedimientos almacenados de Amazon RDS para Db2

Antes de utilizar los procedimientos almacenados del sistema para Amazon RDS para las instancias de bases de datos de Db2 que ejecuten el motor de Db2, revise la información siguiente:

- Antes de ejecutar los procedimientos almacenados, primero debe conectarse a la base de datos de `rdsadmin` como usuario maestro de su instancia de base de datos de RDS para Db2. En el siguiente ejemplo, sustituya *`master_username`* y *`master_password`* por su propia información.

  ```
  db2 "connect to rdsadmin user master_username using master_password"
  ```

- Los procedimientos almacenados devuelven el parámetro `ERR_MESSAGE`, que indica si el procedimiento almacenado se ha ejecutado correctamente o no; en caso negativo, también especifica el motivo.

  Ejemplos

  El siguiente ejemplo indica que el procedimiento almacenado se ha ejecutado correctamente.

  ```
  Parameter Name : ERR_MESSAGE
  Parameter Value : -
  Return Status = 0
  ```

  El siguiente ejemplo indica que el procedimiento almacenado no se ha ejecutado correctamente porque el nombre del bucket de Amazon S3 utilizado en el procedimiento almacenado no era válido.

  ```
  Parameter Name : ERR_MESSAGE
  Parameter Value : Invalid S3 bucket name
  Return Status = -1006
  ```

Para ver los mensajes de error devueltos al llamar a los procedimientos almacenados, consulte the section called “Errores en los procedimientos almacenados”.

Para obtener información sobre cómo comprobar el estado de un procedimiento almacenado, consulte rdsadmin.get_task_status.

Concesión y revocación de privilegios

Los siguientes procedimientos almacenados otorgan y revocan privilegios para bases de datos de Amazon RDS para Db2. Para ejecutar estos procedimientos, el usuario maestro debe conectarse primero a la base de datos `rdsadmin`.

Temas

- rdsadmin.create_role
- rdsadmin.grant_role
- rdsadmin.revoke_role
- rdsadmin.add_user
- rdsadmin.change_password
- rdsadmin.list_users
- rdsadmin.remove_user
- rdsadmin.add_groups
- rdsadmin.remove_groups
- rdsadmin.dbadm_grant
- rdsadmin.dbadm_revoke

rdsadmin.create_role

Crea un rol.

Sintaxis

```
db2 "call rdsadmin.create_role(
    'database_name',
    'role_name')"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

role_name

El nombre del rol que desea crear. El tipo de datos es `varchar`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de creación de un rol, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se crea un rol denominado `MY_ROLE` para la base de datos `DB2DB`.

```
db2 "call rdsadmin.create_role(
    'DB2DB',
    'MY_ROLE')"
```

rdsadmin.grant_role

Asigna un rol a un rol, usuario o grupo.

Sintaxis

```
db2 "call rdsadmin.grant_role(
    ?,
    'database_name',
    'role_name',
    'grantee',
    'admin_option')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetro que genera el identificador único de la tarea. Este parámetro solo acepta ?.

Se requieren los siguientes parámetros de entrada:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

role_name

El nombre del rol que desea crear. El tipo de datos es `varchar`.

grantee

El rol, el usuario o el grupo que recibirá la autorización. El tipo de datos es `varchar`. Valores válidos: `ROLE`, `USER`, `GROUP`, `PUBLIC`.

El formato debe ser un valor seguido del nombre. Separe los valores y los nombres con comas. Ejemplo: "`USER` *`user1`*`, `*`user2`*`, GROUP` *`group1`*`, `*`group2`*". Reemplace los nombres con su propia información.

El siguiente parámetro de entrada es opcional:

admin_option

Especifica si el concesionario `ROLE` tiene la autorización `DBADM` para asignar roles. El tipo de datos es `char`. El valor predeterminado es `N`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de asignación de un rol, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo asigna un rol llamado `ROLE_TEST` para la base de datos `TESTDB` al rol llamado `role1`, al usuario llamado `user1` y al grupo llamado `group1`. `ROLE_TEST` recibe la autorización de administrador para asignar roles.

```
db2 "call rdsadmin.grant_role(
    ?,
    'TESTDB',
    'ROLE_TEST',
    'ROLE role1, USER user1, GROUP group1',
    'Y')"
```

En el siguiente ejemplo, se asigna un rol llamado `ROLE_TEST` para la base de datos `TESTDB` a `PUBLIC`. `ROLE_TEST` no recibe la autorización de administrador para asignar roles.

```
db2 "call rdsadmin.grant_role(
    ?,
    'TESTDB',
    'ROLE_TEST',
    'PUBLIC')"
```

rdsadmin.revoke_role

Revoca un rol de un rol, usuario o grupo.

Sintaxis

```
db2 "call rdsadmin.revoke_role(
    ?,
    'database_name',
    'role_name',
    'grantee')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetro que genera el identificador único de la tarea. Este parámetro solo acepta ?

Se requieren los siguientes parámetros de entrada:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

role_name

El nombre del rol que desea revocar. El tipo de datos es `varchar`.

grantee

El rol, el usuario o el grupo que perderá la autorización. El tipo de datos es `varchar`. Valores válidos: `ROLE`, `USER`, `GROUP`, `PUBLIC`.

El formato debe ser un valor seguido del nombre. Separe los valores y los nombres con comas. Ejemplo: "`USER` *`user1`*`, `*`user2`*`, GROUP` *`group1`*`, `*`group2`*". Reemplace los nombres con su propia información.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de asignación de un rol, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se revoca un rol llamado `ROLE_TEST` para la base de datos `TESTDB` del rol llamado `role1`, del usuario llamado `user1` y del grupo llamado `group1`.

```
db2 "call rdsadmin.revoke_role(
    ?,
    'TESTDB',
    'ROLE_TEST',
    'ROLE role1, USER user1, GROUP group1')"
```

En el siguiente ejemplo, se revoca un rol llamado `ROLE_TEST` para la base de datos `TESTDB` de `PUBLIC`.

```
db2 "call rdsadmin.revoke_role(
    ?,
    'TESTDB',
    'ROLE_TEST',
    'PUBLIC')"
```

rdsadmin.add_user

Agrega un usuario a una lista de autorizaciones.

Sintaxis

```
db2 "call rdsadmin.add_user(
```

```
    'username',
    'password',
    'group_name,group_name')"
```

Parámetros

Se requieren los siguientes parámetros:

username

El nombre de usuario de un usuario. El tipo de datos es `varchar`.

password

La contraseña de un usuario. El tipo de datos es `varchar`.

El siguiente parámetro es opcional:

group_name

El nombre de un grupo al que quiera agregar al usuario. El tipo de datos es `varchar`. El valor predeterminado es una cadena vacía o null.

Notas de uso

Puede agregar un usuario a uno o más grupos separando los nombres de los grupos con comas.

Puede crear un grupo al crear un usuario nuevo o al agregar un grupo a un usuario existente. No puede crear un grupo por sí mismo.

> **Note**
>
> El número máximo de usuarios que puede agregar llamando a `rdsadmin.add_user` es de 5000.

Para obtener más información sobre cómo comprobar el estado al agregar un usuario, consulte rdsadmin.get_task_status.

Ejemplos

En el ejemplo siguiente, se crea un usuario llamado `jorge_souza` y se asigna a los grupos denominados `sales` y `inside_sales`.

```
db2 "call rdsadmin.add_user(
    'jorge_souza',
    '*******',
    'sales,inside_sales')"
```

rdsadmin.change_password

Cambia la contraseña de un usuario

Sintaxis

```
db2 "call rdsadmin.change_password(
    'username',
    'new_password')"
```

Parámetros

Se requieren los siguientes parámetros:

`username`

El nombre de usuario de un usuario. El tipo de datos es `varchar`.

`new_password`

Una nueva contraseña para el usuario. El tipo de datos es `varchar`.

Notas de uso

Para obtener información sobre cómo comprobar el estado de un cambio de contraseña, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo se cambia la contraseña de `jorge_souza`.

```
db2 "call rdsadmin.change_password(
```

```
    'jorge_souza',
    '*******')"
```

rdsadmin.list_users

Muestra los usuarios de una lista de autorización.

Sintaxis

```
db2 "call rdsadmin.list_users()"
```

Notas de uso

Para obtener más información sobre cómo comprobar el estado al mostrar los usuarios, consulte rdsadmin.get_task_status.

rdsadmin.remove_user

Elimina el usuario de la lista de autorizaciones.

Sintaxis

```
db2 "call rdsadmin.remove_user('username')"
```

Parámetros

El siguiente parámetro es obligatorio:

username

El nombre de usuario de un usuario. El tipo de datos es `varchar`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de eliminación de un usuario, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se impide a `jorge_souza` el acceso a las bases de datos de las instancias de bases de datos de RDS para Db2.

```
db2 "call rdsadmin.remove_user('jorge_souza')"
```

rdsadmin.add_groups

Agrega grupos a un usuario.

Sintaxis

```
db2 "call rdsadmin.add_groups(
    'username',
    'group_name,group_name')"
```

Parámetros

Se requieren los siguientes parámetros:

username

El nombre de usuario de un usuario. El tipo de datos es `varchar`.

group_name

El nombre de un grupo al que quiera agregar al usuario. El tipo de datos es `varchar`. El valor predeterminado es una cadena vacía.

Notas de uso

Puede agregar uno o más grupos a un usuario separando los nombres de los grupos con comas. Para obtener más información sobre cómo comprobar el estado al agregar grupos, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se agregan los grupos `direct_sales` y `b2b_sales` al usuario `jorge_souza`.

```
db2 "call rdsadmin.add_groups(
    'jorge_souza',
    'direct_sales,b2b_sales')"
```

rdsadmin.remove_groups

Elimina grupos de un usuario.

Sintaxis

```
db2 "call rdsadmin.remove_groups(
    'username',
    'group_name,group_name')"
```

Parámetros

Se requieren los siguientes parámetros:

username

El nombre de usuario de un usuario. El tipo de datos es `varchar`.

group_name

El nombre de un grupo del que quiera eliminar al usuario. El tipo de datos es `varchar`.

Notas de uso

Puede eliminar uno o más grupos de un usuario separando los nombres de los grupos con comas.

Para obtener más información sobre cómo comprobar el estado de eliminación de grupos, consulte rdsadmin.get_task_status.

Ejemplos

En el ejemplo siguiente se quitan los grupos `direct_sales` y `b2b_sales` del usuario `jorge_souza`.

```
db2 "call rdsadmin.remove_groups(
    'jorge_souza',
    'direct_sales,b2b_sales')"
```

rdsadmin.dbadm_grant

Concede autorización `DBADM`, `ACCESSCTRL` o `DATAACCESS` a un rol, usuario o grupo.

Sintaxis

```
db2 "call rdsadmin.dbadm_grant(
    ?,
    'database_name',
    'authorization',
    'grantee')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetro que genera el identificador único de la tarea. Este parámetro solo acepta ?.

Se requieren los siguientes parámetros de entrada:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

authorization

El tipo de autorización que se va a conceder. El tipo de datos es `varchar`. Valores válidos: `DBADM`, `ACCESSCTRL`, `DATAACCESS`.

Separe los diversos tipos con comas.

grantee

El rol, el usuario o el grupo que recibirá la autorización. El tipo de datos es `varchar`. Valores válidos: `ROLE`, `USER`, `GROUP`.

El formato debe ser un valor seguido del nombre. Separe los valores y los nombres con comas. Ejemplo: "`USER` *`user1`*`, `*`user2`*`, GROUP` *`group1`*`, `*`group2`*". Reemplace los nombres con su propia información.

Notas de uso

El rol que vaya a recibir el acceso debe existir.

Para obtener más información sobre cómo comprobar el estado de concesión de acceso de administrador de base de datos, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo otorga acceso de administrador de base de datos a la base de datos denominada TESTDB para el rol ROLE_DBA.

```
db2 "call rdsadmin.dbadm_grant(
    ?,
    'TESTDB',
    'DBADM',
    'ROLE ROLE_DBA')"
```

El siguiente ejemplo otorga acceso de administrador de base de datos a la base de datos denominada TESTDB para user1 y group1.

```
db2 "call rdsadmin.dbadm_grant(
    ?,
    'TESTDB',
    'DBADM',
    'USER user1, GROUP group1')"
```

El siguiente ejemplo otorga acceso de administrador de base de datos a la base de datos denominada TESTDB para user1, user2, group1 y group2.

```
db2 "call rdsadmin.dbadm_grant(
    ?,
    'TESTDB',
    'DBADM',
    'USER user1, user2, GROUP group1, group2')"
```

rdsadmin.dbadm_revoke

Revoca la autorización DBADM, ACCESSCTRL o DATAACCESS de un rol, usuario o grupo.

Sintaxis

```
db2 "call rdsadmin.dbadm_revoke(
    ?,
    'database_name',
```

```
    'authorization',
    'grantee')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

El identificador único de la tarea. Este parámetro solo acepta ?.

Se requieren los siguientes parámetros de entrada:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

authorization

El tipo de autorización que se va a revocar. El tipo de datos es `varchar`. Valores válidos: `DBADM`, `ACCESSCTRL`, `DATAACCESS`.

Separe los diversos tipos con comas.

grantee

El rol, el usuario o el grupo al que se va a revocar la autorización. El tipo de datos es `varchar`. Valores válidos: `ROLE`, `USER`, `GROUP`.

El formato debe ser un valor seguido del nombre. Separe los valores y los nombres con comas. Ejemplo: "`USER` *`user1`*`, `*`user2`*`, GROUP` *`group1`*`, `*`group2`*". Reemplace los nombres con su propia información.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de revocación de acceso de administrador de base de datos, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo revoca el acceso de administrador de base de datos a la base de datos denominada `TESTDB` para el rol `ROLE_DBA`.

```
db2 "call rdsadmin.dbadm_revoke(
    ?,
    'TESTDB',
    'DBADM',
    'ROLE ROLE_DBA')"
```

El siguiente ejemplo revoca el acceso de administrador de base de datos a la base de datos denominada TESTDB para `user1` y `group1`.

```
db2 "call rdsadmin.dbadm_revoke(
    ?,
    'TESTDB',
    'DBADM',
    'USER user1, GROUP group1')"
```

El siguiente ejemplo revoca el acceso de administrador de base de datos a la base de datos denominada TESTDB para `user1`, `user2`, `group1` y `group2`.

```
db2 "call rdsadmin.dbadm_revoke(
    ?,
    'TESTDB',
    'DBADM',
    'USER user1, user2, GROUP group1, group2')"
```

Procedimientos almacenados para políticas de auditoría de RDS para Db2

Los procedimientos almacenados que se describen en este tema administran las políticas de auditoría para bases de datos de Amazon RDS para Db2 que utilizan el registro de auditoría. Para obtener más información, consulte the section called “Registro de auditoría de Db2”. Para ejecutar estos procedimientos, el usuario maestro debe conectarse primero a la base de datos `rdsadmin`.

Consulte los siguientes procedimientos almacenados integrados para obtener información sobre su sintaxis, parámetros, notas de uso y ejemplos.

Procedimientos almacenados

- rdsadmin.configure_db_audit
- rdsadmin.disable_db_audit

rdsadmin.configure_db_audit

Configura la política de auditoría de la base de datos de RDS para Db2 especificada por *db_name*. Si la política que está configurando no existe, al llamar a este procedimiento almacenado, se creará. Si esta política existe, al llamar a este procedimiento almacenado, se modificará con los valores de los parámetros que proporcione.

Sintaxis

```
db2 "call rdsadmin.configure_db_audit(
    'db_name',
    'category',
    'category_setting',
    '?')"
```

Parámetros

Se requieren los siguientes parámetros.

db_name

El nombre de la base de datos de RDS para Db2 para la que hay que configurar la política de auditoría. El tipo de datos es `varchar`.

categoría

El nombre de la categoría para la que hay que configurar la política de auditoría. El tipo de datos es `varchar`. Esta es una lista de valores válidos para este parámetro.

- `ALL`: con `ALL`, Amazon RDS no incluye las categorías `CONTEXT`, `EXECUTE` o `ERROR`.
- `AUDIT`
- `CHECKING`
- `CONTEXT`
- `ERROR`
- `EXECUTE`: puede configurar esta categoría con o sin datos. La configuración con datos implica registrar también valores de datos de entrada suministrados para cualquier variable de host y marcador de parámetro. La opción predeterminada es la configuración sin datos. Para obtener más información, consulte la descripción del parámetro *`category_setting`* y los the section called “Ejemplos”.
- `OBJMAINT`
- `SECMAINT`
- `SYSADMIN`
- `VALIDATE`

Para obtener más información sobre estas categorías, consulte la documentación de IBM Db2.

category_setting

La configuración de la categoría de auditoría especificada. El tipo de datos es `varchar`.

En la tabla siguiente, se muestran los valores válidos de la configuración de cada categoría.

Categoría	Configuración válidas para las categorías
`ALL`	`BOTH|FAILURE|SUCCESS|NONE`
`AUDIT`	
`CHECKING`	
`CONTEXT`	
`OBJMAINT`	

Categoría	Configuración válidas para las categorías
SECMAINT SYSADMIN VALIDATE	
ERROR	AUDIT|NORMAL . El valor predeterminado es NORMAL.
EXECUTE	BOTH,WITH|BOTH,WITHOUT|FAILURE,WITH| FAILURE,WITHOUT|SUCCESS,WITH|SUCCESS ,WITHOUT|NONE

Notas de uso

Antes de llamar a `rdsadmin.configure_db_audit`, compruebe que la instancia de base de datos de RDS para Db2 con la base de datos para la que está configurando la política de auditoría esté asociada a un grupo de opciones que incluya la opción `DB2_AUDIT`. Para obtener más información, consulte the section called “Configuración del registro de auditoría de Db2”.

Tras configurar la política de auditoría, puede comprobar el estado de la configuración de auditoría de la base de datos siguiendo los pasos que se indican en Comprobar la configuración de la auditoría.

La especificación `ALL` para el parámetro `category` no incluye las categorías `CONTEXT`, `EXECUTE` ni `ERROR`. Para agregar estas categorías a su política de auditoría, llame a `rdsadmin.configure_db_audit` por separado con cada categoría que desee agregar. Para obtener más información, consulte the section called “Ejemplos”.

Ejemplos

Los siguientes ejemplos crean o modifican la política de auditoría de una base de datos denominada `TESTDB`. En los ejemplos 1 a 5, si la categoría `ERROR` no se ha configurado previamente, esta categoría se establece en `NORMAL` (valor predeterminado). Para cambiar esa configuración a `AUDIT`, siga el Example 6: Specifying the ERROR category.

Ejemplo 1: Especificación de la categoría **`ALL`**

```
db2 "call rdsadmin.configure_db_audit('TESTDB', 'ALL', 'BOTH', ?)"
```

En el ejemplo, la llamada configura las categorías AUDIT, CHECKING, OBJMAINT, SECMAINT, SYSADMIN y VALIDATE en la política de auditoría. La especificación de BOTH significa que se auditarán tanto los eventos correctos como incorrectos para cada categoría.

Ejemplo 2: Especificación de la categoría **EXECUTE** con datos

```
db2 "call rdsadmin.configure_db_audit('TESTDB', 'EXECUTE', 'SUCCESS,WITH', ?)"
```

En el ejemplo, la llamada configura la categoría EXECUTE en la política de auditoría. La especificación de SUCCESS,WITH significa que los registros de esta categoría incluirán solo los eventos correctos, así como los valores de datos de entrada proporcionados para variables de host y marcadores de parámetros.

Ejemplo 3: Especificación de la categoría **EXECUTE** sin datos

```
db2 "call rdsadmin.configure_db_audit('TESTDB', 'EXECUTE', 'FAILURE,WITHOUT', ?)"
```

En el ejemplo, la llamada configura la categoría EXECUTE en la política de auditoría. La especificación de FAILURE,WITHOUT significa que los registros de esta categoría incluirán solo los eventos con error, y no incluirán los valores de datos de entrada proporcionados para variables de host o marcadores de parámetros.

Ejemplo 4: Especificación de la categoría **EXECUTE** sin eventos de estado

```
db2 "call rdsadmin.configure_db_audit('TESTDB', 'EXECUTE', 'NONE', ?)"
```

En el ejemplo, la llamada configura la categoría EXECUTE en la política de auditoría. La especificación de NONE significa que no se auditará ningún evento de esta categoría.

Ejemplo 5: Especificación de la categoría **OBJMAINT**

```
db2 "call rdsadmin.configure_db_audit('TESTDB', 'OBJMAINT', 'NONE', ?)"
```

En el ejemplo, la llamada configura la categoría OBJMAINT en la política de auditoría. La especificación de NONE significa que no se auditará ningún evento de esta categoría.

Ejemplo 6: Especificación de la categoría **ERROR**

```
db2 "call rdsadmin.configure_db_audit('TESTDB', 'ERROR', 'AUDIT', ?)"
```

En el ejemplo, la llamada configura la categoría `ERROR` en la política de auditoría. La especificación de `AUDIT` significa que todos los errores, incluidos aquellos que ocurran en el propio registro de auditoría, se capturan en los registros. El tipo de error predeterminado es `NORMAL`. Con `NORMAL`, los errores generados por la auditoría se ignoran y solo se capturan los `SQLCODE` correspondientes a los errores asociados a la operación que se está realizando.

rdsadmin.disable_db_audit

Detiene el registro de auditoría de la base de datos de RDS para Db2 especificada por *db_name* y elimina la política de auditoría configurada para ella.

> **Note**
>
> Este procedimiento almacenado solo elimina las políticas de auditoría que se configuraron mediante una llamada a the section called “rdsadmin.configure_db_audit”.

Sintaxis

```
db2 "call rdsadmin.disable_db_audit('db_name', ?)"
```

Parámetros

Se requieren los siguientes parámetros.

db_name

El nombre de la base de datos de RDS para Db2 para la que se va a deshabilitar el registro de auditoría. El tipo de datos es `varchar`.

Notas de uso

La llamada a `rdsadmin.disable_db_audit` no deshabilita el registro de auditoría de la instancia de base de datos de RDS para Db2. Para deshabilitar el registro de auditoría en el nivel de instancia de la base de datos, elimine el grupo de opciones de la instancia de la base de datos. Para obtener más información, consulte Deshabilitación del registro de auditoría de Db2.

Ejemplos

El siguiente ejemplo deshabilita el registro de auditoría para una base de datos denominada `TESTDB`.

```
db2 "call rdsadmin.disable_db_audit('TESTDB', ?)"
```

Procedimientos almacenados de grupos de búferes de RDS para Db2

Los procedimientos almacenados integrados que se describen en este tema administran grupos de búferes para bases de datos de Amazon RDS para Db2. Para ejecutar estos procedimientos, el usuario maestro debe conectarse primero a la base de datos `rdsadmin`.

Estos procedimientos almacenados se utilizan en diversas tareas. Esta lista no es exhaustiva.

- Tareas comunes para grupos de búferes
- Generación de informes de rendimiento
- Copia de metadatos de bases de datos con db2look
- Creación de una base de datos de repositorios para IBM Db2 Data Management Console

Consulte los siguientes procedimientos almacenados integrados para obtener información sobre su sintaxis, parámetros, notas de uso y ejemplos.

Procedimientos almacenados

- rdsadmin.create_bufferpool
- rdsadmin.alter_bufferpool
- rdsadmin.drop_bufferpool

rdsadmin.create_bufferpool

Crea un grupo de búferes.

Sintaxis

```
db2 "call rdsadmin.create_bufferpool(
    'database_name',
    'buffer_pool_name',
    buffer_pool_size,
    'immediate',
    'automatic',
    page_size,
    number_block_pages,
    block_size)"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

buffer_pool_name

Nombre del grupo de búferes que se va a crear. El tipo de datos es `varchar`.

Los siguientes parámetros son opcionales:

buffer_pool_size

El tamaño del grupo de búferes en número de páginas. El tipo de datos es `integer`. El valor predeterminado es `-1`.

immediate

Especifica si el comando se ejecuta inmediatamente. El tipo de datos es `char`. El valor predeterminado es `Y`.

automatic

Especifica si el grupo de búferes se va a configurar como automático. El tipo de datos es `char`. El valor predeterminado es `Y`.

page_size

El tamaño de página del grupo de búferes El tipo de datos es `integer`. Valores válidos: `4096`, `8192`, `16384`, `32768`. El valor predeterminado es `8192`.

number_block_pages

El número de páginas de bloques en los grupos de búferes. El tipo de datos es `integer`. El valor predeterminado es `0`.

block_size

El tamaño de bloque de las páginas de bloques. El tipo de datos es `integer`. Valores válidos: de `2` a `256`. El valor predeterminado es `32`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de creación de un grupo de búferes, consulte rdsadmin.get_task_status.

Ejemplos

Ejemplo 1: Crear un conjunto de búferes con los parámetros predeterminados

El siguiente ejemplo crea un grupo de búferes llamado BP8 para una base de datos llamada TESTDB con los parámetros predeterminados, de modo que el grupo de búferes utiliza un tamaño de página de 8 KB.

```
db2 "call rdsadmin.create_bufferpool(
    'TESTDB',
    'BP8')"
```

Ejemplo 2: Crear un grupo de búferes para que se ejecute inmediatamente sin asignación automática

En el siguiente ejemplo, se crea un grupo de búferes denominado BP16 para una base de datos denominada TESTDB que utiliza un tamaño de página de 16 KB con un recuento inicial de páginas de 1000 y se establece en automático. Db2 ejecuta el comando inmediatamente. Si utiliza un recuento inicial de páginas de -1, Db2 utilizará la asignación automática de páginas.

```
db2 "call rdsadmin.create_bufferpool(
    'TESTDB',
    'BP16',
    1000,
    'Y',
    'Y',
    16384)"
```

Ejemplo 3: Crear un grupo de búferes para que se ejecute de forma inmediata mediante páginas de bloques

En el siguiente ejemplo, se crea un grupo de búferes llamado BP16 para una base de datos llamada TESTDB. Este grupo de búferes tiene un tamaño de página de 16 KB con un recuento inicial de 10 000 páginas. Db2 ejecuta el comando inmediatamente utilizando 500 páginas de bloque con un tamaño de bloque de 512.

```
db2 "call rdsadmin.create_bufferpool(
```

```
    'TESTDB',
    'BP16',
    10000,
    'Y',
    'Y',
    16384,
    500,
    512)"
```

rdsadmin.alter_bufferpool

Modifica un grupo de búferes.

Sintaxis

```
db2 "call rdsadmin.alter_bufferpool(
    'database_name',
    'buffer_pool_name',
    buffer_pool_size,
    'immediate',
    'automatic',
    change_number_blocks,
    number_block_pages,
    block_size)"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

Nombre de la base de datos en la que se va a ejecutar el comando. El tipo de datos es `varchar`.

buffer_pool_name

Nombre del grupo de búferes que se va a modificar. El tipo de datos es `varchar`.

buffer_pool_size

El tamaño del grupo de búferes en número de páginas. El tipo de datos es `integer`.

Los siguientes parámetros son opcionales:

immediate

Especifica si el comando se ejecuta inmediatamente. El tipo de datos es `char`. El valor predeterminado es `Y`.

automatic

Especifica si el grupo de búferes se va a configurar como automático. El tipo de datos es `char`. El valor predeterminado es `N`.

change_number_blocks

Especifica si se ha producido un cambio en el número de páginas de bloques del conjunto de búferes. El tipo de datos es `char`. El valor predeterminado es `N`.

number_block_pages

El número de páginas de bloques en los grupos de búferes. El tipo de datos es `integer`. El valor predeterminado es `0`.

block_size

El tamaño de bloque de las páginas de bloques. El tipo de datos es `integer`. Valores válidos: de `2` a `256`. El valor predeterminado es `32`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de modificación de un grupo de búferes, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se modifica un grupo de búferes llamado `BP16` para una base de datos llamada `TESTDB` a no automático y se cambia el tamaño a 10 000 páginas. Db2 ejecuta este comando inmediatamente.

```
db2 "call rdsadmin.alter_bufferpool(
    'TESTDB',
    'BP16',
    10000,
    'Y',
    'N')"
```

rdsadmin.drop_bufferpool

Elimina un grupo de búferes.

Sintaxis

```
db2 "call rdsadmin.drop_bufferpool(
    'database_name',
    'buffer_pool_name'"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

El nombre de la base de datos a la que pertenece el grupo de búferes. El tipo de datos es `varchar`.

buffer_pool_name

Nombre del grupo de búferes que se va a eliminar. El tipo de datos es `varchar`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de eliminación de un grupo de búferes, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo elimina un grupo de búferes llamado `BP16` para una base de datos llamada `TESTDB`.

```
db2 "call rdsadmin.drop_bufferpool(
    'TESTDB',
    'BP16')"
```

Administración de bases de datos

Los siguientes procedimientos almacenados administran bases de datos de Amazon RDS para Db2. Para ejecutar estos procedimientos, el usuario maestro debe conectarse primero a la base de datos `rdsadmin`.

Temas

- rdsadmin.create_database
- rdsadmin.drop_database
- rdsadmin.update_db_param
- rdsadmin.set_configuration
- rdsadmin.show_configuration
- rdsadmin.restore_database
- rdsadmin.rollforward_database
- rdsadmin.complete_rollforward
- rdsadmin.db2pd_command
- rdsadmin.force_application
- rdsadmin.set_archive_log_retention
- rdsadmin.show_archive_log_retention

rdsadmin.create_database

Crea una base de datos.

Sintaxis

```
db2 "call rdsadmin.create_database('database_name')"
```

Parámetros

> **Note**
>
> Este procedimiento almacenado no valida la combinación de parámetros necesarios. Al llamar a rdsadmin.get_task_status, la función definida por el usuario podría devolver un error debido a una combinación de `database_codeset`, `database_territory` y

`database_collation` que no es válida. Para obtener más información, consulte Choosing the code page, territory, and collation for your database en la documentación de IBM Db2.

El siguiente parámetro es obligatorio:

`database_name`

El nombre de la base de datos que se va a crear. El tipo de datos es `varchar`.

Los siguientes parámetros son opcionales:

`database_page_size`

El tamaño de página predeterminado de la base de datos. Valores válidos: `4096`, `8192`, `16384`, `32768`. El tipo de datos es `integer`. El valor predeterminado es `8192`.

> **Important**
>
> Amazon RDS admite la atomicidad de escritura para páginas de 4 KiB, 8 KiB y 16 KiB. Por el contrario, las páginas de 32 KiB corren el riesgo de tener errores de escritura o de que se escriban datos parciales en el escritorio. Si utiliza páginas de 32 KiB, le recomendamos habilitar la recuperación a un momento dado y las copias de seguridad automáticas. De lo contrario, corre el riesgo de no poder recuperarse de las páginas con errores. Para obtener más información, consulte the section called “Introducción a las copias de seguridad” y the section called “Recuperación a un momento dado”.

`database_code_set`

El conjunto de códigos de la base de datos. El tipo de datos es `varchar`. El valor predeterminado es `UTF-8`.

`database_territory`

El código de dos letras de la base de datos. El tipo de datos es `varchar`. El valor predeterminado es `US`.

database_collation

La secuencia de intercalación que determina cómo se ordenan y comparan las cadenas de caracteres almacenadas en la base de datos. El tipo de datos es `varchar`.

Valores válidos:

- `COMPATIBILITY`: una secuencia de intercalación de IBM Db2 versión 2.
- `EBCDIC_819_037`: página de códigos ISO latinos, intercalación; CCSID 037 (EBCDIC inglés de EE. UU.).
- `EBCDIC_819_500`: página de códigos ISO latinos, intercalación; CCSID 500 (EBCDIC internacional).
- `EBCDIC_850_037`: página de códigos ASCII latinos, intercalación; CCSID 037 (EBCDIC inglés de EE. UU.).
- `EBCDIC_850_500`: página de códigos ASCII latinos, intercalación; CCSID 500 (EBCDIC internacional).
- `EBCDIC_932_5026`: página de códigos ASCII japoneses, intercalación; CCSID 037 (EBCDIC inglés de EE. UU.).
- `EBCDIC_932_5035`: página de códigos ASCII japoneses, intercalación; CCSID 500 (EBCDIC internacional).
- `EBCDIC_1252_037`: página de códigos Windows latinos, intercalación; CCSID 037 (EBCDIC inglés de EE. UU.).
- `EBCDIC_1252_500`: página de códigos Windows latinos, intercalación; CCSID 500 (EBCDIC internacional).
- `IDENTITY`: intercalación predeterminada. Las cadenas se comparan byte por byte.
- `IDENTITY_16BIT`: el esquema de codificación de compatibilidad para UTF-16: secuencia de intercalación de 8 bits (CESU-8). Para obtener más información, consulte Unicode Technical Report #26 en el sitio web de Unicode Consortium.
- `NLSCHAR`: solo para su uso con la página de códigos en tailandés (CP874).
- `SYSTEM`: si utiliza `SYSTEM`, la base de datos utiliza automáticamente la secuencia de intercalación para `database_codeset` y `database_territory`.

El valor predeterminado es `IDENTITY`.

Además, RDS para Db2 admite los siguientes grupos de intercalaciones: `language-aware-collation` y `locale-sensitive-collation`. Para obtener más información, consulte Choosing a collation for a Unicode database en la documentación de IBM Db2.

database_autoconfigure_str

La sintaxis del comando AUTOCONFIGURE, por ejemplo, 'AUTOCONFIGURE APPLY DB'. El tipo de datos es varchar. El valor predeterminado es una cadena vacía o null.

Para obtener más información, consulte Comando AUTOCONFIGURE en la documentación de IBM Db2.

Notas de uso

Puede crear una base de datos llamando a rdsadmin.create_database si no especificó el nombre de la base de datos al crear la instancia de base de datos de RDS para Db2 mediante la consola de Amazon RDS o la AWS CLI. Para obtener más información, consulte Creación de una instancia de base de datos.

Consideraciones especiales:

- El comando CREATE DATABASE enviado a la instancia de Db2 usa la opción RESTRICTIVE.
- RDS para Db2 solo usa AUTOMATIC STORAGE.
- RDS para Db2 usa los valores predeterminados para NUMSEGS y DFT_EXTENT_SZ.
- RDS para Db2 utiliza el cifrado de almacenamiento y no admite el cifrado de bases de datos.

Para obtener más información sobre estas consideraciones, consulte el comando CREATE DATABASE en la documentación de IBM Db2.

Antes de llamar a rdsadmin.create_database, debe conectarse a la base de datos rdsadmin. En el siguiente ejemplo, sustituya *master_username* y *master_password* por la información de su instancia de base de datos de RDS para Db2:

```
db2 connect to rdsadmin user master_username using master_password
```

Para obtener más información sobre cómo comprobar el estado de creación de una base de datos, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se crea una base de datos llamada TESTJP con una combinación correcta de los parámetros *database_code_set*, *database_territory* y *database_collation* para Japón:

```
db2 "call rdsadmin.create_database('TESTJP', 4096, 'IBM-437', 'JP', 'SYSTEM')"
```

rdsadmin.drop_database

Elimina una base de datos.

Sintaxis

```
db2 "call rdsadmin.drop_database('database_name')"
```

Parámetros

El siguiente parámetro es obligatorio:

database_name

El nombre de la base de datos que se eliminará. El tipo de datos es `varchar`.

Notas de uso

Puede eliminar una base de datos llamando a `rdsadmin.drop_database` solo si se cumplen las siguientes condiciones:

- Si no especificó el nombre de la base de datos al crear la instancia de base de datos de RDS para Db2 mediante la consola de Amazon RDS o la AWS CLI. Para obtener más información, consulte Creación de una instancia de base de datos.
- Si creó la base de datos llamando al procedimiento almacenado the section called “rdsadmin.create_database”.
- Si ha restaurado la base de datos a partir de una imagen sin conexión o de una copia de seguridad llamando al procedimiento almacenado the section called “rdsadmin.restore_database”.

Antes de llamar a `rdsadmin.drop_database`, debe conectarse a la base de datos `rdsadmin`. En el siguiente ejemplo, sustituya *master_username* y *master_password* por la información de su instancia de base de datos de RDS para Db2:

```
db2 connect to rdsadmin user master_username using master_password
```

Para obtener más información sobre cómo comprobar el estado de eliminación de una base de datos, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se elimina una base de datos denominada:TESTDB

```
db2 "call rdsadmin.drop_database('TESTDB')"
```

Ejemplos de respuesta

Si pasa un nombre de base de datos incorrecto, el procedimiento almacenado devuelve el siguiente ejemplo de respuesta:

```
SQL0438N Application raised error or warning with diagnostic text: "Cannot
drop database. Database with provided name does not exist". SQLSTATE=99993
```

Si creó la base de datos mediante la consola de Amazon RDS o mediante la AWS CLI, el procedimiento almacenado devuelve el siguiente ejemplo de respuesta:

```
Return Status = 0
```

Después de recibir `Return Status = 0`, llame al procedimiento almacenado the section called "rdsadmin.get_task_status". Una respuesta similar a la del siguiente ejemplo explica el estado:

```
1 ERROR DROP_DATABASE RDSDB 2023-10-10-16.33.03.744122 2023-10-10-16.33.30.143797 -
 2023-10-10-16.33.30.098857 Task execution has started.
2023-10-10-16.33.30.143797 Caught exception during executing task id 1, Aborting task.
Reason Dropping database created via rds CreateDBInstance api is not allowed.
Only database created using rdsadmin.create_database can be dropped
```

rdsadmin.update_db_param

Actualiza los parámetros de la base de datos.

Sintaxis

```
db2 "call rdsadmin.update_db_param(
    'database_name',
```

```
    'parameter_to_modify',
    'changed_value')"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

Nombre de la base de datos para la que se desea ejecutar la tarea. El tipo de datos es `varchar`.

parameter_to_modify

El nombre del parámetro que se va a modificar. El tipo de datos es `varchar`. Para obtener más información, consulte Parámetros de Amazon RDS para Db2.

changed_value

El valor al que se desea cambiar el valor del parámetro. El tipo de datos es `varchar`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de actualización de los parámetros de base de datos, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo, se actualiza el parámetro `archretrydelay` a `100` para una base de datos denominada:`TESTDB`

```
db2 "call rdsadmin.update_db_param(
    'TESTDB',
    'archretrydelay',
    '100')"
```

El siguiente ejemplo aplaza la validación de los objetos creados en una base de datos denominada `TESTDB` para evitar la comprobación de dependencias:

```
db2 "call rdsadmin.update_db_param(
    'TESTDB',
    'auto_reval',
```

```
    'deferred_force')"
```

Ejemplos de respuesta

Si intenta modificar un parámetro de configuración de base de datos que no es compatible o no se puede modificar, el procedimiento almacenado devuelve el siguiente ejemplo de respuesta:

```
SQL0438N Application raised error or warning with diagnostic text: "Parameter
is either not supported or not modifiable to customers". SQLSTATE=99993
```

rdsadmin.set_configuration

Configura ajustes específicos para la base de datos.

Sintaxis

```
db2 "call rdsadmin.set_configuration(
    'name',
    'value')"
```

Parámetros

Se requieren los siguientes parámetros:

name

El nombre del ajuste de configuración. El tipo de datos es `varchar`.

value

El valor del ajuste de la configuración. El tipo de datos es `varchar`.

Notas de uso

La siguiente tabla muestra los ajustes de configuración que puede controlar con `rdsadmin.set_configuration`.

Nombre	Descripción
`RESTORE_DATABASE_NUM_BUFFERS`	El número de búferes que se van a crear durante una operación de restauración. Este valor debe ser menor que el tamaño de

Nombre	Descripción
	memoria total de la clase de instancia de base de datos. Si este ajuste no está configurado, Db2 determina el valor que se utilizará durante la operación de restauración. Para obtener más información, consulte la Documentación de IBM Db2.
`RESTORE_DATABASE_PARALLELISM`	El número de manipuladores de búferes que se van a crear durante una operación de restauración. Este valor debe ser menor que el doble de la cantidad de vCPU para la instancia de base de datos. Si este ajuste no está configurado, Db2 determina el valor que se utilizará durante la operación de restauración. Para obtener más información, consulte la Documentación de IBM Db2.

Ejemplos

En el siguiente ejemplo, se establece la configuración `RESTORE_DATABASE_PARALLELISM` en `8`.

```
db2 "call rdsadmin.set_configuration(
    'RESTORE_DATABASE_PARALLELISM',
    '8')"
```

En el siguiente ejemplo, se establece la configuración `RESTORE_DATABASE_NUM_BUFFERS` en `150`.

```
db2 "call rdsadmin.set_configuration(
    'RESTORE_DATABASE_NUM_BUFFERS',
    '150')"
```

rdsadmin.show_configuration

Devuelve el ajuste actual que puede establecer mediante el procedimiento almacenado `rdsadmin.set_configuration`.

Sintaxis

```
db2 "call rdsadmin.show_configuration(
    'name')"
```

Parámetros

El siguiente parámetro es opcional:

name

El nombre del ajuste de configuración sobre el que se va a devolver la información. El tipo de datos es `varchar`.

Son válidos los siguientes nombres de configuración:

- RESTORE_DATABASE_NUM_BUFFERS: el número de búferes que se van a crear durante una operación de restauración.
- RESTORE_DATABASE_PARALLELISM: el número de manipuladores de búferes que se van a crear durante una operación de restauración.

Notas de uso

Si no especifica el nombre de un ajuste de configuración, `rdsadmin.show_configuration` devuelve la información de todos los ajustes de configuración que puede establecer mediante el procedimiento almacenado `rdsadmin.set_configuration`.

Ejemplos

En el siguiente ejemplo, se devuelve información sobre la configuración `RESTORE_DATABASE_PARALLELISM` actual.

```
db2 "call rdsadmin.show_configuration(
    'RESTORE_DATABASE_PARALLELISM')"
```

rdsadmin.restore_database

Restaura una base de datos.

Sintaxis

```
db2 "call rdsadmin.restore_database(
    ?,
    'database_name',
    's3_bucket_name',
    's3_prefix',
```

```
    restore_timestamp,
    'backup_type')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta ?.

Se requieren los siguientes parámetros de entrada:

database_name

El nombre de la base de datos que se va a restaurar. Este nombre debe coincidir con el nombre de la base de datos de la imagen de copia de seguridad. El tipo de datos es `varchar`.

s3_bucket_name

El nombre del bucket de Amazon S3 donde se almacena su copia de seguridad. El tipo de datos es `varchar`.

s3_prefix

El prefijo que se utilizará para la coincidencia de archivos durante la descarga. El tipo de datos es `varchar`.

Si este parámetro está vacío, se descargarán todos los archivos del bucket de Amazon S3. A continuación, se muestra un prefijo de ejemplo:

```
backupfolder/SAMPLE.0.rdsdb.DBPART000.20230615010101
```

restore_timestamp

La marca de tiempo de la imagen de copia de seguridad de la base de datos. El tipo de datos es `varchar`.

La marca de tiempo se incluye en el nombre del archivo de copia de seguridad.
Por ejemplo, `20230615010101` es la marca de tiempo del nombre del archivo `SAMPLE.0.rdsdb.DBPART000.20230615010101.001`.

backup_type

El tipo de copia de seguridad. El tipo de datos es `varchar`. Valores válidos: `OFFLINE`, `ONLINE`.

Use `ONLINE` para migraciones con un tiempo de inactividad prácticamente nulo Para obtener más información, consulte Migración de Linux a Linux con un tiempo de inactividad prácticamente nulo para Amazon RDS para Db2.

Notas de uso

Puede restaurar una base de datos llamando a `rdsadmin.restore_database` si no especificó el nombre de la base de datos al crear la instancia de base de datos de RDS para Db2 mediante la consola de Amazon RDS o la AWS CLI. Para obtener más información, consulte Creación de una instancia de base de datos.

Antes de restaurar una base de datos, debe aprovisionar un espacio de almacenamiento para la instancia de base de datos de RDS para Db2 que sea igual o mayor que la suma del tamaño de la copia de seguridad y de la base de datos de Db2 original en el disco. Al restaurar la copia de seguridad, Amazon RDS extrae el archivo de copia de seguridad de la instancia de base de datos de RDS para Db2.

Cada archivo de copia de seguridad debe tener 5 TB o menos. Si un archivo de copia de seguridad supera los 5 TB, debe dividir el archivo de copia de seguridad en archivos más pequeños.

Para restaurar todos los archivos con el procedimiento almacenado `rdsadmin.restore_database`, no incluya el sufijo del número de archivo después de la marca de tiempo en los nombres de los archivos. Por ejemplo, el *s3_prefix* `backupfolder/SAMPLE.0.rdsdb.DBPART000.20230615010101` restaura los siguientes archivos:

```
SAMPLE.0.rdsdb.DBPART000.20230615010101.001
SAMPLE.0.rdsdb.DBPART000.20230615010101.002
SAMPLE.0.rdsdb.DBPART000.20230615010101.003
SAMPLE.0.rdsdb.DBPART000.20230615010101.004
SAMPLE.0.rdsdb.DBPART000.20230615010101.005
```

Para mejorar el rendimiento de las operaciones de restauración de bases de datos, puede configurar el número de búferes y manipuladores de búferes que utilizará RDS. Para comprobar la configuración actual, utilice the section called “rdsadmin.show_configuration”. Para cambiar la configuración, utilice the section called “rdsadmin.set_configuration”.

Para obtener más información sobre cómo comprobar el estado de restauración de su base de datos, consulte rdsadmin.get_task_status.

Para poner la base de datos en línea y aplicar registros de transacciones adicionales después de restaurarla, consulte rdsadmin.rollforward_database.

Ejemplos

El siguiente ejemplo restaura una copia de seguridad sin conexión con uno o varios archivos que tienen el *s3_prefix*:backupfolder/SAMPLE.0.rdsdb.DBPART000.20230615010101

```
db2 "call rdsadmin.restore_database(
    ?,
    'SAMPLE',
    'amzn-s3-demo-bucket',
    'backupfolder/SAMPLE.0.rdsdb.DBPART000.20230615010101',
    20230615010101,
    'OFFLINE')"
```

rdsadmin.rollforward_database

Pone la base de datos en línea y aplicar registros de transacciones adicionales después de restaurar una base de datos llamando a rdsadmin.restore_database.

Sintaxis

```
db2 "call rdsadmin.rollforward_database(
    ?,
    'database_name',
    's3_bucket_name',
    s3_prefix,
    'rollfoward_to_option',
    'complete_rollforward')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta ?.

Se requieren los siguientes parámetros de entrada:

database_name

Nombre de la base de datos en la que se va a realizar la operación. El tipo de datos es `varchar`.

s3_bucket_name

El nombre del bucket de Amazon S3 donde se almacena su copia de seguridad. El tipo de datos es `varchar`.

s3_prefix

El prefijo que se utilizará para la coincidencia de archivos durante la descarga. El tipo de datos es `varchar`.

Si este parámetro está vacío, se descargarán todos los archivos del bucket de S3. A continuación, se muestra un ejemplo de prefijo:

```
backupfolder/SAMPLE.0.rdsdb.DBPART000.20230615010101
```

Los siguientes parámetros de entrada son opcionales:

rollforward_to_option

El punto al que desee realizar la puesta al día. El tipo de datos es `varchar`. Valores válidos: `END_OF_LOGS`, `END_OF_BACKUP`. El valor predeterminado es `END OF LOGS`.

complete_rollforward

Especifica si se debe completar el proceso de puesta al día. El tipo de datos es `varchar`. El valor predeterminado es `TRUE`.

Si es `TRUE`, una vez finalizado el proceso, la base de datos está en línea y accesible. Si es `FALSE`, entonces la base de datos permanece en el estado `ROLL-FORWARD PENDING`.

Notas de uso

Después de llamar a rdsadmin.restore_database, debe llamar a `rollforward_database` para aplicar los registros de archivo de un bucket de S3. También puede usar este procedimiento almacenado para restaurar registros de transacciones adicionales después de llamar a `rdsadmin.restore_database`.

Si configura `complete_rollforward` como `FALSE` la base de datos estará en el estado `ROLL-FORWARD PENDING` y sin conexión. Para poner la base de datos en línea, debe llamar a rdsadmin.complete_rollforward.

Para obtener información sobre cómo comprobar el estado de puesta al día de una base de datos, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo pone al día una base de datos desde una copia de seguridad en línea con los registros de transacciones y pone la base de datos en línea:

```
db2 "call rdsadmin.rollforward_database(
    ?,
    null,
    null,
    'END_OF_LOGS',
    'TRUE')"
```

El siguiente ejemplo pone al día una base de datos desde una copia de seguridad en línea sin los registros de transacciones y pone la base de datos en línea:

```
db2 "call rdsadmin.rollforward_database(
    ?,
    'TESTDB',
    'amzn-s3-demo-bucket',
    'logsfolder/,
    'END_OF_BACKUP',
    'TRUE')"
```

El siguiente ejemplo pone al día una base de datos desde una copia de seguridad en línea con los registros de transacciones y luego no pone la base de datos en línea:

```
db2 "call rdsadmin.rollforward_database(
    ?,
    'TESTDB',
    null,
    'onlinebackup/TESTDB',
    'END_OF_LOGS',
    'FALSE')"
```

El siguiente ejemplo pone al día una base de datos desde una copia de seguridad en línea con los registros de transacciones adicionales y luego no pone la base de datos en línea:

```
db2 "call rdsadmin.rollforward_database(
    ?,
    'TESTDB',
    'amzn-s3-demo-bucket',
    'logsfolder/S0000155.LOG',
    'END_OF_LOGS',
    'FALSE')"
```

rdsadmin.complete_rollforward

Pone en línea la base de datos desde un estado `ROLL-FORWARD PENDING`.

Sintaxis

```
db2 "call rdsadmin.complete_rollforward(
    ?,
    'database_name')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta `?`.

El siguiente parámetro de entrada es obligatorio:

database_name

El nombre de la base de datos que quiera poner en línea. El tipo de datos es `varchar`.

Notas de uso

Si llamó a rdsadmin.rollforward_database con `complete_rollforward` configurado como `FALSE`, la base de datos está en un estado `ROLL-FORWARD PENDING` y sin conexión. Para completar el proceso de puesta al día y poner la base de datos en línea, llame a `rdsadmin.complete_rollforward`.

Para obtener información sobre cómo comprobar el estado de finalización del proceso de puesta al día, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo pone la base de datos TESTDB en línea:

```
db2 "call rdsadmin.complete_rollfoward(
    ?,
    'TESTDB')"
```

rdsadmin.db2pd_command

Recopila información sobre una base de datos de RDS para Db2.

Sintaxis

```
db2 "call rdsadmin.db2pd_command('db2pd_cmd')"
```

Parámetros

El siguiente parámetro de entrada es obligatorio:

db2pd_cmd

El nombre del comando db2pd que desea ejecutar. El tipo de datos es `varchar`.

El parámetro debe comenzar con un guion. Para obtener una lista de parámetros, consulte db2pd - Monitor and troubleshoot Db2 database command en la documentación de IBM.

Las siguientes opciones no son compatibles:

- `-addnode`
- `-alldatabases`
- `-alldbp`
- `-alldbs`
- `-allmembers`
- `-alm_in_memory`
- `-cfinfo`
- `-cfpool`

- `-command`
- `-dbpartitionnum`
- `-debug`
- `-dump`
- `-everything`
- `-file | -o`
- `-ha`
- `-interactive`
- `-member`
- `-pages`

  > **Note**
  >
  > Compatible con `-pages summary`.

- `-pdcollection`
- `-repeat`
- `-stack`
- `-totalmem`

La subopción `file` no es compatible; por ejemplo, `db2pd -db testdb -tcbstats file=tcbstat.out`.

El uso de `stacks` no es compatible; por ejemplo, `db2pd -edus interval=5 top=10 stacks`.

Notas de uso

Este procedimiento almacenado recopila información que puede ayudar a supervisar y solucionar problemas de bases de datos de RDS para Db2.

El procedimiento almacenado utiliza la utilidad `db2pd` de IBM para ejecutar varios comandos. La utilidad `db2pd` requiere una autorización `SYSADM`, que el usuario maestro de RDS para Db2 no tiene. Sin embargo, con el procedimiento almacenado de Amazon RDS, el usuario maestro puede utilizar la utilidad para ejecutar varios comandos. Para obtener más información acerca de la utilidad, consulte db2pd - Monitor and troubleshoot Db2 database command en la documentación de IBM.

El resultado está restringido a un máximo de 2 GB.

Para obtener información sobre cómo comprobar el estado de la recopilación de información sobre la base de datos, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo devuelve el tiempo de actividad de una instancia de base de datos de RDS para Db2:

```
db2 "call rdsadmin.db2pd_command('-')"
```

El siguiente ejemplo devuelve el tiempo de actividad de una base de datos denominada:TESTDB

```
db2 "call rdsadmin.db2pd_command('-db TESTDB -')"
```

El siguiente ejemplo devuelve el uso de memoria de una instancia de base de datos de RDS para Db2:

```
db2 "call rdsadmin.db2pd_command('-dbptnmem')"
```

El siguiente ejemplo devuelve los conjuntos de memoria de una instancia de base de datos de RDS para Db2 y una base de datos denominada:TESTDB

```
db2 "call rdsadmin.db2pd_command('-inst -db TESTDB -memsets')"
```

rdsadmin.force_application

Fuerza a las aplicaciones a salir de una base de datos de RDS para Db2.

Sintaxis

```
db2 "call rdsadmin.force_application(
    ?,
    'applications')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta ?.

El siguiente parámetro de entrada es obligatorio:

applications

Las aplicaciones que quiere forzar a que salgan de una base de datos de RDS para Db2. El tipo de datos es `varchar`. Valores válidos: `ALL` o *application_handle*.

Separe los nombres de varias aplicaciones con comas. Ejemplo: '*application_handle_1*, *application_handle_2*'.

Notas de uso

Este procedimiento almacenado obliga a todas las aplicaciones a salir de una base de datos para que pueda realizar el mantenimiento.

El procedimiento almacenado utiliza el comando `FORCE APPLICATION` de IBM. El comando `FORCE APPLICATION` requiere autorización `SYSADM`, `SYSMAINT` o `SYSCTRL` que el usuario maestro de RDS para Db2 no tiene. Sin embargo, con el procedimiento almacenado de Amazon RDS, el usuario maestro puede utilizar el comando. Para obtener más información, consulte FORCE APPLICATION command en la documentación de IBM.

Para obtener información sobre cómo comprobar el estado al obligar la salida de aplicaciones de una base de datos, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo fuerza a todas las aplicaciones a salir de una base de datos de RDS para Db2:

```
db2 "call rdsadmin.force_application(
    ?,
    'ALL')"
```

El siguiente ejemplo obliga a los controladores de aplicaciones 9991, 8891 y 1192 a salir de una base de datos de RDS para Db2:

```
db2 "call rdsadmin.force_application(
```

```
    ?,
    '9991, 8891, 1192')"
```

rdsadmin.set_archive_log_retention

Configura la cantidad de tiempo (en horas) que se conservarán los archivos de registro de la base de datos de RDS para Db2 especificada.

Sintaxis

```
db2 "call rdsadmin.set_archive_log_retention(
    ?,
    'database_name',
    'archive_log_retention_hours')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta `?`.

Se requieren los siguientes parámetros de entrada:

database_name

El nombre de la base de datos para la que se configura la retención de registros de archivo. El tipo de datos es `varchar`.

archive_log_retention_hours

El número de horas que se van a conservar los archivos de registros de archivo. El tipo de datos es `smallint`. El valor predeterminado es `0` y el máximo es 168 (7 días).

Si el valor es `0`, Amazon RDS no conserva los archivos de registro de archivo.

Notas de uso

De forma predeterminada, RDS para Db2 retiene los registros durante 5 minutos. Si utiliza herramientas de replicación, como AWS DMS para la captura de datos de cambios (CDC) o IBM Q

Replication, le recomendamos que configure la retención de registros en esas herramientas para más de 5 minutos.

Puede ver la configuración actual de conservación de registros de archivo llamando a the section called “rdsadmin.show_archive_log_retention”.

No puede configurar el ajuste de retención de registros de archivos en la base de datos `rdsadmin`.

Ejemplos

El siguiente ejemplo ajusta el tiempo de conservación de registros de archivo para una base de datos denominada `TESTDB` en 24 horas.

```
db2 "call rdsadmin.set_archive_log_retention(
    ?,
    'TESTDB',
    '24')"
```

El siguiente ejemplo deshabilita la conservación de registros de archivo para una base de datos denominada `TESTDB`.

```
db2 "call rdsadmin.set_archive_log_retention(
    ?,
    'TESTDB',
    '0')"
```

rdsadmin.show_archive_log_retention

Devuelve la configuración actual de retención de registros de archivo de la base de datos especificada.

Sintaxis

```
db2 "call rdsadmin.show_archive_log_retention(
    ?,
    'database_name')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta ?.

El siguiente parámetro de entrada es obligatorio:

database_name

El nombre de la base de datos para la que se muestra la configuración de la conservación de registros de archivo. El tipo de datos es `varchar`.

Ejemplos

El siguiente ejemplo muestra el ajuste de conservación de registros de archivo para una base de datos denominada `TESTDB`.

```
db2 "call rdsadmin.show_archive_log_retention(
    ?
    'TESTDB')"
```

Procedimientos almacenados de acceso al almacenamiento de RDS para Db2

Los procedimientos almacenados que se describen en este tema administran el acceso al almacenamiento para bases de datos de RDS para Db2 que utilizan Amazon S3 para la migración de datos. Para obtener más información, consulte the section called “Migración con Amazon S3”.

Consulte los siguientes procedimientos almacenados integrados para obtener información sobre su sintaxis, parámetros, notas de uso y ejemplos.

Procedimientos almacenados

- rdsadmin.catalog_storage_access
- rdsadmin.uncatalog_storage_access

rdsadmin.catalog_storage_access

Cataloga un alias de almacenamiento para acceder a un bucket de Amazon S3 con archivos de datos de Db2.

Sintaxis

```
db2 "call rdsadmin.catalog_storage_access(
    ?,
    'alias',
    's3_bucket_name',
    'grantee_type',
    'grantee'
    )"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. El tipo de datos es `varchar`.

Se requieren los siguientes parámetros de entrada:

alias

El alias para acceder al almacenamiento remoto en un bucket de Amazon S3. El tipo de datos es `varchar`.

s3_bucket_name

El nombre del bucket de Amazon S3 donde residen sus datos. El tipo de datos es `varchar`.

grantee_type

El tipo de beneficiario de la concesión que recibirá la autorización. El tipo de datos es `varchar`. Valores válidos: `USER`, `GROUP`.

grantee

El usuario o el grupo que recibirá la autorización. El tipo de datos es `varchar`.

Notas de uso

Amazon RDS incluye el alias catalogado en el rol de IAM que agregó a su instancia de base de datos de RDS para Db2. Si elimina el rol de IAM de la instancia de base de datos, Amazon RDS elimina el alias. Para obtener más información, consulte the section called “Migración con Amazon S3”.

Para obtener más información sobre cómo comprobar el estado de catalogación de su alias, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo se registra un alias denominado `SAMPLE`. Al usuario `jorge_souza` se le concede acceso al bucket de Amazon S3 denominado `amzn-s3-demo-bucket`.

```
db2 "call rdsadmin.catalog_storage_access(
    ?,
    'SAMPLE',
    'amzn-s3-demo-bucket',
    'USER',
    'jorge_souza')"
```

rdsadmin.uncatalog_storage_access

Elimina un alias de acceso al almacenamiento.

Sintaxis

```
db2 "call rdsadmin.uncatalog_storage_access(
    ?,
    'alias')"
```

Parámetros

El siguiente parámetro de salida es obligatorio:

?

Un marcador de parámetros que genera un mensaje de error. El tipo de datos es `varchar`.

El siguiente parámetro de entrada es obligatorio:

alias

El nombre del alias de almacenamiento que se va a eliminar. El tipo de datos es `varchar`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de eliminación de un alias, consulte rdsadmin.get_task_status.

Ejemplos

En el siguiente ejemplo se elimina un alias denominado `SAMPLE`. Este alias ya no proporciona acceso al bucket de Amazon S3 al que estaba asociado.

```
db2 "call rdsadmin.uncatalog_storage_access(
    ?,
    'SAMPLE')"
```

Procedimientos almacenados de espacios de tablas de RDS para Db2

Los procedimientos almacenados integrados que se describen en este tema administran espacios de tabla de bases de datos de Amazon RDS para Db2. Para ejecutar estos procedimientos, el usuario maestro debe conectarse primero a la base de datos `rdsadmin`.

Estos procedimientos almacenados se utilizan en diversas tareas. Esta lista no es exhaustiva.

- Tareas comunes para espacios de tablas
- Generación de informes de rendimiento
- Copia de metadatos de bases de datos con db2look
- Creación de una base de datos de repositorios para IBM Db2 Data Management Console

Consulte los siguientes procedimientos almacenados integrados para obtener información sobre su sintaxis, parámetros, notas de uso y ejemplos.

Procedimientos almacenados

- rdsadmin.create_tablespace
- rdsadmin.alter_tablespace
- rdsadmin.rename_tablespace
- rdsadmin.drop_tablespace

rdsadmin.create_tablespace

Crea un espacio de tabla.

Sintaxis

```
db2 "call rdsadmin.create_tablespace(
    'database_name',
    'tablespace_name',
    'buffer_pool_name',
    tablespace_page_size,
    tablespace_initial_size,
    tablespace_increase_size,
    'tablespace_type',
    'tablespace_prefetch_size')"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

Nombre de la base de datos en la que se creará el espacio de tabla. El tipo de datos es `varchar`.

tablespace_name

Nombre del espacio tabla que se va a crear. El tipo de datos es `varchar`.

El nombre del espacio de tabla tiene las siguientes restricciones:

- No puede ser el mismo que el nombre de un espacio de tabla existente en esta base de datos.
- Solo puede contener los caracteres `_$#@a-zA-Z0-9`.
- No puede empezar con `_` o `$`.
- No puede empezar con `SYS`.

Los siguientes parámetros son opcionales:

buffer_pool_name

Nombre del grupo de búferes al que se asignará el espacio de tabla. El tipo de datos es `varchar`. El valor predeterminado es una cadena vacía.

> **Important**
>
> Debe tener ya un grupo de búferes del mismo tamaño de página para asociarlo al espacio de tabla.

tablespace_page_size

El tamaño de página del espacio de tabla en bytes. El tipo de datos es `integer`. Valores válidos: `4096`, `8192`, `16384`, `32768`. El tamaño predeterminado es el tamaño de página utilizado al crear la base de datos al llamar a rdsadmin.create_database.

> **Important**
>
> Amazon RDS admite la atomicidad de escritura para páginas de 4 KiB, 8 KiB y 16 KiB. Por el contrario, las páginas de 32 KiB corren el riesgo de tener errores de escritura o de que se escriban datos parciales en el escritorio. Si utiliza páginas de 32 KiB, le recomendamos habilitar la recuperación a un momento dado y las copias de seguridad automáticas. De lo contrario, corre el riesgo de no poder recuperarse de las páginas con errores. Para obtener más información, consulte the section called “Introducción a las copias de seguridad” y the section called “Recuperación a un momento dado”.

tablespace_initial_size

El tamaño inicial del espacio de tabla en kilobytes (KB). El tipo de datos es `integer`. Valores válidos: 48 o superiores. El valor predeterminado es null (nulo).

Si no establece un valor, Db2 establece un valor adecuado para su caso.

> **Note**
>
> Este parámetro no se aplica a los espacios de tabla temporales porque los administra el sistema.

tablespace_increase_size

El porcentaje en el que se va a aumentar el espacio de tabla cuando se llene. El tipo de datos es `integer`. Valores válidos: 1-100. El valor predeterminado es null (nulo).

Si no establece un valor, Db2 establece un valor adecuado para su caso.

> **Note**
>
> Este parámetro no se aplica a los espacios de tabla temporales porque los administra el sistema.

tablespace_type

El tipo de espacio de tabla. El tipo de datos es `char`. Valores válidos: `U` (para datos de usuario), `T` (para datos temporales de usuario) o `S` (para datos temporales del sistema). El valor predeterminado es `U`.

tablespace_prefetch_size

El tamaño de página de captura previa del espacio de tabla. El tipo de datos es `char`. Valores válidos: `AUTOMATIC` (no distingue entre mayúsculas y minúsculas) o enteros positivos distintos de cero que sean menores o iguales a 32767.

Notas de uso

RDS para Db2 siempre crea una base de datos de gran tamaño para los datos.

Para obtener más información sobre cómo comprobar el estado de creación de un espacio de tabla, consulte rdsadmin.get_task_status.

Ejemplos

Ejemplo 1: creación de un espacio de tabla y asignación de un grupo de búferes

En el siguiente ejemplo, se crea un espacio de tabla llamado `SP8` y se asigna un grupo de búferes llamado `BP8` para una base de datos llamada `TESTDB`. El espacio de tabla tiene un tamaño de página de espacio de tabla inicial de 4096 bytes, un espacio de tabla inicial de 1000 KB y el aumento de tamaño de tabla está establecido en el 50 %.

```
db2 "call rdsadmin.create_tablespace(
    'TESTDB',
    'SP8',
    'BP8',
    4096,
    1000,
    50)"
```

Ejemplo 2: creación de un espacio de tabla temporal y asignación de un grupo de búferes

En el siguiente ejemplo, se crea un espacio de tabla temporal llamado `SP8`. Asigna un grupo de búferes denominado `BP8` (con un tamaño de 8 KiB) a una base de datos llamada `TESTDB`.

```
db2 "call rdsadmin.create_tablespace(
    'TESTDB',
    'SP8',
    'BP8',
    8192,
    NULL,
    NULL,
    'T')"
```

Ejemplo 3: Creación de un espacio de tablas y asignar un tamaño de página de captura previa

El siguiente ejemplo crea un espacio de tabla llamado SP8 para una base de datos llamada TESTDB. El espacio de tabla tiene un aumento de tamaño inicial del espacio de tabla de 50 y un tamaño de página de captura previa de 800.

```
db2 "call rdsadmin.create_tablespace(
    'TESTDB',
    'SP8',
    NULL,
    NULL,
    NULL,
    50,
    NULL,
    '800')"
```

rdsadmin.alter_tablespace

Modifica un espacio de tabla.

Sintaxis

```
db2 "call rdsadmin.alter_tablespace(
    'database_name',
    'tablespace_name',
    'buffer_pool_name',
    tablespace_increase_size,
    'max_size',
    'reduce_max',
    'reduce_stop',
    'reduce_value',
    'lower_high_water',
    'lower_high_water_stop',
```

```
    'switch_online',
    'tablespace_prefetch_size')"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

Nombre de la base de datos que usa el espacio de tabla. El tipo de datos es `varchar`.

tablespace_name

El nombre del espacio de tabla que se va a modificar. El tipo de datos es `varchar`.

Los siguientes parámetros son opcionales:

buffer_pool_name

Nombre del grupo de búferes al que se asignará el espacio de tabla. El tipo de datos es `varchar`. El valor predeterminado es una cadena vacía.

> **Important**
>
> Debe tener ya un grupo de búferes del mismo tamaño de página para asociarlo al espacio de tabla.

tablespace_increase_size

El porcentaje en el que se va a aumentar el espacio de tabla cuando se llene. El tipo de datos es `integer`. Valores válidos: `1-100`. El valor predeterminado es `0`.

max_size

El tamaño máximo del espacio de tabla. El tipo de datos es `varchar`. Valores válidos: *número entero* `K` | `M` | `G` o `NONE`. El valor predeterminado es `NONE`.

reduce_max

Especifica si se debe reducir la marca de agua máxima hasta su límite máximo. El tipo de datos es `char`. El valor predeterminado es `N`.

reduce_stop

Especifica si se debe interrumpir un comando `reduce_max` o `reduce_value` anterior. El tipo de datos es `char`. El valor predeterminado es `N`.

reduce_value

El número o porcentaje de reducción del límite máximo del espacio de tabla. El tipo de datos es `varchar`. Valores válidos: *número entero* `K`| `M` | `G` o `1`–`100`. El valor predeterminado es `N`.

lower_high_water

Especifica si se debe ejecutar el comando `ALTER TABLESPACE LOWER HIGH WATER MARK`. El tipo de datos es `char`. El valor predeterminado es `N`.

lower_high_water_stop

Especifica si se debe ejecutar el comando `ALTER TABLESPACE LOWER HIGH WATER MARK STOP`. El tipo de datos es `char`. El valor predeterminado es `N`.

switch_online

Especifica si se debe ejecutar el comando `ALTER TABLESPACE SWITCH ONLINE`. El tipo de datos es `char`. El valor predeterminado es `N`.

tablespace_prefetch_size

El tamaño de página de captura previa del espacio de tabla. El tipo de datos es `char`. Valores válidos: `AUTOMATIC` (no distingue entre mayúsculas y minúsculas) o enteros positivos distintos de cero que sean menores o iguales a 32767.

> **Note**
>
> Este parámetro solo funciona con `buffer_pool_name`, `table_increase_size`, `max_size` y `switch_online`. No funciona con `reduce_max`, `reduce_stop`, `reduce_value`, `lower_high_water` y `lower_high_water_stop`.

Notas de uso

Antes de llamar al procedimiento almacenado, tenga en cuenta lo siguiente:

- El procedimiento almacenado `rdsadmin.alter_tablespace` no funcionará en un espacio de tablas con el valor `tablespace_type` establecido en `T` para los datos temporales del usuario.

- Los parámetros opcionales `reduce_max`, `reduce_stop`, `reduce_value`, `lower_high_water`, `lower_high_water_stop` y `switch_online` son mutuamente excluyentes. No puede combinarlos con ningún otro parámetro opcional, por ejemplo `buffer_pool_name`, en el comando `rdsadmin.alter_tablespace`. Para obtener más información, consulte Statement not valid.

Para obtener más información sobre cómo comprobar el estado de modificación de un espacio de tabla, consulte rdsadmin.get_task_status.

Para ver los mensajes de error devueltos al llamar a los procedimientos almacenados, consulte the section called “Errores en los procedimientos almacenados”.

Ejemplos

Ejemplo 1: bajada de la marca de agua superior

En el siguiente ejemplo, se modifica un espacio de tabla llamado SP8 y se asigna un grupo de búferes llamado BP8 a una base de datos llamada TESTDB para reducir el límite máximo.

```
db2 "call rdsadmin.alter_tablespace(
    'TESTDB',
    'SP8',
    'BP8',
    NULL,
    NULL,
    'Y')"
```

Ejemplo 2: reducción de la marca de agua superior

El siguiente ejemplo ejecuta el comando `REDUCE MAX` en un espacio de tabla llamado `TBSP_TEST` en la base de datos `TESTDB`.

```
db2 "call rdsadmin.alter_tablespace(
    'TESTDB',
    'TBSP_TEST',
    NULL,
    NULL,
    NULL,
    'Y')"
```

Ejemplo 3: interrupción de comandos para reducir la marca de agua superior

El siguiente ejemplo ejecuta el comando `REDUCE STOP` en un espacio de tabla llamado `TBSP_TEST` en la base de datos `TESTDB`.

```
db2 "call rdsadmin.alter_tablespace(
    'TESTDB',
    'TBSP_TEST',
    NULL,
    NULL,
    NULL,
    NULL,
    'Y')"
```

Ejemplo 4: Cambio del tamaño de la página de captura previa existente

En el siguiente ejemplo, se ejecuta el comando `ALTER TABLESPACE SWITCH ONLINE` en un espacio de tabla llamado `TSBP_TEST` y se cambia el tamaño de la página de captura previa existente a `64`.

```
db2 "call rdsadmin.alter_tablespace(
    'TESTDB',
    'TBSP_TEST',
    NULL,
    NULL,
    NULL,
    NULL,
    NULL,
    NULL,
    NULL,
    NULL,
    ‘Y’,
    ‘64’)"
```

rdsadmin.rename_tablespace

Cambia el nombre de un espacio de tabla.

Sintaxis

```
db2 "call rdsadmin.rename_tablespace(
    ?,
    'database_name',
    'source_tablespace_name',
```

```
    'target_tablespace_name')"
```

Parámetros

Se requieren los siguientes parámetros:

?

Un marcador de parámetros que genera un mensaje de error. Este parámetro solo acepta ?

database_name

El nombre de la base de datos al que corresponde el espacio de tabla. El tipo de datos es `varchar`.

source_tablespace_name

El nombre del espacio de tabla que se va a cambiar. El tipo de datos es `varchar`.

target_tablespace_name

En nuevo nombre del espacio de tabla. El tipo de datos es `varchar`.

El nuevo nombre tiene las siguientes restricciones:

- No puede ser el mismo que el nombre de un espacio de tabla existente.
- Solo puede contener los caracteres `_$#@a-zA-Z0-9`.
- No puede empezar con `_` o `$`.
- No puede empezar con `SYS`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de cambio de nombre de un espacio de tabla, consulte rdsadmin.get_task_status.

No puede cambiar el nombre de espacios de tabla que pertenecen a la base de datos `rdsadmin`.

Ejemplos

El siguiente ejemplo cambia el nombre de un espacio de tabla llamado `SP8` a `SP9` una base de datos llamada `TESTDB`.

```
db2 "call rdsadmin.rename_tablespace(
    ?,
    'TESTDB',
    'SP8',
    'SP9')"
```

rdsadmin.drop_tablespace

Elimina un espacio de tabla.

Sintaxis

```
db2 "call rdsadmin.drop_tablespace(
    'database_name',
    'tablespace_name')"
```

Parámetros

Se requieren los siguientes parámetros:

database_name

El nombre de la base de datos al que corresponde el espacio de tabla. El tipo de datos es `varchar`.

tablespace_name

Nombre del espacio de tabla que se va a eliminar. El tipo de datos es `varchar`.

Notas de uso

Para obtener más información sobre cómo comprobar el estado de eliminación de un espacio de tabla, consulte rdsadmin.get_task_status.

Ejemplos

El siguiente ejemplo elimina un espacio de tabla llamado `SP8` de una base de datos llamada `TESTDB`.

```
db2 "call rdsadmin.drop_tablespace(
    'TESTDB',
```

```
    'SP8')"
```

Referencia de funciones definidas por el usuario de Amazon RDS para Db2

Las siguientes funciones definidas por el usuario están disponibles para las instancias de base de datos de Amazon RDS que ejecutan el motor de Db2.

Temas

- rdsadmin.get_task_status
- rdsadmin.list_databases

rdsadmin.get_task_status

Devuelve el estado de una tarea.

Sintaxis

```
db2 "select task_id, task_type, database_name, lifecycle,
    varchar(bson_to_json(task_input_params), 500) as task_params,
    cast(task_output as varchar(500)) as task_output
    from table(rdsadmin.get_task_status(task_id,'database_name','task_type'))"
```

Parámetros

Los siguientes parámetros son opcionales. Si no proporciona ningún parámetro, la función definida por el usuario devuelve el estado de todas las tareas de todas las bases de datos. Amazon RDS conserva el historial de tareas durante 35 días.

`task_id`

El ID de la tarea que se está ejecutando. Este ID se devuelve al ejecutar una tarea. Predeterminado: `0`.

`database_name`

El nombre de la base de datos para la que se está ejecutando la tarea.

`task_type`

El tipo de tarea que se desea consultar. Valores válidos: `ADD_GROUPS`, `ADD_USER`, `ALTER_BUFFERPOOL`, `ALTER_TABLESPACE`, `CHANGE_PASSWORD`, `COMPLETE_ROLLFORWARD`,

CREATE_BUFFERPOOL, CREATE_DATABASE, CREATE_ROLE, CREATE_TABLESPACE, DROP_BUFFERPOOL, DROP_DATABASE, DROP_TABLESPACE, LIST_USERS, REMOVE_GROUPS, REMOVE_USER, RESTORE_DB, ROLLFORWARD_DB_LOG, ROLLFORWARD_STATUS, UPDATE_DB_PARAM.

Notas de uso

Puede utilizar la función definida por el usuario `rdsadmin.get_task_status` para comprobar el estado de las siguientes tareas para Amazon RDS para Db2. Esta lista no es exhaustiva.

- Crear, modificar o eliminar un grupo de búferes
- Crear, modificar o eliminar un espacio de tabla
- Crear o eliminar una base de datos
- Restaurar una copia de seguridad de una base de datos desde Amazon S3
- Poner al día los registros de bases de datos desde Amazon S3

Ejemplos

En el siguiente ejemplo se muestran las columnas devueltas cuando se llama a `rdsadmin.get_task_status`.

```
db2 "describe select * from table(rdsadmin.get_task_status())"
```

En el siguiente ejemplo se muestra el estado de todas las tareas.

```
db2 "select task_id, task_type, database_name, lifecycle,
    varchar(bson_to_json(task_input_params), 500) as task_params,
    cast(task_output as varchar(500)) as task_output
    from table(rdsadmin.get_task_status(null,null,null))"
```

En el siguiente ejemplo se muestra el estado de una tarea específica.

```
db2 "select task_id, task_type, database_name,
    varchar(bson_to_json(task_input_params), 500) as task_params
    from table(rdsadmin.get_task_status(1,null,null))"
```

En el siguiente ejemplo se muestra el estado de una tarea y una base de datos específicas.

```
db2 "select task_id, task_type, database_name,
    varchar(bson_to_json(task_input_params), 500) as task_params
    from table(rdsadmin.get_task_status(2,'SAMPLE',null))"
```

En el siguiente ejemplo se muestra el estado de todas las tareas ADD_GROUPS.

```
db2 "select task_id, task_type, database_name,
    varchar(bson_to_json(task_input_params), 500) as task_params
    from table(rdsadmin.get_task_status(null,null,'add_groups'))"
```

En el siguiente ejemplo se muestra el estado de todas las tareas para una base de datos específica.

```
db2 "select task_id, task_type, database_name,
    varchar(bson_to_json(task_input_params), 500) as task_params
    from table(rdsadmin.get_task_status(null,'testdb', null))"
```

En el siguiente ejemplo aparecen los valores JSON como columnas.

```
db2 "select varchar(r.task_type,25) as task_type, varchar(r.lifecycle,10) as lifecycle,
 r.created_at, u.* from
    table(rdsadmin.get_task_status(null,null,'restore_db')) as r,
 json_table(r.task_input_params, 'strict $' columns(s3_prefix varchar(500)
    null on empty, s3_bucket_name varchar(500) null on empty) error on error ) as U"
```

Respuesta

La función definida por el usuario `rdsadmin.get_task_status` devuelve las siguientes columnas:

`TASK_ID`

El ID de la tarea.

`TASK_TYPE`

Depende de los parámetros de entrada.

- `ADD_GROUPS`: agrega grupos.
- `ADD_USER`: agrega un usuario.
- `ALTER_BUFFERPOOL`: modifica un grupo de búferes.

- ALTER_TABLESPACE: modifica un espacio de tabla.
- CHANGE_PASSWORD : cambia la contraseña de un usuario.
- COMPLETE_ROLLFORWARD: completa una tarea rdsadmin.rollforward_database y activa una base de datos.
- CREATE_BUFFERPOOL: crea un grupo de búferes.
- CREATE_DATABASE: crea una base de datos.
- CREATE_ROLE: crea un rol de Db2 para un usuario.
- CREATE_TABLESPACE: crea un espacio de tabla.
- DROP_BUFFERPOOL: elimina un grupo de búferes.
- DROP_DATABASE: elimina una base de datos.
- DROP_TABLESPACE: elimina un espacio de tabla.
- LIST_USERS: muestra todos los usuarios.
- REMOVE_GROUPS: elimina grupos.
- REMOVE_USER: elimina un usuario.
- RESTORE_DB: restaura una base de datos completa.
- ROLLFORWARD_DB_LOG: realiza una tarea rdsadmin.rollforward_database en los registros de la base de datos.
- ROLLFORWARD_STATUS : devuelve el estado de una tarea rdsadmin.rollforward_database.
- UPDATE_DB_PARAM: actualiza los parámetros de datos.

DATABASE_NAME

El nombre de la base de datos a la que está asociada la tarea.

COMPLETED_WORK_BYTES

Número de bytes restaurados por la tarea.

DURATION_MINS

El tiempo que se tarda en completar la tarea.

LIFECYCLE

El estado de la tarea. Estados posibles:

- CREATED: tras enviar una tarea a Amazon RDS, Amazon RDS establece el estado en CREATED.
- IN_PROGRESS: cuando una tarea comienza, Amazon RDS establece su estado en IN_PROGRESS. El estado puede tardar hasta cinco minutos en cambiar de CREATED a IN_PROGRESS.
- SUCCESS: cuando una tarea se completa, el estado se establece en SUCCESS.
- ERROR: si se produce un error en una tarea de restauración, Amazon RDS establece el estado en ERROR. Para obtener más información acerca del error, consulte TASK_OUPUT.

CREATED_BY

El authid que creó el comando.

CREATED_AT

La fecha y hora en que se creó la tarea.

LAST_UPDATED_AT

La fecha y hora de la última actualización de la tarea.

TASK_INPUT_PARAMS

Los parámetros difieren según el tipo de tarea. Todos los parámetros de entrada se representan como un objeto JSON. Por ejemplo, las claves JSON de la tarea RESTORE_DB son las siguientes:

- DBNAME
- RESTORE_TIMESTAMP
- S3_BUCKET_NAME
- S3_PREFIX

TASK_OUTPUT

Información adicional acerca de la tarea. Si ocurre un error durante la restauración nativa, esta columna incluye información acerca del error.

Ejemplos de respuesta

El siguiente ejemplo de respuesta muestra que la base de datos llamada TESTJP se creó correctamente. Para obtener más información, consulte el procedimiento almacenado the section called “rdsadmin.create_database”.

```
`1 SUCCESS CREATE_DATABASE RDSDB 2023-10-24-18.32.44.962689 2023-10-24-18.34.50.038523
 1 TESTJP { "CODESET" : "IBM-437", "TERRITORY" : "JP", "COLLATION" : "SYSTEM",
 "AUTOCONFIGURE_CMD" : "", "PAGESIZE" : 4096 }
2023-10-24-18.33.30.079048 Task execution has started.

2023-10-24-18.34.50.038523 Task execution has completed successfully`.
```

El siguiente ejemplo de respuesta explica por qué no se pudo eliminar una base de datos. Para obtener más información, consulte el procedimiento almacenado the section called "rdsadmin.drop_database".

```
1 ERROR DROP_DATABASE RDSDB 2023-10-10-16.33.03.744122 2023-10-10-16.33.30.143797 -
 2023-10-10-16.33.30.098857 Task execution has started.
2023-10-10-16.33.30.143797 Caught exception during executing task id 1, Aborting task.
Reason Dropping database created via rds CreateDBInstance api is not allowed.
Only database created using rdsadmin.create_database can be dropped
```

El siguiente ejemplo de respuesta muestra la restauración correcta de una base de datos. Para obtener más información, consulte el procedimiento almacenado the section called "rdsadmin.restore_database".

```
1 RESTORE_DB  SAMPLE  SUCCESS

{ "S3_BUCKET_NAME" : "amzn-s3-demo-bucket", "S3_PREFIX" :
 "SAMPLE.0.rdsdb3.DBPART000.20230413183211.001", "RESTORE_TIMESTAMP" :
 "20230413183211", "BACKUP_TYPE" : "offline" }




2023-11-06-18.31.03.115795 Task execution has started.
2023-11-06-18.31.04.300231 Preparing to download
2023-11-06-18.31.08.368827 Download complete. Starting Restore
2023-11-06-18.33.13.891356 Task Completed Successfully
```

rdsadmin.list_databases

Devuelve una lista de todas las bases de datos que se ejecutan en una instancia de base de datos de RDS para Db2.

Sintaxis

```
db2 "select * from table(rdsadmin.list_databases())"
```

Notas de uso

Esta función definida por el usuario no especifica si las bases de datos están activadas o desactivadas.

Si no ve sus bases de datos en la lista, llame a la función the section called "rdsadmin.get_task_status" definida por el usuario y busque los mensajes de error.

Respuesta

La función definida por el usuario `rdsadmin.list_databases` devuelve las siguientes columnas:

`DATABASE_NAME`

El nombre de una base de datos.

`CREATE_TIME`

La fecha y hora en la que se ha creado la sesión.

Ejemplos de respuesta

El siguiente ejemplo de respuesta muestra una lista de bases de datos y las horas en que se crearon. `rdsadmin` es una base de datos que Amazon RDS administra y que siempre aparece en los resultados.

```
DATABASE_NAME   CREATE_TIME
--------------- --------------------------
rdsadmin        2024-10-22-03.37.48.535671
TEST            2024-10-22-03.39.36.818679
TEST1           2024-10-22-03.57.15.218009
TEST2           2024-10-22-03.59.28.029556
```

Resolución de problemas de Amazon RDS para Db2

El siguiente contenido puede ayudarle a solucionar algunos problemas que puede encontrarse con RDS para Db2.

Para obtener más información acerca de cómo solucionar problemas generales de Amazon RDS, consulte Solución de problemas de Amazon RDS.

Temas

- Error de conexión a la base
- Error de E/S de archivos
- Errores en los procedimientos almacenados

Error de conexión a la base

El siguiente mensaje de error indica que una base de datos no se ha podido conectar porque el servidor no tiene suficiente memoria.

```
SQL1643C The database manager failed to allocate shared memory because the
database manager instance memory limit has been reached.
```

Aumente la memoria de la instancia de base de datos y, a continuación, intente conectarse de nuevo a la base de datos. Para obtener información sobre el uso de la memoria y las recomendaciones para las bases de datos, consulte the section called “Múltiples bases de datos Db2”. Para obtener más información sobre cómo actualizar la memoria de una base de datos de RDS para Db2, consulte the section called “rdsadmin.update_db_param”.

Error de E/S de archivos

Es posible que se produzca un error de E/S en un archivo por distintos motivos; por ejemplo, al utilizar el comando LOAD o al llamar al procedimiento `rdsadmin.restore_database` almacenado.

En este ejemplo, puede ejecutar el comando LOAD siguiente:

```
db2 "call sysproc.admin_cmd('load from "DB2REMOTE://s3test//public/datapump/t6.del" of
 del lobs from "DB2REMOTE://s3test/public/datapump/" modified by lobsinfile MESSAGES ON
 SERVER insert INTO RDSDB.t6 nonrecoverable ')"
```

El comando LOAD devuelve el siguiente mensaje:

```
 Result set 1
 --------------

 ROWS_READ            ROWS_SKIPPED         ROWS_LOADED          ROWS_REJECTED
ROWS_DELETED         ROWS_COMMITTED       ROWS_PARTITIONED     NUM_AGENTINFO_ENTRIES
MSG_RETRIEVAL




MSG_REMOVAL
 -------------------- -------------------- -------------------- --------------------
-------------------- -------------------- -------------------- --------------------
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
                     -                    -                    -                    -
                    -                    -                    -                    -
SELECT SQLCODE, MSG FROM TABLE(SYSPROC.ADMIN_GET_MSGS('1594987316_285548770')) AS MSG




                                                                                    CALL
SYSPROC.ADMIN_REMOVE_MSGS('1594987316_285548770')

 1 record(s) selected.

 Return Status = 0

SQL20397W  Routine "SYSPROC.ADMIN_CMD" execution has completed, but at least
one error, "SQL1652", was encountered during the execution. More information
is available.  SQLSTATE=01H52
```

Para ver el mensaje de error, ejecute el comando de SQL como se sugiere en la respuesta anterior. `SELECT SQLCODE, MSG FROM TABLE(SYSPROC.ADMIN_GET_MSGS('1594987316_285548770')) AS MSG` devuelve el siguiente mensaje:

```
SQLCODE   MSG
```

```
---------
 ------------------------------------------------------------------------------------------
SQL2025N  An I/O error occurred. Error code “438”. Media on which this error occurred:
 “DB2REMOTE://s3test//public/datapump/t6.del”

SQL3500W The utility is beginning the LOAD phase at time “07/05/2024 21:21:48.082954”

SQL1652N File I/O error occurred
```

Los registros de diagnóstico de Db2 contienen un archivo de registro similar al siguiente:

```
2024-07-05-21.20.09.440609+000 I1191321E864          LEVEL: Error
PID     : 2710                 TID : 139619509200640 PROC : db2sysc 0
INSTANCE: rdsdb                NODE : 000            DB   : NTP
APPHDL  : 0-12180              APPID: xxx.xx.x.xxx.xxxxx.xxxxxxxxxxxx
UOWID   : 5                    ACTID: 1
AUTHID  : ADMIN                HOSTNAME: ip-xx-xx-x-xx
EDUID   : 147                  EDUNAME: db2lmr 0
FUNCTION: DB2 UDB, oper system services, sqloS3Client_GetObjectInfo, probe:219
MESSAGE : ZRC=0x870F01B6=-2029059658=SQLO_FAILED
          "An unexpected error is encountered"
DATA #1 : String, 29 bytes
S3:HeadObject request failed.
DATA #2 : signed integer, 4 bytes
99
DATA #3 : String, 0 bytes
Object not dumped: Address: 0x00007EFC08A9AE38 Size: 0 Reason: Zero-length data
DATA #4 : String, 33 bytes
curlCode: 28, Timeout was reached
```

Este error de E/S del archivo puede deberse a varios casos distintos. Por ejemplo, es posible que la VPC asociada al grupo de seguridad utilizado para crear la instancia de base de datos de RDS para Db2 no tenga un punto de conexión de puerta de enlace de Amazon S3. El punto de conexión es esencial para permitir de que RDS para Db2 acceda a Amazon S3. Si la instancia de base de datos de RDS para Db2 está en subredes privadas, necesitará un punto de conexión de puerta de enlace de Amazon S3. Puede especificar si su instancia de base de datos utiliza subredes públicas o privadas configurando los grupos de subredes de Amazon RDS. Para obtener más información, consulte Uso de los grupos de subredes de base de datos.

Temas

- Paso 1: crear un punto de conexión de puerta de enlace de VPC para Amazon S3

- Paso 2: confirme que existe el punto de conexión de la puerta de enlace de Amazon S3

Paso 1: crear un punto de conexión de puerta de enlace de VPC para Amazon S3

Para que la instancia de base de datos de RDS para Db2 interactúe con Amazon S3, cree una VPC y, a continuación, un punto de conexión de puerta de enlace de Amazon S3 para que lo utilicen las subredes privadas.

Creación de un punto de conexión de puerta de enlace de VPC para S3

1. Cree una VPC. Para obtener más información, consulte Creación de una VPC en la Guía del usuario de Amazon Virtual Private Cloud.
2. Cree un punto de conexión de puerta de enlace de Amazon S3 para que lo utilicen las subredes privadas. Para obtener más información, consulte Puntos de conexión de la puerta de enlace en la Guía de AWS PrivateLink.

Paso 2: confirme que existe el punto de conexión de la puerta de enlace de Amazon S3

Confirme que ha creado correctamente un punto de conexión de la puerta de enlace de Amazon S3 mediante el AWS Management Console o el AWS CLI.

Consola

Confirmación de un punto de conexión de puerta de enlace de Amazon S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc.
2. En la esquina superior derecha de la consola, elija la Región de AWS de su VPC.
3. Seleccione la VPC que ha creado.
4. En la pestaña Mapa de recursos, en Conexiones de red, confirme que aparezca un punto de conexión de puerta de enlace de Amazon S3.

AWS CLI

Para confirmar un punto de conexión de la puerta de enlace de Amazon S3, ejecute el comando describe-vpc-endpoints. En el siguiente ejemplo, sustituya *vpc_id* por el ID de VPC, la *región* por su Región de AWSy el *perfil* por su nombre de perfil.

Para Linux, macOS o Unix:

```
aws ec2 describe-vpc-endpoints \
    --filters "Name=vpc-id,Values=$vpc_id" \
    "Name=service-name,\
    Values=com.amazonaws.${region}.s3" \
    --region $region --profile=$profile \
    --query "VpcEndpoints[*].VpcEndpointId" --output text
```

Para Windows:

```
aws ec2 describe-vpc-endpoints ^
    --filters "Name=vpc-id,Values=$vpc_id" ^
    "Name=service-name,^
    Values=com.amazonaws.${region}.s3" ^
    --region $region --profile=$profile ^
    --query "VpcEndpoints[*].VpcEndpointId" --output text
```

El resultado de este comando debería ser similar al siguiente ejemplo si existe un punto de conexión de la puerta de enlace de Amazon S3.

```
[
    "vpce-0ea810434ff0b97e4"
]
```

El resultado de este comando debería ser similar al siguiente ejemplo si no existe un punto de conexión de la puerta de enlace de Amazon S3.

```
[]
```

Si no ve ningún punto de conexión de la puerta de enlace de Amazon S3 en la lista, entonces Paso 1: crear un punto de conexión de puerta de enlace de VPC para Amazon S3.

Errores en los procedimientos almacenados

En esta sección se describen varios errores que se muestran al llamar a los procedimientos almacenados y cómo solucionarlos.

Categoría	Errores en los procedimientos almacenados
Bases de datos	rdsadmin.activate_database errors
Bases de datos	rdsadmin.create_database errors
Bases de datos	Errores de rdsadmin.deactivate_database
Bases de datos	Errores de rdsadmin.drop_database
Bases de datos	Errores de rdsadmin.reactivate_database
Bases de datos	Errores de rdsadmin.restore_database
Bases de datos	Errores de rdsadmin.update_db_param
Espacios de tabla	Errores de rdsadmin.alter_tablespace

Errores de rdsadmin.activate_database

Los siguientes errores pueden producirse al llamar al procedimiento almacenado ???.

Error	Mensaje de error
Failed to allocate shared memory	`SQL1643C The database manager failed to allocate shared memory because the database manager instance memory limit has been reached.`
Unable to activate because of running processes	`The database can’t be activated because it's in the process of being created or restored.`

No se ha podido asignar la memoria compartida

El siguiente mensaje de error indica que el procedimiento almacenado no ha podido activar la base de datos porque la instancia de base de datos no tiene suficiente memoria.

```
SQL1643C The database manager failed to allocate shared memory because the database
 manager instance memory limit has been reached.
```

Aumente la memoria de la instancia de base de datos y, a continuación, vuelva a llamar al procedimiento `rdsadmin.activate_database` almacenado. Para obtener información sobre el uso de la memoria y las recomendaciones para las bases de datos, consulte the section called “Múltiples bases de datos Db2”.

No se puede activar debido a procesos en ejecución

El siguiente mensaje de error indica que el procedimiento almacenado no ha podido activar una base de datos porque el procedimiento almacenado `rdsadmin.create_database` o `rdsadmin.restore_database` se está ejecutando.

```
The database can’t be activated because it's in the process of being created or
 restored.
```

Espere unos minutos y vuelva a llamar al procedimiento almacenado `rdsadmin.activate_database`.

Errores de rdsadmin.alter_tablespace

Los siguientes errores pueden producirse al llamar al procedimiento almacenado the section called “rdsadmin.alter_tablespace”.

Error	Mensaje de error

Statement not valid	`DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned:`
	
	`SQL1763N Invalid ALTER TABLESPACE statement for table space "TBSP_TEST" due to reason "12"`

tablespace_prefetch_size value not valid	`Invalid tablespace_prefetch_size. Set value to AUTOMATIC or to a non-zero positive numerical value.`

Error	Mensaje de error
tablespace_prefetch_size numerical value not valid	`Invalid tablespace_prefetch_size. The number of pages can't be greater than 32767.`
Parameter can't be used with tablespace_prefetch_size	`You can't use tablespace_prefetch_size with {parameter }.`
Tablespace change failed	`The change to tablespace { tablespace_name}  failed because you can only alter LARGE or REGULAR tablespaces.`

La instrucción no es válida

El siguiente mensaje de error indica que el procedimiento almacenado combinó parámetros opcionales mutuamente excluyentes con otros parámetros opcionales. Los parámetros opcionales `reduce_max, reduce_stop`, `reduce_value`, `lower_high_water`, `lower_high_water_stop` y `switch_online` del procedimiento almacenado `rdsadmin.alter_tablespace` son mutuamente excluyentes. No puede combinarlos con ningún otro parámetro opcional, por ejemplo `buffer_pool_name`, en el procedimiento almacenado `rdsadmin.alter_tablespace`. Si los combina, al llamar a la función `rdsadmin.get_task_status` definida por el usuario, Db2 devolverá este mensaje de error.

```
DB21034E The command was processed as an SQL statement because it was not a valid
 Command Line Processor command. During SQL processing it returned:
SQL1763N Invalid ALTER TABLESPACE statement for table space "TBSP_TEST" due to reason
 "12"
```

Vuelva a llamar al procedimiento almacenado `rdsadmin.alter_tablespace` sin combinar parámetros opcionales mutuamente excluyentes con otros parámetros opcionales. A continuación, llame a la función `rdsadmin.get_task_status` definida por el usuario. Para obtener más información, consulte rdsadmin.alter_tablespace y rdsadmin.get_task_status.

Valor de tablespace_prefetch_size no válido

El siguiente mensaje de error indica que no ha establecido `tablespace_prefetch_size` en `AUTOMATIC` o un valor numérico no positivo. Por ejemplo, ha intentado establecerlo en `testinput`.

```
Invalid tablespace_prefetch_size. Set value to AUTOMATIC or to a non-zero positive
 numerical value.
```

Vuelva a llamar al procedimiento almacenado `rdsadmin.alter_tablespace` y establezca `tablespace_prefetch_size` en `AUTOMATIC` o en un valor numérico no positivo.

El valor numérico tablespace_prefetch_size no es válido

El siguiente mensaje de error indica que ha establecido `tablespace_prefetch_size` en un valor numérico superior a 32767.

```
Invalid tablespace_prefetch_size. The number of pages can't be greater than 32767.
```

Vuelva a llamar al procedimiento almacenado `rdsadmin.alter_tablespace` y establezca `tablespace_prefetch_size` en un valor numérico positivo que no sea cero inferior o igual a 32767.

El parámetro no se puede usar con tablespace_prefetch_size

El siguiente mensaje de error indica que intentó utilizar `tablespace_prefetch_size` con un parámetro no compatible.

```
You can't use tablespace_prefetch_size with {parameter}.
```

Vuelva a llamar al procedimiento almacenado `rdsadmin.alter_tablespace` y use `tablespace_prefetch_size` solo con parámetros compatibles. Para obtener información acerca de parámetros que puede usar con `tablespace_prefetch_size`, consulte rdsadmin.alter_tablespace.

Error al cambiar el espacio de tablas

El siguiente mensaje de error indica que intentó modificar un espacio de tabla.

```
The change to tablespace {tablespace_name} failed because you can only alter LARGE or
 REGULAR tablespaces.
```

Errores de rdsadmin.create_database

El siguiente error puede producirse al llamar al procedimiento almacenado the section called “rdsadmin.create_database”.

Error	Mensaje de error
Failed to allocate shared memory	`SQL1643C The database manager failed to allocate shared memory because the database manager instance memory limit has been reached.`

No se ha podido asignar la memoria compartida

El siguiente mensaje de error indica que el procedimiento almacenado no ha podido crear la base de datos porque la instancia de base de datos no tiene suficiente memoria.

```
SQL1643C The database manager failed to allocate shared memory because the database
 manager instance memory limit has been reached.
```

Aumente la memoria de la instancia de base de datos y, a continuación, vuelva a llamar al procedimiento `rdsadmin.create_database` almacenado. Para obtener información sobre el uso de la memoria y las recomendaciones para las bases de datos, consulte the section called “Múltiples bases de datos Db2”.

Para confirmar que se ha creado la base de datos, llame a la función the section called “rdsadmin.list_databases” definida por el usuario y compruebe que la nueva base de datos aparezca en la lista.

Errores de rdsadmin.deactivate_database

El siguiente error puede producirse al llamar al procedimiento almacenado ???.

Error	Mensaje de error
Unable to deactivate because of running processes	`The database can’t be deactivated because it's in the process of being created or restored.`

No se puede desactivar debido a procesos en ejecución

El siguiente mensaje de error indica que el procedimiento almacenado no ha podido desactivar una base de datos porque el procedimiento almacenado `rdsadmin.create_database` o `rdsadmin.restore_database` se está ejecutando.

```
The database can’t be deactivated because it's in the process of being created or
 restored.
```

Espere unos minutos y vuelva a llamar al procedimiento almacenado `rdsadmin.deactivate_database`.

Errores de rdsadmin.drop_database

Los siguientes errores pueden producirse al llamar al procedimiento almacenado the section called “rdsadmin.drop_database”.

Error	Mensaje de error
Database name doesn't exist	`SQL0438N Application raised error or warning with diagnostic text: "Cannot drop database. Database with provided name does not exist". SQLSTATE=99993`
Return status = 0	`Return Status = 0`
Dropping database not allowed	`1 ERROR DROP_DATABASE RDSDB 2023-10-10-16.33.0 3.744122 2023-10-10-16.33.30.143797 - 2023-10-1 0-16.33.30.098857 Task execution has started. 2023-10-10-16.33.30.143797 Caught exception during executing task id 1, Aborting task. Reason Dropping database created via rds CreateDBInstance api is not allowed. Only database created using rdsadmin. create_database can be dropped`

El nombre de la base de datos no existe

El siguiente mensaje de error indica que ha pasado un nombre de base de datos incorrecto en el procedimiento almacenado `rdsadmin.drop_database`.

```
SQL0438N Application raised error or warning with diagnostic text: "Cannot
drop database. Database with provided name does not exist". SQLSTATE=99993
```

Vuelva a llamar al procedimiento almacenado `rdsadmin.drop_database` con un nombre de base de datos correcto. Para confirmar que se ha descartado la base de datos, llame a la función the section called “rdsadmin.list_databases” definida por el usuario y compruebe que la nueva base de datos descartada no aparezca en la lista.

Estado de devolución = 0

El siguiente mensaje de error indica que no se ha podido completar el procedimiento almacenado.

```
Return Status = 0
```

Una vez recibido `Return Status = 0`, llame a la función rdsadmin.get_task_status definida por el usuario.

No se permite borrar la base de datos

El siguiente mensaje de error indica que creó la base de datos mediante la consola de Amazon RDS o mediante la AWS CLI. Solo puede utilizar el procedimiento almacenado `rdsadmin.drop_database` si ha creado la base de datos llamando al procedimiento almacenado the section called “rdsadmin.create_database”.

```
1 ERROR DROP_DATABASE RDSDB 2023-10-10-16.33.03.744122 2023-10-10-16.33.30.143797 -
 2023-10-10-16.33.30.098857 Task execution has started.
2023-10-10-16.33.30.143797 Caught exception during executing task id 1, Aborting task.
Reason Dropping database created via rds CreateDBInstance api is not allowed.
Only database created using rdsadmin.create_database can be dropped
```

Para eliminar una base de datos que haya creado mediante la consola de Amazon RDS o la AWS CLI, utilice un cliente para conectarse a la base de datos y, a continuación, ejecute el comando correspondiente.

Errores de rdsadmin.reactivate_database

El siguiente error puede producirse al llamar al procedimiento almacenado ???.

Error	Mensaje de error
Failed to allocate shared memory	`SQL1643C The database manager failed to allocate shared memory because the database manager instance memory limit has been reached.`
Unable to reactivate because of running processes	`The database can’t be reactivated because it's in the process of being created or restored.`

No se ha podido asignar la memoria compartida

El siguiente mensaje de error indica que el procedimiento almacenado no ha podido activar la base de datos porque la instancia de base de datos no tiene suficiente memoria.

```
SQL1643C The database manager failed to allocate shared memory because the database
 manager instance memory limit has been reached.
```

Aumente la memoria de la instancia de base de datos y, a continuación, vuelva a llamar al procedimiento `rdsadmin.activate_database` almacenado. Para obtener información sobre el uso de la memoria y las recomendaciones para las bases de datos, consulte the section called “Múltiples bases de datos Db2”.

No se puede reactivar debido a procesos en ejecución

El siguiente mensaje de error indica que el procedimiento almacenado no ha podido reactivar una base de datos porque el procedimiento almacenado `rdsadmin.create_database` o `rdsadmin.restore_database` se está ejecutando.

```
The database can’t be reactivated because it's in the process of being created or
 restored.
```

Espere unos minutos y vuelva a llamar al procedimiento almacenado `rdsadmin.reactivate_database`.

Errores de rdsadmin.restore_database

Los siguientes errores pueden producirse al llamar al procedimiento almacenado the section called “rdsadmin.restore_database”.

Error	Mensaje de error
Insufficient disk space	`Aborting task. Reason Restoring your database failed because of insufficient disk space. Increase the storage for your DB instance and rerun the rdsadmin.restore_database stored procedure.`
Internal error	`Caught exception during executing task id 104, Aborting task. Reason Internal Error`
Non-fenced routines not allowed	`Caught exception during executing task id 2, Aborting task. Reason Non fenced routines are not allowed. Please delete the routines and retry the restore.`
Tablespaces not restored	`Reason SQL0970N The system attempted to write to a read-only file. Reason SQL2563W The Restore process has completed successfully. However one or more table spaces from the backup were not restored.`

Espacio en disco insuficiente

El siguiente mensaje de error indica que la instancia de base de datos no tiene suficiente espacio en disco para restaurar la base de datos:

```
Aborting task. Reason Restoring your database failed because of insufficient
 disk space. Increase the storage for your DB instance and rerun the
 rdsadmin.restore_database stored procedure.
```

El espacio libre en la instancia de base de datos debe ser más del doble que el tamaño de la imagen de copia de seguridad. Si la imagen de copia de seguridad está comprimida, el espacio libre en la instancia de base de datos debe ser más del triple que el tamaño de la imagen de copia de seguridad. Para obtener más información, consulte the section called “Aumento de la capacidad de almacenamiento de la instancia de base de datos”.

Aumente el espacio en disco y, a continuación, vuelva a ejecutar el procedimiento `rdsadmin.restore_database` almacenado. Para confirmar que se ha restaurado la base de datos, llame a la función the section called “rdsadmin.list_databases” definida por el usuario y compruebe que la base de datos restaurada aparezca en la lista.

Error interno

El siguiente mensaje de error indica que el procedimiento almacenado ha detectado un error interno:

```
Caught exception during executing task id 104, Aborting task. Reason Internal Error
```

Contacte con AWS Support.

No se permiten rutinas no restringidas

El siguiente mensaje de error indica que la base de datos incluye rutinas no restringidas:

```
Caught exception during executing task id 2, Aborting task. Reason Non fenced routines
 are not allowed. Please delete the routines and retry the restore.
```

RDS para Db2 no admite la creación de rutinas no restringidas. Elimine las rutinas no restringidas de la base de datos de origen y, a continuación, vuelva a llamar a `rdsadmin.restore_database`. Para confirmar que se ha restaurado la base de datos, llame a la función the section called "rdsadmin.list_databases" definida por el usuario y compruebe que la base de datos restaurada aparezca en la lista. Para obtener más información, consulte the section called "Rutinas no restringidas".

No se han restaurado los espacios de tablas

El siguiente mensaje de error indica que RDS para Db2 ha restaurado correctamente la base de datos, pero no ha podido restaurar uno o varios espacios de tabla:

```
Reason SQL0970N The system attempted to write to a read-only file.
Reason SQL2563W The Restore process has completed successfully. However one or more
 table spaces from the backup were not restored.
```

RDS para Db2 no admite almacenamiento no automático. Convierta el almacenamiento no automático en almacenamiento automático y, a continuación, vuelva a llamar a `rdsadmin.restore_database`. Para obtener más información, consulte la sección Converting a nonautomatic storage database to use automatic storage en la documentación de IBM Db2.

Las bases de datos con almacenamiento de SMS no automático requieren una restauración manual. Si su base de datos tiene almacenamiento de SMS no automático, póngase en contacto con AWS Support.

Para obtener información sobre las migraciones únicas y el almacenamiento no automático, consulte the section called “Espacios de tablas de almacenamiento no automáticos durante la migración”.

Errores de rdsadmin.update_db_param

El siguiente error puede producirse al llamar al procedimiento almacenado the section called “rdsadmin.update_db_param”.

Error	Mensaje de error
Parameter not supported or modifiable	`SQL0438N Application raised error or warning with diagnostic text: "Parameter is either not supported or not modifiable to customers". SQLSTATE=99993`

El parámetro no es compatible ni se puede modificar

El siguiente mensaje de error indica que intentó modificar un parámetro de configuración de base de datos que no es compatible o no se puede modificar.

```
SQL0438N Application raised error or warning with diagnostic text: "Parameter
is either not supported or not modifiable to customers". SQLSTATE=99993
```

Puede ver qué parámetros se pueden modificar consultando sus grupos de parámetros. Para obtener más información, consulte the section called “Visualización de valores de parámetros en un grupo de parámetros de base de datos”.

Amazon RDS para MariaDB

Amazon RDS admite varias versiones de instancias de MariaDB para base de datos. Para obtener toda la información necesaria sobre versiones compatibles, consulte Versiones de MariaDB en Amazon RDS.

Para crear una instancia de base de datos de MariaDB, utilice las herramientas o interfaces de administración de Amazon RDS. A continuación, puede utilizar las herramientas de Amazon RDS para realizar acciones de administración para la instancia de base de datos. Incluyen acciones como las siguientes:

- Reconfiguración o cambio de tamaño de la instancia de base de datos
- Autorización de las conexiones a la instancia de base de datos
- Creación y restauración a partir de copias de seguridad o instantáneas
- Creación de secundarios Multi-AZ
- Creación de réplicas de lectura
- Supervisión del rendimiento de su instancia de base de datos

Para almacenar y acceder a los datos de la instancia de base de datos, use las utilidades y aplicaciones estándar de MariaDB.

MariaDB está disponible en todas las Regiones de AWS. Para obtener más información acerca de Regiones de AWS, consulte Regiones, zonas de disponibilidad y Local Zones.

Puede utilizar Amazon RDS para bases de datos de Amazon RDS for MariaDB para crear aplicaciones compatibles con HIPAA. Puede guardar información de contenido sanitario, incluida información sanitaria protegida (PHI), si ha firmado un Acuerdo para socio empresarial (BAA) de AWS. Para obtener más información, consulte Conformidad con HIPAA. AWS Los servicios en el ámbito han sido evaluados completamente por un auditor externo y dan como resultado una certificación, declaración de conformidad o autoridad para operar (ATO). Para obtener más información, consulte Servicios de AWS incluidos en el ámbito por programa de conformidad.

Antes de crear una instancia de base de datos, complete los pasos que se describen en Configuración del entorno para Amazon RDS. Cuando crea una instancia de base de datos, el usuario maestro de RDS obtiene privilegios de DBA, con algunas limitaciones. Utilice esta cuenta para tareas administrativas, como crear cuentas de base de datos adicionales.

Puede crear lo siguiente:

- Instancias de base de datos
- Instantáneas de base de datos
- Restauraciones a un momento dado
- Copias de seguridad automatizadas
- Copias de seguridad manuales

Puede utilizar instancias de base de datos que ejecuten MariaDB en una nube privada virtual (VPC) basada en Amazon VPC. También puede agregar características a la instancia de base de datos de MariaDB; para ello, habilite diversas opciones. Amazon RDS admite implementaciones multi-AZ para MariaDB como una solución de conmutación por error de alta disponibilidad.

> **Important**
>
> Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Puede acceder a la base de datos con clientes estándar de SQL, como mysql. No obstante, no puede acceder al host directamente mediante Telnet o Secure Shell (SSH).

Temas

- Compatibilidad de características de MariaDB en Amazon RDS
- Versiones de MariaDB en Amazon RDS
- Conexión a la instancia de base de datos de MariaDB
- Protección de las conexiones de instancias de base de datos MariaDB
- Mejora del rendimiento de las consultas de RDS para MariaDB con lecturas optimizadas de Amazon RDS
- Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB
- Actualizaciones del motor de base de datos de MariaDB
- Actualización de una versión del motor de instantáneas de base de datos de MariaDB
- Importación de datos en una instancia de base de datos de Amazon RDS para MariaDB
- Uso de la replicación de MariaDB en Amazon RDS

- Opciones para el motor de base de datos de MariaDB
- Parámetros de MariaDB
- Migración de datos desde una instantánea de base de datos de MySQL a una instancia de base de datos MariaDB
- Referencia de MariaDB en Amazon RDS SQL
- Zona horaria local para instancias de base de datos de MariaDB
- Problemas conocidos y limitaciones de RDS para MariaDB

Compatibilidad de características de MariaDB en Amazon RDS

RDS para MariaDB admite la mayoría de las características y capacidades de MariaDB. Algunas características pueden disponer de una compatibilidad limitada o de privilegios restringidos.

Puede filtrar nuevas características de Amazon RDS en la página Novedades de Database. En el filtro Products (Productos), elija Amazon RDS. A continuación, busque con palabras clave como **`MariaDB 2023`**.

> **Note**
>
> Las listas que siguen no son exhaustivas.

Para obtener más información sobre la compatibilidad de características de MariaDB en Amazon RDS, consulte los siguientes temas.

Temas

- Motores de almacenamiento de MariaDB admitidos en Amazon RDS
- Calentamiento de caché para MariaDB en Amazon RDS
- Características de MariaDB que no admite Amazon RDS

Compatibilidad de características de MariaDB en las versiones principales de Amazon RDS para MariaDB

En las siguientes secciones, encontrará información sobre la compatibilidad de características de MariaDB en Amazon RDS para MariaDB para las versiones principales de MariaDB:

Temas

- Compatibilidad con MariaDB 11.4 en Amazon RDS
- Compatibilidad con MariaDB 10.11 en Amazon RDS
- Compatibilidad con MariaDB 10.6 en Amazon RDS
- Compatibilidad con MariaDB 10.5 en Amazon RDS
- Compatibilidad con MariaDB 10.4 en Amazon RDS

Para obtener información acerca de la compatibilidad de las versiones secundarias de Amazon RDS for MariaDB, consulte Versiones de MariaDB en Amazon RDS.

Compatibilidad con MariaDB 11.4 en Amazon RDS

Amazon RDS admite las siguientes características nuevas de las instancias de base de datos en las que se ejecuta la versión 11.4 de MariaDB o una posterior.

- Biblioteca criptográfica: RDS para MariaDB ha sustituido a OpenSSL por AWS Libcrypto Libcrypto (AWS-LC-LC), que cuenta con la certificación FIPS 140-3.
- Complemento simple de verificación de contraseñas: puede usar el complemento simple de verificación de contraseñas para MariaDB para verificar si una contraseña contiene al menos un número específico de caracteres de un tipo específico. Para obtener más información, consulte the section called “Complementos de validación de contraseñas”.
- Complemento de verificación de contraseñas Cracklib: puede usar el complemento de verificación de contraseñas Cracklib para MariaDB para comprobar la seguridad de las nuevas contraseñas. Para obtener más información, consulte the section called “Complementos de validación de contraseñas”.
- Mejoras de InnoDB: estas mejoras incluyen los siguientes elementos:
  - Se ha eliminado el búfer de cambios. Para obtener más información, consulte InnoDB Change Buffering.
  - Se ha eliminado la desfragmentación de InnoDB. Para obtener más información, consulte InnoDB Defragmentation.
- Nuevo privilegio: el usuario administrador ahora también tiene el privilegio `SHOW CREATE ROUTINE`. Este privilegio permite al concesionario ver la declaración de definición `SHOW CREATE` de una rutina que es propiedad de otro usuario. Para obtener más información acerca de los privilegios, consulte Database Privileges.

- Mejora de la replicación: las instancias de base de datos MariaDB versión 11.4 admiten la indexación binlog. Puede crear un índice GTID para cada archivo binlog. Estos índices mejoran el rendimiento de la replicación al reducir el tiempo que se tarda en localizar un GTID. Para obtener más información, consulte Binlog Indexing.
- Parámetros obsoletos o eliminados: los siguientes parámetros han quedado obsoletos o se han eliminado para las instancias de base de datos de la versión 11.4 de MariaDB:
  - `engine_condition_pushdown` se ha eliminado de optimizer_switch
  - innodb_change_buffer_max_size
  - innodb_defragment
  - `TLSv1.0` y `TLSv1.1` se han eliminado de tls_version
- Nuevos valores predeterminados de un parámetro: el valor predeterminado del parámetro innodb_undo_tablespaces ha cambiado de `0` a `3`.
- Nuevos valores válidos de los parámetros: los siguientes parámetros tienen nuevos valores válidos para las instancias de base de datos de la versión 11.4 de MariaDB:
  - Los valores válidos del parámetro binlog_row_image ahora incluyen `FULL_NODUP`.
  - Los valores válidos del parámetro OLD_MODE ahora incluyen `NO_NULL_COLLATION_IDS`.
- Nuevos parámetros: los siguientes parámetros son nuevos para las instancias de base de datos de la versión 11.4 de MariaDB:
  - El parámetro transaction_isolation reemplaza al parámetro tx_isolation.
  - El parámetro transaction_read_only reemplaza al parámetro tx_read_only.
  - El parámetro block_encryption_mode define el modo de cifrado por bloques predeterminado para las funciones AES_ENCRYPT() y AES_DECRYPT().
  - El parámetro character_set_collations define las anulaciones de las intercalaciones predeterminadas del conjunto de caracteres.
  - Los parámetros binlog_gtid_index, binlog_gtid_index_page_size y binlog_gtid_index_span_min definen las propiedades del índice GTID de binlog. Para obtener más información, consulte Binlog Indexing.

Para ver una lista de todas las características de MariaDB 11.4 y de su documentación, consulte Changes and improvements in MariaDB 11.4 y Release notes - MariaDB 11.4 series en el sitio web de MariaDB.

Para ver una lista de las características no admitidas, consulte Características de MariaDB que no admite Amazon RDS.

Compatibilidad con MariaDB 10.11 en Amazon RDS

Amazon RDS admite las siguientes características nuevas de las instancias de base de datos en las que se ejecuta la versión 10.11 de MariaDB o una posterior.

- Complemento Password Reuse Check: puede utilizar el complemento Password Reuse Check de MariaDB para evitar que los usuarios reutilicen las contraseñas y para establecer el período de retención de las contraseñas. Para obtener más información, consulte el complemento Password Reuse Check.
- Autorización GRANT TO PUBLIC: puede conceder privilegios a todos los usuarios que tengan acceso a su servidor. Para obtener más información, consulte GRANT TO PUBLIC.
- Disociación de los privilegios SUPER y READ ONLY ADMIN: puede eliminar los privilegios READ ONLY ADMIN de todos los usuarios, incluidos los usuarios que antes tenían privilegios SUPER.
- Seguridad: ahora puede configurar la opción `--ssl`como predeterminada para su cliente MariaDB. MariaDB ya no deshabilita silenciosamente la SSL si la configuración es incorrecta.
- Comandos y funciones de SQL: ahora puede utilizar el comando `SHOW ANALYZE FORMAT=JSON` y las funciones `ROW_NUMBER`, `SFORMAT` y `RANDOM_BYTES`. `SFORMAT` permite el formato de cadena y está habilitado de forma predeterminada. Puede convertir la partición en tabla y la tabla en partición con un solo comando. También hay varias mejoras en torno a las funciones `JSON_*()`. Las funciones `DES_ENCRYPT` y `DES_DECRYPT` han quedado obsoletas para la versión 10.10 y versiones posteriores. Para obtener más información, consulte SFORMAT.
- Mejoras de InnoDB: estas mejoras incluyen los siguientes elementos:
  - Mejoras en el rendimiento del registro REDO para reducir la amplificación de la escritura y mejorar la simultaneidad.
  - Posibilidad de cambiar el espacio de tabla UNDO sin reinicializar el directorio de datos. Esta mejora reduce la sobrecarga del plano de control. Se requiere un reinicio, pero no se requiere reinicialización después de cambiar el espacio de tabla UNDO.
  - Soporte para `CHECK TABLE … EXTENDED` y para índices descendentes internamente.
  - Mejoras en la inserción masiva.
- Cambios de binlog: estos cambios incluyen los siguientes elementos:
  - Registro `ALTER` en dos fases para reducir la latencia de replicación. El parámetro `binlog_alter_two_phase` está deshabilitado de forma predeterminada, pero se puede habilitar mediante grupos de parámetros.
  - Registro `explicit_defaults_for_timestamp`.

  - Ya no se registra `INCIDENT_EVENT` si la transacción se puede anular de forma segura.
- Mejoras de replicación: las instancias de base de datos de la versión 10.11 de MariaDB utilizan la replicación GTID de forma predeterminada si el maestro la admite. Además, `Seconds_Behind_Master` es más preciso.
- Clientes: puede utilizar las nuevas opciones de línea de comandos para `mysqlbinglog` y `mariadb-dump`. Puede utilizar `mariadb-dump` para volcar y restaurar datos históricos.
- Control de versiones del sistema: es posible modificar el historial. MariaDB crea automáticamente nuevas particiones.
- DDL atómico: ahora `CREATE OR REPLACE` es atómico. La instrucción se lleva a cabo correctamente o se revierte por completo.
- Escritura del registro REDO: el registro REDO se escribe de forma asíncrona.
- Funciones almacenadas: las funciones almacenadas ahora admiten los mismos parámetros `IN`, `OUT` e `INOUT` que los procedimientos almacenados.
- Parámetros obsoletos o eliminados: los siguientes parámetros han quedado obsoletos o se han eliminado para las instancias de base de datos de la versión 10.11 de MariaDB:
  - innodb_change_buffering
  - innodb_disallow_writes
  - innodb_log_write_ahead_size
  - innodb_prefix_index_cluster_optimization
  - keep_files_on_create
  - old
- Parámetros dinámicos: los siguientes parámetros son ahora dinámicos para las instancias de base de datos de la versión 10.11 de MariaDB:
  - innodb_log_file_size
  - innodb_write_io_threads
  - innodb_read_io_threads
- Valores nuevos predeterminados para los parámetros: los siguientes parámetros tienen valores predeterminados nuevos para las instancias de base de datos de la versión 10.11 de MariaDB:
  - El valor predeterminado del parámetro explicit_defaults_for_timestamp ha cambiado de `OFF` a `ON`.
  - El valor predeterminados del parámetro optimizer_prune_level ha cambiado de 1 a 2.

- Valores nuevos válidos de los parámetros: los siguientes parámetros tienen valores predeterminados nuevos para las instancias de base de datos de la versión 10.11 de MariaDB:
  - Los valores válidos del parámetro old se fusionaron con los del parámetro old_mode.
  - Los valores válidos del parámetro histogram_type ahora incluyen `JSON_HB`.
  - El rango de valores válido para el parámetro innodb_log_buffer_size ahora es de `262144` a `4294967295` (256 KB a 4096 MB).
  - El rango de valores válido para el parámetro innodb_log_file_size ahora es de `4194304` a `512GB` (4 MB a 512 GB).
  - Los valores válidos del parámetro optimizer_prune_level ahora incluyen 2.
- Nuevos parámetros: los siguientes parámetros son nuevos para las instancias de base de datos de la versión 10.11 de MariaDB:
  - El parámetro binlog_alter_two_phase puede mejorar el rendimiento de la replicación.
  - El parámetro log_slow_min_examined_row_limit puede mejorar el rendimiento.
  - El parámetro log_slow_query y el parámetro log_slow_query_file son alias de `slow_query_log` y `slow_query_log_file`, respectivamente.
  - optimizer_extra_pruning_depth
  - system_versioning_insert_history

Para ver una lista de todas las características de MariaDB 10.11 y de su documentación, consulte Changes and improvements in MariaDB 10.11 y Release notes - MariaDB 10.11 series en el sitio web de MariaDB.

Para ver una lista de las características no admitidas, consulte Características de MariaDB que no admite Amazon RDS.

Compatibilidad con MariaDB 10.6 en Amazon RDS

Amazon RDS admite las siguientes características nuevas de las instancias de base de datos en las que se ejecuta la versión 10.6 de MariaDB o una posterior:

- Motor de almacenamiento MyRocks: puede utilizar el motor de almacenamiento MyRocks con RDS for MariaDB para optimizar el consumo de almacenamiento de las aplicaciones web con uso intensivo de escritura y de alto rendimiento. Para obtener más información, consulte Motores de almacenamiento de MariaDB admitidos en Amazon RDS y MyRocks.

- Autenticación de base de datos de AWS Identity and Access Management (IAM): puede utilizar la autenticación de base de datos de IAM para mejorar la seguridad y la administración central de las conexiones a sus instancias de base de datos de MariaDB. Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.
- Opciones de actualización: ahora puede actualizar a la versión 10.6 de RDS for MariaDB desde cualquier versión principal anterior (10.3, 10.4, 10.5). También puede restaurar una instantánea de una instancia de base de datos MySQL 5.6 o 5.7 existente a una instancia de MariaDB 10.6. Para obtener más información, consulte Actualizaciones del motor de base de datos de MariaDB.
- Replicación retrasada: ahora puede establecer un periodo de tiempo configurable durante el cual una réplica de lectura se retrasa con respecto a la base de datos de origen. En una configuración de replicación estándar de MariaDB, hay un retraso de replicación mínimo entre el origen y la réplica. Con la replicación retrasada, puede configurar un retraso intencional como estrategia de recuperación de desastres. Para obtener más información, consulte Configuración de la replicación retrasada con MariaDB.
- Compatibilidad con Oracle PL/SQL: mediante el uso de la versión 10.6 de RDS for MariaDB puede migrar con más facilidad sus aplicaciones Oracle heredadas a Amazon RDS. Para obtener más información, consulte SQL_MODE=ORACLE.
- Atomic DDL: las instrucciones de lenguaje de datos dinámicos (DDL) pueden ser relativamente seguras frente a bloqueos con la versión 10.6 de RDS for MariaDB. `CREATE TABLE`, `ALTER TABLE`, `RENAME TABLE`, `DROP TABLE`, `DROP DATABASE` y las instrucciones DDL relacionadas ahora son atómicas. La instrucción se lleva a cabo correctamente o se revierte por completo. Para obtener más información, consulte Atomic DDL.
- Otras mejoras: estas mejoras incluyen una función `JSON_TABLE` para transformar datos JSON a un formato relacional dentro de SQL y una carga más rápida de datos de tablas vacías con InnoDB. También incluyen un nuevo `sys_schema` para el análisis y la solución de problemas, la mejora del optimizador que permite ignorar los índices no utilizados, y las mejoras de rendimiento. Para obtener más información, consulte JSON_TABLE.
- Valores nuevos predeterminados para los parámetros: los siguientes parámetros tienen valores predeterminados nuevos para las instancias de base de datos de la versión 10.6 de MariaDB:
  - El valor predeterminado para los siguientes parámetros ha cambiado de `utf8` a `utf8mb3`:
    - character_set_client
    - character_set_connection
    - character_set_results
    - character_set_system

Si bien los valores predeterminados han cambiado para estos parámetros, no hay ningún cambio funcional. Para obtener más información, consulte Supported Character Sets and Collations (Conjuntos de caracteres e intercalaciones admitidos) en la documentación de MariaDB.

- El valor predeterminado del parámetro collation_connection ha cambiado de `utf8_general_ci` a `utf8mb3_general_ci`. Si bien el valor predeterminado ha cambiado para este parámetro, no hay ningún cambio funcional.
- El valor predeterminado del parámetro old_mode ha cambiado de sin establecer a `UTF8_IS_UTF8MB3`. Si bien el valor predeterminado ha cambiado para este parámetro, no hay ningún cambio funcional.

Para ver una lista de todas las características de la versión 10.6 de MariaDB y la documentación correspondiente, consulte Cambios y mejoras de la versión 10.6 de MariaDB y Notas de la versión: serie 10.6 de MariaDB en el sitio web de MariaDB.

Para ver una lista de las características no admitidas, consulte Características de MariaDB que no admite Amazon RDS.

Compatibilidad con MariaDB 10.5 en Amazon RDS

Amazon RDS admite las siguientes características nuevas de sus instancias de base de datos en las que se ejecuta la versión 10.5 de MariaDB o una posterior:

- Mejoras de InnoDB – en la versión 10.5 de MariaDB se incluyen mejoras de InnoDB. Para obtener más información, consulte InnoDB: Performance Improvements etc. (InnoDB: mejoras de rendimiento, etc.) en la documentación de MariaDB.
- Actualizaciones del esquema de rendimiento – en la versión 10.5 de MariaDB se incluyen actualizaciones del esquema de rendimiento. Para obtener más información, consulte Performance Schema Updates to Match MySQL 5.7 Instrumentation and Tables (Actualizaciones del esquema de rendimiento para lograr la coincidencia con la instrumentación y las tablas de MySQL 5.7) en la documentación de MariaDB.
- Un solo archivo en el registro REDO de InnoDB – en las versiones de MariaDB anteriores a la versión 10.5, el valor del parámetro `innodb_log_files_in_group` estaba establecido en 2. En la versión 10.5 de MariaDB, el valor de este parámetro está establecido en 1.

  Si efectúa la actualización desde una versión anterior a la versión 10.5 de MariaDB y no modifica los parámetros, el valor del parámetro `innodb_log_file_size` no cambia. Sin embargo, vale

para un solo archivo de registro en lugar de para dos. El resultado es que la instancia de base de datos actualizada de MariaDB, versión 10.5, utiliza la mitad del tamaño del registro REDO que usaba antes de la actualización. Este cambio puede tener un efecto notable en el rendimiento. Para solucionar este problema, puede duplicar el valor del parámetro `innodb_log_file_size`. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

- No se admite el comando SHOW SLAVE STATUS – en las versiones de MariaDB anteriores a la versión 10.5, el comando `SHOW SLAVE STATUS` requería el privilegio `REPLICATION SLAVE`. En la versión 10.5 de MariaDB, el comando `SHOW REPLICA STATUS` equivalente requiere el privilegio `REPLICATION REPLICA ADMIN`. Este privilegio nuevo no se otorga al usuario maestro de RDS.

  En lugar de utilizar el comando `SHOW REPLICA STATUS`, ejecute el procedimiento almacenado `mysql.rds_replica_status` nuevo para devolver información similar. Para obtener más información, consulte mysql.rds_replica_status.
- No se admite el comando SHOW RELAYLOG EVENTS – en las versiones de MariaDB anteriores a la versión 10.5, el comando `SHOW RELAYLOG EVENTS` requería el privilegio `REPLICATION SLAVE`. En la versión 10.5 de MariaDB, este comando requiere el privilegio `REPLICATION REPLICA ADMIN`. Este privilegio nuevo no se otorga al usuario maestro de RDS.
- Valores predeterminados nuevos para los parámetros – los siguientes parámetros tienen valores predeterminados nuevos para las instancias de base de datos de MariaDB, versión 10.5:
  - El valor predeterminado del parámetro max_connections ha cambiado a `LEAST({DBInstanceClassMemory/25165760},12000)`. Para obtener información sobre la función de parámetro `LEAST`, consulte Funciones de parámetros de base de datos.
  - El valor predeterminado del parámetro innodb_adaptive_hash_index ha cambiado a `OFF` (`0`).
  - El valor predeterminado del parámetro innodb_checksum_algorithm ha cambiado a `full_crc32`.
  - El valor predeterminado del parámetro innodb_log_file_size ha cambiado a 2 GB.

Para ver una lista de todas las características de la versión 10.5 de MariaDB y la documentación respectiva, consulte Changes & Improvements in MariaDB 10.5 (Cambios y mejoras de la versión 10.5 de MariaDB) y Release Notes - MariaDB 10.5 Series (Notas de la versión: Serie 10.5 de MariaDB), en el sitio web de MariaDB.

Para ver una lista de las características no admitidas, consulte Características de MariaDB que no admite Amazon RDS.

Compatibilidad con MariaDB 10.4 en Amazon RDS

Amazon RDS admite las siguientes nuevas características de sus instancias de base de datos en las que se ejecuta la versión de MariaDB 10.4 o posterior:

- Mejoras en la seguridad de la cuenta de usuario – Mejoras del vencimiento de la contraseña y bloqueo de cuentas
- Mejoras del optimizador: Característica de seguimiento del optimizador
- Mejoras de InnoDB – Compatibilidad con DROP COLUMN instantánea y extensión `VARCHAR` instantánea para `ROW_FORMAT=DYNAMIC` y `ROW_FORMAT=COMPACT`
- Nuevos parámetros – Incluidos tcp_nodedelay, tls_version y gtid_cleanup_batch_size

Para ver una lista de todas las características de MariaDB 10.4 y de su documentación, consulte Changes & Improvements in MariaDB 10.4 y Release Notes - MariaDB 10.4 Series en el sitio web de MariaDB.

Para ver una lista de las características no admitidas, consulte Características de MariaDB que no admite Amazon RDS.

Motores de almacenamiento de MariaDB admitidos en Amazon RDS

RDS for MariaDB es compatible con los siguientes motores de almacenamiento.

Temas

- Motor de almacenamiento InnoDB
- Motor de almacenamiento MyRocks

Otros motores de almacenamiento no son compatibles actualmente con RDS for MariaDB.

Motor de almacenamiento InnoDB

Si bien MariaDB admite varios motores de almacenamiento con diversas capacidades, no todos están optimizados para la recuperación y la durabilidad de los datos. InnoDB es el motor de almacenamiento recomendado para las instancias de base de datos MariaDB en Amazon RDS.

Las características de Amazon RDS de recuperación a un momento dado y la restauración de instantáneas requieren un motor de almacenamiento que pueda recuperarse y solo son compatibles con el motor de almacenamiento recomendado para la versión de MariaDB.

Para obtener más información, consulte InnoDB.

Motor de almacenamiento MyRocks

El motor de almacenamiento MyRocks está disponible en la versión 10.6 de RDS for MariaDB y versiones posteriores. Antes de utilizar el motor de almacenamiento MyRocks en una base de datos de producción, recomendamos que realice análisis comparativos y pruebas exhaustivas para verificar cualquier beneficio potencial sobre InnoDB para su caso de uso.

El grupo de parámetros predeterminado para la versión 10.6 de MariaDB incluye parámetros de MyRocks. Para obtener más información, consulte Parámetros de MariaDB y Grupos de parámetros para Amazon RDS.

Para crear una tabla que utilice el motor de almacenamiento MyRocks, especifique `ENGINE=RocksDB` en la instrucción `CREATE TABLE`. En el siguiente ejemplo, se crea una tabla que utiliza el motor de almacenamiento MyRocks.

```
CREATE TABLE test (a INT NOT NULL, b CHAR(10)) ENGINE=RocksDB;
```

Se recomienda no ejecutar transacciones que abarquen las tablas InnoDB y MyRocks. MariaDB no garantiza ACID (atomicidad, consistencia, aislamiento, durabilidad) para transacciones entre motores de almacenamiento. Si bien es posible tener tablas InnoDB y MyRocks en una instancia de base de datos, no recomendamos este enfoque, excepto durante la migración de un motor de almacenamiento a otro. Cuando existen tablas InnoDB y MyRocks en una instancia de base de datos, cada motor de almacenamiento tiene su propio grupo de búferes, lo que podría provocar una degradación del rendimiento.

MyRocks no admite aislamiento `SERIALIZABLE` o bloqueos de espacio. Por lo tanto, en general, no puede utilizar MyRocks con replicación basada en instrucciones. Para obtener más información, consulte MyRocks y replicación.

En la actualidad, puede modificar solo los siguientes parámetros de MyRocks:

- `rocksdb_block_cache_size`
- `rocksdb_bulk_load`

- rocksdb_bulk_load_size
- rocksdb_deadlock_detect
- rocksdb_deadlock_detect_depth
- rocksdb_max_latest_deadlocks

El motor de almacenamiento MyRocks y el motor de almacenamiento InnoDB pueden competir por la memoria en función de la configuración de los parámetros `rocksdb_block_cache_size` y `innodb_buffer_pool_size`. En algunos casos, es posible que solo tenga la intención de utilizar el motor de almacenamiento MyRocks en una instancia de base de datos determinada. Si es así, recomendamos configurar el parámetro `innodb_buffer_pool_size minimal` en un valor mínimo y configurar el `rocksdb_block_cache_size` lo más alto posible.

Puede acceder a los archivos de registro de MyRocks mediante las operaciones `DescribeDBLogFiles` y `DownloadDBLogFilePortion`.

Para obtener más información sobre MyRocks, consulte MyRocks en el sitio web de MariaDB.

Calentamiento de caché para MariaDB en Amazon RDS

El calentamiento de caché de InnoDB puede proporcionar ganancias de rendimiento para la instancia de base de datos de MariaDB al guardar el estado actual del grupo del búfer cuando se cierra la instancia de base de datos y volver a cargar el grupo del búfer desde la información guardada cuando se inicia la instancia de base de datos. Este método elimina la necesidad de que el grupo del búfer "se caliente" con respecto al uso normal de la base de datos y, en su lugar, precarga el grupo del búfer con las páginas de las consultas frecuentes conocidas. Para obtener más información acerca del calentamiento de caché consulte Volcado y restauración del grupo de búferes en la documentación de MariaDB.

El calentamiento de caché se habilita de forma predeterminada en MariaDB 10.3 y en instancias de base de datos superiores. Para habilitarlo, establezca los parámetros `innodb_buffer_pool_dump_at_shutdown` e `innodb_buffer_pool_load_at_startup` en 1 en el grupo de parámetros de la instancia de base de datos. Cambiar los valores de estos parámetros en un grupo de parámetros afecta a todas las instancias de base de datos de MariaDB que utilicen ese grupo de parámetros. Para habilitar el calentamiento de caché para instancias de base de datos de MariaDB concretas, es posible que deba crear un nuevo grupo de parámetros para esas instancias de base de datos. Para obtener información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

El calentamiento de caché proporciona principalmente un beneficio de desempeño para las instancias de bases de datos que utilizan almacenamiento estándar. Si utiliza almacenamiento PIOPS, normalmente no se observa un beneficio de desempeño significativo.

Important

Si la instancia de base de datos MariaDB no se cierra de forma normal como, por ejemplo, durante una conmutación por error, el estado del grupo del búfer no se guarda en el disco. En este caso, MariaDB carga cualquier archivo de grupo del búfer que esté disponible cuando se reinicia la instancia de base de datos. No es perjudicial, pero el grupo del búfer restaurado podría no reflejar el estado más reciente del grupo del búfer antes del reinicio. Para asegurarse de que tiene un estado reciente del grupo del búfer disponible para calentar la caché de al iniciar, recomendamos que vuelque periódicamente el grupo del búfer "bajo demanda". Puede volcar o cargar el grupo del búfer bajo demanda.
Puede crear un evento para volcar el grupo del búfer automáticamente a intervalos regulares. Por ejemplo, la siguiente instrucción crea un evento denominado `periodic_buffer_pool_dump` que vuelca el grupo del búfer cada hora.

```
CREATE EVENT periodic_buffer_pool_dump
   ON SCHEDULE EVERY 1 HOUR
   DO CALL mysql.rds_innodb_buffer_pool_dump_now();
```

Para obtener más información, consulte Events en la documentación de MariaDB.

Volcado y carga del grupo del búfer bajo demanda

Puede guardar y cargar la caché de bajo demanda usando los siguientes procedimientos almacenados:

- Para volcar el estado actual del grupo del búfer en el disco, llame al procedimiento almacenado mysql.rds_innodb_buffer_pool_dump_now.
- Para cargar el estado guardado del grupo del búfer desde el disco, llame al procedimiento almacenado mysql.rds_innodb_buffer_pool_load_now.
- Para cancelar una operación de carga en curso, llame al procedimiento almacenado mysql.rds_innodb_buffer_pool_load_abort.

Características de MariaDB que no admite Amazon RDS

Las siguientes características de MariaDB no se admiten en Amazon RDS:

- Motor de almacenamiento S3
- Complemento de autenticación: GSSAPI
- Complemento de autenticación: conector Unix
- AWSComplemento de cifrado de Key Management
- Replicación retrasada para versiones de MariaDB anteriores a la versión 10.6
- Cifrado nativo de MariaDB en reposo para InnoDB y Aria

  Puede habilitar el cifrado en reposo para una instancia de base de datos de MariaDB siguiendo las instrucciones en Cifrado de recursos de Amazon RDS.
- HandlerSocket
- Tipo de tabla JSON para versiones de MariaDB anteriores a la versión 10.6
- ColumnStore de MariaDB
- Clúster Galera de MariaDB
- Replicación de varios orígenes
- Motor de almacenamiento MyRocks para versiones de MariaDB anteriores a la versión 10.6
- Complemento de validación de contraseñas, `simple_password_check` y `cracklib_password_check` para versiones de MariaDB inferiores a 11.4
- Motor de almacenamiento Spider
- Motor de almacenamiento Sphinx
- Motor de almacenamiento TokuDB
- Atributos de objetos específicos de motores de almacenamiento, como se describe en Engine-defined New Table/Field/Index Attributes en la documentación de MariaDB
- Cifrado de tabla y espacio de tabla
- Complemento Hashicorp Key Management
- Ejecución de dos actualizaciones en paralelo

Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Amazon RDS permite el acceso a las bases

de datos de una instancia de base de datos usando cualquier aplicación cliente de SQL estándar. Amazon RDS no permite el acceso de anfitrión directo a una instancia de base de datos a través de Telnet, Secure Shell (SSH) o conexión a escritorio remoto de Windows.

Versiones de MariaDB en Amazon RDS

En MariaDB, los números de la versión se organizan como versión X.Y.Z. En la terminología de Amazon RDS, X.Y denota la versión principal y Z es el número de la versión secundaria. Para implementaciones de Amazon RDS, un cambio de versión se considera principal si cambia el número de la versión principal: por ejemplo, si se pasa de la versión 10.5 a la 10.6. Un cambio de versión se considera secundario si solo cambia el número de la versión secundaria: por ejemplo, si se pasa de la versión 10.6.14 a la 10.6.16.

Temas

- Versiones secundarias de MariaDB compatibles en Amazon RDS
- Versiones principales de MariaDB compatibles en Amazon RDS
- Trabajo con el entorno de vista previa de bases de datos
- MariaDB versión 11.4 en el entorno de vista previa de bases de datos
- Versiones obsoletas para Amazon RDS para MariaDB

Versiones secundarias de MariaDB compatibles en Amazon RDS

Amazon RDS admite actualmente las siguientes versiones secundarias de MariaDB.

> **Note**
>
> Las fechas con solo un mes y un año son aproximadas y se actualizan con una fecha exacta cuando se conoce.

En la siguiente tabla se muestran las versiones secundarias de MariaDB 10.11 compatibles actualmente con Amazon RDS.

Versión del motor MariaDB	Fecha de versiones de la comunidad	Fecha de versión de RDS	Fecha de fin de soporte estándar de RDS
10.11.8	16 de mayo de 2024	14 de junio de 2024	Septiembre de 2025
10.11.7	7 de febrero de 2024	26 de febrero de 2024	Marzo de 2025

Versión del motor MariaDB	Fecha de versiones de la comunidad	Fecha de versión de RDS	Fecha de fin de soporte estándar de RDS
10.11.6	13 de noviembre de 2023	12 de diciembre de 2023	Marzo de 2025
10.11.5	14 de agosto de 2023	7 de septiembre de 2023	Marzo de 2025
10.11.4	7 de junio de 2023	21 de agosto de 2023	Marzo de 2025

En la siguiente tabla se muestran las versiones secundarias de MariaDB 10.6 compatibles actualmente con Amazon RDS.

Versión del motor MariaDB	Fecha de versiones de la comunidad	Fecha de versión de RDS	Fecha de fin de soporte estándar de RDS
10.6.18	16 de mayo de 2024	14 de junio de 2024	Septiembre de 2025
10.6.17	7 de febrero de 2024	26 de febrero de 2024	Marzo de 2025
10.6.16	13 de noviembre de 2023	12 de diciembre de 2023	Marzo de 2025
10.6.15	14 de agosto de 2023	7 de septiembre de 2023	Marzo de 2025
10.6.14	7 de junio de 2023	22 de junio de 2023	Marzo de 2025
10.6.13	10 de mayo de 2023	15 de junio de 2023	Marzo de 2025

En la siguiente tabla se muestran las versiones secundarias de MariaDB 10.5 compatibles actualmente con Amazon RDS.

Versión del motor MariaDB	Fecha de versiones de la comunidad	Fecha de versión de RDS	Fecha de fin de soporte estándar de RDS
10.5.25	16 de mayo de 2024	14 de junio de 2024	Septiembre de 2025
10.5.24	7 de febrero de 2024	26 de febrero de 2024	Marzo de 2025
10.5.23	13 de noviembre de 2023	12 de diciembre de 2023	Marzo de 2025
10.5.22	14 de agosto de 2023	7 de septiembre de 2023	Marzo de 2025
10.5.21	7 de junio de 2023	22 de junio de 2023	Marzo de 2025
10.5.20	10 de mayo de 2023	15 de junio de 2023	Marzo de 2025

En la siguiente tabla se muestran las versiones secundarias de MariaDB 10.4 compatibles actualmente con Amazon RDS.

Versión del motor MariaDB	Fecha de versiones de la comunidad	Fecha de versión de RDS	Fecha de fin de soporte estándar de RDS
10.4.34	16 de mayo de 2024	14 de junio de 2024	Febrero de 2025
10.4.33	7 de febrero de 2024	26 de febrero de 2024	Febrero de 2025
10.4.32	13 de noviembre de 2023	12 de diciembre de 2023	Febrero de 2025
10.4.31	14 de agosto de 2023	7 de septiembre de 2023	Febrero de 2025
10.4.30	7 de junio de 2023	22 de junio de 2023	Febrero de 2025
10.4.29	10 de mayo de 2023	15 de junio de 2023	Febrero de 2025

Puede especificar cualquier versión de MariaDB admitida actualmente al crear una nueva instancia de base de datos. Puede especificar la versión principal (como MariaDB 10.5) y versiones secundarias compatibles con la versión principal especificada. Si no se especifica ninguna versión, Amazon RDS cambia de forma predeterminada a una versión admitida, normalmente la más reciente. Si se especifica una versión principal pero no una versión secundaria, Amazon RDS usa de manera predeterminada una versión reciente de la versión principal especificada. Para ver una lista de las versiones admitidas, así como de las versiones predeterminadas para instancias de bases de datos recién creadas, utilice el comando `describe-db-engine-versions` de la AWS CLI.

Por ejemplo, para enumerar las versiones del motor compatibles con RDS para MariaDB, ejecute el siguiente comando de la CLI:

```
aws rds describe-db-engine-versions --engine mariadb --query "*[].
{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

La versión predeterminada de MariaDB puede variar según la Región de AWS. Para crear una instancia de base de datos con una versión secundaria concreta, especifique la versión secundaria durante la creación de la instancia de base de datos. Puede determinar la versión secundaria predeterminada de una Región de AWS mediante el siguiente comando de la:AWS CLI

```
aws rds describe-db-engine-versions --default-only --engine mariadb
 --engine-version major-engine-version --region region --query "*[].
{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

Reemplace *`major-engine-version`* por la versión principal del motor y reemplace *`region`* por la Región de AWS. Por ejemplo, el siguiente comando de la AWS CLI devuelve la versión secundaria predeterminada del motor de MariaDB para la versión principal 10.5 y la Región de AWS de Oeste de EE. UU. (Oregón) (us-west-2):

```
aws rds describe-db-engine-versions --default-only --engine mariadb --engine-version
 10.5 --region us-west-2 --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --
output text
```

Versiones principales de MariaDB compatibles en Amazon RDS

Las versiones principales de RDS para MariaDB permanecen disponibles al menos hasta el final de la vida útil de la comunidad para la versión de la comunidad correspondiente. Puede utilizar las siguientes fechas para planificar sus ciclos de prueba y actualización. Si Amazon amplía

la compatibilidad con una versión de RDS para MariaDB durante más tiempo de lo previsto originalmente, esta tabla se actualizará para reflejar la fecha posterior.

> **Note**
>
> Las fechas en las que solo aparece el mes y el año son aproximadas y se cambiarán por la fecha exacta cuando se conozca.

Versión principal de MariaDB	Fecha de versión de la comunidad	Fecha de versiones de RDS	Fecha de fin de vida útil de la comunidad	Fecha de fin de soporte estándar de RDS
MariaDB 10.11	16 de febrero de 2023	21 de agosto de 2023	16 de febrero de 2028	Febrero de 2028
MariaDB 10.6	6 de julio de 2021	3 de febrero de 2022	6 de julio de 2026	Julio de 2016
MariaDB 10.5	24 de junio de 2020	21 de enero de 2021	24 de junio de 2025	Junio de 2025
MariaDB 10.4	18 de junio de 2019	6 de abril de 2020	18 de junio de 2024	Febrero de 2025

Trabajo con el entorno de vista previa de bases de datos

Las instancias de base de datos de RDS para MariaDB en el entorno de vista previa de bases de datos son funcionalmente similares a otras instancias de bases de datos de RDS para MariaDB. Sin embargo, no puede usar el entorno de vista previa de bases de datos para las cargas de trabajo de producción.

Los entornos de vista previa presentan las siguientes limitaciones:

- Amazon RDS elimina todas las instancias de base de datos 60 días después de crearlas, junto con las copias de seguridad e instantáneas.
- Solo puede utilizar almacenamiento SSD de uso general y SSD IOPS provisionadas.

- No puede obtener ayuda de Soporte con instancias de bases de datos. En su lugar, puede publicar sus preguntas en la comunidad de preguntas y respuestas administrada de AWS, AWS re:Post.
- No puede copiar una instantánea de una instancia de base de datos en un entorno de producción.

Las siguientes opciones son compatibles con la vista previa.

- Puede crear instancias de base de datos con las clases de instancias de base de datos db.m6i, db.r6i, db.m6g, db.m5, db.t3, db.r6g y db.r5. Para obtener más información sobre las clases de instancias de RDS, consulte Clases de instancia de base de datos de .
- Puede utilizar implementaciones single-AZ y multi-AZ.
- Puede utilizar las funciones estándar de volcado y carga de MariaDB para importar bases de datos desde el entorno de la vista previa de base de datos o para exportarlas a este.

Características no compatibles en el entorno de vista previa de bases de datos

Las siguientes características no están disponibles en el entorno de vista previa de bases de datos:

- Copia de instantáneas entre regiones
- Réplicas de lectura entre regiones
- RDS Proxy

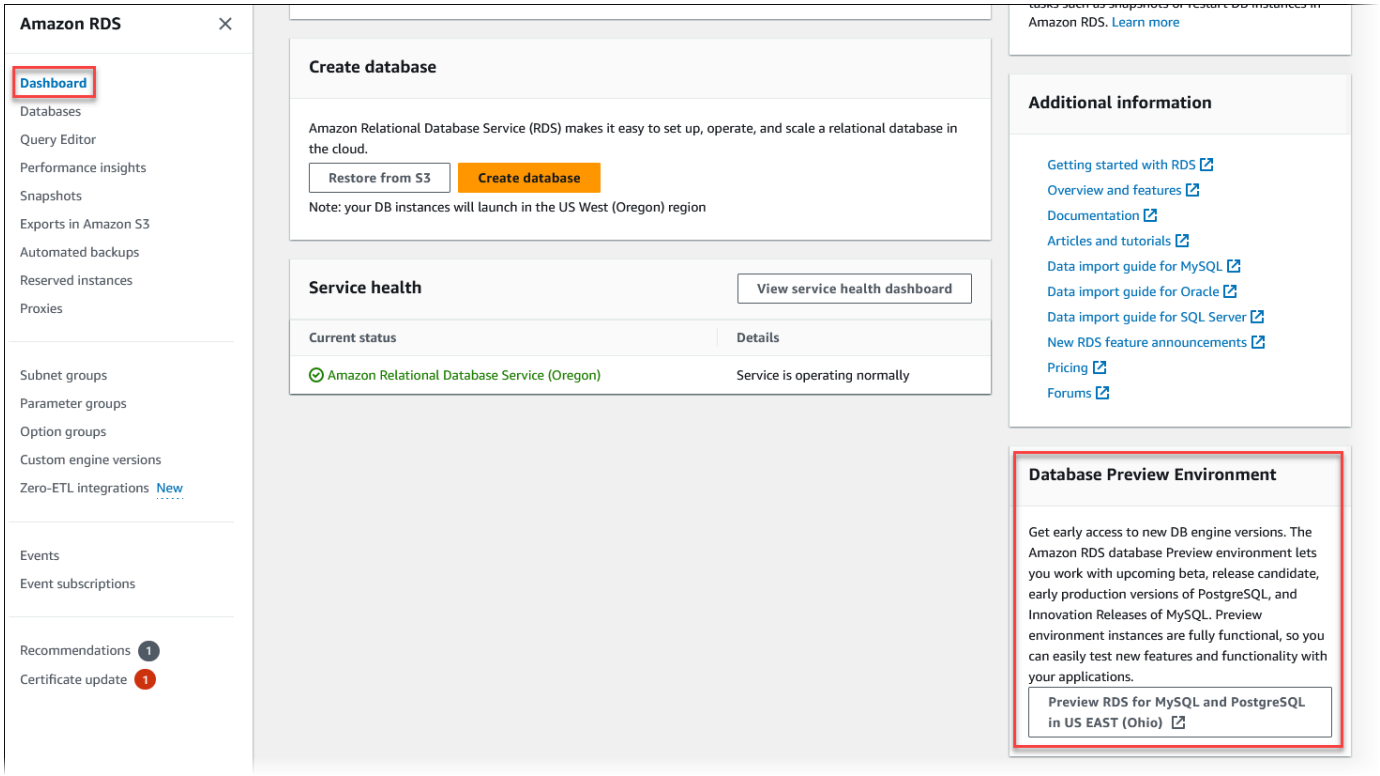
Creación de una nueva instancia de base de datos en el entorno de vista previa de bases de datos

Puede crear una instancia de base de datos en el entorno de vista previa de la base de datos utilizando AWS Management Console, AWS CLI o la API de RDS.

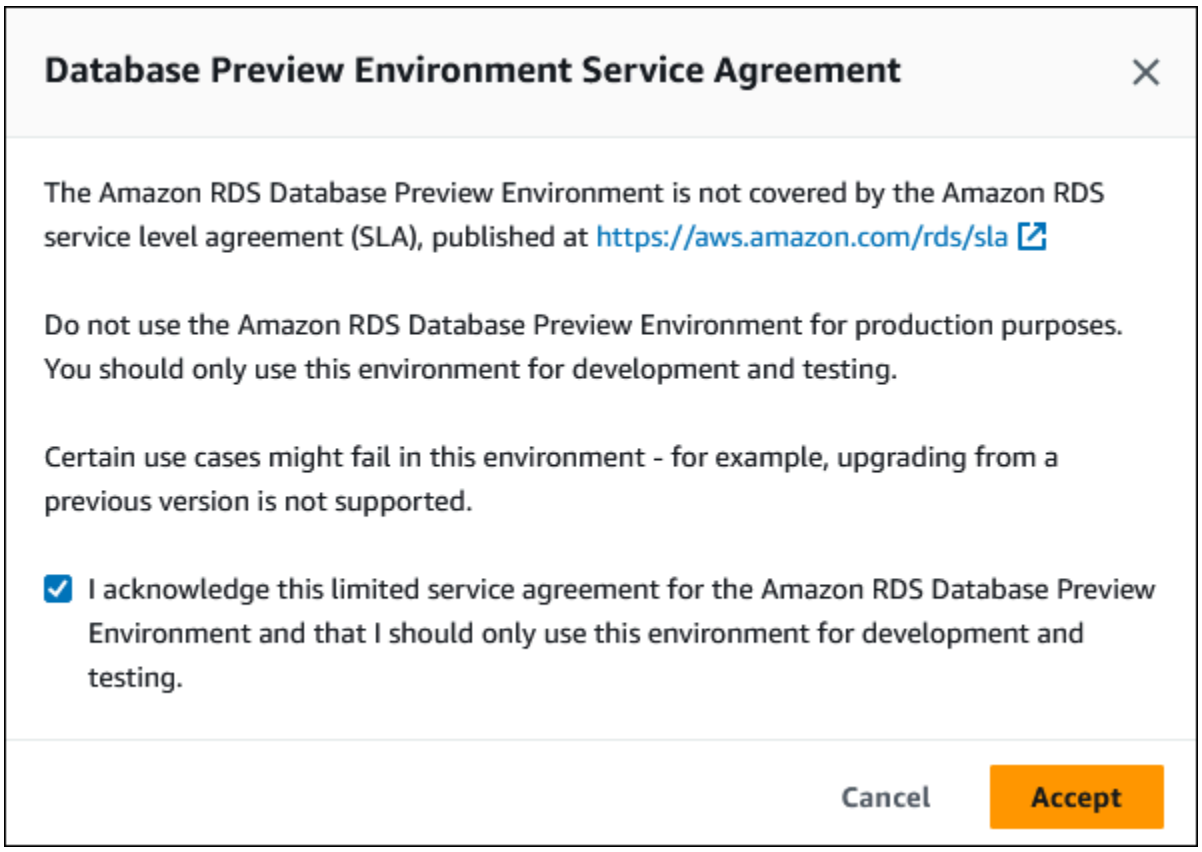
Consola

Para crear una instancia de base de datos en el entorno de vista previa de bases de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Dashboard (Panel) en el panel de navegación.
3. En la página Panel, busque la sección Database Preview Environment, tal y como se muestra en la siguiente imagen.



Puede navegar directamente a Database Preview Environment. Antes de continuar, debe reconocer y aceptar las limitaciones.



4. Para crear la instancia de base de datos de RDS para MariaDB, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento Consola en Creación de una instancia de base de datos.

AWS CLI

Para crear una instancia de base de datos en el entorno de vista previa de base de datos mediante la AWS CLI, utilice el siguiente punto de conexión.

```
rds-preview.us-east-2.amazonaws.com
```

Para crear la instancia de base de datos de RDS para MariaDB, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento AWS CLI en Creación de una instancia de base de datos.

API de RDS

Para crear una instancia de base de datos en el entorno de vista previa de base de datos mediante la API de RDS, utilice el siguiente punto de conexión.

```
rds-preview.us-east-2.amazonaws.com
```

Para crear la instancia de base de datos de RDS para MariaDB, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento API de RDS en Creación de una instancia de base de datos.

MariaDB versión 11.4 en el entorno de vista previa de bases de datos

MariaDB versión 11.4 ya está disponible en el entorno de vista previa de bases de datos de Amazon RDS. MariaDB versión 11.4 contiene varias mejoras que se describen en Changes and improvements in MariaDB 11.4. Puede usar el entorno de vista previa de bases de datos para probar sus cargas de trabajo con respecto a esta versión antes de que esté disponible en todas las Regiones de AWS para las cargas de trabajo de producción.

Para obtener información acerca del entorno de vista previa de base de datos, consulte the section called “El entorno de vista previa de bases de datos”. Para acceder al entorno de vista previa desde la consola, seleccione rds-preview/.

Versiones obsoletas para Amazon RDS para MariaDB

Las versiones 10.0, 10.1, 10.2 y 10.3 de Amazon RDS para MariaDB están obsoletas.

Para obtener información sobre la política de obsolescencia de Amazon RDS para MariaDB, consulte las preguntas frecuentes sobre Amazon RDS.

Conexión a la instancia de base de datos de MariaDB

Después de que Amazon RDS aprovisione una instancia de base de datos, puede usar cualquier utilidad o aplicación cliente estándar de MariaDB para conectarse a la instancia. En la cadena de conexión, especifique la dirección del sistema de nombre de dominio (DNS) del punto de enlace de la instancia de base de datos como el parámetro del host. Especifique también el número de puerto del punto de enlace de la instancia de base de datos como el parámetro del puerto.

Puede conectarse a una instancia de base de datos de Amazon RDS for MariaDB mediante herramientas como la utilidad de línea de comandos de MySQL. Para obtener más información acerca del uso de la utilidad de línea de comandos de MySQL, consulte mysql command-line client en la documentación de MariaDB. Heidi es una de las aplicaciones basadas en interfaz gráfica de usuario (GUI) que puede utilizar para conectarse. Para obtener más información, consulte la página Download HeidiSQL. Para obtener información sobre la instalación de MySQL (incluida la utilidad de línea de comandos de MySQL), consulte Installing and upgrading MySQL (Instalación y actualización de MySQL).

La mayoría de las distribuciones de Linux incluyen el cliente MariaDB en lugar del cliente Oracle MySQL. Para instalar el cliente de línea de comandos de MySQL en Amazon Linux 2023, ejecute el siguiente comando:

```
sudo dnf install mariadb105
```

Para instalar el cliente de línea de comandos de MySQL en Amazon Linux 2, ejecute el siguiente comando:

```
sudo yum install mariadb
```

Para instalar la utilidad de línea de comandos de MySQL en la mayoría de las distribuciones Linux basadas en DEB, ejecute el siguiente comando:

```
apt-get install mariadb-client
```

Para verificar la versión de la utilidad de línea de comandos de MySQL, ejecute el siguiente comando:

```
mysql --version
```

Para leer la documentación de MySQL de la versión actual del cliente, ejecute el siguiente comando:

```
man mysql
```

Para conectarse a una instancia de base de datos desde fuera de una nube virtual privada (VPC) basada en Amazon VPC, la instancia de base de datos debe ser accesible públicamente. Además, el acceso debe concederse mediante las reglas entrantes del grupo de seguridad de la instancia de base de datos y deben cumplirse otros requisitos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Puede utilizar el cifrado SSL en las conexiones a una instancia de base de datos de MariaDB. Para obtener información, consulte Compatibilidad con SSL/TLS para instancias de base de datos de MariaDB en Amazon RDS.

Para buscar una instancia de base de datos de RDS para MariaDB y conectarse a ella, consulte los siguientes temas.

Temas

- Búsqueda de la información de conexión para una instancia de base de datos de MariaDB
- Conexión desde el cliente de línea de comandos de MySQL (sin cifrar) de RDS para MariaDB
- Conexión a RDS para MariaDB con el controlador JDBC de AWS y el controlador Python de AWS;
- Solución de problemas de conexiones a la instancia de base de datos MariaDB

Búsqueda de la información de conexión para una instancia de base de datos de MariaDB

La información de conexión de una instancia de base de datos incluye su punto de enlace, puerto y un usuario de base de datos válido, como el usuario maestro. Por ejemplo, supongamos que un valor de punto de enlace es `mydb.123456789012.us-east-1.rds.amazonaws.com`. En este caso, el valor del puerto es `3306` y el usuario de la base de datos es `admin`. Dada esta información, se especifican los siguientes valores en una cadena de conexión:

- Para nombre de host o host o nombre DNS, especifique `mydb.123456789012.us-east-1.rds.amazonaws.com`.
- Para el puerto, especifique `3306`.
- Para el usuario, especifique `admin`.

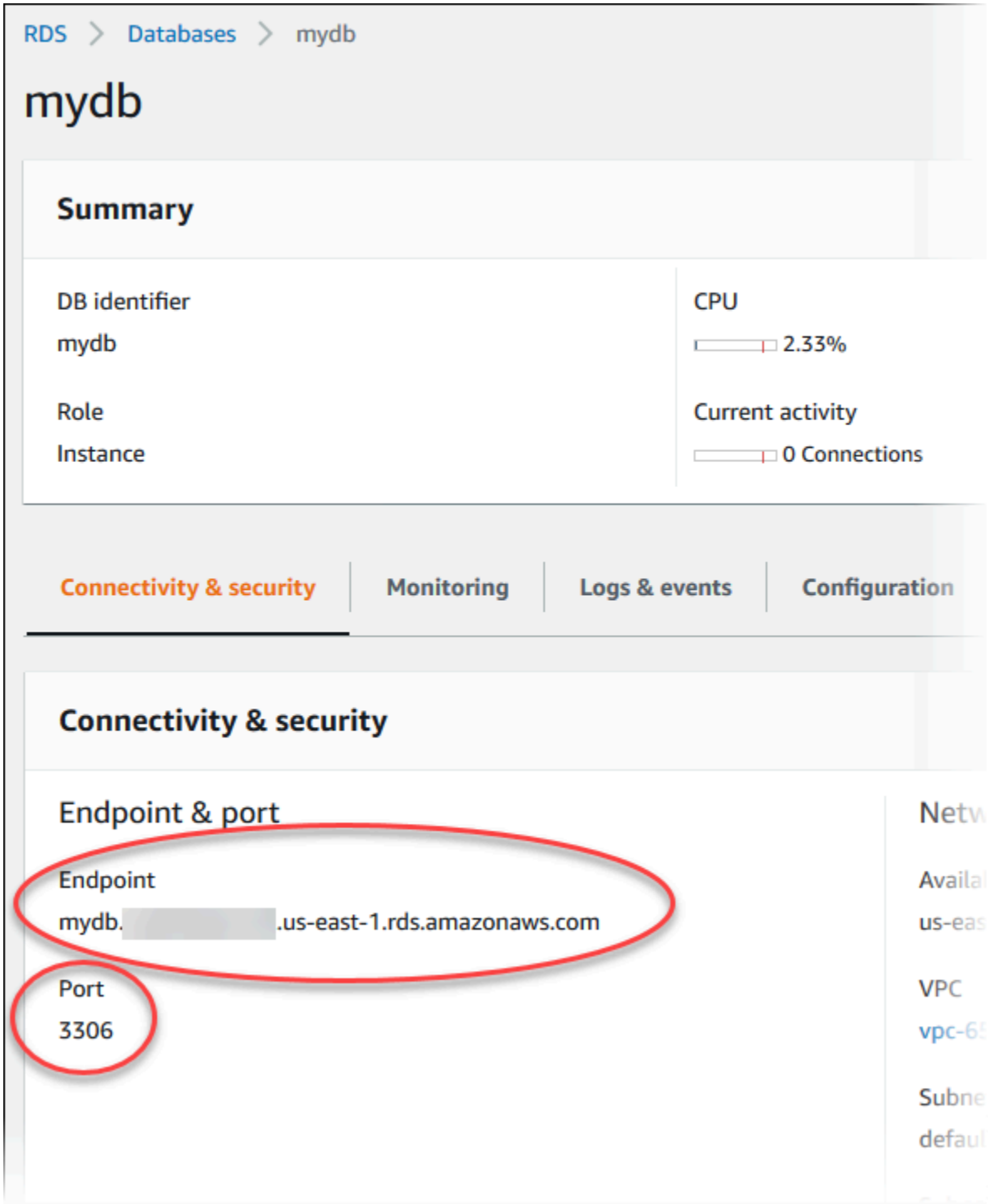
Para conectarse a una instancia de base de datos, utilice cualquier cliente para un motor de base de datos de MariaDB. Por ejemplo, puede usar la utilidad de línea de comandos de MySQL o MySQL Workbench.

Para buscar la información de conexión de una instancia de base de datos, puede utilizar la AWS Management Console, el comando de describe-db-instances de la AWS Command Line Interface (AWS CLI) o la operación de la API de Amazon RDS DescribeDBInstances para enumerar sus detalles.

Consola

Para buscar la información de conexión para una instancia de base de datos en AWS Management Console

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) para ver una lista de las instancias de base de datos.
3. Seleccione el nombre de la instancia de base de datos de MariaDB para mostrar sus detalles.
4. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



5. Si necesita encontrar el nombre de usuario maestro, elija la ficha Configuration (Configuración) y vea el valor de Master username (Nombre de usuario maestro) .

AWS CLI

Para encontrar la información de conexión para una instancia de base de datos MariaDB usando la AWS CLI, ejecute el comando describe-db-instances. En la llamada, consulte el ID de instancia de base de datos, el punto de enlace, el puerto y el nombre de usuario maestro.

Para Linux, macOS o Unix:

```
aws rds describe-db-instances \
  --filters "Name=engine,Values=mariadb" \
  --query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

Para Windows:

```
aws rds describe-db-instances ^
  --filters "Name=engine,Values=mariadb" ^
  --query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

El resultado debería ser similar al siguiente.

```
[
    [
        "mydb1",
        "mydb1.123456789012.us-east-1.rds.amazonaws.com",
        3306,
        "admin"
    ],
    [
        "mydb2",
        "mydb2.123456789012.us-east-1.rds.amazonaws.com",
        3306,
        "admin"
    ]
]
```

API de RDS

Para buscar la información de conexión de una instancia de base de datos mediante la API Amazon RDS, llame a la operación DescribedBInstances . En el resultado, busque los valores de la dirección del punto de enlace, el puerto del punto de enlace y el nombre de usuario maestro.

Conexión desde el cliente de línea de comandos de MySQL (sin cifrar) de RDS para MariaDB

> **Important**
>
> Utilice sólo una conexión MySQL sin cifrar cuando el cliente y el servidor están en la misma VPC y la red es de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte Conexión a la instancia de base de datos de MariaDB en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado).

Para conectarse a una instancia de base de datos mediante la utilidad de línea de comandos de MySQL, ingrese el siguiente comando en un símbolo del sistema en un equipo cliente. Al hacerlo, se conecta a una base de datos en una instancia de base de datos MariaDB. Sustituya el nombre DNS (punto de enlace) de la instancia de base de datos por *<endpoint>* y el nombre de usuario maestro que utilizó para *<mymasteruser>*. Proporcione la contraseña maestra que utilizó cuando se le solicite una contraseña.

```
mysql -h <endpoint> -P 3306 -u <mymasteruser> -p
```

Una vez especificada la contraseña del usuario, verá un resultado similar al siguiente.

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.10-MariaDB-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Conexión a RDS para MariaDB con el controlador JDBC de AWS y el controlador Python de AWS;

Conéctese a RDS para las instancias de base de datos de MariaDB con el controlador JDBC de AWS y el controlador Python de AWS. Para obtener más información, consulte los siguientes temas.

Temas

- Conexión a RDS para MariaDB con el controlador JDBC de Amazon Web Services (AWS)
- Conexión a RDS para MariaDB con el controlador de Python de Amazon Web Services (AWS)

Conexión a RDS para MariaDB con el controlador JDBC de Amazon Web Services (AWS)

El controlador JDBC de Amazon Web Services (AWS) se ha diseñado como un contenedor JDBC avanzado. Este contenedor complementa y amplía la funcionalidad del controlador JDBC existente. El controlador se admite con el controlador Connector/J de la comunidad MySQL y el controlador Connector/J de la comunidad MariaDB.

Para instalar el controlador JDBC de AWS, añada el archivo .jar del controlador JDBC de AWS (ubicado en la aplicación `CLASSPATH`) y conserve las referencias al controlador de la comunidad correspondiente. Actualice el prefijo de la URL de conexión correspondiente de la siguiente manera:

- De `jdbc:mysql://` a `jdbc:aws-wrapper:mysql://`
- De `jdbc:mariadb://` a `jdbc:aws-wrapper:mariadb://`

Para obtener más información sobre el controlador JDBC de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador JDBC de Amazon Web Services (AWS).

Conexión a RDS para MariaDB con el controlador de Python de Amazon Web Services (AWS)

El controlador de Python de Amazon Web Services (AWS) se ha diseñado como un contenedor de Python avanzado. Este contenedor complementa y amplía la funcionalidad del controlador de Psycopg de código abierto. El controlador de Python de AWS se admite con las versiones 3.8 y posteriores de Python. Puede instalar el paquete de `aws-advanced-python-wrapper` mediante el comando `pip`, junto con los paquetes de código abierto de `psycopg`.

Para obtener más información sobre el controlador de Python de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador de Python de Amazon Web Services (AWS).

Solución de problemas de conexiones a la instancia de base de datos MariaDB

Hay dos causas frecuentes de errores de conexión a una instancia de base de datos nueva:

- La instancia de base de datos se creó usando un grupo de seguridad que no autoriza las conexiones desde el dispositivo o la instancia Amazon EC2 en la que se está ejecutando la utilidad o la aplicación de MariaDB. La instancia de base de datos debe tener un grupo de seguridad de VPC que autorice las conexiones. Para obtener más información, consulte VPC de Amazon y Amazon RDS.

  Puede añadir o editar una regla de entrada en el grupo de seguridad. Para Source (Origen), elija My IP (Mi IP). Esto permite el acceso a la instancia de base de datos desde la dirección IP detectada en su navegador.
- La instancia de base de datos se creó con el puerto predeterminado 3306, y su compañía tiene reglas de firewall que bloquean las conexiones a ese puerto desde los dispositivos de la red de la organización. Para solucionar este error, vuelva a crear la instancia con un puerto diferente.

Para obtener más información sobre problemas de conexión, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Protección de las conexiones de instancias de base de datos MariaDB

Administre la seguridad de las instancias de base de datos MariaDB.

Temas

- Seguridad de MariaDB en Amazon RDS
- Uso de complementos de validación de contraseñas de RDS para MariaDB
- Cifrado de conexiones de cliente con SSL/TLS a instancias de base de datos de MariaDB en Amazon RDS
- Actualización de aplicaciones para la conexión a las instancias de MariaDB con los nuevos certificados SSL/TLS

Seguridad de MariaDB en Amazon RDS

La seguridad de las instancias de bases de datos de MariaDB se administra en tres niveles:

- AWS Identity and Access Management controla quién puede realizar acciones de administración de Amazon RDS en las instancias de base de datos. Cuando se conecta a AWS con credenciales de IAM, la cuenta de IAM debe tener políticas de IAM que concedan los permisos necesarios para realizar operaciones de administración de Amazon RDS. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.
- Al crear una instancia de base de datos, se usa un grupo de seguridad de VPC para controlar qué dispositivos e instancias de Amazon EC2 pueden abrir conexiones al punto de conexión y al puerto de la instancia de base de datos. Puede establecer estas conexiones de puerto y punto de enlace mediante la capa de sockets seguros (SSL) y la seguridad de la capa de transporte (TLS). Además, las reglas del firewall de su compañía pueden controlar si los dispositivos que se ejecutan en ella pueden abrir conexiones a la instancia de base de datos.
- Una vez que se ha abierto una conexión a una instancia de base de datos de MariaDB, la autenticación del inicio de sesión y los permisos se aplican de la misma forma que en una instancia independiente de MariaDB. Los comandos como `CREATE USER`, `RENAME USER`, `GRANT`, `REVOKE` y `SET PASSWORD` funcionan de la misma forma que en las bases de datos independientes, al igual que la modificación directa de las tablas de los esquemas de las bases de datos.

Cuando se crea una instancia de base de datos de Amazon RDS, el usuario maestro tiene los siguientes privilegios predeterminados:

- `alter`
- `alter routine`
- `create`
- `create routine`
- `create temporary tables`
- `create user`
- `create view`
- `delete`
- `drop`
- `event`
- `execute`
- `grant option`
- `index`
- `insert`
- `lock tables`
- `process`
- `references`
- `reload`

  Este privilegio está limitado en instancias de base de datos de MariaDB. No permite el acceso a las operaciones `FLUSH LOGS` o `FLUSH TABLES WITH READ LOCK`.
- `replication client`
- `replication slave`
- `select`
- `show create routine`

  Este privilegio solo está disponible en las instancias de base de datos MariaDB que ejecutan la versión 11.4 y versiones posteriores.

- `show databases`
- `show view`
- `trigger`
- `update`

Para obtener más información acerca de estos privilegios, consulte MariaDB User Account Management en la documentación de MariaDB.

> **Note**
>
> Aunque puede eliminar el usuario maestro en una instancia de base de datos, no es recomendable hacerlo. Para volver a crear el usuario maestro, utilice la `ModifyDBInstance` API o el `modify-db-instance` AWS CLI y especifique una nueva contraseña de usuario maestro con el parámetro adecuado. Si no existe el usuario maestro en la instancia, se crea con la contraseña especificada.

Para proporcionar servicios de administración para cada instancia de base de datos, se crea el usuario `rdsadmin` al crear la instancia de base de datos. Al intentar eliminar la cuenta `rdsadmin` o cambiar su nombre, su contraseña o sus privilegios, se producirá un error.

Para permitir la administración de la instancia de base de datos, los comandos estándar `kill` y `kill_query` se han restringido. Los comandos de Amazon RDS `mysql.rds_kill`, `mysql.rds_kill_query` y `mysql.rds_kill_query_id` se proporcionan para el uso en MariaDB y también en MySQL para que pueda finalizar las sesiones de usuario o las consultas en las instancias de base de datos.

Uso de complementos de validación de contraseñas de RDS para MariaDB

A partir de la versión 11.4 de RDS para MariaDB, puede utilizar los siguientes complementos de validación de contraseñas para mejorar la seguridad de las conexiones de su base de datos:

- simple_password_check: comprueba si una contraseña contiene al menos un número específico de caracteres de un tipo concreto.
- cracklib_password_check: comprueba si una contraseña aparece en un archivo de diccionario de la biblioteca CrackLib.

Para habilitar estos complementos, defina el valor del parámetro `simple_password_check` o `cracklib_password_check` en `FORCE_PLUS_PERMANENT` en el grupo de parámetros de base de datos asociado a la instancia de base de datos. Cuando se establece este valor, el complemento no se puede desinstalar mediante la declaración `UNINSTALL PLUGIN` en tiempo de ejecución.

Para deshabilitar estos complementos, establezca el valor del parámetro `simple_password_check` o `cracklib_password_check` en `OFF` en el grupo de parámetros de base de datos asociado a la instancia de base de datos. Cuando se establece este valor, las reglas de validación del complemento ya no se aplican a las contraseñas nuevas.

Para obtener información acerca de cómo establecer los valores de parámetros en grupos de parámetros, consulte the section called “Modificación de parámetros de un grupo de parámetros de base de datos”.

Cifrado de conexiones de cliente con SSL/TLS a instancias de base de datos de MariaDB en Amazon RDS

La capa de conexión segura (SSL) es un protocolo estándar del sector que se utiliza para proteger las conexiones de red entre el cliente y el servidor. Después de la versión 3.0 de SSL, el nombre se cambió por seguridad de la capa de transporte (TLS). Amazon RDS admite el cifrado SSL para las instancias de base de datos MariaDB. Con SSL/TLS puede cifrar una conexión entre el cliente de la aplicación y la instancia de base de datos MariaDB. La compatibilidad con SSL/TLS está disponible en todas las Regiones de AWS.

Con Amazon RDS, puede proteger los datos en tránsito cifrando las conexiones de los clientes a las instancias de base de datos de MariaDB con SSL/TLS, exigiendo el uso de SSL/TLS para todas las conexiones a una instancia de base de datos de MariaDB y conectándose desde el cliente de línea de comandos de MySQL con SSL/TLS (cifrado). En las siguientes secciones, se proporciona orientación sobre la configuración y el uso del cifrado SSL para las instancias de base de datos de MariaDB en Amazon RDS.

Temas

- Compatibilidad con SSL/TLS para instancias de base de datos de MariaDB en Amazon RDS
- Necesidad de uso de SSL/TLS para cuentas de usuario específicas en una instancia de base de datos de MariaDB en Amazon RDS
- Necesidad de uso de SSL/TLS para todas las conexiones a una instancia de base de datos de MariaDB en Amazon RDS

- Conexión a la instancia de base de datos de MariaDB en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado)

Compatibilidad con SSL/TLS para instancias de base de datos de MariaDB en Amazon RDS

Amazon RDS crea un certificado de SSL/TLS e instala el certificado en la instancia de base de datos cuando Amazon RDS aprovisiona la instancia. Estos certificados están firmados por una autoridad de certificación. El certificado SSL/TLS incluye el punto de enlace de la instancia de base de datos como nombre común (CN) que el certificado de SSL/TLS debe proteger frente a los ataques de suplantación.

Un certificado SSL/TLS creado por Amazon RDS es la entidad raíz de confianza y debería funcionar en la mayoría de los casos, pero podría fallar si la aplicación no acepta cadenas de certificados. Si la aplicación no acepta cadenas de certificados, intente utilizar un certificado intermedio para conectarse a la Región de AWS. Por ejemplo, debe utilizar un certificado intermedio para conectarse a las regiones de AWS GovCloud (US) con SSL/TLS.

Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener más información acerca de cómo usar SSL/TLS con MySQL, consulte Actualización de aplicaciones para la conexión a las instancias de MariaDB con los nuevos certificados SSL/TLS.

Amazon RDS para MariaDB es compatible con las versiones 1.3, 1.2, 1.1 y 1.0 de la seguridad de la capa de transporte (TLS). La compatibilidad con TLS depende de la versión secundaria de MariaDB. En la tabla siguiente se muestra la compatibilidad de TLS con versiones secundarias de MariaDB.

Versión de TLS	MariaDB 11.4	MariaDB 10.11	MariaDB 10.6	MariaDB 10.5	MariaDB 10.4
TLS 1.3	Todas las versiones secundarias	Todas las versiones secundarias	Todas las versiones secundarias	Todas las versiones secundarias	Todas las versiones secundarias
TLS 1.2	Todas las versiones secundarias	Todas las versiones secundarias	Todas las versiones secundarias	Todas las versiones secundarias	Todas las versiones secundarias

Versión de TLS	MariaDB 11.4	MariaDB 10.11	MariaDB 10.6	MariaDB 10.5	MariaDB 10.4
TLS 1.1	No compatible	10.11.6 y versiones anteriores	10.6.16 y versiones anteriores	10.5.23 y versiones anteriores	10.4.32 y versiones anteriores
TLS 1.0	No compatible	10.11.6 y versiones anteriores	10.6.16 y versiones anteriores	10.5.23 y versiones anteriores	10.4.32 y versiones anteriores

Necesidad de uso de SSL/TLS para cuentas de usuario específicas en una instancia de base de datos de MariaDB en Amazon RDS

Puede exigir el uso del cifrado SSL/TLS para determinadas conexiones de cuentas de usuario a las instancias de base de datos de MariaDB en Amazon RDS. Proteger la información confidencial del acceso o la interceptación no autorizados es fundamental para hacer cumplir las políticas de seguridad en los casos en los que la confidencialidad de los datos sea importante.

Para exigir el uso de conexiones SSL/TLS en determinadas cuentas de usuarios, utilice una de las siguientes instrucciones, en función de la versión de MySQL, para exigir conexiones SSL/TLS en la cuenta de usuario `encrypted_user`.

Para ello, utilice la siguiente instrucción.

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

Para obtener más información acerca de las conexiones SSL/TLS con MariaDB, consulte Securing Connections for Client and Server (Protección de conexiones para el cliente y el servidor) en la documentación de MariaDB.

Necesidad de uso de SSL/TLS para todas las conexiones a una instancia de base de datos de MariaDB en Amazon RDS

Utilice el parámetro `require_secure_transport` para requerir que todas las conexiones de usuario a su instancia de base de datos de MariaDB utilicen SSL/TLS. De forma predeterminada, el parámetro `require_secure_transport` está definido como `OFF`. Puede definir el parámetro

`require_secure_transport` en `ON` (activado) para imponer SSL/TLS para las conexiones a la instancia de base de datos.

> **Note**
>
> El parámetro `require_secure_transport` solo es compatible con las versiones 10.5 y posteriores de MariaDB.

Puede definir el valor del parámetro `require_secure_transport` actualizando el grupo de parámetros de base de datos a su instancia de base de datos. No es necesario reiniciar la instancia de base de datos para que el cambio surta efecto.

Cuando el parámetro `require_secure_transport` se establece en `ON` para un clúster de base de datos, un cliente de base de datos puede conectarse a él si puede establecer una conexión cifrada. De lo contrario, se devuelve al cliente un mensaje de error similar al siguiente:

```
ERROR 1045 (28000): Access denied for user 'USER'@'localhost' (using password: YES |
 NO)
```

Para obtener información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Para obtener más información sobre el parámetro `require_secure_transport`, consulte la documentación de MariaDB.

Conexión a la instancia de base de datos de MariaDB en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado)

Los parámetros `mysql` del programacliente son ligeramente diferentes si está utilizando la versión de MySQL 5.7, la versión de MySQL 8.0 o la versión de MariaDB.

Para saber qué versión tiene, ejecute el comando `mysql` con la opción de comando `--version`. En el ejemplo siguiente, el resultado muestra que el programa cliente es de MariaDB.

```
$ mysql --version
mysql  Ver 15.1 Distrib 10.5.15-MariaDB, for osx10.15 (x86_64) using readline 5.1
```

La mayoría de las distribuciones de Linux, como Amazon Linux, CentOS, SUSE y Debian han reemplazado MySQL por MariaDB, y la versión de `mysql` en ellos es de MariaDB.

Para conectarse a la instancia de base de datos mediante SSL/TLS, siga estos pasos:

Para conectarse a una instancia de base de datos mediante SSL/TLS con el cliente de la línea de comandos de MySQL

1. Descargue un certificado raíz que funcione para todas las Regiones de AWS.

   Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

2. Utilice un cliente de línea de comandos de MySQL para conectarse a una instancia de base de datos con cifrado SSL/TLS. Para el parámetro `-h`, escriba el nombre de DNS (punto de conexión) de la instancia de base de datos. Para el parámetro `--ssl-ca`, sustituya el nombre del archivo de certificado SSL/TLS. Para el parámetro `-P`, sustituya el puerto de la instancia de base de datos. Para el parámetro `-u`, sustituya el nombre de usuario de un usuario de base de datos válido, como el usuario maestro. Escriba la contraseña del usuario maestro cuando se le pida.

   En el siguiente ejemplo, se muestra cómo lanzar un cliente con el parámetro `--ssl-ca` con el MariaDB.

   ```
   mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-bundle.pem --ssl -P 3306 -u myadmin -p
   ```

   Para exigir que la conexión SSL/TLS verifique el punto de conexión de la instancia de la base de datos en el punto de conexión del certificado SSL/TLS, introduzca el siguiente comando:

   ```
   mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-bundle.pem --ssl-verify-server-cert -P 3306 -u myadmin -p
   ```

   En el siguiente ejemplo, se muestra cómo lanzar un cliente con el parámetro `--ssl-ca` con el cliente MySQL 5.7 y versiones posteriores.

   ```
   mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-bundle.pem --ssl-mode=REQUIRED -P 3306 -u myadmin -p
   ```

3. Escriba la contraseña del usuario maestro cuando se le pida.

Debería ver un resultado similar a este.

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.10-MariaDB-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Actualización de aplicaciones para la conexión a las instancias de MariaDB con los nuevos certificados SSL/TLS

El 13 de enero de 2023, Amazon RDS publicó nuevos certificados de entidades de certificación (CA) para la conexión a sus instancias de base de datos de RDS mediante la capa de sockets seguros o seguridad de la capa de transporte (SSL/TLS). Después, puede encontrar la información sobre la actualización de sus aplicaciones para utilizar los nuevos certificados.

Este tema puede ayudarle a determinar si sus aplicaciones precisan una verificación de certificados para conectarse a sus instancias de base de datos.

> **Note**
>
> Algunas aplicaciones solo están configuradas para conectarse a MariaDB solo si pueden verificar con éxito el certificado del servidor. Para esas aplicaciones, debe actualizar los almacenes de confianza de la aplicación de su cliente para incluir los nuevos certificados de CA.
>
> Puede especificar los siguientes modos SSL: `disabled`, `preferred` y `required`. Cuando utiliza el modo SSL `preferred` y el certificado de CA no existe o no está actualizado, la conexión vuelve a no utilizar SSL y se sigue conectando correctamente.
>
> Recomendamos evitar el modo `preferred`. En modo `preferred`, si la conexión encuentra un certificado no válido, deja de usar el cifrado y continúa sin cifrar.

Después actualizar sus certificados de CA en los almacenes de confianza de la aplicación de su cliente, puede rotar los certificados en sus instancias de base de datos. Recomendamos encarecidamente probar estos procedimientos en un entorno de desarrollo o ensayo antes de implementarlos en sus entornos de producción.

Para obtener más información acerca de la rotación de certificados, consulte Rotar certificados SSL/TLS. Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener información sobre el uso de SSL/TLS con las instancias de base de datos de MariaDB, consulte Compatibilidad con SSL/TLS para instancias de base de datos de MariaDB en Amazon RDS.

Temas

- Determinación de si un cliente necesita una verificación de certificados para conectarse
- Actualización del almacén de confianza de su aplicación
- Ejemplo de código Java para el establecimiento de conexiones SSL

Determinación de si un cliente necesita una verificación de certificados para conectarse

Puede comprobar si los cliente de JDBC y MySQL precisan la verificación de certificados para conectarse.

JDBC

El siguiente ejemplo con el conector de MySQL/J 8.0 muestra una manera de comprobar las propiedades de conexión de JDBC de una aplicación para determinar si las conexiones exitosas precisan un certificado válido. Para obtener más información sobre todas las opciones de conexión de JDBC para MySQL, consulte Propiedades de la configuración en la documentación de MySQL.

Al utilizar el conector de MySQL/J 8.0, una conexión precisa una verificación frente al certificado de CA del servidor si sus propiedades de conexión han configurado `sslMode` como `VERIFY_CA` o `VERIFY_IDENTITY`, como en el siguiente ejemplo.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

> **Note**
>
> Si utiliza MySQL Java Connector v5.1.38 o posterior, o MySQL Java Connector v8.0.9 o posterior para conectarse a sus bases de datos, incluso si no ha configurado explícitamente

sus aplicaciones para usar SSL/TLS al conectarse a sus bases de datos, estos controladores cliente utilizan de forma predeterminada SSL/TLS. Además, al utilizar SSL/TLS, realizan una verificación parcial del certificado y producen un error al conectarse si el certificado del servidor de base de datos ha caducado.
Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

MySQL

Los siguientes ejemplos con el cliente de MySQL muestran dos maneras de comprobar la conexión a MySQL de un script para determinar si las conexiones exitosas precisan un certificado válido. Para obtener más información sobre todas las opciones de conexión con el cliente de MySQL, consulte Configuración del lado del cliente para las conexiones cifradas en la documentación de MySQL.

Al utilizar el cliente de MySQL 5.7 o 8.0, una conexión SSL precisa una verificación frente al certificado de CA del servidor si para la opción de `--ssl-mode` especifica `VERIFY_CA` o `VERIFY_IDENTITY`, como en el siguiente ejemplo.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem
 --ssl-mode=VERIFY_CA
```

Al utilizar el cliente de MySQL 5.6, una conexión SSL precisa una verificación frente al certificado de CA del servidor si especifica la opción `--ssl-verify-server-cert`, como en el siguiente ejemplo.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem
 --ssl-verify-server-cert
```

Actualización del almacén de confianza de su aplicación

Para obtener más información acerca de la actualización del almacén de confianza para las aplicaciones de MySQL, consulte Uso de TLS/SSL con MariaDB Connector/J en la documentación de MariaDB.

Para obtener información sobre la descarga del certificado raíz, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Para obtener secuencias de comandos de ejemplo que importan certificados, consulte Script de muestra para la importación de certificados en su almacén de confianza.

> **Note**
>
> Cuando actualice el almacén de confianza, puede retener certificados antiguos además de añadir los nuevos certificados.

Si utiliza el controlador de MariaDB Connector/J JDBC en una aplicación, establezca las siguientes propiedades en la aplicación.

```
System.setProperty("javax.net.ssl.trustStore", certs);
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

Cuando inicie la aplicación, establezca las siguientes propiedades.

```
java -Djavax.net.ssl.trustStore=/path_to_truststore/MyTruststore.jks -
Djavax.net.ssl.trustStorePassword=my_truststore_password com.companyName.MyApplication
```

> **Note**
>
> Especifique contraseñas distintas de las que se muestran aquí como práctica recomendada de seguridad.

Ejemplo de código Java para el establecimiento de conexiones SSL

El siguiente ejemplo de código muestra cómo configurar la conexión SSL mediante JDBC.

```
private static final String DB_USER = "admin";

        private static final String DB_USER = "user name";
        private static final String DB_PASSWORD = "password";
        // This key store has only the prod root ca.
        private static final String KEY_STORE_FILE_PATH = "file-path-to-keystore";
        private static final String KEY_STORE_PASS = "keystore-password";

    public static void main(String[] args) throws Exception {
        Class.forName("org.mariadb.jdbc.Driver");

        System.setProperty("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
        System.setProperty("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);

        Properties properties = new Properties();
        properties.put("user", DB_USER);
        properties.put("password", DB_PASSWORD);


        Connection connection = DriverManager.getConnection("jdbc:mysql://ssl-mariadb-
public.cni62e2e7kwh.us-east-1.rds.amazonaws.com:3306?useSSL=true",properties);
        Statement stmt=connection.createStatement();

        ResultSet rs=stmt.executeQuery("SELECT 1 from dual");

        return;
    }
```

Important

Después de que haya determinado que sus conexiones de base de datos utilizan SSL/TLS y haya actualizado el almacén de confianza de su aplicación, puede actualizar su base de datos para que utilice los certificados de rds-ca-rsa2048-g1. Para obtener instrucciones, consulte el paso 3 en Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos.

Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Mejora del rendimiento de las consultas de RDS para MariaDB con lecturas optimizadas de Amazon RDS

Puede procesar las consultas más rápido para RDS para MariaDB con lecturas optimizadas de Amazon RDS. Una instancia de base de datos de RDS para Maria que utilice lecturas optimizadas de RDS puede procesar las consultas hasta dos veces más rápido en comparación con una instancia de base de datos que no la usa.

Temas

- Información general de las lecturas optimizadas de RDS
- Casos de uso de lecturas optimizadas para RDS
- Prácticas recomendadas para lecturas optimizadas de RDS
- Uso de lecturas optimizadas de RDS
- Supervisión de instancias de base de datos que utilizan lecturas optimizadas de RDS
- Limitaciones de las lecturas optimizadas de RDS

Información general de las lecturas optimizadas de RDS

Cuando utiliza una instancia de base de datos de RDS para MariaDB que tiene activadas las lecturas optimizadas de RDS, la instancia de base de datos realiza las consultas más rápido mediante el uso de un almacén de instancias. El almacén de instancias ofrece un almacenamiento de nivel de bloques temporal para la instancia de base de datos. El almacenamiento se encuentra en unidades de estado sólido (SSD) de memoria rápida no volátil (NVMe) que están conectadas físicamente al servidor host. Este almacenamiento está optimizado para una latencia baja, un rendimiento de E/S aleatorio alto y un alto rendimiento de lectura secuencial.

Las lecturas optimizadas de RDS se activan de forma predeterminada cuando una instancia de base de datos usa una clase de instancia de base de datos con un almacén de instancias, como db.m5d o db.m6gd. Con las lecturas optimizadas de RDS, algunos objetos temporales se almacenan en el almacén de instancias. Estos objetos temporales incluyen archivos temporales internos, tablas temporales internas en disco, archivos de mapas de memoria y archivos de caché de registros binarios (binlog). Para obtener más información sobre el almacén de instancias, consulte Almacén de instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para las instancias de Linux.

Las cargas de trabajo que generan objetos temporales en MariaDB para el procesamiento de consultas pueden aprovechar el almacén de instancias para procesar las consultas más rápido. Este tipo de carga de trabajo incluye consultas que implican ordenaciones, agregaciones de hash, uniones de alta carga, expresiones de tablas comunes (CTE) y consultas en columnas no indexadas. Estos volúmenes de almacenes de instancias proporcionan mayores IOPS y rendimiento, independientemente de las configuraciones de almacenamiento utilizadas para el almacenamiento persistente de Amazon EBS. Dado que RDS Optimized Reads descarga las operaciones de los objetos temporales al almacén de instancias, ahora las operaciones de entrada/salida por segundo (IOPS) o el rendimiento del almacenamiento persistente (Amazon EBS) se pueden utilizar para operaciones en objetos persistentes. Estas operaciones incluyen las lecturas y escrituras habituales de archivos de datos y las operaciones del motor en segundo plano, como vaciar e insertar combinaciones de búferes.

> **Note**
>
> Tanto las instantáneas de RDS manuales como las automatizadas solo contienen archivos de motor para objetos persistentes. Los objetos temporales creados en el almacén de instancias no se incluyen en las instantáneas de RDS.

Casos de uso de lecturas optimizadas para RDS

Si tiene cargas de trabajo que dependen en gran medida de objetos temporales, como tablas o archivos internos, para ejecutar consultas, puede beneficiarse de activar las lecturas optimizadas de RDS. Los siguientes casos de uso son candidatos a las lecturas optimizadas para RDS:

- Aplicaciones que ejecutan consultas analíticas con expresiones de tablas comunes (CTE) complejas, tablas derivadas y operaciones de agrupamiento
- Réplicas de lectura que atienden un tráfico de lectura intenso con consultas no optimizadas
- Aplicaciones que ejecutan consultas de generación de informes dinámicas o bajo demanda que implican operaciones complejas, como consultas con cláusulas `GROUP BY` y `ORDER BY`.
- Cargas de trabajo que utilizan tablas temporales internas para el procesamiento de consultas

  Puede supervisar la variable de estado del motor `created_tmp_disk_tables` para determinar el número de tablas temporales basadas en discos que se han creado en la instancia de base de datos.

- Aplicaciones que crean tablas temporales de gran tamaño, ya sea directamente o en procedimientos, para almacenar resultados intermedios
- Consultas de bases de datos que agrupan u ordenan columnas no indexadas

Prácticas recomendadas para lecturas optimizadas de RDS

Utilice estas prácticas recomendadas para utilizar lecturas optimizadas de RDS:

- Añada una lógica de reintento para las consultas de solo lectura en caso de que fallen debido a que el almacén de instancias está lleno durante la ejecución.
- Supervise el espacio de almacenamiento disponible en el almacén de instancias con la métrica de CloudWatch `FreeLocalStorage`. Si el almacén de instancias alcanza su límite debido a la carga de trabajo de la instancia de base de datos, modifíquela para usar una clase de instancia de base de datos más grande.
- Cuando la instancia de base de datos tenga memoria suficiente pero siga alcanzando el límite de almacenamiento del almacén de instancias, aumente el valor `binlog_cache_size` para mantener en la memoria las entradas del binlog específicas de la sesión. Esta configuración impide escribir las entradas de binlog en los archivos temporales de caché de binlog en el disco.

  El parámetro `binlog_cache_size` es específico de la sesión. Puede cambiar el valor para cada nueva sesión. La configuración de este parámetro puede aumentar la utilización de memoria en la instancia de base de datos durante los picos de carga de trabajo. Por lo tanto, considere aumentar el valor del parámetro en función del patrón de carga de trabajo de la aplicación y de la memoria disponible en la instancia de base de datos.
- Utilice el valor predeterminado de `MIXED` para el `binlog_format`. Según el tamaño de las transacciones, si se establece `binlog_format` en `ROW` se pueden generar archivos de caché binlog de gran tamaño en el almacén de instancias.
- Evite realizar cambios masivos en una sola transacción. Estos tipos de transacciones pueden generar archivos de caché binlog de gran tamaño en el almacén de instancias y pueden causar problemas cuando el almacén de instancias está lleno. Considere la posibilidad de dividir las escrituras en varias transacciones pequeñas para minimizar el uso de almacenamiento de los archivos de caché binlog.

Uso de lecturas optimizadas de RDS

Al aprovisionar una instancia de base de datos de RDS para MariaDB con una de las siguientes clases de instancia de base de datos en una implementación de instancia de base de datos Single-AZ o Multi-AZ, la instancia de base de datos utiliza automáticamente lecturas optimizadas de RDS.

Para activar las lecturas optimizadas de RDS, realice una de las siguientes acciones:

- Cree una instancia de base de datos de RDS para MariaDB utilizando una de estas clases de instancia de base de datos. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de RDS para MariaDB para utilizar una de estas clases de instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Las lecturas optimizadas de RDS están disponibles en todas las Regiones de AWS donde se admite una o más de las clases de instancia de base de datos con almacenamiento SSD NVMe local. Para obtener información acerca de las clases de instancia de base de datos, consulte the section called “Clases de instancia de base de datos”.

La disponibilidad de las clases de instancia de base de datos es diferente en las Regiones de AWS. Para determinar si una clase de instancia de base de datos se admite en una Región de AWS específica, consulte the section called “Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS”.

Si no desea utilizar lecturas optimizadas de RDS, modifique la instancia de base de datos para que no utilice una clase de instancia de base de datos que admita la característica.

Supervisión de instancias de base de datos que utilizan lecturas optimizadas de RDS

Puede supervisar las instancias de base de datos que utilizan lecturas optimizadas de RDS con las siguientes métricas de CloudWatch:

- `FreeLocalStorage`
- `ReadIOPSLocalStorage`
- `ReadLatencyLocalStorage`

- `ReadThroughputLocalStorage`
- `WriteIOPSLocalStorage`
- `WriteLatencyLocalStorage`
- `WriteThroughputLocalStorage`

Estas métricas proporcionan datos sobre el almacén de instancias disponible, las IOPS y el rendimiento. Para obtener más información sobre estas métricas, consulte Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS.

Limitaciones de las lecturas optimizadas de RDS

Las limitaciones siguientes se aplican a las lecturas optimizadas de RDS:

- Las lecturas optimizadas de RDS son compatibles con las siguientes versiones de RDS para MariaDB:
  - Versión 10.11.4 y versiones posteriores a la 10.11
  - Versión 10.6.7 y versiones posteriores a la 10.6
  - Versión 10.5.16 y versiones posteriores a la 10.5
  - Versión 10.4.25 y versiones posteriores a la 10.4

  Para obtener más información acerca de las versiones de RDS para MariaDB, consulte Versiones de MariaDB en Amazon RDS.
- No puede cambiar la ubicación de los objetos temporales al almacenamiento persistente (Amazon EBS) en las clases de instancias de base de datos que admiten lecturas optimizadas de RDS.
- Cuando se habilita el registro binario en una instancia de base de datos, el tamaño máximo de transacción está limitado por el tamaño del almacén de instancias. En MariaDB, cualquier sesión que requiera más almacenamiento que el valor de `binlog_cache_size` escribe los cambios de transacciones en archivos de caché binlog temporales, que se crean en el almacén de instancias.
- Las transacciones pueden fallar cuando el almacén de instancias está lleno.

Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB

Puede mejorar el rendimiento de las transacciones de escritura con Escrituras optimizadas para RDS para MariaDB. Cuando su base de datos de RDS para MariaDB utiliza escrituras optimizadas para RDS, puede lograr un rendimiento de transacciones de escritura hasta dos veces mayor.

Temas

- Información general de las escrituras optimizadas de RDS
- Uso de escrituras optimizadas de RDS
- Habilitar las escrituras optimizadas para RDS en una base de datos existente
- Limitaciones de las escrituras optimizadas de RDS

Información general de las escrituras optimizadas de RDS

Al activar las Escrituras optimizadas para RDS, las bases de datos de RDS para MariaDB escriben solo una vez cuando vacían los datos en un almacenamiento duradero sin necesidad de utilizar un búfer de escritura doble. Las bases de datos siguen protegiendo las propiedades de ACID para realizar transacciones de bases de datos fiables, además de mejorar el rendimiento.

Las bases de datos relacionales, como MariaDB, proporcionan las propiedades ACID de atomicidad, consistencia, aislamiento y durabilidad para transacciones de bases de datos fiables. Para ayudar a proporcionar estas propiedades, MariaDB utiliza un área de almacenamiento de datos denominada búfer de escritura doble que evita errores de escritura parcial de páginas. Estos errores se producen cuando se produce un error de hardware mientras la base de datos actualiza una página, como en el caso de un corte de luz. Una base de datos MariaDB puede detectar escrituras parciales de páginas y recuperarlas con una copia de la página en el búfer de escritura doble. Si bien esta técnica proporciona protección, también produce operaciones de escritura adicionales. Para obtener más información sobre el búfer de escritura doble de MariaDB, consulte Doublewrite Buffer (Búfer de escritura doble) en la documentación de MariaDB.

Con las escrituras optimizadas para RDS activadas, las bases de datos de RDS para MariaDB escriben solo una vez cuando vacían los datos en un almacenamiento duradero sin utilizar el búfer de escritura doble. Las escrituras optimizadas para RDS son útiles si ejecuta cargas de trabajo con muchas escrituras en sus bases de datos de RDS para MariaDB. Entre los ejemplos de bases de

datos con cargas de trabajo que requieren muchas escrituras, se incluyen las que admiten pagos digitales, operaciones financieras y aplicaciones de juegos.

Estas bases de datos se ejecutan en clases de instancias de base de datos que utilizan el sistema AWS Nitro. Gracias a la configuración del hardware de estos sistemas, la base de datos puede escribir páginas de 16 KiB directamente en archivos de datos de forma fiable y duradera en un solo paso. El sistema AWS Nitro permite las escrituras optimizadas de RDS.

Puede configurar el nuevo parámetro de base de datos `rds.optimized_writes` para controlar la característica de escrituras optimizadas para RDS para bases de datos RDS para MariaDB. Acceda a este parámetro en los grupos de parámetros de base de datos de RDS para MariaDB para las siguientes versiones:

- Versión 11.4.3 y versiones posteriores a la 11.4
- Versión 10.11.4 y versiones posteriores a la 10.11
- Versión 10.6.10 y versiones posteriores a la 10.6

Establezca el parámetro con uno de los siguientes valores:

- `AUTO`: activa las escrituras optimizadas de RDS si la base de datos las admite. Desactiva las escrituras optimizadas de RDS si la base de datos no las admite. Esta configuración es la predeterminada.
- `OFF`: desactiva las escrituras optimizadas de RDS aunque la base de datos las admita.

Si migra una base de datos de RDS para MariaDB que está configurada para utilizar escrituras optimizadas para RDS en una clase de instancia de base de datos que no admite esta característica, RDS desactiva automáticamente las escrituras optimizadas para RDS para la base de datos.

Cuando las escrituras optimizadas para RDS están desactivadas, la base de datos utiliza el búfer de escritura doble de MariaDB.

Para determinar si una base de datos de RDS para MariaDB utiliza escrituras optimizadas para RDS, consulte el valor actual del parámetro `innodb_doublewrite` de la base de datos. Si la base de datos utiliza escrituras optimizadas de RDS, este parámetro se establece en `FALSE` (`0`).

Uso de escrituras optimizadas de RDS

Puede activar las escrituras optimizadas para RDS al crear una base de datos RDS para MariaDB con la consola de RDS, la AWS CLI o la API de RDS. Las escrituras optimizadas de RDS se activan automáticamente cuando se cumplen las dos condiciones siguientes durante la creación de la base de datos:

- Debe especificar una clase de instancia de base de datos y una versión de motor de base de datos que admitan escrituras optimizadas de RDS.
  - Las escrituras optimizadas de RDS son compatibles con las siguientes versiones de RDS para MariaDB:
    - Versión 11.4.3 y versiones posteriores a la 11.4
    - Versión 10.11.4 y versiones posteriores a la 10.11
    - Versión 10.6.10 y versiones posteriores a la 10.6

    Para obtener más información acerca de las versiones de RDS para MariaDB, consulte Versiones de MariaDB en Amazon RDS.
  - Las bases de datos RDS para MariaDB que utilizan las siguientes clases de instancias de base de datos son compatibles con las escrituras optimizadas para RDS:
    - db.m7i
    - db.m7g
    - db.m6g
    - db.m6gd
    - db.m6i
    - db.m5
    - db.m5d
    - db.r7i
    - db.r7g
    - db.r6g
    - db.r6gd
    - db.r6i
    - db.r5
    - db.r5b

- db.r5d
- db.x2idn
- db.x2iedn

  Para obtener información acerca de las clases de instancia de base de datos, consulte the section called “Clases de instancia de base de datos”.

  La disponibilidad de las clases de instancia de base de datos es diferente en las Regiones de AWS. Para determinar si una clase de instancia de base de datos se admite en una Región de AWS específica, consulte the section called “Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS”.

- En el grupo de parámetros asociado a la base de datos, el parámetro `rds.optimized_writes` se establece en `AUTO`. En los grupos de parámetros predeterminados, este parámetro siempre se establece en `AUTO`.

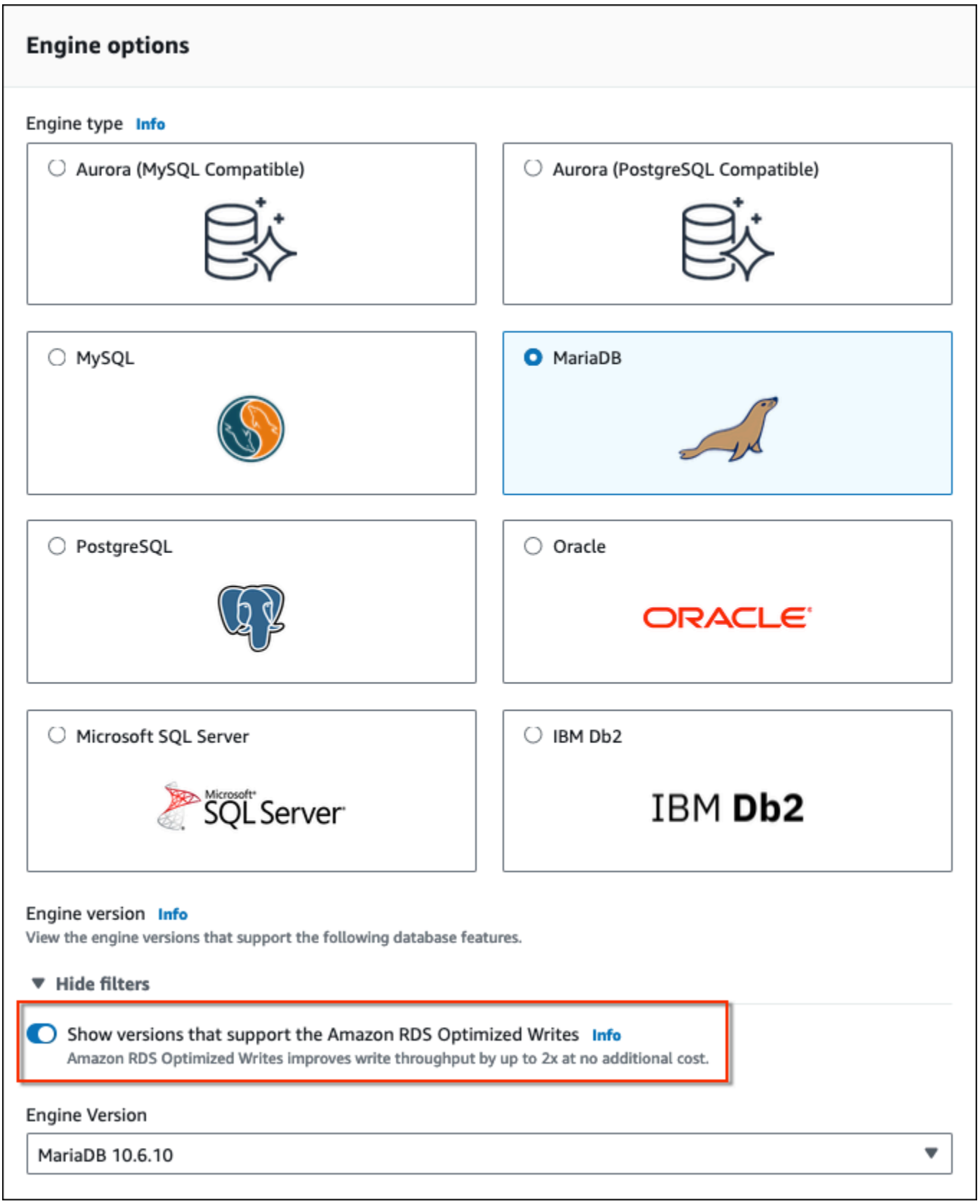
Si desea utilizar una versión del motor de base de datos y una clase de instancia de base de datos que admita las escrituras optimizadas para RDS, pero no quiere utilizar esta característica, especifique un grupo de parámetros personalizado al crear la base de datos. En este grupo de parámetros, defina el parámetro `rds.optimized_writes` en `OFF`. Si desea que la base de datos utilice las escrituras optimizadas de RDS más adelante, puede configurar el parámetro `AUTO` para activarla. Para obtener información sobre cómo trabajar con grupos de parámetros personalizados y establecer parámetros, consulte Grupos de parámetros para Amazon RDS.

Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

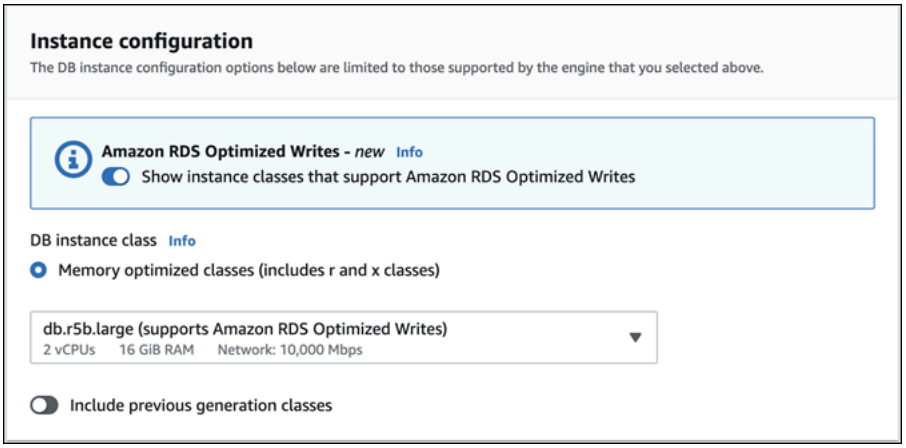
Consola

Al utilizar la consola de RDS para crear una base de datos RDS para MariaDB, puede filtrar las versiones del motor de base de datos y las clases de instancia de base de datos que admiten las escrituras optimizadas para RDS. Tras activar los filtros, puede elegir entre las clases de instancia de base de datos y las versiones del motor de base de datos disponibles.

Para elegir una versión del motor de base de datos que admita escrituras optimizadas para RDS, filtre las versiones del motor de base de datos RDS para MariaDB que la admitan en Versión del motor y, a continuación, elija una versión.


Engine options
Engine type Info
Aurora (MySQL Compatible)
Aurora (PostgreSQL Compatible)
MySQL
MariaDB
PostgreSQL
Oracle
ORACLE
Microsoft SQL Server
Microsoft SQL Server
IBM Db2
IBM Db2
Engine version Info
View the engine versions that support the following database features.
Hide filters
Show versions that support the Amazon RDS Optimized Writes Info
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.
Engine Version
MariaDB 10.6.10

En la sección Instance configuration (Configuración de instancias), filtre las clases de instancias de base de datos que admiten escrituras optimizadas de RDS y, a continuación, elija una clase de instancia de base de datos.



Tras realizar estas selecciones, puede elegir otras configuraciones que cumplan sus requisitos y terminar de crear la base de datos RDS para MariaDB con la consola.

AWS CLI

Para crear una instancia de base de datos con la AWS CLI, utilice el comando create-db-instance. Asegúrese de que los valores `--engine-version` y `--db-instance-class` admitan escrituras optimizadas de RDS. Además, asegúrese de que el grupo de parámetros asociado a la instancia de base de datos tiene el parámetro `rds.optimized_writes` configurado en AUTO. En este ejemplo, se asocia el grupo de parámetros predeterminado con la instancia de base de datos.

Example Creación de una instancia de base de datos que utilice escrituras optimizadas de RDS

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --engine mariadb \
    --engine-version 10.6.10 \
    --db-instance-class db.r5b.large \
    --manage-master-user-password \
    --master-username admin \
    --allocated-storage 200
```

Para Windows:

```
aws rds create-db-instance ^
```

```
    --db-instance-identifier mydbinstance ^
    --engine mariadb ^
    --engine-version 10.6.10 ^
    --db-instance-class db.r5b.large ^
    --manage-master-user-password ^
    --master-username admin ^
    --allocated-storage 200
```

API de RDS

Puede crear una instancia de base de datos mediante la operación CreateDBInstance. Cuando realice esta operación, asegúrese de que los valores `EngineVersion` y `DBInstanceClass` admitan escrituras optimizadas de RDS. Además, asegúrese de que el grupo de parámetros asociado a la instancia de base de datos tiene el parámetro `rds.optimized_writes` configurado en `AUTO`.

Habilitar las escrituras optimizadas para RDS en una base de datos existente

A fin de modificar una base de datos RDS para MariaDB existente y activar las escrituras optimizadas para RDS, la base de datos debe haberse creado con una versión de motor de base de datos y una clase de instancia de base de datos compatibles. Además, la base de datos debe haberse creado después del lanzamiento de las escrituras optimizadas para RDS el 7 de marzo de 2023, ya que la configuración del sistema de archivos subyacente requerida es incompatible con la de las bases de datos creadas antes de su publicación. Si se cumplen estas condiciones, puede activar las escrituras optimizadas para RDS poniendo el parámetro `rds.optimized_writes` en `AUTO`.

Si la base de datos no se creó con una versión de motor, una clase de instancia o una configuración de sistema de archivos compatibles, puede usar las implementaciones azul/verde de RDS para migrar a una configuración compatible. Al crear la implementación azul/verde, haga lo siguiente:

- Seleccione Habilitar escrituras optimizadas en base de datos verde y especifique una versión del motor y una clase de instancia de base de datos que admitan escrituras optimizadas de RDS. Para ver una lista de las versiones de motor y las clases de instancias compatibles, consulte the section called “Uso con una base de datos nueva”.
- En Almacenamiento, seleccione Actualizar la configuración del sistema de archivos de almacenamiento. Esta opción actualiza la base de datos a una configuración de sistema de archivos subyacente compatible.

Al crear la implementación azul/verde, si el parámetro `rds.optimized_writes` se ha configurado en `AUTO`, las escrituras optimizadas de RDS se habilitarán automáticamente en el entorno verde. A continuación, puede conmutar la implementación azul/verde para que el entorno verde sea el nuevo entorno de producción.

Para obtener más información, consulte the section called “Creación de una implementación azul/verde”.

Limitaciones de las escrituras optimizadas de RDS

Al restaurar una base de datos de RDS para MariaDB a partir de una instantánea, solo puede activar las escrituras optimizadas para RDS para la base de datos si se cumplen todas las condiciones siguientes:

- La instantánea se creó a partir de una base de datos que admite escrituras optimizadas de RDS.
- La instantánea se ha creado a partir de una base de datos que se creó después del lanzamiento de las escrituras optimizadas para RDS.
- La instantánea se restaura en una base de datos que admite escrituras optimizadas de RDS.
- La base de datos restaurada está asociada a un grupo de parámetros que tiene el parámetro `rds.optimized_writes` establecido en `AUTO`.

Actualizaciones del motor de base de datos de MariaDB

Cuando Amazon RDS admita una nueva versión de un motor de base de datos, podrá actualizar sus instancias de base de datos a la nueva versión. Hay dos tipos de actualizaciones para las instancias de base de datos de MariaDB: actualizaciones de versiones principales y actualizaciones de versiones secundarias.

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de las aplicaciones. Por lo tanto, debe realizar manualmente las actualizaciones de versiones principales de sus instancias de base de datos. Puede iniciar una actualización de versión principal modificando su instancia de base de datos. Sin embargo, antes de realizar una actualización de versión principal, recomendamos que siga las instrucciones descritas en Actualizaciones de versiones principales de RDS para MariaDB.

Por su parte, las actualizaciones de versiones secundarias solo incluyen cambios compatibles con las versiones anteriores de las aplicaciones. Puede iniciar manualmente una actualización de versiones secundarias modificando su instancia de base de datos. O puede habilitar la opción Auto minor version upgrade (Actualización automática de versiones secundarias) al crear o modificar una instancia de base de datos. Si lo hace, su instancia de base de datos se actualizará automáticamente después de que Amazon RDS pruebe y apruebe la nueva versión. Para obtener información sobre cómo realizar una actualización, consulte Actualización de una versión del motor de una instancia de base de datos.

Si la instancia de base de datos de MariaDB usa las réplicas de lectura, debe actualizar todas las réplicas de lectura antes de actualizar la instancia de origen. Si la instancia de base de datos está en una implementación Multi-AZ, se actualizan las réplicas en espera y de escritor. Es posible que su instancia de base de datos no esté disponible hasta que se complete la actualización.

Para obtener más información acerca de las versiones de MariaDB compatibles y la administración de las versiones, consulte Versiones de MariaDB en Amazon RDS.

Las actualizaciones del motor de base de datos requieren tiempo de inactividad El tiempo que dura la interrupción varía según el tamaño de la instancia de base de datos.

> **Tip**
>
> Puede minimizar el tiempo de inactividad necesario para la actualización de la instancia de base de datos mediante una implementación azul/verde. Para obtener más información,

consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Temas

- Aspectos a tener en cuenta sobre las actualizaciones de MariaDB
- Búsqueda de objetivos de actualización válidos
- Números de versión de MariaDB
- Números de versión de RDS en RDS para MariaDB
- Actualizaciones de versiones principales de RDS para MariaDB
- Actualización de una instancia de base de datos MariaDB
- Actualizaciones de versiones secundarias automáticas de RDS para MariaDB
- Uso de una réplica de lectura para reducir el tiempo de inactividad al actualizar una base de datos de RDS para MariaDB

Aspectos a tener en cuenta sobre las actualizaciones de MariaDB

Amazon RDS toma dos o más instantáneas de la base de datos durante el proceso de actualización. Amazon RDS toma hasta dos instantáneas de la instancia de base de datos antes de realizar cualquier cambio en la actualización. Si la actualización de las bases de datos no funciona, puede restaurar una de estas instantáneas para crear una instancia de base de datos que ejecute la versión antigua. Amazon RDS toma otra instantánea de la instancia de base de datos cuando se completa la actualización. Amazon RDS toma estas instantáneas independientemente de si AWS Backup administra las copias de seguridad de la instancia de base de datos.

Note

Amazon RDS solo realiza instantáneas de base de datos si ha definido el periodo de retención de copia de seguridad de su instancia de base de datos en un número mayor que 0. Para cambiar el periodo de retención de copia de seguridad, consulte Modificación de una instancia de base de datos de Amazon RDS.

Después de completar la actualización, no puede volver a la versión anterior del motor de base de datos. Si desea volver a la versión anterior, restaure la primera instantánea de base de datos que se realizó para crear una nueva instancia de base de datos.

Puede controlar cuándo debe actualizar la instancia de base de datos a una nueva versión admitida por Amazon RDS. Este nivel de control le ayuda a mantener la compatibilidad con versiones de base de datos específicas y probar nuevas versiones con una aplicación antes de implementarlas en producción. Cuando esté listo, podrá efectuar actualizaciones de versiones en el momento que le resulte más conveniente.

Si la instancia de base de datos de usa la replicación de lectura, debe actualizar todas las réplicas de lectura antes de actualizar la instancia de origen.

Si la instancia de base de datos se encuentra en un despliegue Multi-AZ, se actualizan la instancia de base de datos principal y la instancia en espera. Las instancias de base de datos principal y en espera se actualizan al mismo tiempo y se produce una interrupción hasta que finaliza la actualización. El tiempo que dura la interrupción varía según el motor de base de datos, la versión del motor y el tamaño de la instancia de base de datos.

Búsqueda de objetivos de actualización válidos

Cuando se utiliza la AWS Management Console para actualizar una instancia de base de datos, muestra los destinos de actualización válidos para la instancia de base de datos. También puede utilizar el siguiente comando de la AWS CLI para identificar los destinos de actualización válidos para una instancia de base de datos:

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
  --engine mariadb \
  --engine-version version_number \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
  --engine mariadb ^
  --engine-version version_number ^
```

```
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Por ejemplo, para identificar los destinos de actualización válidos para una instancia de base de datos de MariaDB versión 10.5.17, ejecute el siguiente comando de la AWS CLI:

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
  --engine mariadb \
  --engine-version 10.5.17 \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
  --engine mariadb ^
  --engine-version 10.5.17 ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Números de versión de MariaDB

La secuencia de numeración de las versiones del motor de la base de datos RDS para MariaDB tiene el formato principal.secundaria.parche.aaaammdd o principal.secundaria.parche (por ejemplo, 10.11.5.R2.20231201 o 10.4.30). El formato utilizado depende de la versión del motor de MariaDB.

principal

El número de versión principal es tanto el entero como la primera parte fraccional del número de versión (por ejemplo, 10.11). Una actualización de versión principal aumenta la parte principal del número de versión. Por ejemplo, una actualización de 10.5.20 a 10.6.12 es una actualización de versión principal, donde 10.5 y 10.6 son los números de la versión principal.

secundaria.

El número de versión secundaria es la tercera parte del número de versión (por ejemplo, el 5 en 10.11.5).

parche

El parche es la cuarta parte del número de versión (por ejemplo, el R2 en 10.11.5.R2). Una versión de parche de RDS incluye correcciones de errores importantes que se agregan a una versión secundaria después de su lanzamiento.

AAAAMMDD

La fecha es la quinta parte del número de versión (por ejemplo, 20231201 en 10.11.5.R2.20231201). Una versión de fecha de RDS es un parche de seguridad que incluye correcciones de seguridad importantes que se agregan a una versión secundaria después de su lanzamiento. No incluye ninguna corrección que pueda cambiar el comportamiento de un motor.

La siguiente tabla explica el esquema de nomenclatura de RDS para MariaDB versión 10.11.

Versión secundaria 10.11	Esquema de nomenclatura
≥5	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 10.11.5.R2.20231201). Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 10.11.5.R2) hasta la próxima actualización de la versión principal o secundaria.
< 5	Las instancias de base de datos existentes utilizan el formato principal.secundaria.parche (por ejemplo, 10.11.4.R2).

La siguiente tabla explica el esquema de nomenclatura de RDS para MariaDB versión 10.6.

Versión secundaria 10.6	Esquema de nomenclatura
≥ 14	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 10.6.14.R2.20231201).

Versión secundaria 10.6	Esquema de nomenclatura
	Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 10.6.14.R2) hasta la próxima actualización de la versión principal o secundaria.
< 14	Las instancias de base de datos existentes utilizan el formato principal.secundaria.parche (por ejemplo, 10.6.13.R2).

La siguiente tabla explica el esquema de nomenclatura de RDS para MariaDB versión 10.5.

Versión secundaria 10.5	Esquema de nomenclatura
≥ 21	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 10.5.21.R2.20231201). Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 10.5.21.R2) hasta la próxima actualización de la versión principal o secundaria.
< 21	Las instancias de base de datos existentes utilizan el formato principal.secundaria.parche (por ejemplo, 10.5.20.R2).

La siguiente tabla explica el esquema de nomenclatura de RDS para MariaDB versión 10.4.

Versión secundaria 10.4	Esquema de nomenclatura
≥ 30	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 10.4.30.R2.20231201). Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 10.4.30.R

Versión secundaria 10.4	Esquema de nomenclatura
	2) hasta la próxima actualización de la versión principal o secundaria.
< 30	Las instancias de base de datos existentes utilizan el formato principal.secundaria.parche (por ejemplo, 10.4.29.R2).

Números de versión de RDS en RDS para MariaDB

Los números de versión de RDS utilizan el esquema de nomenclatura *major*.*minor*.*patch* o *major*.*minor*.*patch*.*YYYYMMDD*. Una versión de parche de RDS incluye correcciones de errores importantes que se agregan a una versión secundaria después de su lanzamiento. Una versión de fecha de RDS (*AAMMDD*) es un parche de seguridad. Un parche de seguridad no incluye ninguna corrección que pueda cambiar el comportamiento de un motor.

Para identificar el número de versión de Amazon RDS de la base de datos, primero debe crear la extensión `rds_tools` mediante el siguiente comando:

```
CREATE EXTENSION rds_tools;
```

Puede averiguar el número de versión de RDS de su base de datos de RDS para MariaDB con la siguiente consulta SQL:

```
mysql> select mysql.rds_version();
```

Por ejemplo, la consulta de una base de datos de RDS para MariaDB 10.6.14 muestra lo siguiente:

```
+---------------------+
| mysql.rds_version() |
+---------------------+
| 10.6.14.R2.20231201  |
+---------------------+
1 row in set (0.01 sec)
```

Actualizaciones de versiones principales de RDS para MariaDB

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de las aplicaciones. En consecuencia, Amazon

RDS no aplica automáticamente actualizaciones de versión principal. Debe modificar manualmente su instancia de base de datos. Recomendamos que pruebe exhaustivamente cualquier actualización antes de aplicarla a las instancias de producción.

Amazon RDS es compatible con las siguientes actualizaciones locales para versiones principales del motor de base de datos de MariaDB:

- Cualquier versión de MariaDB hasta MariaDB 11.4
- Cualquier versión de MariaDB hasta MariaDB 10.11
- Cualquier versión de MariaDB hasta MariaDB 10.6
- MariaDB 10.4 a MariaDB 10.5

Si desea usar un grupo de parámetros personalizado y realiza una actualización de versión principal, debe especificar un grupo de parámetros predeterminado para la nueva versión del motor de base de datos o crear su grupo de parámetros personalizado para la nueva versión del motor de base de datos. Para asociar el nuevo grupo de parámetros con la instancia de base de datos se requiere un reinicio de la base de datos iniciado por el cliente una vez que se haya completado la actualización. El estado del grupo de parámetros de la instancia mostrará `pending-reboot` si la instancia se tiene que reiniciar para aplicar los cambios del grupo de parámetros. El estado del grupo de parámetros de una instancia se puede visualizar en la AWS Management Console o ejecutando una llamada "describe", como `describe-db-instances`.

Actualización de una instancia de base de datos MariaDB

Para obtener más información acerca de la actualización automática o manual de una instancia de base de datos MariaDB, consulte Actualización de una versión del motor de una instancia de base de datos.

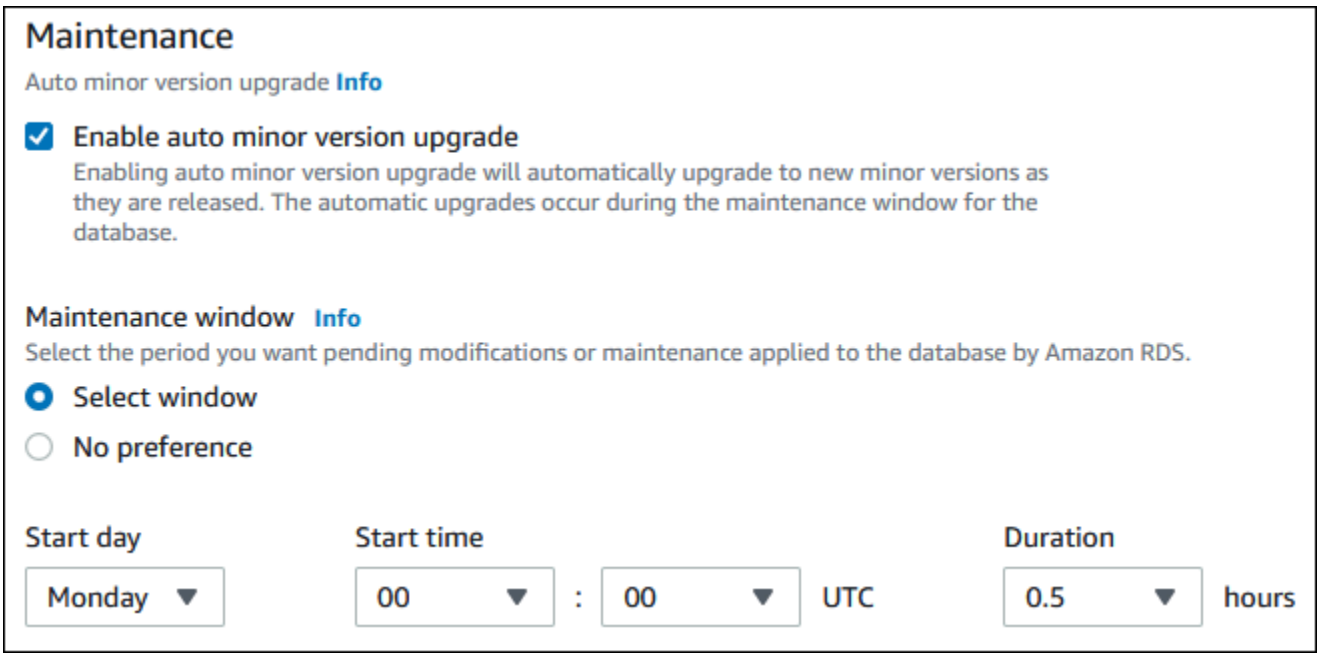
Actualizaciones de versiones secundarias automáticas de RDS para MariaDB

Si especifica la siguiente configuración al crear o modificar una instancia de base de datos, puede actualizar automáticamente la instancia de base de datos.

- La opción Auto minor version upgrade (Actualización automática de versión secundaria) está habilitada.

- La configuración del Backup retention period (periodo de retención de copia de seguridad) es mayor que 0.

En la AWS Management Console, esta configuración se encuentra en Additional configuration (Configuración adicional). En la siguiente imagen se muestra la configuración Auto minor version upgrade (Actualización automática de versiones secundarias).



Para obtener más información sobre estas opciones, consulte Configuración de instancias de base de datos.

Para algunas versiones principales de RDS para MariaDB en algunas Regiones de AWS, RDS designa una versión secundaria como versión de actualización automática. Después de que Amazon RDS pruebe y apruebe una versión secundaria, la actualización de versión secundaria se produce automáticamente durante el periodo de mantenimiento. RDS no configura automáticamente versiones secundarias publicadas recientemente como la versión de actualización automática. Antes de que RDS asigne una versión de actualización automática más reciente, deben considerarse algunos criterios, como, por ejemplo, los que se indican a continuación:

- Problemas de seguridad conocidos
- Errores en la versión de la comunidad de MariaDB
- Estabilidad general de la flota desde que se publicó la versión secundaria

> **Note**
>
> Se ha eliminado la compatibilidad con las versiones 1.0 y 1.1 de TLS a partir de versiones secundarias específicas de MariaDB. Para obtener información acerca de la compatibilidad de las versiones secundarias de MariaDB, consulte the section called “Compatibilidad con SSL/TLS para MariaDB”.

Puede utilizar el siguiente comando de la AWS CLI para determinar la versión actual de destino de actualización secundaria automática para una versión secundaria de MariaDB especificada en una Región de AWS específica.

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine mariadb \
--engine-version minor_version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine mariadb ^
--engine-version minor_version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

Por ejemplo, el siguiente comando de la AWS CLI determina el destino de actualización secundario automático para la versión secundaria 10.5.16 de MariaDB en la Región de AWS de Este de EE. UU. (Ohio) (us-east-2).

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine mariadb \
--engine-version 10.5.16 \
```

```
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine mariadb ^
--engine-version 10.5.16 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Su resultado es similar al siguiente.

```
-----------------------------------
|    DescribeDBEngineVersions    |
+--------------+-----------------+
|  AutoUpgrade |  EngineVersion  |
+--------------+-----------------+
|  True        |  10.5.17        |
|  False       |  10.5.18        |
|  False       |  10.5.19        |
|  False       |  10.6.5         |
|  False       |  10.6.7         |
|  False       |  10.6.8         |
|  False       |  10.6.10        |
|  False       |  10.6.11        |
|  False       |  10.6.12        |
+--------------+-----------------+
```

En este ejemplo, el valor `AutoUpgrade` es `True` para MariaDB versión 10.5.17. Por lo tanto, el objetivo de actualización secundaria automática es MariaDB versión 10.5.17., que está resaltado en el resultado.

Una instancia de base de datos de MariaDB se actualiza automáticamente durante el periodo de mantenimiento si se cumplen los siguientes criterios:

- La opción Auto minor version upgrade (Actualización automática de versión secundaria) está habilitada.

- La configuración del Backup retention period (periodo de retención de copia de seguridad) es mayor que 0.
- La instancia de base de datos se ejecuta en una versión secundaria de motor de base de datos que es anterior a la versión secundaria de actualización automática actual.

Para obtener más información, consulte Actualización automática de la versión secundaria del motor.

Uso de una réplica de lectura para reducir el tiempo de inactividad al actualizar una base de datos de RDS para MariaDB

En la mayoría de los casos, una implementación azul/verde es la mejor opción para reducir el tiempo de inactividad al actualizar una instancia de base de datos MariaDB. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Si no puede usar una implementación azul/verde y en la actualidad se está utilizando su instancia de base de datos de MariaDB con una aplicación de producción, puede utilizar el siguiente procedimiento para actualizar la versión de base de datos de la instancia de base de datos. Este procedimiento puede reducir la duración del tiempo de inactividad de la aplicación.

Al utilizar una réplica de lectura, puede realizar la mayoría de los pasos de mantenimiento con anticipación y minimizar los cambios necesarios durante la interrupción real. Con esta técnica, puede probar y preparar la nueva instancia de base de datos sin realizar ningún cambio en su instancia de base de datos existente.

El siguiente procedimiento muestra un ejemplo de actualización de la versión 10.5 de MariaDB a la 10.6. Puede usar los mismos pasos generales para actualizaciones a otras versiones principales.

Para actualizar una base de datos MariaDB mientras se está utilizando una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Cree una réplica de lectura para la instancia de base de datos de MariaDB 10.5. Este proceso permite crear una copia actualizable de su base de datos. También pueden existir otras réplicas de lectura de la instancia de base de datos.

a. En la consola, elija Databases (Bases de datos) y, después, seleccione la instancia de base de datos que desea actualizar.

b. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).

c. Proporcione un valor de DB instance identifier (Identificador de instancias de bases de datos) para su réplica de lectura y asegúrese de que el valor de DB instance class (Clase de instancia de base de datos) y otros ajustes coinciden con su instancia de base de datos de MariaDB 10.5.

d. Elija Create read replica (Crear réplica de lectura).

3. (Opcional) Cuando se ha creado la réplica de lectura y Status (Estado) se muestra como Available (Disponible), convierta la réplica de lectura en una implementación Multi-AZ y habilite las copias de seguridad.

   De forma predeterminada, una réplica de lectura se crea como una implementación Single-AZ con copias de seguridad deshabilitadas. Dado que la réplica de lectura se convierte en la instancia de base de datos de producción, es una práctica recomendada configurar una implementación Multi-AZ y habilitar ahora las copias de seguridad.

   a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de crear.

   b. Elija Modify.

   c. Para Multi-AZ deployment (Implementación Multi-AZ), elija Create a standby instance (Crear una instancia en espera).

   d. En Backup Retention Period (Periodo de retención de copia de seguridad), elija un valor positivo distinto de cero, por ejemplo, 3 días y, después, elija Continue (Continuar).

   e. En Programación de modificaciones, elija Aplicar inmediatamente.

   f. Elija Modificar la instancia de base de datos.

4. Cuando el Status (Estado) de la réplica de lectura se muestra como Available (Disponible), actualice la réplica de lectura a MariaDB 10.6.

   a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de crear.

   b. Elija Modify.

   c. En DB engine version (Versión del motor de base de datos), elija la versión de MariaDB 10.6. a la que se realizará la actualización y, luego, elija Continue (Continuar).

d. En Programación de modificaciones, elija Aplicar inmediatamente.

e. Elija Modify DB instance (Modificar instancia de base de datos) para comenzar la actualización.

5. Cuando haya finalizado la actualización y el Status (Estado) se muestre como Available (Disponible), verifique que la réplica de lectura actualizada esté al día con la instancia de base de datos de MariaDB 10.5 de origen. Para comprobarlo, conéctese a la réplica de lectura y ejecute el comando `SHOW REPLICA STATUS`. Si el campo `Seconds_Behind_Master` muestra `0`, significa que la replicación está al día.

> **Note**
>
> Versiones anteriores de MariaDB utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MariaDB anterior a la 10.6, utilice `SHOW SLAVE STATUS`.

6. (Opcional) Cree una réplica de lectura de su réplica de lectura.

   Si desea que la instancia de base de datos tenga una réplica de lectura después de promocionarse a una instancia de base de datos independiente, puede crear la réplica de lectura ahora.

   a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de actualizar.

   b. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).

   c. Proporcione un valor de DB instance identifier (Identificador de instancias de bases de datos) para su réplica de lectura y asegúrese de que el valor de DB instance class (Clase de instancia de base de datos) y otros ajustes coinciden con su instancia de base de datos de MariaDB 10.5.

   d. Elija Create read replica (Crear réplica de lectura).

7. (Opcional) Configure un grupo de parámetros de base de datos personalizado para la réplica de lectura.

   Si desea que la instancia de base de datos utilice un grupo de parámetros personalizado después de promocionarse a una instancia de base de datos independiente, puede crear el grupo de parámetros de base de datos ahora y asociarlo con la réplica de lectura.

a. Cree un grupo de parámetros de base de datos personalizado para MariaDB 10.6. Para obtener instrucciones, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.

b. Modifique los parámetros que desea cambiar en el grupo de parámetros de base de datos que acaba de crear. Para obtener instrucciones, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

c. En la consola, elija Databases (Bases de datos) y, a continuación, elija la réplica de lectura.

d. Elija Modify.

e. En DB parameter group (Grupo de parámetros de base de datos), elija el grupo de parámetros de base de datos de MariaDB 10.6 que acaba de crear y, a continuación, elija Continue (Continuar).

f. En Programación de modificaciones, elija Aplicar inmediatamente.

g. Elija Modify DB instance (Modificar instancia de base de datos) para comenzar la actualización.

8. Haga que su réplica de lectura de MariaDB 10.6 sea una instancia de base de datos independiente.

> **Important**
>
> Cuando promocione su réplica de lectura de MariaDB 10.6 a una instancia de base de datos independiente, dejará de ser una réplica de su instancia de base de datos de MariaDB 10.5. Recomendamos que promocione su réplica de lectura de MariaDB 10.6 durante un período de mantenimiento cuando su instancia de base de datos de MariaDB 10.5 de origen esté en modo de solo lectura y se hayan suspendido todas las operaciones de escritura. Cuando haya finalizado la promoción, puede dirigir sus operaciones de escritura a la instancia de base de datos de MariaDB 10.6 actualizada para asegurarse de que no se ha perdido ninguna operación de escritura.
> Además, recomendamos que, antes de promocionar su réplica de lectura de MariaDB 10.6, realice todas las operaciones de lenguaje de definición de datos (DDL) necesarias en la réplica de lectura de MariaDB 10.6. Un ejemplo es la creación de índices. Este enfoque evita los efectos negativos en el rendimiento de la réplica de lectura de MariaDB 10.6 después de su promoción. Para promocionar una réplica de lectura, siga este procedimiento.

a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de actualizar.

b. En Actions (Acciones), seleccione Promote (Promover).

c. Elija Yes (Sí) para habilitar las copias de seguridad automatizadas para la instancia de réplica de lectura. Para obtener más información, consulte Introducción a las copias de seguridad.

d. Elija Continue.

e. Elija Promote Read Replica.

9. Ahora tiene una versión actualizada de su base de datos MariaDB. En este punto, puede dirigir sus aplicaciones a la nueva instancia de base de datos de MariaDB 10.6.

Actualización de una versión del motor de instantáneas de base de datos de MariaDB

Con Amazon RDS, puede crear una instantánea de base de datos de volumen de almacenamiento de la instancia de base de datos de MariaDB. Cuando se crea una instantánea de base de datos, esta se basa en la versión del motor empleada por la instancia de base de datos. Puede actualizar la versión del motor para las instantáneas de base de datos.

En el caso de RDS para MariaDB, puede actualizar a todas las versiones de motor disponibles. Puede actualizar instantáneas de base de datos cifradas o no cifradas.

Para ver las versiones de motor disponibles para la instantánea de base de datos de RDS para MariaDB, utilice el siguiente ejemplo de AWS CLI.

```
aws rds describe-db-engine-versions --engine mariadb --include-all --engine-
version example-engine-version --query "DBEngineVersions[*].ValidUpgradeTarget[*].
{EngineVersion:EngineVersion}" --output text
```

Si no ve los resultados de la instantánea, es posible que la versión del motor esté obsoleta. Si la versión del motor ha quedado obsoleta, le recomendamos que actualice al destino de actualización de versión principal más reciente o a uno de los demás destinos de actualización disponibles para esa versión. Para obtener más información, consulte Opciones de actualización para instantáneas de bases de datos con versiones de motor no compatibles con RDS para MariaDB.

Después de restaurar una instantánea de base de datos actualizada a una nueva versión del motor, asegúrese que la actualización se ha realizado correctamente. Para obtener más información acerca de una actualización de versión principal, consulte the section called “Actualizaciones del motor de base de datos de MariaDB”. Para aprender a restaurar una instantánea de base de datos, consulte the section called “Restauración a una instancia de base de datos”.

> **Note**
>
> No puede actualizar las instantáneas de base de datos automatizadas que se hayan creado durante el proceso de copia de seguridad automatizado.

Puede actualizar una instantánea de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS.

Console

Para actualizar la versión del motor de una instantánea de base de datos mediante la AWS Management Console, siga el siguiente procedimiento.

Para actualizar una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea que desea actualizar.
4. En Actions (Acciones), seleccione Upgrade Snapshot (Actualizar instantánea). Aparece la página Upgrade snapshot.
5. Elija la New engine version (Nueva versión del motor) a la que actualizarse.
6. Elija Save changes (Guardar cambios) para actualizar la instantánea.

   Durante el proceso de actualización, todas las acciones están deshabilitadas para esta instantánea de base de datos. Además, el estado de la instantánea de base de datos cambia de Disponible a Actualizando y después cambia a Activo al completarse. Si la instantánea de base de datos no se puede actualizar porque se ha dañado, el estado cambia a No disponible. No puede recuperar el snapshot desde este estado.

   > **Note**
   >
   > Si la actualización de la base de datos falla, la instantánea se revierte al estado original con la versión original.

AWS CLI

Para actualizar una instantánea de base de datos a una nueva versión del motor de base de datos, ejecute el comando modify-db-snapshot de la AWS CLI.

Opciones

- `--db-snapshot-identifier`: identificador de la instantánea de base de datos que se va a actualizar. El identificador debe ser un Nombre de recurso de Amazon (ARN). Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

- `--engine-version`: versión del motor a la que se va a actualizar la instantánea de base de datos.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-snapshot \

    --db-snapshot-identifier my_db_snapshot \
    --engine-version new_version
```

Para Windows:

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier my_db_snapshot ^
    --engine-version new_version
```

Amazon RDS API

Para actualizar una instantánea de base de datos a una nueva versión del motor de base de datos, llame a la operación ModifyDBSnapshot de la API de RDS.

Parámetros

- `DBSnapshotIdentifier`: identificador de la instantánea de base de datos que se va a actualizar. El identificador debe ser un Nombre de recurso de Amazon (ARN). Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.
- `EngineVersion`: versión del motor a la que se va a actualizar la instantánea de base de datos.

Opciones de actualización para instantáneas de bases de datos con versiones de motor no compatibles con RDS para MariaDB

En la siguiente tabla, se muestran las versiones de motor a las que puede actualizar desde una versión de motor no compatible con las instantáneas de base de datos de RDS para MariaDB.

> **Note**
>
> Puede que tenga que actualizar la instantánea de base de datos más de una vez para actualizar a la versión de motor que haya elegido.

Versión del motor de instantáneas de base de datos	Versiones del motor disponibles para su actualización
10.0.17, 10.0.24, 10.0.28, 10.0.31, 10.0.32, 10.0.34, 10.0.35	10.0.38, 10.1.48, 10.6.19, 10.6.20, 10.11.9, 10.11.10, 11.4.3, 11.4.4
10.1.14, 10.1.16, 10.1.19, 10.1.23, 10.1.26, 10.1.31, 10.1.34	10.1.48, 10.2.44, 10.6.19, 10.6.20, 10.11.9, 10.11.10, 11.4.3, 11.4.4
10.2.11, 10.2.12, 10.2.15, 10.2.21, 10.2.32, 10.2.37, 10.2.39, 10.2.40, 10.2.41, 10.2.43	10.2.44, 10.3.39, 10.6.19, 10.6.20, 10.6.21, 10.11.9, 10.11.10, 10.11.11, 11.4.3, 11.4.4
10.3.8, 10.3.13, 10.3.20, 10.3.23, 10.3.28, 10.3.31, 10.3.32	10.3.39, 10.4.34, 10.6.19, 10.6.20, 10.6.21, 10.11.9, 10.11.10, 10.11.11, 11.4.3, 11.4.4
10.4.8	10.4.34, 10.5.16, 10.5.17, 10.5.18, 10.5.20, 10.5.21, 10.5.22, 10.5.23, 10.5.24, 10.5.25, 10.5.26, 10.5.27, 10.5.28, 10.6.8, 10.6.10, 10.6.11, 10.6.13, 10.6.14, 10.6.15, 10.6.16, 10.6.18, 10.6.19, 10.6.20, 10.6.21, 10.11.4, 10.6.17, 10.11.5, 10.11.6, 10.11.7, 10.11.8, 10.11.9, 10.11.10, 10.11.11

Importación de datos en una instancia de base de datos de Amazon RDS para MariaDB

Puede utilizar varias técnicas diferentes para importar datos en una instancia de base de datos de RDS for MariaDB. El mejor enfoque depende de varios factores:

- Origen de los datos
- Cantidad de datos
- Importar una vez o de forma continua
- Cantidad de tiempo de inactividad

Si también está migrando una aplicación con los datos, es importante tener en cuenta la cantidad de tiempo de inactividad.

En la siguiente tabla se muestran técnicas para importar datos en una instancia de base de datos de RDS para MariaDB:

> **Note**
>
> Amazon RDS solo admite la importación de instancias de base de datos de Amazon S3 a RDS para MySQL. Actualmente, no se admite la importación de copias de seguridad creadas con `mariadb-backup` a RDS para MariaDB.

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Base de datos de MariaDB	Cualquiera	Continuo	Mínima	Configure la replicación con una base de datos de MariaDB existente como origen de replicación.	Configuración de la replicaci

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
existente en las instalaciones o en Amazon E				Puede configurar la replicación en una instancia de base de datos de MariaDB mediante el uso de identificadores de transacciones globales (GTID) de MariaDB cuando la instancia externa sea de la versión 10.0.24 o posterior de MariaDB, o mediante coordenadas de registro binario para las instancias de MariaDB en versiones anteriores a 10.0.24. Los identificadores de transacciones globales (GTID) de MariaDB se implementan de un modo distinto al de los GTID de MySQL, que no son compatibles con Amazon RDS.	ón de posición de archivo de registro binario con una instancia de origen externa Importación de datos a una instancia de base de datos de Amazon RDS para MariaDB con tiempo de

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
					inactividad reducido
Cualquier base de datos existente	Cualquiera	Una vez o continua	Mínima	Utilizar AWS Database Migration Service para migrar la base de datos con un tiempo de inactividad mínimo y, para numerosos motores de base de datos, continuar las replicaciones en curso.	Qué es AWS Database Migration Service y Uso de una base de datos compatible con MySQL como destino para AWS DMS en la Guía del usuario de AWS Database Migration Service

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Instancia de base de datos de MariaDB existente	Cualquiera	Una vez o continua	Mínima	Cree una réplica de lectura para la replicación continua. Promocione la réplica de lectura para la creación única de una nueva instancia de base de datos.	Trabajo con réplicas de lectura de instancias de base de datos

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Base de datos existente de MariaDB	Pequeña	Una vez	Alguno	Copie los datos directamente en la instancia de base de datos de MariaDB con una utilidad de línea de comandos.	Importación de datos de una base de datos de MariaDB externa a una instancia de base de datos de Amazon RDS para MariaDB

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Datos no almacenados en una base de datos existente	Media	Una vez	Alguno	Cree archivos sin formato e impórtelos con instrucciones `LOAD DATA LOCAL INFILE` de MariaDB.	Importación de datos de cualquier origen a una instancia de base de datos de Amazon RDS para MariaDB

> **Note**
>
> La base de datos del sistema `mysql` contiene la información de autenticación y autorización necesaria para iniciar sesión en la instancia de base de datos y obtener acceso a los datos. La eliminación, la modificación, el cambio de nombre o el truncamiento de tablas, datos u otros contenidos de la base de datos `mysql` de la instancia de base de datos puede provocar errores e impedir el acceso a la instancia de base de datos y a los datos. En ese caso, puede restaurar la instancia de base de datos desde una instantánea usando el comando AWS CLI de la restore-db-instance-from-db-snapshot. Puede recuperar la instancia de base de datos con el comando restore-db-instance-to-point-in-time.

Consideraciones sobre la importación de datos para MariaDB

En el siguiente contenido se encuentra información técnica relacionada con la carga de datos en MariaDB. Este contenido está dirigido a usuarios familiarizados con la arquitectura del servidor de MariaDB.

Registro binario

La habilitación del registro binario reduce el rendimiento de la carga de datos y requiere hasta cuatro veces más espacio en disco en comparación con el registro desactivado. El tamaño de la transacción utilizado para cargar los datos afecta directamente al rendimiento del sistema y a las necesidades de espacio en disco, las transacciones más grandes requieren más recursos.

Tamaño de la transacción

El tamaño de la transacción influye en los siguientes aspectos de las cargas de datos de MariaDB:

- Consumo de recursos
- Utilización del espacio en disco
- Reanudación del proceso
- Tiempo de recuperación
- Formato de entrada (archivos sin formato o SQL)

En esta sección se describe el modo en que el tamaño de transacción afecta al registro binario y se argumentan los beneficios de desactivar el registro binario durante la carga de grandes volúmenes de datos. Puede habilitar y desactivar el registro binario estableciendo el periodo de retención de copia de seguridad automatizado de Amazon RDS. Un valor distinto de cero activa el registro binario y el valor cero lo desactiva. Para obtener más información, consulte Backup retention period (Periodo de retención de copia de seguridad).

En esta sección también se describe el impacto de las transacciones de gran tamaño en InnoDB y por qué es importante que los tamaños de transacción sean pequeños.

Transacciones pequeñas

En las transacciones pequeñas, el registro binario duplica el número de escrituras en disco requeridas para cargar los datos. Este efecto puede degradar el desempeño notablemente en otras

sesiones de base de datos y aumentar el tiempo requerido para cargar los datos. La degradación experimentada depende en parte de los siguientes factores:

- Tasa de carga
- Otra actividad de la base de datos que tenga lugar durante la carga
- Capacidad de la instancia de base de datos de Amazon RDS

Los registros binarios también consumen un espacio en disco aproximadamente igual al volumen de datos cargado hasta que se hace una copia de seguridad de los registros y se eliminan. Amazon RDS minimiza este impacto creando copias de seguridad de los registros binarios y retirándolos con frecuencia.

Transacciones grandes

En el caso de transacciones grandes, el registro binario triplica IOPS y el uso del disco por los siguientes motivos:

- La caché del registro binario almacena temporalmente los datos de las transacciones en el disco.
- Esta caché crece con el tamaño de la transacción, lo que consume espacio en disco.
- Cuando se completa la transacción (confirmación o reversión), el sistema copia la caché en el registro binario.

Este proceso crea tres copias de los datos:

- Los datos originales
- La caché en el disco
- La entrada del registro binario final

Cada operación de escritura implica una E/S adicional, lo que repercute aún más en el rendimiento.

Por este motivo, el registro binario requiere el triple de espacio en disco en comparación con el registro desactivado. Por ejemplo, si se cargan 10 GiB de datos en una sola transacción, se crean tres copias:

- 10 GiB para los datos de la tabla
- 10 GiB para la caché del registro binario
- 10 GiB para el archivo del registro binario

El espacio total en disco temporal necesario es 30 GiB.

Consideraciones importantes sobre el espacio en disco:

- El archivo de caché persiste hasta que finaliza la sesión o hasta que una nueva transacción crea otra caché.
- El registro binario permanece hasta que se realiza una copia de seguridad, lo que podría retener 20 GiB (caché y registro) durante un periodo prolongado.

Si se usa `LOAD DATA LOCAL INFILE` para cargar los datos, la recuperación de datos crea una cuarta copia en caso de que la base de datos deba recuperarse desde una copia de seguridad realizada antes de la carga. Durante la recuperación, MariaDB extrae los datos desde el registro binario en un archivo sin formato. Luego, MariaDB ejecuta `LOAD DATA LOCAL INFILE`. En función del ejemplo anterior, esta recuperación requiere un espacio total en disco temporal de 40 GiB o 10 GiB cada uno para la tabla, la caché, el registro y el archivo local. Sin al menos 40 GiB de espacio libre en disco, la recuperación produce un error.

Optimización de grandes cargas de datos

Para grandes cargas de datos, desactive el registro binario para reducir la sobrecarga y los requisitos de espacio en disco. Puede desactivar el registro binario estableciendo el periodo de retención de copias de seguridad en 0. Una vez completada la carga, restaure el periodo de retención de copias de seguridad al valor apropiado distinto de cero. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS y Periodo de retención de copia de seguridad en la tabla de configuración.

> **Note**
>
> Si la instancia de base de datos es una instancia de base de datos de origen para réplicas de lectura, no puede establecer el periodo de retención de copia de seguridad en 0.

Antes de cargar los datos, recomendamos que cree una instantánea de base de datos. Para obtener más información, consulte Administración de copias de seguridad manuales.

InnoDB

La siguiente información sobre las opciones de registro y recuperación para deshacer ayuda a mantener pequeñas las transacciones de InnoDB para optimizar el rendimiento de la base de datos.

Descripción del registro para deshacer InnoDB

Deshacer es un mecanismo de registro que permite la reversión de transacciones y admite el control de concurrencia multiversión (MVCC).

Para MariaDB 10.11 y versiones anteriores, los registros para deshacer se almacenan en el espacio de tablas del sistema InnoDB (normalmente ibdata1) y se retienen hasta que el subproceso de purga los elimina. De este modo, las transacciones de carga de datos de gran tamaño pueden provocar que el espacio de tablas del sistema sea muy grande y consumir espacio en disco que no puede recuperar si no recrea la base de datos.

Para todas las versiones de MariaDB, el subproceso de purga debe esperar para eliminar cualquier registro para deshacer hasta que la transacción activa más antigua se confirme o se revierta. Si la base de datos procesa otras transacciones durante la carga, los registros para deshacer también se acumulan y no pueden eliminarse, incluso si se confirman las transacciones y ninguna otra transacción necesita registros para deshacer MVCC. En esta situación, todas las transacciones, incluidas las de solo lectura, se ralentizan. Esta ralentización se produce porque todas las transacciones acceden a todas las filas que cualquier transacción (no solo la transacción de carga) cambia. En efecto, las transacciones deben examinar los registros para deshacer que las transacciones de carga de larga duración impidieron purgar durante una limpieza del registro para deshacer. Esto afecta al rendimiento de cualquier operación que acceda a las filas modificadas.

Opciones de recuperación de transacciones de InnoDB

Aunque InnoDB optimiza las operaciones de confirmación, las reversiones de transacciones grandes son lentas. Para una recuperación más rápida, realice una recuperación en un momento dado o restaure una instantánea de base de datos. Para obtener más información, consulte Recuperación a un momento dado y Restauración a una instancia de base de datos.

Formatos de importación de datos

MariaDB admite dos formatos de importación de datos: archivos sin formato y SQL. Revise la información sobre cada formato para determinar cuál es la mejor opción para sus necesidades.

Archivos sin formato

Para transacciones pequeñas, cargue archivos sin formato con `LOAD DATA LOCAL INFILE`. Este formato de importación de datos puede proporcionar los siguientes beneficios en comparación con el uso de SQL:

- Menos tráfico de red
- Costos de transmisión de datos más bajos
- Menor sobrecarga de procesamiento de bases de datos
- Procesamiento más rápido

`LOAD DATA LOCAL INFILE` carga todo el archivo sin formato en una sola transacción. Mantenga pequeño el tamaño de los archivos individuales para obtener las siguientes ventajas:

- Posibilidad de reanudación: puede hacer un seguimiento de los archivos que se han cargado. Si surge un problema durante la carga, puede continuar donde se detuvo. Es posible que sea necesario volver a transmitir algunos datos a Amazon RDS, pero con los archivos pequeños, el volumen es mínimo.
- Carga de datos en paralelo: si tiene IOPS y ancho de banda de la red suficiente para la carga de un solo archivo, la carga en paralelo podría ahorrar tiempo.
- Control de la velocidad de carga: si la carga de datos tiene un impacto negativo en otros procesos, puede controlar la velocidad de carga aumentando el intervalo entre los archivos.

Las transacciones de gran tamaño reducen los beneficios de usar `LOAD DATA LOCAL INFILE` para importar datos. Cuando no pueda dividir una gran cantidad de datos en archivos más pequeños, considere la posibilidad de utilizar SQL.

SQL

SQL tiene una ventaja fundamental con respecto a los archivos sin formato: puede mantener pequeños los tamaños de transacción. Sin embargo, SQL puede tardar mucho más en cargar que los archivos sin formato. Además, después de un error, puede ser difícil determinar dónde reanudar, ya que no se pueden reiniciar los archivos mariadb-dump. Si se produce un error durante la carga de un archivo mariadb-dump, debe modificarlo o sustituirlo antes de poder reanudar la carga. Otra opción, después de corregir la causa del error, puede restaurar a un momento anterior a la carga antes de cargar y volver a enviar el archivo. Para obtener más información, consulte Recuperación a un momento dado.

Uso de instantáneas de base de datos de Amazon RDS para puntos de comprobación de la base de datos

Si carga datos durante periodos prolongados, como horas o días, sin registro binario, utilice las instantáneas de base de datos para proporcionar puntos de comprobación periódicos para garantizar

la seguridad de los datos. Cada instantánea de base de datos crea una copia coherente de la instancia de base de datos que sirve como punto de recuperación durante errores del sistema o eventos de corrupción de datos. Como las instantáneas de base de datos son rápidas, los puntos de comprobación frecuentes tienen un impacto mínimo en el rendimiento de la carga. Puede eliminar las instantáneas de base de datos anteriores sin que ello afecte a la durabilidad de la base de datos ni a las capacidades de recuperación. Para obtener más información acerca de las instantáneas de base de datos, consulte Administración de copias de seguridad manuales.

Reducción de los tiempos de carga de bases de datos

Los siguientes elementos son consejos adicionales para reducir los tiempos de carga:

- Cree todos los índices secundarios antes de cargar los datos en las bases de datos MariaDB. A diferencia de otros sistemas de bases de datos, MariaDB reconstruye toda la tabla al agregar o modificar índices secundarios. Este proceso crea una nueva tabla con los cambios de índice, copia todos los datos y elimina la tabla original.
- Cargue los datos en el orden de la clave principal. Para las tablas de InnoDB, esto puede reducir los tiempos de carga entre un 75 % y un 80 % y reducir el tamaño del archivo de datos en un 50 %.
- Desactive las restricciones de clave externa estableciendo `foreign_key_checks` en `0`. Esto es obligatorio en muchos casos para archivos sin formato cargados con `LOAD DATA LOCAL INFILE`. Para cualquier carga, desactivar las comprobaciones de claves externas acelera la carga de datos. Una vez completada la carga, vuelva a habilitar las restricciones configurando `foreign_key_checks` en 1 y verifique los datos.
- Cargue datos en paralelo a no ser que se aproxime al límite de los recursos. Para habilitar la carga simultánea en varios segmentos de la tabla, use tablas particionadas cuando sea apropiado.
- Para reducir la sobrecarga de ejecución de SQL, combine varias instrucciones `INSERT` en operaciones `INSERT` únicas con varios valores. `mariadb-dump` implementa esta optimización automáticamente.
- Reduzca las operaciones de E/S de registro de InnoDB estableciendo `innodb_flush_log_at_trx_commit` en `0`. Una vez completada la carga, restaure `innodb_flush_log_at_trx_commit` a 1.

> **Warning**
>
> Si se establece `innodb_flush_log_at_trx_commit` en `0`, InnoDB vaciará sus registros cada segundo en lugar de hacerlo con cada confirmación. Esta configuración

aumenta el rendimiento, pero puede conllevar el riesgo de perder transacciones si se produce un error en el sistema.

- Si va a cargar datos en una instancia de base de datos que no tiene réplicas de lectura, establezca `sync_binlog` en `0`. Una vez completada la carga, restaure `sync_binlog parameter` a `1`.
- Cargue los datos en una instancia de base de datos de Single-AZ antes de convertir la instancia de base de datos en una implementación Multi-AZ. Si la instancia de base de datos ya usa una implementación Multi-AZ, no se recomienda cambiar a una implementación Single-AZ para la carga de datos. Hacerlo solo proporciona mejoras marginales

Importación de datos de una base de datos de MariaDB externa a una instancia de base de datos de Amazon RDS para MariaDB

Puede importar datos desde una base de datos de MariaDB o MySQL existente a una instancia de base de datos de RDS para MariaDB o RDS para MySQL. Esto se lleva a cabo copiando la base de datos con mysqldump y canalizándola de forma directa en la instancia de base de datos de RDS para MariaDB o RDS para MySQL. La utilidad de línea de comandos `mysqldump` suele utilizarse para crear copias de seguridad y transferir datos de un servidor de MySQL o MariaDB a otro. Se incluye con el software cliente de MySQL y MariaDB.

En MariaDB 10.5, el cliente se llama mariadb-dump. A partir de MariaDB 11.0.1, debe usar `mariadb-dump` en lugar de `mysqldump`.

> **Note**
>
> Si importa o exporta grandes cantidades de datos con una instancia de base de datos de MySQL, lo más fiable y rápido para introducir y sacar los datos de Amazon RDS es mediante archivos de copia de seguridad `xtrabackup` y Amazon S3. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..
>
> Amazon RDS no admite `xtrabackup` para MariaDB o `mariabackup`. Amazon RDS solo admite la importación de Amazon S3 para MySQL.

Un comando `mysqldump` típico para mover datos de una base de datos externa a una instancia de base de datos de Amazon RDS tiene el aspecto del ejemplo siguiente. Sustituya valores con

su propia información. Para MariaDB 11.0.1 y versiones posteriores, sustituya `mysqldump` por `mariadb-dump` y `mysql` por `mariadb`.

```
mysqldump -u local_user \
    --databases database_name \
    --single-transaction \
    --compress \
    --order-by-primary  \
    --routines=0 \
    --triggers=0 \
    --events=0 \
    -plocal_password | mysql -u RDS_user \
        --port=port_number \
        --host=host_name \
        -pRDS_password
```

> **Important**
>
> Asegúrese de no dejar un espacio entre la opción `-p` y la contraseña especificada. Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en este ejemplo.

Asegúrese de conocer las siguientes recomendaciones y consideraciones:

- Excluya los siguientes esquemas del archivo de volcado:
  - `sys`
  - `performance_schema`
  - `information_schema`

  La utilidad `mysqldump` y `mariadb-dump` excluye estos esquemas de forma predeterminada.
- Si necesita migrar usuarios y privilegios, considere la posibilidad de usar una herramienta que genere el lenguaje de control de datos (DCL) para volver a crearlos, como la utilidad pt-show-grants.
- Para realizar la importación, asegúrese de que el usuario que lo haga tenga acceso a la instancia de base de datos. Para obtener más información, consulte Control de acceso con grupos de seguridad.

Los parámetros son los siguientes:

- `-u` *`local_user`*: use este parámetro para especificar un nombre de usuario. La primera vez que utilice este parámetro, especifique el nombre de una cuenta de usuario en la base de datos de MariaDB o MySQL local que identifique con el parámetro `--databases`.
- `--databases` *`database_name`*: use este parámetro para especificar el nombre de la base de datos en la instancia de MySQL o MariaDB local que desea importar a Amazon RDS.
- `--single-transaction`: use este parámetro para asegurarse de que todos los datos cargados desde la base de datos local sean coherentes en un momento determinado. Si hay otros procesos que modifican los datos mientras `mysqldump` los lee, el uso de este parámetro ayuda a mantener la integridad de los datos.
- `--compress`: use este parámetro para reducir el consumo de ancho de banda mediante la compresión de los datos de la base de datos local antes de su envío a Amazon RDS.
- `--order-by-primary`: use este parámetro para reducir el tiempo de carga mediante la ordenación de los datos de cada tabla según su clave primaria.
- `--routines`: Úselo si existen rutinas como procedimientos almacenados o funciones en la base de datos que está copiando. Establezca el parámetro en `0`, lo que excluye las rutinas durante el proceso de importación. Después, vuelva a crear manualmente las rutinas en la base de datos de Amazon RDS.
- `--triggers`: Úselo si existen desencadenadores en la base de datos que va a copiar. Establezca el parámetro en `0`, lo que excluye los desencadenadores durante el proceso de importación. Después, vuelva a crear manualmente los desencadenadores en la base de datos de Amazon RDS.
- `--events`: Úselo si existen eventos en la base de datos que está copiando. Establezca el parámetro en `0`, lo que excluye los eventos durante el proceso de importación. Después, vuelva a crear manualmente los eventos en la base de datos de Amazon RDS.
- `-p`*`local_password`*: use este parámetro para especificar una contraseña. La primera vez que use este parámetro, especifique la contraseña de la cuenta de usuario identificada con el primer parámetro `-u`.
- `-u` *`RDS_user`*: use este parámetro para especificar un nombre de usuario. La segunda vez que utilice este parámetro, especifique el nombre de una cuenta de usuario en la base de datos predeterminada de la instancia de base de datos de MariaDB o MySQL identificada con el parámetro `--host`.

- `--port port_number`: se utiliza para especificar el puerto de la instancia de base de datos de MySQL o MariaDB. El valor predeterminado es 3306, salvo que se haya cambiado al crear la instancia de base de datos.
- `--host host_name`: se utiliza para especificar el nombre del sistema de nombres de dominio (DNS) del punto de conexión de la instancia de base de datos de Amazon RDS, por ejemplo, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la instancia de base de datos en la consola de Amazon RDS.
- `-pRDS_password`: use este parámetro para especificar una contraseña. La segunda vez que use este parámetro, debe especificar la contraseña de la cuenta de usuario identificada por el segundo parámetro `-u`.

Asegúrese de crear de forma manual procedimientos almacenados, desencadenadores, funciones o eventos en su base de datos de Amazon RDS. Si hay alguno de estos objetos en la base de datos que va a copiar, exclúyalo cuando ejecute `mysqldump` o `mariadb-dump`. Para hacerlo, incluya los siguientes parámetros con el comando `mysqldump` o `mariadb-dump`:

- `--routines=0`
- `--triggers=0`
- `--events=0`

Ejemplo

En el siguiente ejemplo se copia la base de datos de ejemplo `world` del host local en una instancia de base de datos de RDS para MySQL. Sustituya valores con su propia información. Para copiar la base de datos de ejemplo en una instancia de base de datos de RDS para MariaDB, sustituya `mysqldump` por `mariadb-dump` y `mysql` por `mariadb`.

Para Linux, macOS o Unix:

```
sudo mysqldump -u local_user \
    --databases world \
    --single-transaction \
    --compress \
    --order-by-primary  \
    --routines=0 \
    --triggers=0 \
    --events=0 \
    -plocal_password | mysql -u rds_user \
```

```
        --port=3306 \
        --host=my_instance.123456789012.us-east-1.rds.amazonaws.com \
        -pRDS_password
```

Para Windows:

Ejecute el siguiente comando en un símbolo del sistema que se haya abierto con un clic con el botón derecho en Símbolo del sistema del menú de programas de Windows y con la selección de Ejecutar como administrador. Sustituya valores con su propia información. Para copiar la base de datos de ejemplo en una instancia de base de datos de RDS para MariaDB, sustituya `mysqldump` por `mariadb-dump` y `mysql` por `mariadb`.

```
mysqldump -u local_user ^
    --databases world ^
    --single-transaction ^
    --compress ^
    --order-by-primary  ^
    --routines=0 ^
    --triggers=0 ^
    --events=0 ^
    -plocal_password | mysql -u RDS_user ^
        --port=3306 ^
        --host=my_instance.123456789012.us-east-1.rds.amazonaws.com ^
        -pRDS_password
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.

Importación de datos a una instancia de base de datos de Amazon RDS para MariaDB con tiempo de inactividad reducido

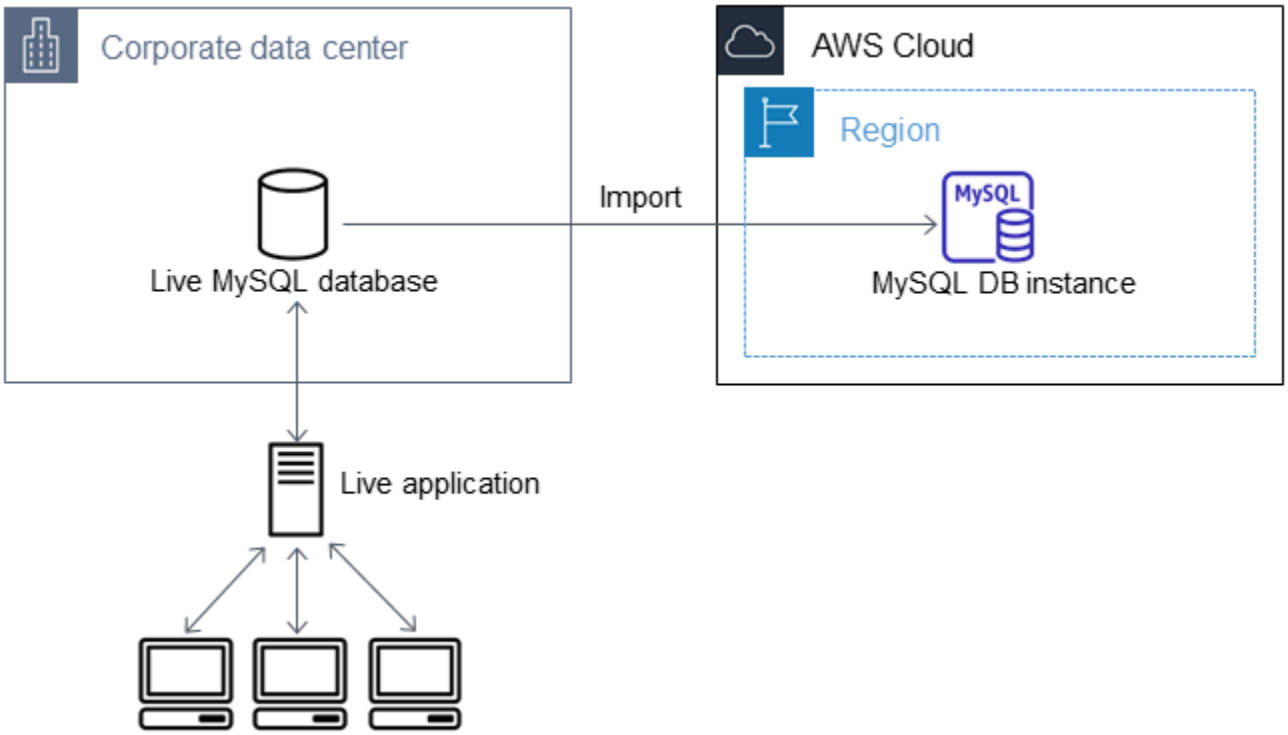
En algunos casos, es posible que sea necesario importar datos de una base de datos de MySQL o MariaDB externa, que sea compatible con una aplicación activa, a una instancia de base de datos de RDS para MariaDB o un clúster de base de datos de Multi-AZ de RDS para MySQL. Utilice el siguiente procedimiento para minimizar el impacto en la disponibilidad de las aplicaciones. Este procedimiento también puede resultar útil al trabajar con una base de datos de gran tamaño. Con

este procedimiento, puede reducir el coste de la importación al reducir la cantidad de datos que se transfieren a través de la red a AWS.

En el procedimiento, se transfiere primero una copia de los datos de la base de datos a una instancia de Amazon EC2 y después se importan los datos a una nueva base de datos de Amazon RDS. A continuación, se usa la replicación para actualizar la base de datos de Amazon RDS al estado de la instancia externa activa, antes de redirigir la aplicación a la base de datos de Amazon RDS. Si la instancia externa es MariaDB 10.0.24 o superior y la instancia de destino es RDS para MariaDB, configure la replicación de MariaDB en función de los identificadores de transacción globales (GTID). De lo contrario, debe configurar la replicación en función de las coordenadas de los registros binarios. Si la base de datos externa la admite, recomendamos la replicación basada en GTID porque es un método más fiable. Para obtener más información, consulte Global Transaction ID en la documentación de MariaDB.

> **Note**
>
> Si desea importar datos a una instancia de base de datos de RDS para MySQL y el escenario lo admite, recomendamos importar y exportar los datos de Amazon RDS mediante el uso de archivos de copia de seguridad y Amazon S3. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..

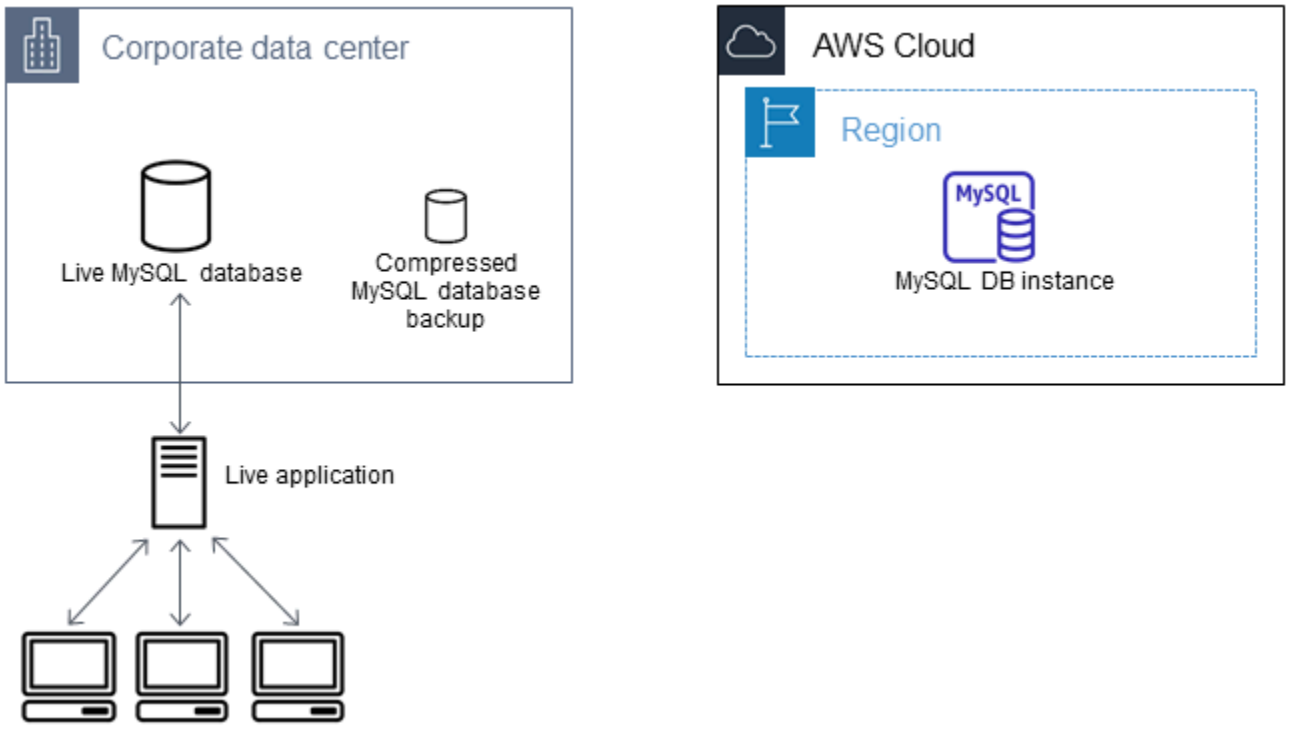
El siguiente diagrama muestra la importación de una base de datos de MySQL externa a una base de datos de MySQL en Amazon RDS.



Tarea 1: Crear una copia de la base de datos existente

El primer paso del proceso de migración de una gran cantidad de datos a una base de datos de RDS para MariaDB o RDS para MySQL con un tiempo de inactividad mínimo es crear una copia de los datos de origen.

El siguiente diagrama muestra la creación de una copia de seguridad de la base de datos de MySQL.



Con la utilidad `mysqldump` puede crear una copia de seguridad de la base de datos, ya sea en formato SQL o como texto delimitado. En MariaDB 10.5, el cliente se llama mariadb-dump. A partir de MariaDB 11.0.1, debe usar `mariadb-dump` en lugar de `mysqldump`. Se recomienda hacer una prueba con cada formato en un entorno que no sea de producción para determinar con qué método tarda menos la ejecución de mysqldump.

También se recomienda comparar el rendimiento de `mysqldump` con el beneficio que ofrece el uso del formato de texto delimitado para la carga. Una copia de seguridad con formato de texto delimitado crea un archivo de texto separado por tabuladores por cada tabla volcada. Los archivos obtenidos pueden cargarse en paralelo con el comando `LOAD DATA LOCAL INFILE` para reducir el tiempo necesario para importar la base de datos. Para obtener más información, consulte Cargar los datos para MariaDB o Cargar los datos para MySQL.

Antes de iniciar la operación de copia de seguridad, asegúrese de configurar las opciones de replicación para la base de datos de MySQL o MariaDB que va a copiar en Amazon RDS. Las opciones de replicación incluyen la activación del registro binario y la configuración de un ID de servidor único. La activación de estas opciones hace que el servidor comience a registrar las transacciones de la base de datos y la prepare para ser una instancia de replicación de origen en una fase posterior del proceso.

Asegúrese de conocer las siguientes recomendaciones y consideraciones:

- Utilice la opción `--single-transaction` con `mysqldump` porque vuelca un estado coherente de la base de datos. Para garantizar un archivo de volcado válido, no ejecute instrucciones de lenguaje de definición de datos (DDL) mientras `mysqldump` se está ejecutando. Puede programar un periodo de mantenimiento para estas operaciones.
- Excluya los siguientes esquemas del archivo de volcado:
  - `sys`
  - `performance_schema`
  - `information_schema`

  La utilidad `mysqldump` y `mariadb-dump` excluye estos esquemas de forma predeterminada.
- Si necesita migrar usuarios y privilegios, considere la posibilidad de usar una herramienta que genere el lenguaje de control de datos (DCL) para volver a crearlos, como la utilidad pt-show-grants.

Para establecer las opciones de replicación

1. Edite el archivo `my.cnf`. Este archivo se suele encontrar en `/etc`.

   ```
   sudo vi /etc/my.cnf
   ```

   Añada las opciones `log_bin` y `server_id` a la sección `[mysqld]`. La opción `log_bin` proporciona un identificador de nombre de archivo para los archivos de log binarios. La opción `server_id` proporciona un identificador único para el servidor en las relaciones origen-réplica.

   El siguiente ejemplo muestra la sección `[mysqld]` actualizada de un archivo `my.cnf`:

   ```
   [mysqld]
   log-bin=mysql-bin
   server-id=1
   ```

   Para obtener más información, consulte Setting the Replication Source Configuration en la documentación de MySQL.
2. Para la replicación con un clúster de base de datos Multi-AZ, establezca `ENFORCE_GTID_CONSISTENCY` y el parámetro `GTID_MODE` en `ON`.

   ```
   mysql> SET @@GLOBAL.ENFORCE_GTID_CONSISTENCY = ON;
   ```

```
mysql> SET @@GLOBAL.GTID_MODE = ON;
```

Esta configuración no es necesaria para la replicación con una instancia de base de datos.

3. Reinicie el servicio `mysql`.

```
sudo service mysqld restart
```

Para crear una copia de seguridad de la base de datos existente

1. Cree una copia de seguridad de los datos con la utilidad `mysqldump` o la utilidad `mariadb-dump`, especificando el formato SQL o de texto delimitado.

   Para MySQL 8.0.25 y versiones anteriores, especifique `--master-data=2` para crear un archivo de copia de seguridad que se pueda utilizar para iniciar la replicación entre servidores. Para MySQL 8.0.26 y versiones posteriores, especifique `--source-data=2` para crear un archivo de copia de seguridad que se pueda utilizar para iniciar la replicación entre servidores. Para obtener más información, consulte mysqldump - Un programa de copia de seguridad de base de datos en la documentación de MySQL.

   Para mejorar el desempeño y asegurar la integridad de los datos, use las opciones `--order-by-primary` y `--single-transaction` para `mysqldump`.

   Para evitar incluir la base de datos de sistema de MySQL en la copia de seguridad, no use la opción `--all-databases` con `mysqldump`. Para obtener más información, consulte Creating a Data Snapshot Using mysqldump en la documentación de MySQL.

   Use `chmod`, si es necesario, para asegurarse de que es posible escribir en el directorio donde se va a crear el archivo de copia de seguridad.

   > **Important**
   >
   > En Windows, ejecute el símbolo del sistema como administrador.

   - Para generar la salida en formato SQL, use el siguiente comando:

     Para Linux, macOS o Unix:

```
sudo mysqldump \
    --databases database_name \
    --master-data=2  \
    --single-transaction \
    --order-by-primary \
    -r backup.sql \
    -u local_user \
    -ppassword
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.

Para Windows:

```
mysqldump ^
    --databases database_name ^
    --master-data=2  ^
    --single-transaction ^
    --order-by-primary ^
    -r backup.sql ^
    -u local_user ^
    -ppassword
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.

- Para generar la salida en formato de texto delimitado, ejecute el siguiente comando:

  Para Linux, macOS o Unix:

```
sudo mysqldump \
    --tab=target_directory \
    --fields-terminated-by ',' \
    --fields-enclosed-by '"' \
```

```
    --lines-terminated-by 0x0d0a \
    database_name \
    --master-data=2 \
    --single-transaction \
    --order-by-primary \
    -ppassword
```

Para Windows:

```
mysqldump ^
    --tab=target_directory ^
    --fields-terminated-by "," ^
    --fields-enclosed-by """ ^
    --lines-terminated-by 0x0d0a ^
    database_name ^
    --master-data=2 ^
    --single-transaction ^
    --order-by-primary ^
    -ppassword
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.
> Asegúrese de crear de forma manual procedimientos almacenados, desencadenadores, funciones o eventos en su base de datos de Amazon RDS. Si hay alguno de estos objetos en la base de datos que va a copiar, exclúyalos cuando ejecute `mysqldump`. Para hacerlo, incluya los siguientes argumentos con el comando `mysqldump`:
>
> - `--routines=0`
> - `--triggers=0`
> - `--events=0`

Para MySQL 8.0.22 y versiones anteriores y versiones de MariaDB, al ejecutar `mysqldump` y especificar el formato de texto delimitado, se devuelve un comentario `CHANGE MASTER TO`. Este comentario contiene el nombre y la ubicación del archivo de registro maestro. Para MySQL 8.0.23 y versiones posteriores, cuando ejecuta `mysqldump` con el formato de texto delimitado, se devuelve un comentario `CHANGE REPLICATION SOURCE TO`. Este comentario contiene

el nombre y la ubicación del archivo de registro de origen. Si la instancia externa es distinta de MariaDB versión 10.0.24 y posteriores o MySQL 8.0.23 y versiones posteriores, tenga en cuenta los valores de `MASTER_LOG_FILE` y `MASTER_LOG_POS`. Necesita estos valores al configurar la replicación.

Se devuelve la siguiente salida para las versiones de MariaDB y para MySQL 8.0.22 y versiones anteriores:

```
-- Position to start replication or point-in-time recovery from
--
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031',
 MASTER_LOG_POS=107;
```

Se devuelve la siguiente salida para MySQL 8.0.23 y versiones posteriores:

```
-- Position to start replication or point-in-time recovery from
--
-- CHANGE SOURCE TO SOURCE_LOG_FILE='mysql-bin-changelog.000031',
 SOURCE_LOG_POS=107;
```

Para MySQL 8.0.22 y versiones anteriores, si utiliza el formato SQL, puede obtener el nombre y la posición del archivo de registro principal en el comentario `CHANGE MASTER TO` del archivo de copia de seguridad. Para MySQL 8.0.23 y versiones posteriores, si utiliza el formato SQL, puede obtener el nombre y la posición del archivo de registro de origen en el comentario `CHANGE REPLICATION SOURCE TO` del archivo de copia de seguridad. Si la instancia externa corresponde a MariaDB versión 10.0.24 o posterior, puede obtener el GTID en el paso siguiente.

2. Si la instancia externa que utiliza es MariaDB versión 10.0.24 o posterior, use la reproducción basada en GTID. Ejecute `SHOW MASTER STATUS` en la instancia de MariaDB externa para obtener el nombre y ubicación del archivo de registro binario y, a continuación, conviértalos en un GTID ejecutando `BINLOG_GTID_POS` en la instancia de MariaDB externa.

   ```
   SELECT BINLOG_GTID_POS('binary_log_file_name', binary_log_file_position);
   ```

   Tenga en cuenta el GTID devuelto. Necesita GTID para configurar la replicación.

3. Comprima los datos copiados para reducir los recursos de red necesarios para copiarlos a la base de datos de Amazon RDS. Tenga en cuenta el tamaño del archivo de copia de seguridad.

Necesitará esta información para determinar el tamaño de la instancia de Amazon EC2 que se debe crear. Cuando haya terminado, comprima el archivo de copia de seguridad con GZIP o la utilidad de compresión que prefiera.

- Para comprimir la salida en formato SQL, ejecute el siguiente comando:

```
gzip backup.sql
```

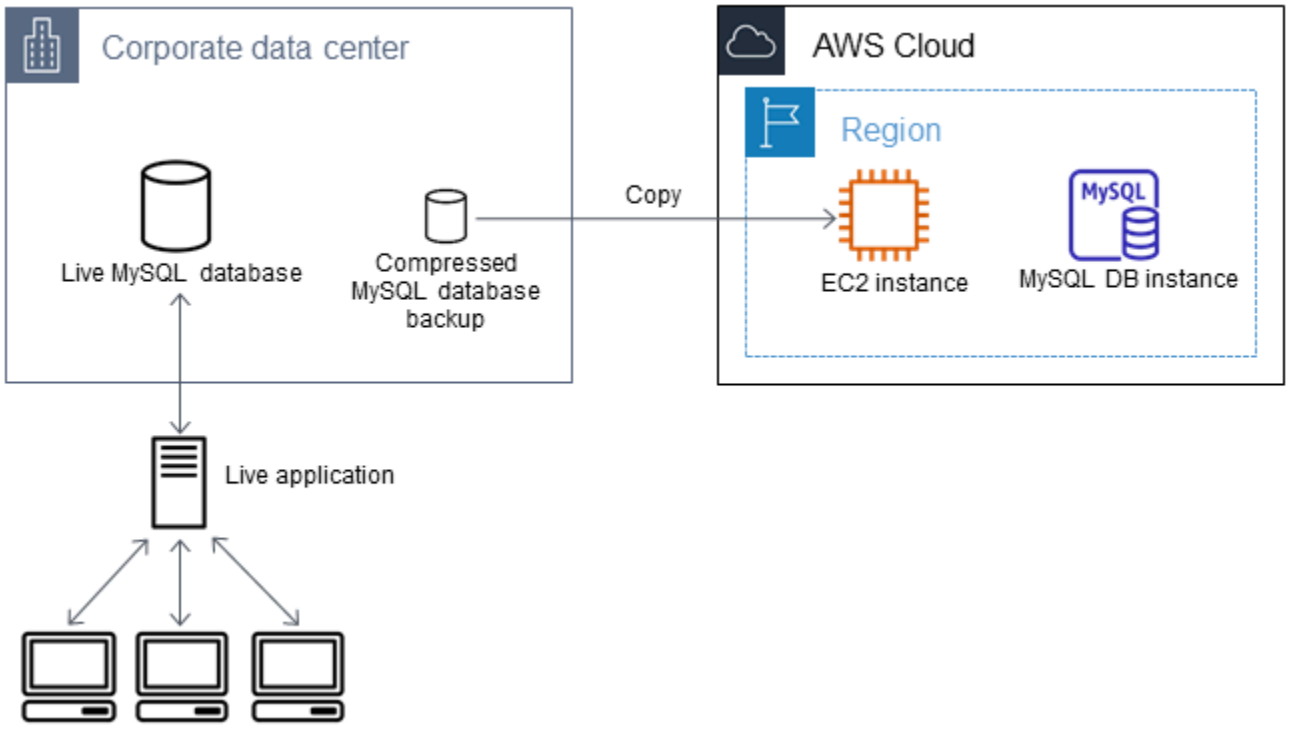
- Para comprimir la salida en formato de texto delimitado, ejecute el siguiente comando:

```
tar -zcvf backup.tar.gz target_directory
```

Tarea 2: Crear una instancia de Amazon EC2 y copiar la base de datos comprimida

La copia del archivo de copia de seguridad comprimido a una instancia Amazon EC2 requiere menos recursos de red que una copia directa de los datos sin comprimir entre las instancias de base de datos. Una vez que los datos se encuentran en Amazon EC2, puede copiarlos desde allí directamente a la base de datos de MySQL o MariaDB. Para ahorrar en el costo de los recursos de red, la instancia de Amazon EC2 debe estar en la misma Región de AWS que la instancia de base de datos de Amazon RDS. Tener la instancia de Amazon EC2 en la misma Región de AWS que la base de datos de Amazon RDS también reduce la latencia de red durante la importación.

El siguiente diagrama muestra cómo copiar la copia de seguridad de la base de datos a una instancia de Amazon EC2.



Para crear una instancia Amazon EC2 y copiar los datos

1. En la Región de AWS donde tiene pensado crear la base de datos de Amazon RDS, cree una nube privada virtual (VPC), un grupo de seguridad de VPC y una subred de VPC. Asegúrese de que las reglas de entrada del grupo de seguridad de VPC permiten las direcciones IP necesarias para que la aplicación se conecte a AWS. Puede especificar un intervalo de direcciones IP, por ejemplo, `203.0.113.0/24`, u otro grupo de seguridad de VPC. Puede usar la Consola de Amazon VPC para crear y administrar VPC, subredes y grupos de seguridad. Para obtener más información, consulte Introducción a Amazon VPC en la Guía del usuario de Amazon Virtual Private Cloud.
2. Abra la consola de Amazon EC2 y elija la Región de AWS que contendrá la instancia de Amazon EC2 y la base de datos de Amazon RDS. Lance una instancia Amazon EC2 utilizando la VPC, la subred y el grupo de seguridad que creó en el paso 1. Asegúrese de seleccionar un tipo de instancia con suficiente espacio de almacenamiento para el archivo de copia de seguridad de base de datos sin comprimir. Para obtener más información sobre las instancias de Amazon EC2, consulte Introducción a Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud.
3. Para conectarse a la base de datos de Amazon RDS desde la instancia de Amazon EC2, edite el grupo de seguridad de VPC. Agregue una regla de entrada que especifique la dirección IP privada de la instancia de EC2. La dirección IP privada aparece en la pestaña Details (Detalles) del panel Instance (Instancia) de la consola de EC2. Para editar el grupo de seguridad de VPC y agregar

una regla de entrada, elija Security Groups (Grupos de seguridad) en el panel de navegación de la consola de EC2, elija el grupo de seguridad y, luego, agregue una regla de entrada para MySQL o Aurora que especifique la dirección IP privada de la instancia de EC2. Para obtener información sobre cómo agregar una regla de entrada a un grupo de seguridad de VPC, consulte Reglas de grupo de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

4. Copie el archivo de copia de seguridad de base de datos comprimido del sistema local a la instancia Amazon EC2. Use `chmod`, si es necesario, para asegurarse de que tiene permiso de escritura para el directorio de destino de la instancia de Amazon EC2. Puede utilizar `scp` o un cliente de Secure Shell (SSH) para copiar el archivo. El siguiente comando es un comando `scp` de ejemplo:

```
scp -r -i key pair.pem backup.sql.gz ec2-user@EC2 DNS:/target_directory/backup.sql.gz
```

> **Important**
>
> Al copiar la información confidencial, asegúrese de usar un protocolo de transferencia de red seguro.

5. Establezca una conexión con la instancia Amazon EC2 e instale las últimas actualizaciones y las herramientas de cliente MySQL con los comandos siguientes:

```
sudo yum update -y
sudo yum install mysql -y
```

Para obtener más información, consulte Conexión a la instancia para instancias de Linux en la Guía del usuario de Amazon Elastic Compute Cloud.

> **Important**
>
> En este ejemplo se instala el cliente de MySQL en una imagen de máquina de Amazon (AMI) para una distribución de Amazon Linux. Este ejemplo no instala el cliente de MySQL en una distribución diferente, como Ubuntu o Red Hat Enterprise Linux. Para obtener información sobre la instalación de MySQL, consulte Instalación de MySQL en la documentación de MySQL.

6. Una vez establecida la conexión la instancia Amazon EC2 descomprima el archivo de copia de seguridad de base de datos. Los siguientes comandos son ejemplos.

- Para descomprimir la salida en formato SQL, ejecute el siguiente comando:

```
gzip backup.sql.gz -d
```

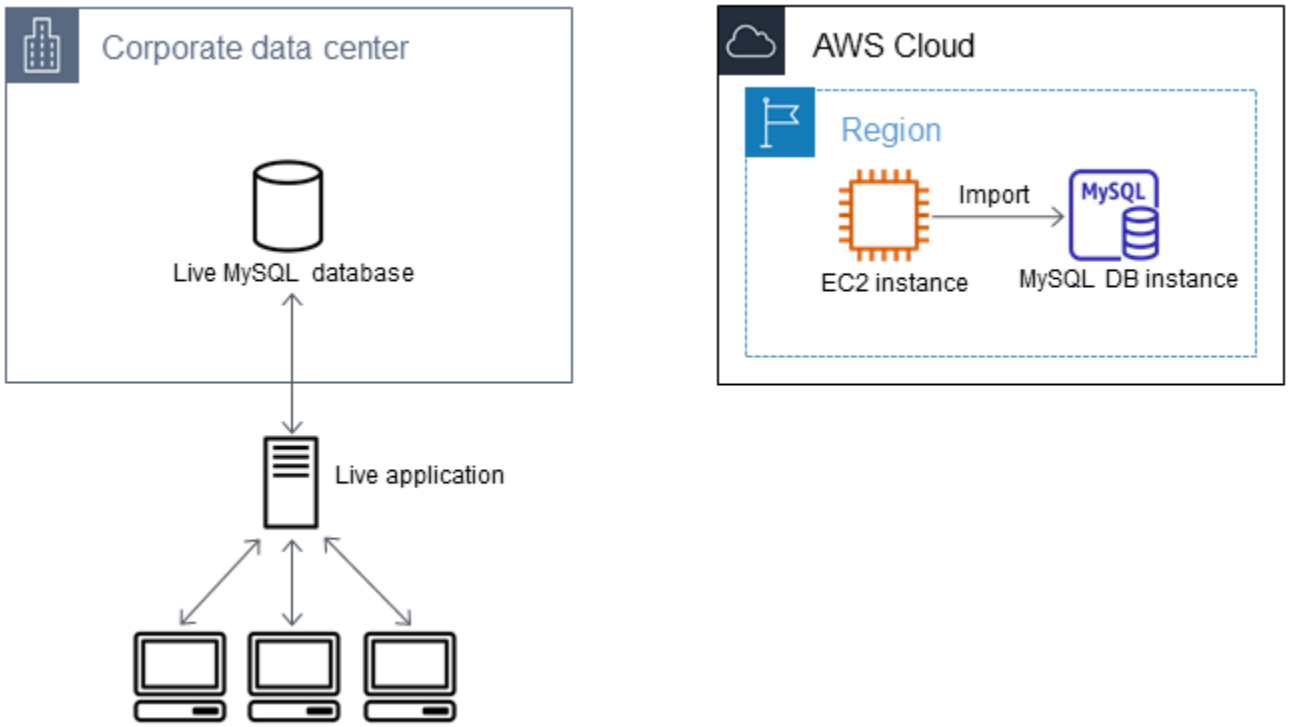
- Para descomprimir la salida en formato de texto delimitado, ejecute el siguiente comando:

```
tar xzvf backup.tar.gz
```

Tarea 3: Crear una base de datos de MySQL o MariaDB e importar los datos desde la instancia de Amazon EC2

Al crear una instancia de base de datos de RDS para MariaDB, una instancia de base de datos de RDS para MySQL o un clúster de base de datos Multi-AZ de MySQL en la misma Región de AWS que la instancia de Amazon EC2, puede importar el archivo de copia de seguridad de la base de datos desde Amazon EC2 más rápido que a través de Internet.

El siguiente diagrama muestra la importación de la copia de seguridad desde una instancia de Amazon EC2 a una base de datos de MySQL.



Para crear una base de datos de MySQL o MariaDB e importar los datos

1. Determine la clase de la instancia de base de datos y la cantidad de espacio de almacenamiento requeridas para atender la carga de trabajo prevista para esta base de datos de Amazon RDS. Como parte de este proceso, decida cuánto espacio y qué capacidad de procesamiento requieren los procedimientos de carga de datos. Decida también lo que se necesita para manejar la carga de trabajo de producción. Puede estimar esto en función del tamaño y los recursos de la base de datos de MySQL o MariaDB de origen. Para obtener más información, consulte Clases de instancia de base de datos de .
2. Cree una instancia de base de datos o un clúster de base de datos Multi-AZ en la Región de AWS que contenga la instancia de Amazon EC2.

   Para crear un clúster de base de datos Multi-AZ de RDS para MySQL, siga las instrucciones de Creación de un clúster de base de datos multi-AZ para Amazon RDS.

   Para crear una instancia de base de datos de RDS para MariaDB o RDS para MySQL, siga las instrucciones en Creación de una instancia de base de datos de Amazon RDS y use las siguientes directrices:

   - Especifique una versión del motor de base de datos compatible con la instancia de base de datos de origen.
     - Si la instancia de origen es MySQL 5.5.x, la instancia de base de datos de Amazon RDS debe ser MySQL.
     - Si la instancia de origen es MySQL 5.6.x o 5.7.x, la instancia de base de datos de Amazon RDS debe ser MySQL o MariaDB.
     - Si la instancia de origen es MySQL 8.0.x, la instancia de base de datos de Amazon RDS debe ser MySQL 8.0.x.
     - Si la instancia de origen es MySQL 8.4.x, la instancia de base de datos de Amazon RDS debe ser MySQL 8.4.x.
     - Si la instancia de origen es MariaDB 5.5 o superior, la instancia de base de datos de Amazon RDS debe ser MariaDB.
   - Especifique la misma nube privada virtual (VPC) y el mismo grupo de seguridad de VPC que para la instancia de Amazon EC2. De este modo se asegura de que la instancia Amazon EC2 y la instancia de Amazon RDS sean visibles mutuamente a través de la red. Asegúrese de que la instancia de base de datos sea de acceso público. Para configurar la replicación con la base

de datos de origen como se describe en la siguiente sección, la instancia de base de datos debe ser accesible públicamente.

- No configure varias zonas de disponibilidad, retenciones de copia de seguridad ni réplicas de lectura hasta haber importado la copia de seguridad de la base de datos. Una vez completada la importación, puede configurar Multi-AZ y la retención de copia de seguridad para la instancia de producción.

3. Revise las opciones de configuración predeterminadas para la base de datos de Amazon RDS. Si el grupo de parámetros predeterminado para la base de datos no tiene las opciones de configuración que desea, busque otro que sea adecuado o cree un grupo de parámetros nuevo. Para obtener más información acerca de cómo crear un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.
4. Conéctese a la nueva base de datos de Amazon RDS como usuario maestro. Cree los usuarios necesarios para admitir a los administradores, las aplicaciones y los servicios que necesitan acceso a la instancia de base de datos. El nombre de host para la base de datos de Amazon RDS es el valor de Punto de conexión para esta instancia de base de datos, sin el número de puerto; por ejemplo, `mysampledb.123456789012.us-west-2.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la base de datos en la consola de Amazon RDS.
5. Conéctese a la instancia de Amazon EC2. Para obtener más información, consulte Conexión a la instancia para instancias de Linux en la Guía del usuario de Amazon Elastic Compute Cloud.
6. Conecte con la base de datos de Amazon RDS como host remoto desde la instancia de Amazon EC2 con el comando `mysql`. El siguiente comando es un ejemplo:

```
mysql -h host_name -P 3306 -u db_master_user -p
```

   El *host_name* es el punto de conexión de la base de datos de Amazon RDS.
7. En la petición de `mysql`, ejecute el comando `source` y pásele el nombre del archivo de volcado de la base de datos. Este comando carga los datos en la instancia de base de datos de Amazon RDS.

   - Para el formato SQL, utilice el siguiente comando:

```
mysql> source backup.sql;
```

   - Para el formato de texto delimitado, cree primero la base de datos, si no es la predeterminada que se creó cuando se configuró la base de datos de Amazon RDS.

```
mysql> create database database_name;
mysql> use database_name;
```

A continuación, cree las tablas.

```
mysql> source table1.sql
mysql> source table2.sql
etc...
```

Importe entonces los datos.

```
mysql> LOAD DATA LOCAL INFILE 'table1.txt' INTO TABLE table1 FIELDS TERMINATED BY
 ',' ENCLOSED BY '"' LINES TERMINATED BY '0x0d0a';
mysql> LOAD DATA LOCAL INFILE 'table2.txt' INTO TABLE table2 FIELDS TERMINATED BY
 ',' ENCLOSED BY '"' LINES TERMINATED BY '0x0d0a';
etc...
```

Para mejorar el rendimiento, puede ejecutar estas operaciones en paralelo desde varias conexiones, de modo que todas las tablas se creen y luego se carguen al mismo tiempo.

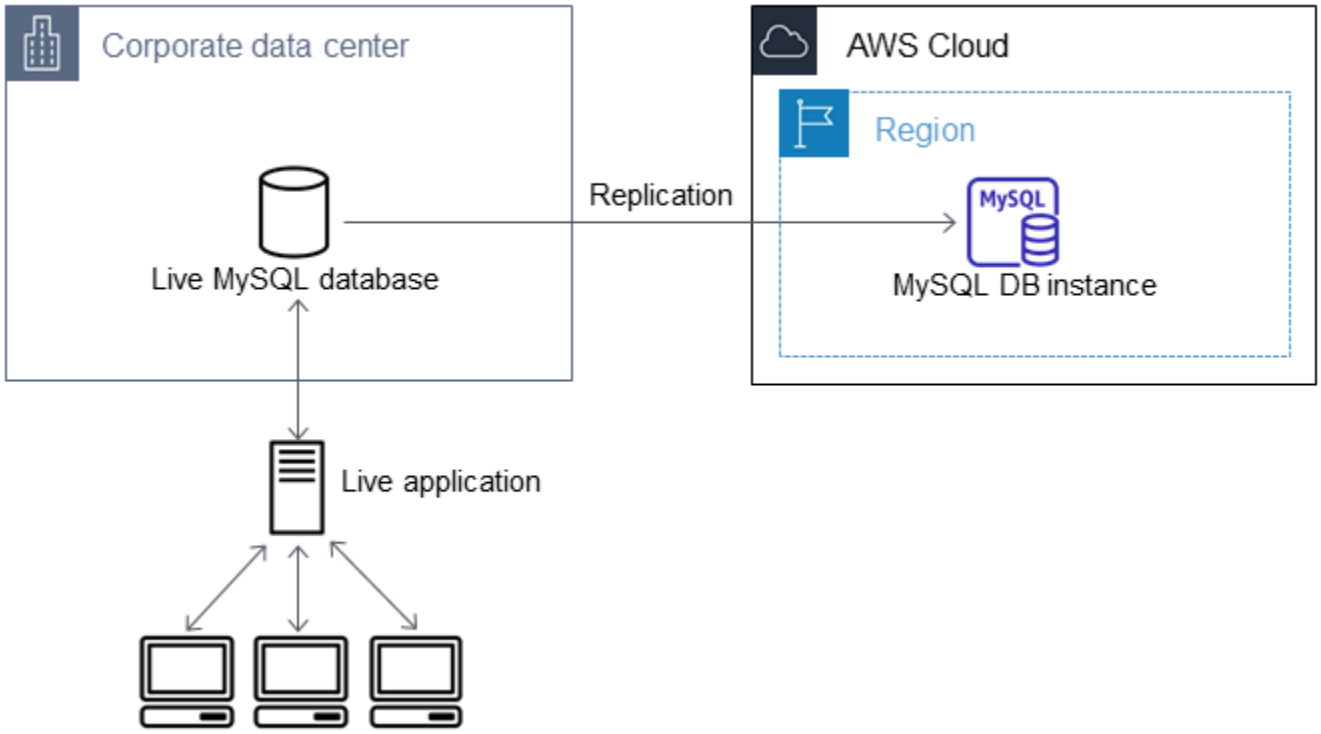
> **Note**
>
> Si utilizó alguna opción de formato de datos con `mysqldump` en el volcado inicial de la tabla, asegúrese de utilizar las mismas opciones con `LOAD DATA LOCAL INFILE` para garantizar una interpretación adecuada del contenido del archivo de datos.

8. Ejecute una consulta `SELECT` sencilla en una o dos de las tablas de la base de datos importada para comprobar que la importación se ha completado correctamente.

Si ya no necesita la instancia de Amazon EC2 utilizada en este procedimiento, termine la instancia de EC2 para reducir el uso de recursos de AWS. Para terminar una instancia de EC2, consulte Terminación de una instancia en la Guía del usuario de Amazon Elastic Compute Cloud.

Tarea 4: Replicar los datos de la base de datos externa a la nueva base de datos de Amazon RDS

Es probable que su base de datos de origen se haya actualizado durante el tiempo que tardó en copiar y transferir los datos a la base de datos MariaDB o MySQL. Por tanto, puede utilizar la replicación para actualizar la base de datos copiada con la base de datos de origen.



Los permisos requeridos para comenzar la replicación en una base de datos de Amazon RDS están restringidos y no están disponibles para el usuario principal de Amazon RDS. Por ello, utilice el procedimiento almacenado de Amazon RDS adecuado para la versión principal del motor:

- mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_external_master_gtid para configurar la replicación y mysql.rds_start_replication para iniciar la replicación

Para iniciar la replicación

En la tarea 1, cuando estableció las opciones de replicación, activó el registro binario y estableció un ID de servidor único para la base de datos de origen. Ahora puede configurar la base de datos de

Amazon RDS como réplica estableciendo la base de datos activa como instancia de replicación de origen.

1. En la consola de Amazon RDS, agregue la dirección IP del servidor que aloja la base de datos de origen al grupo de seguridad de VPC configurado para la base de datos de Amazon RDS. Para obtener más información sobre la configuración de un grupo de seguridad de VPC, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

   Es posible que también necesite configurar la red local para permitir las conexiones desde la dirección IP de la base de datos de Amazon RDS para que se pueda comunicar con la instancia de origen. Para encontrar la dirección IP de la base de datos de Amazon RDS, use el comando `host`:

   ```
   host host_name
   ```

   El *`host_name`* es el nombre de DNS del punto de conexión de la base de datos de Amazon RDS, por ejemplo, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la instancia de base de datos en la consola de Amazon RDS.

2. Con el cliente que prefiera, conecte con la instancia de origen y cree un usuario para la replicación. Esta cuenta se usa únicamente para la replicación y debe estar limitada a su dominio para mejorar la seguridad. El siguiente comando es un ejemplo:

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

   > **Note**
   >
   > Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

3. En la instancia de origen, conceda al usuario de replicación los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE`. Por ejemplo, para conceder los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` referidos a todas las bases de datos al usuario "`repl_user`" del dominio, ejecute el siguiente comando:

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
   ```

4. Si utilizó el formato SQL para crear el archivo de copia de seguridad y la instancia externa no es MariaDB 10.0.24 o posterior, observe el contenido de ese archivo ejecutando el siguiente comando:

```
cat backup.sql
```

   El archivo contiene un comentario `CHANGE MASTER TO` que contiene el nombre y la posición del archivo de registro maestro. Este comentario se incluye en el archivo de copia de seguridad cuando se usa la opción `--master-data` con `mysqldump`. Tenga en cuenta los valores de `MASTER_LOG_FILE` y `MASTER_LOG_POS`.

```
--
-- Position to start replication or point-in-time recovery from
--

-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

   Si utilizó el formato de texto delimitado para crear el archivo de copia de seguridad y la instancia externa no es MariaDB 10.0.24 o posterior, ya debe haber obtenido las coordenadas del registro binario del paso 1 del procedimiento descrito en “Creación de una copia de seguridad de la base de datos existente” en la tarea 1.

   Si la instancia externa es MariaDB 10.0.24 o posterior, ya debe haber obtenido el GTID desde el que inicia la replicación en el paso 2 del procedimiento descrito en “Creación de una copia de seguridad de la base de datos existente” en la tarea 1.

5. Convertir la base de datos de Amazon RDS en la réplica. Si la instancia externa no es MariaDB 10.0.24 o una versión posterior, conéctese a la base de datos de Amazon RDS como usuario principal e identifique la base de datos de origen como la instancia de replicación de origen con el procedimiento almacenado de Amazon RDS adecuado:

   - mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
   - mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)

   Si tiene un archivo de copia de seguridad con formato SQL, utilice el nombre de archivo de registro y la ubicación del registro principal que determinó en el paso 4. Si utilizó formato de texto delimitado, utilice el nombre y la posición que determinó cuando se crearon los archivos de copia de seguridad. Los siguientes comandos son ejemplos:

MySQL 8.4 y versiones posteriores

```
CALL mysql.rds_set_external_source ('myserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
```

MariaDB y MySQL 8.0 y versiones anteriores

```
CALL mysql.rds_set_external_master ('myserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
```

> **Note**
>
> Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

Si la instancia externa no es MariaDB 10.0.24 o una versión posterior, conéctese a la base de datos de Amazon RDS como usuario maestro e identifique la base de datos de origen como la instancia de replicación de origen con el comando mysql.rds_set_external_master_gtid. Utilice el GTID que determinó en el paso 2 del procedimiento descrito en “Creación de una copia de seguridad de la base de datos existente” en la tarea 1. El siguiente comando es un ejemplo:

```
CALL mysql.rds_set_external_master_gtid ('source_server_ip_address', 3306,
 'ReplicationUser', 'password', 'GTID', 1);
```

source_server_ip_address es la dirección IP de la instancia de replicación de origen. Una dirección DNS privada de EC2 no se admite actualmente.

> **Note**
>
> Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

6. En la base de datos de Amazon RDS, para empezar la replicación, ejecute el comando mysql.rds_start_replication siguiente:

```
CALL mysql.rds_start_replication;
```

7. En la base de datos de Amazon RDS, para determinar si la réplica está actualizada con la instancia de replicación de origen, ejecute el comando SHOW REPLICA STATUS. Los resultados del comando `SHOW REPLICA STATUS` incluyen el campo `Seconds_Behind_Master`. Cuando el campo `Seconds_Behind_Master` devuelve 0, la réplica está actualizada con la instancia de replicación de origen.

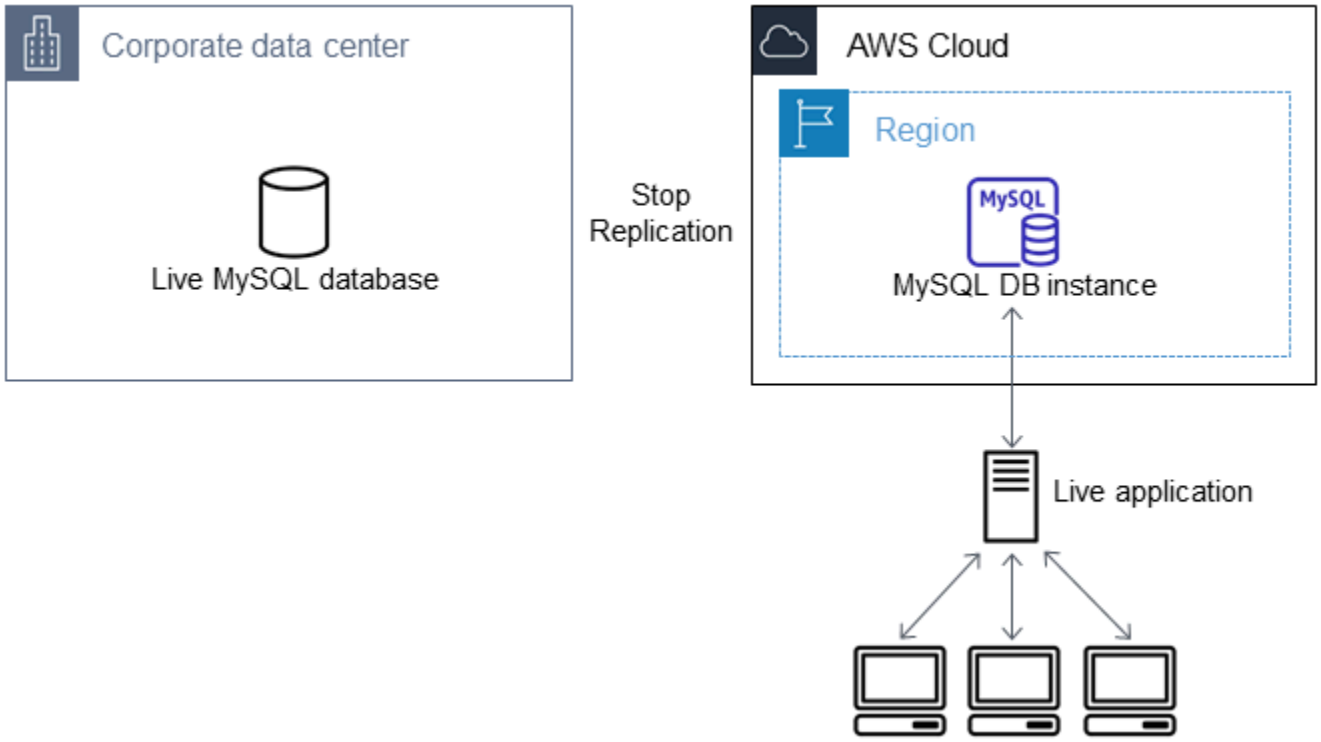
   > **Note**
   >
   > Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

   Para una instancia de base de datos de MariaDB 10.5, 10.6 o 10.11, ejecute el procedimiento almacenado mysql.rds_replica_status en lugar del comando de MySQL.

8. Una vez que la base de datos de Amazon RDS esté actualizada, active las copias de seguridad automatizadas para poder restaurar la base de datos si es necesario. Puede activar o modificar copias de seguridad automatizadas para la base de datos de Amazon RDS mediante la consola de Amazon RDS. Para obtener más información, consulte Introducción a las copias de seguridad.

Tarea 5: Redirigir la aplicación en funcionamiento a la instancia de Amazon RDS

Una vez que la base de datos de MySQL o MariaDB esté actualizada con la instancia de replicación de origen, puede actualizar la aplicación activa para utilizar la instancia de Amazon RDS.



Para redirigir una aplicación activa a una base de datos de MySQL o MariaDB y detener la replicación

1. Para añadir el grupo de seguridad de VPC para la base de datos de Amazon RDS, añada la dirección IP del servidor que aloja la aplicación. Para obtener más información sobre la modificación de un grupo de seguridad de VPC, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.
2. Compruebe que el valor del campo `Seconds_Behind_Master` en el comando SHOW REPLICA STATUS sea 0, lo que indica que la réplica está actualizada con la instancia de replicación de origen.

```
SHOW REPLICA STATUS;
```

> **Note**
>
> Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

Para una instancia de base de datos de MariaDB 10.5 o 10.6 o 10.11 ejecute el procedimiento mysql.rds_replica_status en lugar del comando de MySQL.

3. Cierre todas las conexiones con el origen cuando se completen las transacciones.
4. Actualice la aplicación para que use la base de datos de Amazon RDS. Normalmente, la actualización implicará cambar la configuración de conexión para identificar el nombre de host y el puerto de la base de datos de Amazon RDS, la cuenta de usuario y la contraseña con las que conectarse y la base de datos que se debe emplear.
5. Conéctese a la instancia de base de datos.

   Para un clúster de base de datos Multi-AZ, conéctese a la instancia de base de datos de escritor.
6. Detenga la replicación para la instancia de Amazon RDS con el comando mysql.rds_stop_replication siguiente:

   ```
   CALL mysql.rds_stop_replication;
   ```
7. Ejecute el procedimiento almacenado de Amazon RDS adecuado en la base de datos de Amazon RDS para restablecer la configuración de replicación y que la instancia deje de considerarse una réplica.

   - mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
   - mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)

   MySQL 8.4 y versiones posteriores

   ```
   CALL mysql.rds_reset_external_source;
   ```

   MariaDB y MySQL 8.0 y versiones anteriores

   ```
   CALL mysql.rds_reset_external_master;
   ```
8. Active las características adicionales de Amazon RDS, como la compatibilidad con Multi-AZ y las réplicas de lectura. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS y Trabajo con réplicas de lectura de instancias de base de datos.

Importación de datos de cualquier origen a una instancia de base de datos de Amazon RDS para MariaDB

Los siguientes pasos le guiarán a través del proceso de importación de datos a una instancia de base de datos de Amazon RDS:

Paso 1: crear archivos sin formato con los datos que se van a cargar

Utilice un formato habitual, como valores separados por comas (CSV), para almacenar los datos que se deben cargar. Cada tabla debe tener su propio archivo. No puede combinar los datos de varias tablas en el mismo archivo. Dé a cada archivo el nombre de la tabla correspondiente. Puede elegir la extensión que desee para el nombre de los archivos. Por ejemplo, si el nombre de la tabla es `sales`, el nombre del archivo podría ser `sales.csv` o `sales.txt`.

Si es posible, ordene los datos según la clave principal de la tabla que se va a cargar. Esto mejorará drásticamente los tiempos de carga y minimizará los requisitos de almacenamiento en disco.

La velocidad y la eficiencia de este procedimiento dependen de que el tamaño de los archivos sea pequeño. Si el tamaño sin comprimir de algún archivo es mayor de 1 GiB, divídalo en varios archivos y cárguelos por separado.

En los sistemas de tipo Unix (incluido Linux), utilice el comando `split`. Por ejemplo, el siguiente comando divide el archivo `sales.csv` en varios archivos de menos de 1 GiB y los divide solo en los saltos de línea (-C 1024m). Los nombres de los nuevos archivos incluyen sufijos numéricos ascendentes. El siguiente comando genera archivos con nombres como `sales.part_00` y `sales.part_01`.

```
split -C 1024m -d sales.csv sales.part_
```

Otros sistemas operativos disponen de utilidades similares.

Puede almacenar los archivos sin formato en cualquier lugar. No obstante, cuando cargue los datos en el paso 5, debe invocar el intérprete de comandos de `mysql` desde la misma ubicación donde existen los archivos o utilizar la ruta absoluta de los archivos cuando ejecute `LOAD DATA LOCAL INFILE`.

Paso 2: Detener las aplicaciones con acceso a la instancia de base de datos de destino

Antes de iniciar una carga grande, detenga toda la actividad de aplicaciones de acceder a la instancia de base de datos de destino que prevé cargar. Se recomienda esto en particular si otras sesiones modificarán las tablas que se cargan o las tablas a las que hacen referencia. Hacer esto reduce el riesgo de violaciones de restricciones que se producen durante la carga y mejoran el desempeño de carga. También permite restaurar la instancia de base de datos al estado inmediatamente anterior a la carga sin perder los cambios efectuados por los procesos no implicados en la carga.

Por supuesto, en ocasiones esto no será posible o no resultará práctico. Si no puede detener el acceso de las aplicaciones con acceso a la instancia de base de datos antes de la carga, tome las medidas oportunas para asegurar la disponibilidad e integridad de los datos. Los pasos específicos requeridos varían mucho en función de cada caso y de los requisitos del sitio.

Paso 3: crear una instantánea de base de datos

Si tiene previsto cargar los datos en una nueva instancia de base de datos que aún está vacía, puede omitir este paso. De lo contrario, recomendamos crear instantáneas de bases de datos de la instancia de base de datos de Amazon RDS elegida como destino antes y después de la carga de los datos. Las instantáneas de base de datos de Amazon RDS son copias de seguridad completas de la instancia de base de datos que puede usar para restaurar la instancia de base de datos a un estado conocido. Cuando se inicia una instantánea de base de datos, las operaciones de E/S de la instancia de base de datos se suspenden de forma temporal mientras se crea una copia de seguridad de la base de datos.

La creación de una instantánea de base de datos inmediatamente antes de la carga permite restaurar la base de datos al estado previo a la carga, si es necesario. Una instantánea de base de datos tomada inmediatamente después de la carga le evita tener que volver a cargar los datos en caso de error. También puede usar instantáneas de bases de datos después de la carga para importar datos a nuevas instancias de bases de datos.

En el ejemplo siguiente se ejecuta el comando create-db-snapshot de la AWS CLI para crear una instantánea de base de datos de la instancia `AcmeRDS` y se otorga el identificador `"preload"` a la instantánea de base de datos.

Para Linux, macOS o Unix:

```
aws rds create-db-snapshot \
    --db-instance-identifier AcmeRDS \
    --db-snapshot-identifier preload
```

Para Windows:

```
aws rds create-db-snapshot ^
    --db-instance-identifier AcmeRDS ^
    --db-snapshot-identifier preload
```

También puede utilizar la funcionalidad de restauración de instantáneas de bases de datos para crear instancias de bases de datos de prueba para simulacros o para deshacer cambios realizados durante la carga.

Tenga en cuenta que al restaurar una base de datos a partir de una instantánea de base de datos se crea una instancia nueva de base de datos que, como todas las instancias de base de datos, tiene un identificador y un punto de conexión únicos. Para restaurar la instancia de base de datos sin cambiar de punto de conexión, primero, elimine la instancia de base de datos para poder reutilizar el mismo punto de conexión.

Por ejemplo, para crear una instancia de base de datos para simulacros u otras pruebas, asigne a la instancia de base de datos su propio identificador. En el ejemplo, el identificador es `AcmeRDS-2`. El ejemplo se conecta a la instancia de base de datos mediante el punto de conexión asociado con `AcmeRDS-2`. Para obtener más información, consulte restore-db-instance-from-db-snapshot.

Para Linux, macOS o Unix:

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier AcmeRDS-2 \
    --db-snapshot-identifier preload
```

Para Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier AcmeRDS-2 ^
    --db-snapshot-identifier preload
```

Para reutilizar el punto de conexión existente, es necesario eliminar primero la instancia de base de datos y, luego, asignar el mismo identificador a la base de datos restaurada. Para obtener más información, consulte delete-db-instance.

En el ejemplo siguiente se toma una instantánea de base de datos final de la instancia de base de datos antes de eliminarla. Esto es opcional, pero recomendable.

Para Linux, macOS o Unix:

```
aws rds delete-db-instance \
    --db-instance-identifier AcmeRDS \
    --final-db-snapshot-identifier AcmeRDS-Final

aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier AcmeRDS \
    --db-snapshot-identifier preload
```

Para Windows:

```
aws rds delete-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --final-db-snapshot-identifier AcmeRDS-Final

aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier AcmeRDS ^
    --db-snapshot-identifier preload
```

Paso 4 (opcional): Desactivar copias de seguridad automatizadas de Amazon RDS

> **Warning**
>
> No desactive las copias de seguridad automatizadas si necesita realizar una recuperación en un momento dado.

La desactivación de las copias de seguridad automatizadas es una optimización del rendimiento y no es un requisito para las cargas de datos. La desactivación de las copias de seguridad automatizadas elimina todas las copias de seguridad existentes. Como resultado, después de desactivar las copias de seguridad automatizadas, no es posible la recuperación en un momento dado. Las instantáneas de base de datos manuales no se ven afectadas por la desactivación de las copias de seguridad automatizadas. Todas las instantáneas de base de datos manuales existentes seguirán estando disponibles para su restauración.

La desactivación de las copias de seguridad automatizadas reduce el tiempo de carga en aproximadamente un 25 % y reduce el espacio de almacenamiento necesario durante la carga. Si planea cargar los datos en una instancia de base de datos nueva que no contiene datos, desactivar las copias de seguridad es una forma sencilla de acelerar la carga y evitar utilizar el almacenamiento adicional que las copias de seguridad necesitan. Sin embargo, en algunos casos, es posible que tenga previsto cargar en una instancia de base de datos que ya contiene datos. Si es así, evalúe los beneficios de la desactivación de las copias de seguridad frente al impacto de perder la capacidad de realizar una recuperación a un momento dado.

Las instancias de base de datos tienen copias de seguridad automatizadas activadas de forma predeterminada (con un periodo de retención de un día). Para desactivar las copias de seguridad automatizadas, configure el periodo de retención de copia de seguridad en cero. Después de la carga, puede volver a activar las copias de seguridad mediante la configuración del periodo de retención de copia de seguridad en un valor distinto de cero. Para activar o desactivar las copias de seguridad, Amazon RDS apaga la instancia de base de datos y, a continuación, la reinicia para activar o desactivar el registro de MariaDB o MySQL.

Ejecute el comando `modify-db-instance` de la AWS CLI para establecer el valor cero como período de retención de copia de seguridad y aplicar el cambio inmediatamente. Al configurar cero como periodo de retención es necesario reiniciar la instancia de base de datos, por lo que debe esperar a que la operación se complete para poder continuar. Para obtener más información, consulte modify-db-instance.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier AcmeRDS \
    --apply-immediately \
    --backup-retention-period 0
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --apply-immediately ^
    --backup-retention-period 0
```

Puede comprobar el estado de la instancias de base de datos con el comando describe-db-instances de la AWS CLI. En el siguiente ejemplo se muestra el estado de la instancia de base de datos de la instancia de base de datos `AcmeRDS`:

```
aws rds describe-db-instances --db-instance-identifier AcmeRDS --query "*[].
{DBInstanceStatus:DBInstanceStatus}"
```

Cuando el estado de la instancia de base de datos es `available`, está listo para continuar con el siguiente paso.

Paso 5: cargar los datos

Para leer las filas de los archivos sin formato en las tablas de base de datos, use la instrucción `LOAD DATA LOCAL INFILE` de MySQL.

> **Note**
>
> Debe invocar el intérprete de comandos de `mysql` desde la misma ubicación donde existen los archivos o utilizar la ruta absoluta de los archivos cuando ejecute `LOAD DATA LOCAL INFILE`.

En el siguiente ejemplo, se muestra cómo cargar datos de un archivo denominado `sales.txt` en una tabla denominada `Sales` en la base de datos:

```
mysql> LOAD DATA LOCAL INFILE 'sales.txt' INTO TABLE Sales FIELDS TERMINATED BY ' '
 ENCLOSED BY '' ESCAPED BY '\\';
Query OK, 1 row affected (0.01 sec)
Records: 1  Deleted: 0  Skipped: 0  Warnings: 0
```

Para obtener más información sobre la instrucción `LOAD DATA`, consulte la instrucción LOAD DATA en la documentación de MySQL.

Paso 6: Activar las copias de seguridad automatizadas de Amazon RDS

Si desactiva las copias de seguridad automatizadas de Amazon RDS en el paso 4, una vez terminada la carga, active las copias de seguridad automatizadas estableciendo nuevamente el periodo de retención de copia de seguridad en el valor que había antes de la carga. Como se ha

indicado en el paso 4, Amazon RDS reinicia la instancia de base de datos, por lo que debe estar preparado para una breve interrupción del servicio.

El siguiente ejemplo ejecuta el comando modify-db-instance de la AWS CLI para activar las copias de seguridad automatizadas para la instancia de base de datos `AcmeRDS` y establecer el periodo de retención en un día:

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier AcmeRDS \
    --backup-retention-period 1 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --backup-retention-period 1 ^
    --apply-immediately
```

Uso de la replicación de MariaDB en Amazon RDS

Normalmente se utilizan réplicas de lectura para configurar la replicación entre instancias de base de datos de Amazon RDS. Para obtener información general acerca de las réplicas de lectura, consulte Trabajo con réplicas de lectura de instancias de base de datos. Para obtener información específica acerca de cómo utilizar las réplicas de lectura en Amazon RDS for MariaDB, consulte Uso de réplicas de lectura de MariaDB.

También puede configurar la replicación en función de las coordenadas de los registros binarios para las instancias de base de datos de MariaDB. Para las instancias de MariaDB, también puede configurar la replicación en función de los ID de transacción global (GTID), lo que proporciona más seguridad en caso de bloqueo. Para obtener más información, consulte Configuración de la replicación basada en GTID con una instancia de origen externa.

Estas opciones de replicación están disponibles con for MariaDB:

- Puede configurar la replicación entre una instancia de base de datos de RDS for MySQL o MariaDB y una instancia MySQL o MariaDB externa a Amazon RDS. Para obtener más información sobre cómo configurar la replicación con un origen externo, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.
- Puede configurar la replicación para importar bases de datos desde una instancia de MySQL o MariaDB externa a Amazon RDS o para exportar bases de datos a esas instancias. Para obtener más información, consulte Importación de datos a una instancia de base de datos de Amazon RDS para MariaDB con tiempo de inactividad reducido y Exportación de datos desde una instancia de base de datos MySQL mediante replicación.

Para cualquiera de estas opciones de replicación, puede utilizar replicación basada en filas, basada en instrucciones o mixta. La replicación basada en filas solo replica las filas cambiadas que resulten de una instrucción SQL. La replicación basada en instrucciones replica toda la instrucción SQL. La replicación mixta utiliza la replicación basada en instrucciones siempre que sea posible, pero alterna a la replicación basada en filas cuando se ejecutan las instrucciones SQL que no son seguras para la replicación basada en instrucciones. En la mayoría de los casos, se recomienda la replicación mixta. El formato de registro binario de la instancia de base de datos determina si la replicación se basa en filas, instrucciones o mixta. Para obtener información acerca de la configuración del formato de registro binario, consulte Configuración de registros binarios de MariaDB.

Para obtener información sobre la compatibilidad de replicación entre las versiones de MariaDB, consulte Replication Compatibility en la documentación de MariaDB.

Temas

- Uso de réplicas de lectura de MariaDB
- Configuración de la replicación basada en GTID con una instancia de origen externa
- Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Uso de réplicas de lectura de MariaDB

A continuación, encontrará información específica acerca de cómo utilizar las réplicas de lectura en Amazon RDS for MySQL. Para obtener información general sobre las réplicas de lectura e instrucciones sobre cómo usarlas, consulte Trabajo con réplicas de lectura de instancias de base de datos.

- Configuración de filtros de replicación con MariaDB
- Configuración de la replicación retrasada con MariaDB
- Eliminación de réplicas de lectura con MariaDB
- Implementaciones de réplicas de lectura Multi-AZ con MariaDB
- Uso de réplicas de lectura en cascada con RDS para MariaDB
- Monitoreo de réplicas de lectura de MariaDB
- Inicio y detención de replicaciones con réplicas de lectura de MariaDB
- Solución de problemas de una réplica de lectura de MariaDB

Eliminación de réplicas de lectura con MariaDB

Para que una instancia de base de datos de MariaDB pueda servir como origen de replicación, debe habilitar las copias de seguridad automáticas en la instancia de base de datos de origen estableciendo el periodo de retención de copia de seguridad en un valor distinto de 0. Este requisito también es válido para una réplica de lectura que sea la instancia de base de datos de origen de otra réplica de lectura.

Puede crear hasta 15 réplicas de lectura a partir de una instancia de base de datos de dentro de la misma región. Para que la replicación sea eficaz, cada réplica de lectura debe tener la misma cantidad de recursos informáticos y de almacenamiento que la instancia de base de datos de origen. Si modifica la escala de la instancia de base de datos de origen, debe ajustar también la escala de las réplicas de lectura.

RDS para MariaDB admite réplicas de lectura en cascada. Para obtener información sobre cómo configurar réplicas de lectura en cascada, consulte Uso de réplicas de lectura en cascada con RDS para MariaDB.

Puede ejecutar varias acciones de creación y eliminación de réplicas de lectura al mismo tiempo que hagan referencia a la misma instancia de base de datos de origen. Al realizar estas acciones, permanezca dentro del límite de 15 réplicas de lectura para cada instancia de origen.

Configuración de filtros de replicación con MariaDB

Puede utilizar filtros de replicación para especificar qué bases de datos y tablas se replican con una réplica de lectura. Los filtros de replicación pueden incluir bases de datos y tablas en la replicación o excluirlas de la replicación.

Los siguientes son algunos casos de uso para filtros de replicación:

- Para reducir el tamaño de una réplica de lectura. Con el filtrado de replicación, puede excluir las bases de datos y las tablas que no son necesarias en la réplica de lectura.
- Para excluir bases de datos y tablas de réplicas de lectura por razones de seguridad.
- Para replicar diferentes bases de datos y tablas para casos de uso específicos en diferentes réplicas de lectura. Por ejemplo, puede utilizar réplicas de lectura específicas para análisis o fragmentación.
- Con una instancia de base de datos que tiene réplicas de lectura en diferentes Regiones de AWS, para replicar diferentes bases de datos o tablas en diferentes regiones de Regiones de AWS.

> **Note**
>
> También puede utilizar filtros de reproducción para especificar qué bases de datos y tablas se reproducen con una instancia de base de datos primaria de MariaDB que está configurada como una réplica en una topología de reproducción entrante. Para obtener más información acerca de esta configuración, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

Temas

- Parámetros de filtrado de replicación con Amazon RDS for MariaDB
- Limitaciones del filtrado de replicación con for MariaDB

- Ejemplos de filtrado de replicación con for MariaDB
- Visualización de los filtros de replicación para una réplica de lectura

Parámetros de filtrado de replicación con Amazon RDS for MariaDB

Para configurar filtros de replicación, establezca los siguientes parámetros de filtrado de replicación en la réplica de lectura:

- `replicate-do-db` – Replicar los cambios en las bases de datos especificadas. Cuando se establece este parámetro para una réplica de lectura, solo se replican las bases de datos especificadas en el parámetro.
- `replicate-ignore-db` – No replicar los cambios en las bases de datos especificadas. Cuando el parámetro `replicate-do-db` se establece para una réplica de lectura, este parámetro no se evalúa.
- `replicate-do-table` – Replicar los cambios en las tablas especificadas. Cuando se establece este parámetro para una réplica de lectura, solo se replican las tablas especificadas en el parámetro. Además, cuando se establece el parámetro `replicate-do-db` o `replicate-ignore-db`, la base de datos que incluye las tablas especificadas debe incluirse en la replicación con la réplica de lectura.
- `replicate-ignore-table` – No replicar los cambios en las tablas especificadas. Cuando el parámetro `replicate-do-table` se establece para una réplica de lectura, este parámetro no se evalúa.
- `replicate-wild-do-table` – Replicar tablas en función de la base de datos y los patrones de nombre de tabla especificados. Se admiten los caracteres comodín `%` y `_`. Cuando se establece el parámetro `replicate-do-db` o `replicate-ignore-db`, asegúrese de incluir la base de datos que incluye las tablas especificadas en la replicación con la réplica de lectura.
- `replicate-wild-ignore-table` – No replicar tablas en función de la base de datos y los patrones de nombre de tabla especificados. Se admiten los caracteres comodín `%` y `_`. Cuando el parámetro `replicate-do-table` o `replicate-wild-do-table` se establece para una réplica de lectura, este parámetro no se evalúa.

Los parámetros se evalúan en el orden en que se enumeran. Para obtener más información sobre cómo funcionan estos parámetros, consulte la documentación de MariaDB.

Por defecto, cada uno de estos parámetros tiene un valor vacío. En cada réplica de lectura, puede utilizar estos parámetros para establecer, cambiar y eliminar los filtros de replicación. Cuando establezca uno de estos parámetros, separe cada filtro de los demás con una coma.

Puede utilizar los caracteres comodín `%` y `_` en los parámetros `replicate-wild-do-table` y `replicate-wild-ignore-table`. El comodín `%` coincide con cualquier número de caracteres y el comodín `_` solo coincide con un carácter.

El formato de registro binario de la instancia de base de datos de origen es importante para la replicación, ya que determina el registro de los cambios en los datos. La configuración del parámetro `binlog_format` determina si la replicación está basada en filas o en instrucciones. Para obtener más información, consulte Configuración de registros binarios de MariaDB.

> **Note**
>
> Todas las instrucciones de lenguaje de definición de datos (DDL) se replican como instrucciones, independientemente de la configuración de `binlog_format` en la instancia de base de datos de origen.

Limitaciones del filtrado de replicación con for MariaDB

Las siguientes limitaciones se aplican al filtrado de replicación con for MariaDB:

- Cada parámetro de filtrado de replicación tiene un límite de 2000 caracteres.
- Las comas no son compatibles con los filtros de replicación.
- Las opciones `binlog_do_db` y `binlog_ignore_db` de MariaDB para el filtrado de registros binarios no son compatibles.
- El filtrado de replicación no es compatible con transacciones XA.

  Para obtener más información, consulte Restricciones a las transacciones XA en la documentación de MySQL.
- No se admite el filtrado de reproducción con para MariaDB versión 10.2.

Ejemplos de filtrado de replicación con for MariaDB

Para configurar el filtrado de replicación para una réplica de lectura, modifique los parámetros de filtrado de replicación en el grupo de parámetros asociado a la réplica de lectura.

> **Note**
>
> No puede modificar un grupo de parámetros predeterminado. Si la réplica de lectura emplea un grupo de parámetros predeterminado, cree un nuevo grupo de parámetros y asócielo con la réplica de lectura. Para obtener más información acerca de los grupos de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.

Puede establecer parámetros en un grupo de parámetros mediante la API de RDS, AWS Management Console o AWS CLI. Para obtener información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS. Cuando se establecen parámetros en un grupo de parámetros, todas las instancias de base de datos asociadas al grupo de parámetros utilizan la configuración de los parámetros. Si establece los parámetros de filtrado de replicación en un grupo de parámetros, asegúrese de que el grupo de parámetros está asociado solo con réplicas de lectura. Deje los parámetros de filtrado de replicación vacíos para las instancias de base de datos de origen

En los siguientes ejemplos se establecen los parámetros mediante el uso de AWS CLI. Estos ejemplos establecen `ApplyMethod` en `immediate` para que los cambios de los parámetros se produzcan inmediatamente después de que se complete el comando de la CLI. Si desea que se aplique un cambio pendiente después de reiniciar la réplica de lectura, establezca `ApplyMethod` en `pending-reboot`.

Los siguientes ejemplos establecen filtros de replicación:

- Including databases in replication
- Including tables in replication
- Including tables in replication with wildcard characters
- Escaping wildcard characters in names
- Excluding databases from replication
- Excluding tables from replication
- Excluding tables from replication using wildcard characters

Example Inclusión de bases de datos en la replicación

En el ejemplo siguiente se incluyen las bases de datos `mydb1` y `mydb2` en la replicación. Cuando se establece `replicate-do-db` para una réplica de lectura, solo se replican las bases de datos especificadas en el parámetro.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-do-db", "ParameterValue": "mydb1,mydb2",
 "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "[{"ParameterName": "replicate-do-db", "ParameterValue": "mydb1,mydb2",
 "ApplyMethod":"immediate"}]"
```

Example Inclusión de tablas en la replicación

En el siguiente ejemplo se incluyen las tablas `table1` y `table2` en la base de datos `mydb1` en la replicación.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-do-table", "ParameterValue":
 "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "[{"ParameterName": "replicate-do-table", "ParameterValue":
 "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

Example Inclusión de tablas en la replicación mediante el uso de caracteres comodín

En el ejemplo siguiente se incluyen tablas con nombres que empiezan con `orders` y `returns` en la base de datos `mydb` en la replicación.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue":
 "mydb.orders%,mydb.returns%", "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue":
 "mydb.orders%,mydb.returns%", "ApplyMethod":"immediate"}]"
```

Example Escape de caracteres comodín en nombres

En el siguiente ejemplo se muestra cómo utilizar el carácter de escape \ para aplicar el escape de un carácter comodín que forma parte de un nombre.

Supongamos que tiene varios nombres de tabla en la base de datos `mydb1` que comienzan con `my_table` y desea incluir estas tablas en la replicación. Los nombres de tabla incluyen un guion bajo, que también es un carácter comodín, por lo que el ejemplo aplica el escape al guion bajo en los nombres de tabla.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "my
\_table%", "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
```

```
  --parameters "[{"ParameterName": "replicate-wild-do-table", "ParameterValue": "my
\_table%", "ApplyMethod":"immediate"}]"
```

Example Exclusión de bases de datos de la replicación

En el siguiente ejemplo se excluyen las bases de datos `mydb1` y `mydb2` de la replicación.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-ignore-db", "ParameterValue":
 "mydb1,mydb2", "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "[{"ParameterName": "replicate-ignore-db", "ParameterValue":
 "mydb1,mydb2", "ApplyMethod":"immediate"}]"
```

Example Exclusión de tablas de la replicación

En el siguiente ejemplo se excluyen las tablas `table1` y `table2` en la base de datos `mydb1` de la replicación.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-ignore-table", "ParameterValue":
 "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "[{"ParameterName": "replicate-ignore-table", "ParameterValue":
 "mydb1.table1,mydb1.table2", "ApplyMethod":"immediate"}]"
```

Example Exclusión de tablas de la replicación mediante el uso de caracteres comodín

En el siguiente ejemplo se excluyen las tablas con nombres que empiezan con `orders` y `returns` en la base de datos `mydb` de la replicación.

Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "[{"ParameterName": "replicate-wild-ignore-table", "ParameterValue":
 "mydb.orders%,mydb.returns%", "ApplyMethod":"immediate"}]"
```

En:Windows

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "[{"ParameterName": "replicate-wild-ignore-table", "ParameterValue":
 "mydb.orders%,mydb.returns%", "ApplyMethod":"immediate"}]"
```

Visualización de los filtros de replicación para una réplica de lectura

Puede ver los filtros de replicación para una réplica de lectura de las siguientes maneras:

- Verifique la configuración de los parámetros de filtrado de replicación en el grupo de parámetros asociado a la réplica de lectura.

  Para obtener instrucciones, consulte Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS.
- En un cliente de MariaDB, conéctese a la réplica de lectura y ejecute la instrucción `SHOW REPLICA STATUS`.

  En la salida, los siguientes campos muestran los filtros de replicación para la réplica de lectura:

  - `Replicate_Do_DB`
  - `Replicate_Ignore_DB`
  - `Replicate_Do_Table`
  - `Replicate_Ignore_Table`
  - `Replicate_Wild_Do_Table`

- `Replicate_Wild_Ignore_Table`

Para obtener más información acerca de estos campos, consulte Comprobación del estado de replicación en la documentación de MySQL.

> **Note**
>
> Versiones anteriores de MariaDB utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MariaDB anterior a la 10.5, utilice `SHOW SLAVE STATUS`.

Configuración de la replicación retrasada con MariaDB

Puede utilizar la replicación retrasada como estrategia de recuperación de desastres. Con la replicación retardada, se especifica el tiempo mínimo, en segundos, que se retardará la replicación desde la instancia de origen a la réplica de lectura. En caso de desastre, por ejemplo, si se elimina una tabla involuntariamente, el procedimiento siguiente permite recuperarse rápidamente del desastre:

- Detenga la replicación en la réplica de lectura antes de que se envíe a ella el cambio que provocó el desastre.

  Para detener la replicación, utilice el procedimiento almacenado mysql.rds_stop_replication.
- Promocione la réplica de lectura para que sea la nueva instancia de base de datos de origen; para ello, siga las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

> **Note**
>
> - La replicación retrasada es compatible con MariaDB 10.6 y versiones posteriores.
> - Use procedimientos almacenados para configurar la replicación retardada. La reproducción retrasada no se puede configurar con la AWS Management Console, la AWS CLI o la API de Amazon RDS.
> - Puede usar la replicación basada en identificadores de transacciones globales (GTID) en una configuración de replicación retrasada.

Temas

- Configuración de la replicación retrasada durante la creación de réplicas de lectura
- Modificación de la replicación retrasada para una réplica de lectura existente
- Promoción de una réplica de lectura

Configuración de la replicación retrasada durante la creación de réplicas de lectura

Para configurar la replicación retardada para cualquier réplica de lectura futura creada a partir de una instancia de base de datos, ejecute el procedimiento almacenado mysql.rds_set_configuration con el parámetro `target delay`.

Para configurar la replicación retardada durante la creación de réplicas de lectura

1. Utilice un cliente de MariaDB para conectarse como usuario maestro a la instancia de base de datos MariaDB que vaya a ser el origen de las réplicas de lectura.
2. Ejecute el procedimiento almacenado mysql.rds_set_configuration con el parámetro `target delay`.

   Por ejemplo, ejecute el siguiente procedimiento almacenado para especificar que la replicación se retardará al menos una hora (3600 segundos) para todas las réplicas de lectura creadas desde la instancia de base de datos actual.

   ```
   call mysql.rds_set_configuration('target delay', 3600);
   ```

   > **Note**
   >
   > Después de ejecutar este procedimiento almacenado, todas las réplicas de lectura que cree mediante la AWS CLI o la API de Amazon RDS se configurarán con la reproducción retardada el número de segundos especificado.

Modificación de la replicación retrasada para una réplica de lectura existente

Para modificar la replicación retardada para una réplica de lectura existente, ejecute el procedimiento almacenado mysql.rds_set_source_delay.

Para modificar la replicación retardada de una réplica de lectura existente

1. Use un cliente de MariaDB para conectarse como usuario maestro a la réplica de lectura.
2. Utilice el procedimiento almacenado mysql.rds_stop_replication para detener la replicación.
3. Ejecute el procedimiento almacenado mysql.rds_set_source_delay.

   Por ejemplo, ejecute el siguiente procedimiento almacenado para especificar que la replicación en la réplica de lectura se retardará al menos una hora (3600 segundos).

   ```
   call mysql.rds_set_source_delay(3600);
   ```
4. Utilice el procedimiento almacenado mysql.rds_start_replication para iniciar la replicación.

Promoción de una réplica de lectura

Después de que se detenga la replicación, en una situación de recuperación de desastres, puede promocionar una réplica de lectura para que sea la nueva instancia de base de datos de origen. Para obtener información acerca de la promoción de una réplica de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Eliminación de réplicas de lectura con MariaDB

Las réplicas de lectura se han diseñado para permitir las consultas de lectura, pero puede necesitar actualizaciones ocasionales. Por ejemplo, puede necesitar añadir un índice para acelerar los tipos concretos de consultas que obtienen acceso a la réplica. Puede habilitar las actualizaciones estableciendo el parámetro `read_only` en 0 en el grupo de parámetros de base de datos para la réplica de lectura.

Implementaciones de réplicas de lectura Multi-AZ con MariaDB

Puede crear una réplica de lectura a partir de implementaciones de instancia de base de datos Single-AZ o Multi-AZ. Puede usar implementaciones Multi-AZ para mejorar la durabilidad y la disponibilidad de los datos críticos, pero no puede usar la implementación Multi-AZ secundaria para responder a consultas de solo lectura. En lugar de ello, puede crear réplicas de lectura a partir de una instancia de base de datos Multi-AZ con un tráfico elevado para descargar las consultas de solo lectura. Si la instancia de origen de una implementación Multi-AZ conmuta a la secundaria, las réplicas de lectura asociadas cambian automáticamente para usar la secundaria (ahora principal) como origen de replicación. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Puede crear una réplica de lectura como instancia de base de datos de Multi-AZ. Amazon RDS crea una réplica en espera en otra zona de disponibilidad para permitir la conmutación por error de la réplica. La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.

Uso de réplicas de lectura en cascada con RDS para MariaDB

RDS para MariaDB admite réplicas de lectura en cascada. Con réplicas de lectura en cascada, puede escalar las lecturas sin agregar sobrecarga a su instancia de base de datos de RDS para MariaDB de origen.

Con réplicas de lectura en cascada, la instancia de base de datos de RDS para MariaDB envía datos a la primera réplica de lectura de la cadena. Esa réplica de lectura envía datos a la segunda réplica de la cadena, etc. El resultado final es que todas las réplicas de lectura de la cadena tienen los cambios de la instancia de base de datos de RDS para MariaDB, pero sin la sobrecarga únicamente en la instancia de base de datos de origen.

Puede crear una serie de hasta tres réplicas de lectura en cadena a partir de una instancia de base de datos RDS para MariaDB de origen. Por ejemplo, suponga que tiene una instancia de base de datos de RDS para MariaDB, `mariadb-main`. Puede hacer lo siguiente:

- A partir de `mariadb-main`, cree la primera réplica de lectura de la cadena, `read-replica-1`.
- A continuación, a partir de `read-replica-1`, cree la siguiente réplica de lectura de la cadena, `read-replica-2`.
- Por último, a partir de `read-replica-2`, cree la tercera réplica de lectura de la cadena, `read-replica-3`.

No se puede crear otra réplica de lectura más allá de esta tercera réplica de lectura en cascada de la serie para `mariadb-main`. Una serie completa de instancias desde una instancia de base de datos de origen de RDS para MariaDB hasta el final de una serie de réplicas de lectura en cascada puede constar de cuatro instancias de base de datos como máximo.

Para que las réplicas de lectura en cascada funcionen, cada instancia de origen de RDS para MariaDB debe tener las copias de seguridad automáticas activadas. Para habilitar las copias de seguridad automáticas en una réplica de lectura, primero debe crear la réplica de lectura y modificarla a continuación para habilitar las copias de seguridad automáticas. Para obtener más información, consulte Creación de una réplica de lectura.

Al igual que con cualquier réplica de lectura, puede promocionar una réplica de lectura que forma parte de una cascada. La promoción de una réplica de lectura desde dentro de una cadena de réplicas de lectura elimina esa réplica de la cadena. Por ejemplo, suponga que desea trasladar parte de la carga de trabajo de su Instancia de base de datos de `mariadb-main` a una nueva instancia para que la utilice únicamente el departamento de contabilidad. Tomando la cadena de tres réplicas de lectura del ejemplo, decide promocionar `read-replica-2`. La cadena se ve afectada de la siguiente manera:

- Promover `read-replica-2` la elimina de la cadena de replicación.
  - Ahora es una instancia de base de datos de lectura o escritura completa.
  - Continúa replicando en `read-replica-3`, tal como hacía antes de la promoción.
- Su `mariadb-main` sigue replicándose en `read-replica-1`.

Para obtener más información acerca de la promoción de réplicas de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Monitoreo de réplicas de lectura de MariaDB

Para las réplicas de lectura de MariaDB, puede monitorear el retraso de replicación en Amazon CloudWatch mediante la visualización de la métrica `ReplicaLag` de Amazon RDS. La métrica `ReplicaLag` indica el valor del campo `Seconds_Behind_Master` del comando `SHOW REPLICA STATUS`.

> **Note**
>
> Versiones anteriores de MariaDB utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MariaDB anterior a la 10.5, utilice `SHOW SLAVE STATUS`.

Los motivos comunes de retardo de la replicación para MariaDB son los siguientes:

- Una interrupción de la red.
- Escritura en tablas con índices en una réplica de lectura. Si el parámetro `read_only` no se ha establecido en 0 en la réplica de lectura, puede interrumpirse la replicación.
- Uso de un motor de almacenamiento no transaccional como MyISAM. La reproducción solo se admite para el motor de almacenamiento InnoDB en MariaDB.

Cuando la métrica `ReplicaLag` llegue a 0, la réplica estará funcionando al mismo ritmo que la instancia de base de datos de origen. Si la métrica `ReplicaLag` devuelve -1, la replicación no está activa. `ReplicaLag` = -1 es equivalente a `Seconds_Behind_Master` = `NULL`.

Inicio y detención de replicaciones con réplicas de lectura de MariaDB

Puede detener y reiniciar el proceso de replicación en una instancia de base de datos de Amazon RDS llamando a los procedimientos mysql.rds_stop_replication y mysql.rds_start_replication almacenados en el sistema. Puede hacerlo cuando replique entre dos instancias de Amazon RDS para las operaciones de larga duración, como la creación de índices grandes. También debe detener y comenzar la replicación cuando importe o exporte bases de datos. Para obtener más información, consulte Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido y Exportación de datos desde una instancia de base de datos MySQL mediante replicación.

Si la replicación se detiene durante más de 30 días consecutivos, ya sea manualmente o a causa de un error de replicación, Amazon RDS termina la replicación entre la instancia de base de datos de origen y todas las réplicas de lectura. Realiza ese procedimiento para impedir que aumenten los requisitos de almacenamiento en la instancia de base de datos de origen y que se incrementen los tiempos de conmutación por error. La instancia de base de datos de la réplica de lectura seguirá estando disponible. Sin embargo, la replicación no se podrá reanudar porque los registros binarios requeridos por la réplica de lectura se eliminan de la instancia de base de datos de origen cuando finaliza la replicación. Puede crear una nueva réplica de lectura para la instancia de base de datos de origen si desea restablecer la replicación.

Solución de problemas de una réplica de lectura de MariaDB

Las tecnologías de replicación para MariaDB son asíncronas. Como son asíncronas, cabe esperar aumentos ocasionales de `BinLogDiskUsage` en la instancia de base de datos de origen y de `ReplicaLag` en la réplica de lectura. Por ejemplo, en paralelo se pueden realizar gran volumen de operaciones de escritura en la instancia de base de datos de origen. En cambio, las operaciones de escritura en la réplica de lectura se serializan con un único subproceso E/S que puede provocar un retraso entre la instancia de origen y la réplica de lectura. Para obtener más información acerca de las réplicas de solo lectura en la documentación de MariaDB, vaya a Replication Overview.

Puede hacer varias cosas para reducir el retraso entre las actualizaciones de una instancia de base de datos de origen y las actualizaciones posteriores de la réplica de lectura. Por ejemplo, puede hacer lo siguiente:

- Dimensionar una réplica de lectura para que tenga un tamaño de almacenamiento y una clase de instancia de base de datos comparables a los de la instancia de base de datos de origen.
- Asegurarse de que los valores de los parámetros de los grupos de parámetros de base de datos utilizados en la instancia de base de datos de origen y la réplica de lectura son compatibles. Para obtener más información y un ejemplo, consulte el análisis del parámetro `max_allowed_packet` que se puede encontrar más adelante en esta sección.

Amazon RDS monitorea el estado de la replicación de las réplicas de lectura y actualiza el campo `Replication State` de la instancia de la réplica de lectura a `Error` si la replicación se detiene por cualquier motivo. Un ejemplo de ello pueden ser las consultas DML que se ejecutan en la réplica de lectura y que entran en conflicto con las actualizaciones realizadas en la instancia de base de datos de origen.

Puede revisar los detalles del error asociado mostrado por el motor de MariaDB visualizando el campo `Replication Error`. También se generan eventos que indican el estado de la réplica de lectura, entre los que se incluyen RDS-EVENT-0045, RDS-EVENT-0046 y RDS-EVENT-0047. Para obtener más información acerca de los eventos y la suscripción a ellos, consulte Uso de notificaciones de eventos de Amazon RDS. Si aparece un mensaje de error de MariaDB, revise el error en la documentación sobre los mensajes de error de MariaDB.

Un problema frecuente que puede causar errores de replicación es que el valor del parámetro `max_allowed_packet` de una réplica de lectura sea inferior al parámetro `max_allowed_packet` de la instancia de base de datos de origen. El parámetro `max_allowed_packet` es un parámetro personalizado que se puede establecer en un grupo de parámetros de base de datos y que se usa para especificar el tamaño máximo del código DML que se puede ejecutar en la base de datos. En algunos casos, el valor del parámetro `max_allowed_packet` en el grupo de parámetros de base de datos asociado a una instancia de base de datos de origen es inferior al valor del parámetro `max_allowed_packet` del grupo de parámetros de base de datos asociado a la réplica de lectura de origen. En estos casos, el proceso de replicación puede provocar un error (paquete mayor que los bytes de "max_allowed_packet") y parar la replicación. Puede resolver el error haciendo que el origen y la réplica de lectura usen grupos de parámetros de base de datos con los mismos valores del parámetro `max_allowed_packet`.

Entre las situaciones comunes que pueden causar errores de replicación se incluyen las siguientes:

- Escritura en tablas en una réplica de lectura. Si desea crear índices en una réplica de lectura, debe establecer el parámetro `read_only` en 0 para crear los índices. Si se escribe en las tablas de la réplica de lectura, podría interrumpirse la replicación.

- Uso de un motor de almacenamiento no transaccional como MyISAM. Las réplicas de lectura requieren un motor de almacenamiento transaccional. La reproducción solo se admite para el motor de almacenamiento InnoDB en MariaDB.
- Uso de consultas no deterministas que no sean seguras, como `SYSDATE()`. Para obtener más información, consulte Determinación de instrucciones seguras e inseguras en el registro binario.

Si decide que es seguro hacer caso omiso de un error, puede seguir los pasos que se describen en la sección Omisión del error de replicación actual de RDS para MySQL. De lo contrario, puede eliminar la réplica de lectura y crear una instancia que use el mismo identificador de instancias de bases de datos para que el punto de enlace siga siendo el mismo que en la réplica de lectura antigua. Si se corrige un error de replicación, `Replication State` cambia a replicating.

Para las instancias de base de datos de MariaDB, en algunos casos las réplicas de lectura no se pueden cambiar a la secundaria si algunos eventos de binlog no se vacían durante el error. En estos casos, elimine y vuelva a crear manualmente las réplicas de lectura. Puede reducir la probabilidad de que esto ocurra al establecer los siguientes valores de parámetro: `sync_binlog=1` y `innodb_flush_log_at_trx_commit=1`. Estos ajustes pueden reducir el desempeño, así que es aconsejable probar su impacto antes de implementar los cambios en un entorno de producción.

Configuración de la replicación basada en GTID con una instancia de origen externa

Se puede configurar la reproducción basada en identificadores de transacciones globales (GTID) desde una instancia de MariaDB externa de una versión 10.0.24 o posterior en una instancia de base de datos MariaDB. Siga estas directrices al configurar una instancia de origen externa y una réplica en Amazon RDS:

- Monitorice los eventos de conmutación por error para la instancia de base de datos de for MariaDB que sea su réplica. Si se produce una conmutación por error, la instancia de base de datos que es la réplica se puede volver a crear en un nuevo host con una dirección de red diferente. Para obtener información acerca de la monitorización de los eventos de conmutación por error, consulte Uso de notificaciones de eventos de Amazon RDS.
- Mantenga los registros binarios (binlogs) en la instancia de origen hasta que haya verificado que se han aplicado en la réplica. Este mantenimiento garantiza que puede restaurar la instancia de origen en caso de error.
- Active las copias de seguridad automatizadas en su instancia de base de datos de MariaDB en Amazon RDS. La activación de las copias de seguridad automatizadas garantiza que puede

restaurar su réplica a un momento dado si necesita volver a sincronizar la instancia de origen y la réplica. Para obtener información acerca de las copias de seguridad y la restauración a un momento dado, consulte Copia de seguridad, restauración y exportación de datos.

> **Note**
>
> Los permisos requeridos para comenzar la replicación en una instancia de base de datos MariaDB están restringidos y no están disponibles para el usuario maestro Amazon RDS. Por este motivo, debe usar los comandos Amazon RDS, mysql.rds_set_external_master_gtid y mysql.rds_start_replication para configurar la replicación entre su base de datos en funcionamiento y su base de datos de Amazon RDS for MariaDB.

Para iniciar la replicación entre una instancia de origen externa y una instancia de base de datos de MariaDB en Amazon RDS, utilice el siguiente procedimiento.

Para iniciar la replicación

1. Configure la instancia de MariaDB de origen como de solo lectura:

   ```
   mysql> FLUSH TABLES WITH READ LOCK;
   mysql> SET GLOBAL read_only = ON;
   ```

2. Obtenga el GTID actual de la instancia de MariaDB externa. Puede hacerlo usando `mysql` o el editor de consultas que prefiera para ejecutar `SELECT @@gtid_current_pos;`.

   El GTID tiene el formato `<domain-id>-<server-id>-<sequence-id>`. Un GTID típico tiene un aspecto similar a **`0-1234510749-1728`**. Para obtener más información acerca de los GTID y sus componentes, consulte Global Transaction ID en la documentación de MariaDB.

3. Copie la base de datos de la instancia de MariaDB externa en la instancia de base de datos de MariaDB co `mysqldump`. Para las bases de datos muy grandes, puede usar el procedimiento que se describe en Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido.

   Para Linux, macOS o Unix:

   ```
   mysqldump \
       --databases database_name \
       --single-transaction \
   ```

```
    --compress \
    --order-by-primary \
    -u local_user \
    -plocal_password | mysql \
        --host=hostname \
        --port=3306 \
        -u RDS_user_name \
        -pRDS_password
```

Para Windows:

```
mysqldump ^
    --databases database_name ^
    --single-transaction ^
    --compress ^
    --order-by-primary \
    -u local_user \
    -plocal_password | mysql ^
        --host=hostname ^
        --port=3306 ^
        -u RDS_user_name ^
        -pRDS_password
```

> **Note**
>
> Asegúrese de que no haya ningún espacio entre la opción `-p` y la contraseña que haya escrito.
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Use las opciones `--host`, `--user (-u)`, `--port` y `-p` del comando `mysql` para especificar el nombre de host, el nombre de usuario, el puerto y la contraseña para conectarse a la instancia de base de datos MariaDB. El nombre de host es el nombre de DNS tomado del punto de enlace de la instancia de base de datos MariaDB, por ejemplo `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de enlace en los detalles de la instancia en la consola de administración de Amazon RDS.

4. Haga que la instancia de MariaDB de origen vuelva a admitir la escritura.

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

5. En la consola de administración Amazon RDS, agregue la dirección IP del servidor que aloja la base de datos MariaDB externa en el grupo de seguridad de VPC de la instancia de base de datos MariaDB. Para obtener más información acerca de la modificación de un grupo de seguridad de VPC, vaya a Grupos de seguridad de su VPC en la Guía del usuario de Amazon Virtual Private Cloud.

   La dirección IP puede cambiar cuando se cumplen las siguientes condiciones:

   - Está usando una dirección IP pública para la comunicación entre la instancia de origen externa y la instancia de base de datos.
   - La instancia de origen externa se detuvo y se reinició.

   Si se cumplen esas condiciones, compruebe la dirección IP antes de añadirla.

   Es posible que también necesite configurar la red local para permitir las conexiones desde la dirección IP de la instancia de base de datos MariaDB, para que pueda comunicarse con la instancia de MariaDB externa. Para encontrar la dirección IP de la instancia de base de datos MariaDB, use el comando `host`.

   ```
   host db_instance_endpoint
   ```

   El nombre de host es el nombre de DNS tomado del punto de enlace de la instancia de base de datos MariaDB.

6. Con el cliente que prefiera, conéctese a la instancia de MariaDB externa y cree un usuario de MariaDB que se usará para la replicación. Esta cuenta se usa únicamente para la replicación y debe estar limitada a su dominio para mejorar la seguridad. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

7. Para la instancia de MariaDB externa, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. Por ejemplo, para conceder los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario "`repl_user`" del dominio, ejecute el siguiente comando.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

8. Defina la instancia de base de datos MariaDB como réplica. Conéctese a la instancia de base de datos MariaDB como usuario maestro e identifique la base de datos MariaDB externa como instancia de origen de replicación mediante el comando mysql.rds_set_external_master_gtid. Use el GTID que determinó en el paso 2. A continuación se muestra un ejemplo.

```
CALL mysql.rds_set_external_master_gtid ('mymasterserver.mydomain.com', 3306,
 'repl_user', 'password', 'GTID', 1);
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

9. En la instancia de base de datos MariaDB, ejecute el comando mysql.rds_start_replication para comenzar la replicación:

```
CALL mysql.rds_start_replication;
```

Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Puede configurar la replicación entre una instancia de base de datos de RDS for MySQL o MariaDB y una instancia MySQL o MariaDB externa a Amazon RDS.

Temas

- Antes de empezar
- Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Antes de empezar

Puede configurar la replicación usando la posición de los archivos de registro binarios de transacciones replicadas.

Los permisos requeridos para comenzar la replicación en una instancia de base de datos de Amazon RDS están restringidos y no están disponibles para el usuario maestro de Amazon RDS. Por este motivo, asegúrese de usar los comandos mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) o mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) y mysql.rds_start_replication de Amazon RDS para configurar la replicación entre la base de datos en funcionamiento y la base de datos de Amazon RDS.

Para establecer el formato de registro binario para una base de datos MySQL o MariaDB, actualice el parámetro `binlog_format`. Si su instancia de base de datos usa el grupo de parámetros de instancia de base de datos predeterminado, cree un nuevo grupo de parámetros de base de datos para modificar el parámetro `binlog_format`. En MariaDB y MySQL 8.0 y versiones anteriores, el valor predeterminado de `binlog_format` es `MIXED`. Sin embargo, también puede configurar `binlog_format` como `ROW` o `STATEMENT` si necesita un formato de registro binario (binlog) concreto. Reinicie la instancia de base de datos para que el cambio entre en vigor. En MySQL 8.4 y versiones posteriores, el valor predeterminado de `binlog_format` es `ROW`.

Para obtener más información sobre configurar el parámetro `binlog_format`, consulte Configuración del registro binario de RDS para MySQL para bases de datos de Single-AZ. Para obtener más información acerca de las implicaciones de distintos tipos de replicación de MySQL, consulte Advantages and Disadvantages of Statement-Based and Row-Based Replication en la documentación de MySQL.

Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Siga estas directrices al configurar una instancia de origen externa y una réplica en Amazon RDS:

- Monitorice los eventos de conmutación por error para la instancia de base de datos de Amazon RDS que usa como réplica. Si se produce una conmutación por error, la instancia de base de datos que es la réplica se puede volver a crear en un nuevo host con una dirección de red diferente. Para obtener información acerca de la monitorización de los eventos de conmutación por error, consulte Uso de notificaciones de eventos de Amazon RDS.
- Mantenga los binlogs en la instancia de origen hasta que haya verificado que se han aplicado a la réplica. Este mantenimiento garantiza que se pueda restaurar la instancia de origen en caso de error.
- Active las copias de seguridad automatizadas para la instancia de base de datos de Amazon RDS. La activación de las copias de seguridad automatizadas garantiza que puede restaurar su réplica a un momento dado si necesita volver a sincronizar la instancia de origen y la réplica. Para obtener información acerca de las copias de seguridad y la restauración a un momento dado, consulte Copia de seguridad, restauración y exportación de datos.

Para configurar la replicación de archivos de registro binario con una instancia de origen externa

1. Configure la instancia de base de datos MySQL o MariaDB de origen como de solo lectura.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Ejecute el comando `SHOW MASTER STATUS` en la instancia de base de datos MySQL o MariaDB para determinar la ubicación del binlog.

   Se recibe un resultado similar al del siguiente ejemplo.

```
File                          Position
------------------------------------
 mysql-bin-changelog.000031      107
------------------------------------
```

3. Copie la base de datos de la instancia externa a la instancia de Amazon RDS con `mysqldump`. Para las bases de datos muy grandes, puede usar el procedimiento que se describe en Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido.

   Para Linux, macOS o Unix:

```
mysqldump --databases database_name \
```

```
    --single-transaction \
    --compress \
    --order-by-primary \
    -u local_user \
    -plocal_password | mysql \
        --host=hostname \
        --port=3306 \
        -u RDS_user_name \
        -pRDS_password
```

Para Windows:

```
mysqldump --databases database_name ^
    --single-transaction ^
    --compress ^
    --order-by-primary ^
    -u local_user ^
    -plocal_password | mysql ^
        --host=hostname ^
        --port=3306 ^
        -u RDS_user_name ^
        -pRDS_password
```

> **Note**
>
> Asegúrese de que no haya ningún espacio entre la opción `-p` y la contraseña que haya escrito.

Para especificar el nombre de host, el nombre de usuario, el puerto y la contraseña para conectarse a su instancia de base de datos en Amazon RDS, use las opciones `--host`, `--user (-u)`, `--port` y `-p` en el comando `mysql`. El nombre de host es el nombre del servicio de nombre de dominio (DNS) tomado del punto de enlace de la instancia de base de datos de Amazon RDS, por ejemplo, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la instancia en la AWS Management Console.

4. Haga que la instancia MySQL o MariaDB de origen vuelvan a admitir la escritura.

```
mysql> SET GLOBAL read_only = OFF;
```

```
mysql> UNLOCK TABLES;
```

Para obtener más información sobre cómo hacer copias de seguridad para su uso con replicación, consulte la documentación de MySQL.

5. En la AWS Management Console, agregue la dirección IP del servidor que aloja la base de datos externa al grupo de seguridad de la nube virtual privada (VPC) para la instancia de base de datos de Amazon RDS. Para obtener más información acerca de la modificación de un grupo de seguridad de VPC, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon Virtual Private Cloud.

   La dirección IP puede cambiar cuando se cumplen las siguientes condiciones:

   - Está usando una dirección IP pública para la comunicación entre la instancia de origen externa y la instancia de base de datos.
   - La instancia de origen externa se detuvo y se reinició.

   Si se cumplen esas condiciones, compruebe la dirección IP antes de añadirla.

   Es posible que también necesite configurar su red local para permitir las conexiones desde la dirección IP de la instancia de base de datos de Amazon RDS. Eso se hace para que la red local se pueda comunicar con la instancia de MySQL o MariaDB externa. Para encontrar la dirección IP de la instancia de base de datos de Amazon RDS, use el comando `host`.

   ```
   host db_instance_endpoint
   ```

   El nombre de host es el nombre de DNS tomado del punto de conexión de la instancia de base de datos de Amazon RDS.

6. Con el cliente que prefiera, conecte con la instancia externa y cree un usuario para la replicación. Use esta cuenta únicamente para la replicación y limítela a su dominio para mejorar la seguridad. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

7. Para la instancia externa, conceda los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` al usuario de replicación. Por ejemplo, para conceder los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario "`repl_user`" del dominio, ejecute el siguiente comando.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

8. Defina la instancia de base de datos de Amazon RDS como réplica, Para ello, en primer lugar, conéctese a la instancia de base de datos de Amazon RDS como usuario maestro. A continuación, identifique la base de datos de MySQL o MariaDB externa como instancia de origen usando el comando mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) o mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores). Use el nombre del archivo de registro maestro y la posición del registro maestro que determinó en el paso 2. Los siguientes comandos son ejemplos.

   MySQL 8.4

```
CALL mysql.rds_set_external_source ('mysourceserver.mydomain.com', 3306,
 'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
```

   MariaDB y MySQL 8.0 y 5.7

```
CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306,
 'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
```

> **Note**
>
> En RDS para MySQL, puede aplicar la replicación retrasada si lo desea ejecutando el procedimiento mysql.rds_set_external_source_with_delay (RDS para las versiones principales de MySQL 8.4 y superiores) o mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e

inferiores) almacenado en su lugar. Un motivo para usar la replicación retrasada en RDS para MySQL es activar la recuperación de desastres con el procedimiento almacenado mysql.rds_start_replication_until. En la actualidad, RDS para MariaDB es compatible con la replicación retrasada, pero no con el procedimiento `mysql.rds_start_replication_until`.

9. En la instancia de base de datos de Amazon RDS, ejecute el comando mysql.rds_start_replication para comenzar la replicación.

```
CALL mysql.rds_start_replication;
```

Opciones para el motor de base de datos de MariaDB

A continuación, se incluyen descripciones de las opciones, o características adicionales, que están disponibles para las instancias de Amazon RDS que ejecutan el motor de base de datos MariaDB. Para activar estas opciones, puede agregarlas a un grupo de opciones personalizado y, a continuación, asociar el grupo de opciones a la instancia de base de datos. Para obtener más información acerca de cómo trabajar con grupos de opciones, consulte Trabajo con grupos de opciones.

Amazon RDS admite las siguientes opciones para MariaDB:

ID de la opción	Versiones del motor
`MARIADB_AUDIT_PLUGIN`	MariaDB 10.3 y posteriores

Compatibilidad con el complemento de auditoría MariaDB

Amazon RDS permite utilizar el complemento de auditoría de MariaDB en las instancias de base de datos de MariaDB. El complemento de auditoría de MariaDB registra la actividad de la base de datos, como el registro de los usuarios en la base de datos, las consultas ejecutadas en la base de datos, etc. El registro de la actividad de la base de datos se almacena en un archivo de registro.

Configuración de opciones del complemento de auditoría

Amazon RDS admite la siguiente configuración para la opción del complemento de auditoría de MariaDB.

> **Note**
>
> Si no configura una opción en la consola de RDS, RDS utilizará la configuración predeterminada.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_FILE_PATH	/rdsdbdata/log/audit/	/rdsdbdata/log/audit/	La ubicación del archivo de registro. El archivo de registro contiene el registro de la actividad especificada en SERVER_AUDIT_EVENTS . Para obtener más información, consulte Visualización y descripción de archivos de registro de base de datos y Archivos de registro de base de datos de MariaDB.
SERVER_AUDIT_FILE_ROTATE_SIZE	1–1 000 000 000	1000000	El tamaño en bytes que, al alcanzarse, hace que se rote el archivo. Para obtener más información, consulte Rotación y retención de registros para MariaDB.
SERVER_AUDIT_FILE_ROTATIONS	0–100	9	Es el número de rotaciones de registro que se debe guardar cuando server_audit_output_type=file . Si se establece en 0, el archivo de registro no gira nunca. Para obtener más información, consulte Rotación y retención de registros para MariaDB y Descarga de un archivo de registro de base de datos.
SERVER_AUDIT_EVENTS	CONNECT, QUERY, TABLE, QUERY_DDL , QUERY_DML , QUERY_DML_NO_SELECT , QUERY_DCL	CONNECT, QUERY	Los tipos de actividad que se van a registrar en el registro. La instalación del complemento de auditoría de MariaDB también se registra. • CONNECT: registra las conexiones a la base de datos completadas y no completadas y también las desconexiones. • QUERY: registra el texto de todas las consultas que se ejecutan en la base de datos.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
			• TABLE: registra las tablas afectadas por las consultas cuando estas se ejecutan en la base de datos. • QUERY_DDL : similar al evento QUERY, pero solo devuelve consultas en lenguaje de definición de datos (DDL) (CREATE, ALTER, etc.). • QUERY_DML : similar al evento QUERY, pero solo devuelve consultas en lenguaje de manipulación de datos (DML) (INSERT, UPDATE, etc. y también SELECT). • QUERY_DML_NO_SELECT : similar al evento QUERY_DML , pero no registra consultas SELECT. • QUERY_DCL : similar al evento QUERY, pero solo devuelve consultas en lenguaje de control de datos (DCL) (GRANT, REVOKE, etc.).
SERVER_AUDIT_INCL_USERS	Varios valores separados por comas	Ninguno	Incluya solo la actividad de los usuarios especificados. De forma predeterminada, la actividad se registra para todos los usuarios. SERVER_AUDIT_INCL_USERS y SERVER_AUDIT_EXCL_USERS se excluyen mutuamente. Si agrega valores a SERVER_AUDIT_INCL_USERS , asegúrese de que no se agregan valores a SERVER_AUDIT_EXCL_USERS .

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_EXCL_USERS	Varios valores separados por comas	Ninguno	Excluya la actividad de los usuarios especificados. De forma predeterminada, la actividad se registra para todos los usuarios. SERVER_AUDIT_INCL_USERS y SERVER_AUDIT_EXCL_USERS se excluyen mutuamente. Si agrega valores a SERVER_AUDIT_EXCL_USERS, asegúrese de que no se agregan valores a SERVER_AUDIT_INCL_USERS. El usuario rdsadmin consulta la base de datos cada segundo para comprobar su estado. Dependiendo de otros ajustes de configuración, esta actividad puede hacer que el tamaño del archivo de registro llegue a ser muy grande muy deprisa. Si no necesita registrar esta actividad, añada el usuario rdsadmin a la lista SERVER_AUDIT_EXCL_USERS. **Note** CONNECTLa actividad de siempre se registra para todos los usuarios, aunque se especifique el usuario de esta configuración de opciones.
SERVER_AUDIT_LOGGING	ON	ON	El registro está activo. El único valor válido es ON. Amazon RDS no permite desactivar el registro. Si desea desactivar el registro, elimine el complemento de auditoría de MariaDB. Para obtener más información, consulte Eliminación del complemento de auditoría de MariaDB.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_QUERY_LOG_LIMIT	0–2147483647	1024	Límite de la longitud de la cadena de consulta en un registro.

Adición del complemento de auditoría de MariaDB

El proceso general para añadir el complemento de auditoría de MariaDB a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir el complemento de auditoría de MariaDB, no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, comenzará la auditoría.

Para añadir el complemento de auditoría de MariaDB

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado. Elija mariadb en Engine (Motor) y 10.3 o posteriores en Major engine version (Versión principal del motor). Para obtener más información, consulte Creación de un grupo de opciones.
2. Añada la opción MARIADB_AUDIT_PLUGIN al grupo de opciones y configure los ajustes de las opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones. Para obtener más información acerca de cada opción, consulte Configuración de opciones del complemento de auditoría.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente.

- Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia de base de datos y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Visualización y descarga del registro del complemento de auditoría de MariaDB

Después de habilitar un complemento de auditoría de MariaDB, podrá obtener acceso a los resultados de los archivos de registro de la misma forma que a los de los demás archivos de registro basados en texto. Los archivos del registro de auditoría se encuentran en `/rdsdbdata/log/audit/`. Para obtener información acerca de la visualización del archivo de registro en la consola, consulte Visualización y descripción de archivos de registro de base de datos. Para obtener información acerca de la descarga del archivo de registro, consulte Descarga de un archivo de registro de base de datos.

Modificación de la configuración del complemento de auditoría de MariaDB

Después de habilitar el complemento de auditoría de MariaDB, puede modificar la configuración del complemento. Para obtener más información acerca de cómo modificar la configuración de las opciones, consulte Modificación de una configuración de opciones. Para obtener más información acerca de cada opción, consulte Configuración de opciones del complemento de auditoría.

Eliminación del complemento de auditoría de MariaDB

Amazon RDS no permite desactivar el registro del complemento de auditoría de MariaDB. Sin embargo, puede eliminar el complemento de una instancia de base de datos. Cuando elimina el complemento de auditoría de MariaDB, la instancia de base de datos se reinicia automáticamente para detener la auditoría.

Para eliminar el complemento de auditoría de MariaDB de una instancia de base de datos, realice una de las siguientes operaciones:

- Elimine la opción del complemento de auditoría de MariaDB del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones

- Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya el complemento. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Parámetros de MariaDB

De manera predeterminada, una instancia de base de datos de MariaDB usa un grupo de parámetros de base de datos específico de una base de datos de MariaDB. Este grupo de parámetros contiene algunos de los parámetros (no todos) incluidos en los grupos de parámetros de base de datos de Amazon RDS para el motor de base de datos de MySQL. También contiene varios nuevos parámetros específicos de MariaDB. Para obtener información sobre cómo trabajar con grupos de parámetros y establecer parámetros, consulte Grupos de parámetros para Amazon RDS.

Visualización de los parámetros de MariaDB

Los parámetros de RDS for MariaDB se establecen en los valores predeterminados del motor de almacenamiento seleccionado. Para obtener más información sobre los parámetros de MariaDB, consulte la documentación de MariaDB. Para obtener más información sobre los motores de almacenamiento de MariaDB, consulte Motores de almacenamiento de MariaDB admitidos en Amazon RDS.

Puede ver los parámetros disponibles para una versión específica de RDS for MariaDB mediante la consola de RDS o AWS CLI. Para obtener información sobre cómo ver los parámetros en un grupo de parámetros de MariaDB en la consola de RDS, consulte Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Con la AWS CLI, puede ver los parámetros de una versión de RDS for MariaDB a través del comando `describe-engine-default-parameters`. Especifique uno de los siguientes valores para la opción `--db-parameter-group-family`:

- `mariadb10.11`
- `mariadb10.6`
- `mariadb10.5`
- `mariadb10.4`
- `mariadb10.3`

Por ejemplo, para ver los parámetros de la versión 10.6 de RDS for MySQL, ejecute el siguiente comando.

```
aws rds describe-engine-default-parameters --db-parameter-group-family mariadb10.6
```

El resultado tiene un aspecto similar al siguiente.

```
{
    "EngineDefaults": {
        "Parameters": [
            {
                "ParameterName": "alter_algorithm",
                "Description": "Specify the alter table algorithm.",
                "Source": "engine-default",
                "ApplyType": "dynamic",
                "DataType": "string",
                "AllowedValues": "DEFAULT,COPY,INPLACE,NOCOPY,INSTANT",
                "IsModifiable": true
            },
            {
                "ParameterName": "analyze_sample_percentage",
                "Description": "Percentage of rows from the table ANALYZE TABLE will
 sample to collect table statistics.",
                "Source": "engine-default",
                "ApplyType": "dynamic",
                "DataType": "float",
                "AllowedValues": "0-100",
                "IsModifiable": true
            },
            {
                "ParameterName": "aria_block_size",
                "Description": "Block size to be used for Aria index pages.",
                "Source": "engine-default",
                "ApplyType": "static",
                "DataType": "integer",
                "AllowedValues": "1024-32768",
                "IsModifiable": false
            },
            {
                "ParameterName": "aria_checkpoint_interval",
                "Description": "Interval in seconds between automatic checkpoints.",
                "Source": "engine-default",
                "ApplyType": "dynamic",
                "DataType": "integer",
                "AllowedValues": "0-4294967295",
                "IsModifiable": true
            },
        ...
```

Para enumerar solo los parámetros modificables de la versión 10.6 de RDS for MariaDB, ejecute el siguiente comando.

Para Linux, macOS o:Unix

```
aws rds describe-engine-default-parameters --db-parameter-group-family mariadb10.6 \
   --query 'EngineDefaults.Parameters[?IsModifiable==`true`]'
```

En:Windows

```
aws rds describe-engine-default-parameters --db-parameter-group-family mariadb10.6 ^
   --query "EngineDefaults.Parameters[?IsModifiable==`true`]"
```

Parámetros de MySQL que no están disponibles

Los siguientes parámetros de MySQL no están disponibles en los grupos de parámetros de base de datos específicos de MariaDB:

- bind_address
- binlog_error_action
- binlog_gtid_simple_recovery
- binlog_max_flush_queue_time
- binlog_order_commits
- binlog_row_image
- binlog_rows_query_log_events
- binlogging_impossible_mode
- block_encryption_mode
- core_file
- default_tmp_storage_engine
- div_precision_increment
- end_markers_in_json
- enforce_gtid_consistency
- eq_range_index_dive_limit
- explicit_defaults_for_timestamp
- gtid_executed

- gtid-mode
- gtid_next
- gtid_owned
- gtid_purged
- log_bin_basename
- log_bin_index
- log_bin_use_v1_row_events
- log_slow_admin_statements
- log_slow_slave_statements
- log_throttle_queries_not_using_indexes
- master-info-repository
- optimizer_trace
- optimizer_trace_features
- optimizer_trace_limit
- optimizer_trace_max_mem_size
- optimizer_trace_offset
- relay_log_info_repository
- rpl_stop_slave_timeout
- slave_parallel_workers
- slave_pending_jobs_size_max
- slave_rows_search_algorithms
- storage_engine
- table_open_cache_instances
- timed_mutexes
- transaction_allow_batching
- validate-password
- validate_password_dictionary_file
- validate_password_length
- validate_password_mixed_case_count
- validate_password_number_count

- validate_password_policy
- validate_password_special_char_count

Para obtener más información sobre los parámetros de MySQL, visite la documentación de MySQL.

Migración de datos desde una instantánea de base de datos de MySQL a una instancia de base de datos MariaDB

Puede migrar una instantánea de base de datos de RDS for MySQL a una nueva instancia de base de datos en la que se ejecuta MariaDB mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS. Debe usar la instantánea de base de datos creada desde una instancia de base de datos de Amazon RDS que ejecute MySQL 5.6 o 5.7. Para aprender a crear una instantánea de base de datos RDS for MYSQL, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

La migración de la instantánea no afecta a la instancia de base de datos original desde la que se tomó la instantánea. Puede probar y validar la nueva instancia de base de datos antes de desviar el tráfico a ella como reemplazo de la instancia de base de datos original.

Después de migrar de MySQL a MariaDB, la instancia de base de datos MariaDB se asocia con el grupo de parámetros de base de datos predeterminado y el grupo de opciones correspondiente. Después de restaurar la instantánea de base de datos, puede asociar un grupo de parámetros de base de datos personalizado con la nueva instancia de base de datos. Sin embargo, un grupo de parámetros de MariaDB tiene un conjunto diferente de variables de sistema configurables. Para obtener información acerca de las diferencias entre las variables de sistema de MySQL y MariaDB, consulte System Variable Differences between MariaDB and MySQL (Diferencias de la variable de sistema entre MariaDB y MySQL). Para obtener información acerca de los grupos de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS. Para obtener información acerca de los grupos de opciones, consulte Trabajo con grupos de opciones.

Realización de la migración

Se puede migrar una instantánea de base de datos de RDS for MySQL a una nueva instancia de base de datos de MariaDB mediante la AWS Management Console, la AWS CLI o la API de RDS.

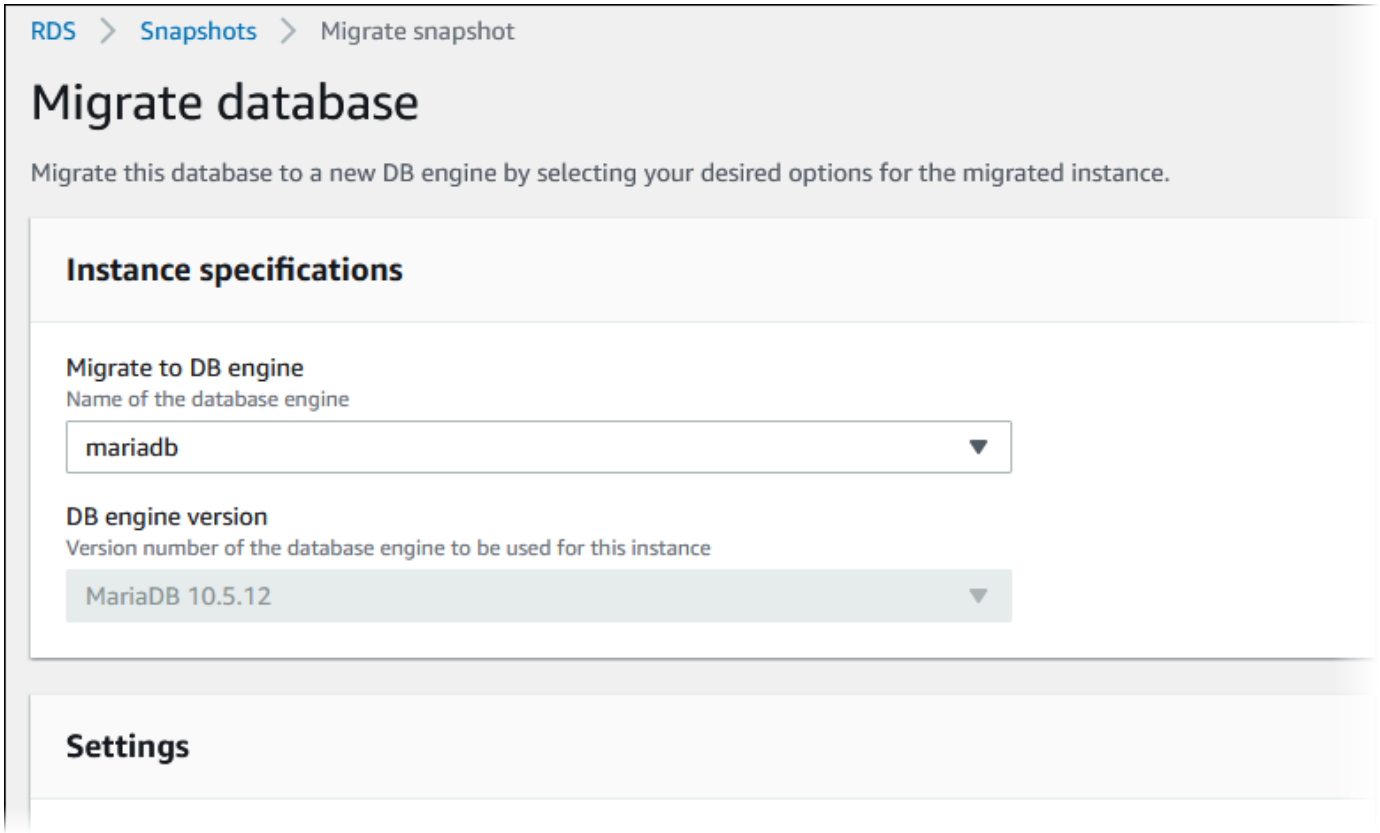
Consola

Para migrar una instantánea de base de datos de MySQL a una instancia de base de datos MariaDB

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas) y, a continuación, seleccione la instantánea de base de datos MySQL que desea migrar.

3. En Actions (Acciones), elija Migrate Snapshot (Migrar instantánea). Aparece la página Migrate Database (Migrar base de datos).
4. En Migrate to DB Engine (Migrar a motor de base de datos), elija mariadb.

   Amazon RDS selecciona la DB engine version (Versión del motor de base de datos) automáticamente. No se puede cambiar la versión del motor de base de datos.



5. En el resto de secciones, especifique los ajustes de configuración de la instancia de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.
6. Elija Migrate (Migrar).

AWS CLI

Para migrar datos desde una instantánea de base de datos de MySQL a una instancia de base de datos de MariaDB, ejecute el comando `restore-db-instance-from-db-snapshot` de la AWS CLI con las siguientes opciones:

- --db-instance-identifier: nombre de la instancia de base de datos que se debe crear a partir de la instantánea de base de datos.

- --db-snapshot-identifier: identificador de la instantánea de base de datos desde la que se debe restaurar.
- --engine: motor de base de datos que se va a usar para la nueva instancia.

Example

Para Linux, macOS o Unix:

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier newmariadbinstance \
    --db-snapshot-identifier mysqlsnapshot \
    --engine mariadb
```

Para Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier newmariadbinstance ^
    --db-snapshot-identifier mysqlsnapshot ^
    --engine mariadb
```

API

Para migrar los datos desde una instantánea de base de datos de MySQL a una instancia de base de datos de MariaDB, llame a la operación `RestoreDBInstanceFromDBSnapshot` de la API de Amazon RDS.

Incompatibilidades entre MariaDB y MySQL

Entre las incompatibilidades entre MySQL y MariaDB se incluyen las siguientes:

- No puede migrar una instantánea de base de datos creada con MySQL 8.0 a MariaDB.
- Si la base de datos de MySQL de origen utiliza un hash de contraseña SHA256, asegúrese de restablecer las contraseñas de usuario con hash SHA256 antes de conectarse a la base de datos MariaDB. El siguiente código muestra cómo restablecer una contraseña con hash SHA256.

```
SET old_passwords = 0;
UPDATE mysql.user SET plugin = 'mysql_native_password',
Password = PASSWORD('new_password')
```

```
WHERE (User, Host) = ('master_user_name', %);
FLUSH PRIVILEGES;
```

- Si su cuenta de usuario maestro de RDS utiliza el hash de contraseña SHA-256, asegúrese de restablecer la contraseña mediante la AWS Management Console, el comando `modify-db-instance` de la AWS CLI o la operación ModifyDBInstance de la API de RDS. Para obtener más información sobre la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.
- MariaDB no admite el complemento Memcached. Sin embargo, los datos que utiliza el complemento Memcached se almacenan como tablas InnoDB. Después de migrar una instantánea de base de datos de MySQL, puede obtener acceso a los datos empleados por el complemento Memcached usando SQL. Para obtener más información acerca de la base de datos innodb_memcache, consulte InnoDB memcached Plugin Internals.

Referencia de MariaDB en Amazon RDS SQL

A continuación, puede encontrar las descripciones de los procedimientos almacenados del sistema que están disponibles para las instancias de Amazon RDS que ejecutan el motor de base de datos MariaDB.

Puede utilizar los procedimientos almacenados del sistema que están disponibles para instancias de base de datos de MySQL y de MariaDB. Estos procedimientos almacenados están documentados en Referencia de procedimientos almacenados de RDS para MySQL. Las instancias de base de datos de MariaDB admiten todos los procedimientos almacenados, excepto `mysql.rds_start_replication_until` y `mysql.rds_start_replication_until_gtid`.

Además, los siguientes procedimientos almacenados del sistema solo son compatibles con las instancias de base de datos de Amazon RDS en las que se ejecuta MariaDB:

- mysql.rds_replica_status
- mysql.rds_set_external_master_gtid
- mysql.rds_kill_query_id

mysql.rds_replica_status

Muestra el estado de replicación de una réplica de lectura de MariaDB.

Llama a este procedimiento en la réplica de lectura para mostrar información de estado sobre los parámetros esenciales de los subprocesos de replicación.

Sintaxis

```
CALL mysql.rds_replica_status;
```

Notas de uso

Este procedimiento solo es compatible con instancias de base de datos de MariaDB que se ejecuten con las versiones 10.5 y superiores de MariaDB.

Este procedimiento es el equivalente del comando `SHOW REPLICA STATUS`. Este comando no es compatible con las versiones 10.5 y superiores de las instancias de base de datos de MariaDB.

En las versiones anteriores de MariaDB, el comando `SHOW SLAVE STATUS` equivalente requería el privilegio `REPLICATION SLAVE`. En la versión 10.5 y versiones posteriores de MariaDB, se requiere el privilegio `REPLICATION REPLICA ADMIN`. Para proteger la administración de RDS de instancias de base de datos de la versión 10.5 de MariaDB y versiones posteriores, este nuevo privilegio no se otorga al usuario maestro de RDS.

Ejemplos

En el siguiente ejemplo se muestra el estado de una réplica de lectura de MariaDB:

```
call mysql.rds_replica_status;
```

La respuesta será similar a la siguiente:

```
*************************** 1. row ***************************
               Replica_IO_State: Waiting for master to send event
                    Source_Host: XX.XX.XX.XXX
                    Source_User: rdsrepladmin
                    Source_Port: 3306
                  Connect_Retry: 60
                Source_Log_File: mysql-bin-changelog.003988
            Read_Source_Log_Pos: 405
                 Relay_Log_File: relaylog.011024
                  Relay_Log_Pos: 657
          Relay_Source_Log_File: mysql-bin-changelog.003988
             Replica_IO_Running: Yes
            Replica_SQL_Running: Yes
                Replicate_Do_DB:
            Replicate_Ignore_DB:
             Replicate_Do_Table:
         Replicate_Ignore_Table:
mysql.rds_sysinfo,mysql.rds_history,mysql.rds_replication_status
        Replicate_Wild_Do_Table:
    Replicate_Wild_Ignore_Table:
                     Last_Errno: 0
                     Last_Error:
                   Skip_Counter: 0
            Exec_Source_Log_Pos: 405
                Relay_Log_Space: 1016
                Until_Condition: None
                 Until_Log_File:
                  Until_Log_Pos: 0
```

```
              Source_SSL_Allowed: No
              Source_SSL_CA_File:
              Source_SSL_CA_Path:
                 Source_SSL_Cert:
               Source_SSL_Cipher:
                  Source_SSL_Key:
           Seconds_Behind_Master: 0
   Source_SSL_Verify_Server_Cert: No
                  Last_IO_Errno: 0
                  Last_IO_Error:
                 Last_SQL_Errno: 0
                 Last_SQL_Error:
     Replicate_Ignore_Server_Ids:
                Source_Server_Id: 807509301
                  Source_SSL_Crl:
              Source_SSL_Crlpath:
                      Using_Gtid: Slave_Pos
                     Gtid_IO_Pos: 0-807509301-3980
         Replicate_Do_Domain_Ids:
     Replicate_Ignore_Domain_Ids:
                   Parallel_Mode: optimistic
                       SQL_Delay: 0
             SQL_Remaining_Delay: NULL
       Replica_SQL_Running_State: Reading event from the relay log
              Replica_DDL_Groups: 15
Replica_Non_Transactional_Groups: 0
    Replica_Transactional_Groups: 3658
1 row in set (0.000 sec)

Query OK, 0 rows affected (0.000 sec)
```

mysql.rds_set_external_master_gtid

Configura la reproducción basada en GTID desde una instancia de MariaDB que se ejecuta fuera de Amazon RDS a una instancia de base de datos de MariaDB. Este procedimiento almacenado solo se admite cuando la instancia de MariaDB externa tiene la versión 10.0.24 o posterior. Cuando configure una replicación en la que una o las dos instancias no admitan los identificadores de transacciones globales (GTID) de MariaDB, use mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores).

El uso de GTID para la replicación proporciona características de seguridad en caso de bloqueo que no ofrece la replicación con registros binarios, así que es el procedimiento recomendado cuando las instancias que se van a replicar lo admiten.

Sintaxis

```
CALL mysql.rds_set_external_master_gtid(
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , gtid
  , ssl_encryption
);
```

Parámetros

host_name

Cadena. El nombre de host o dirección IP de la instancia de MariaDB ejecutada fuera de Amazon RDS que se convertirá en instancia de origen.

host_port

Entero. El puerto usado por la instancia de MariaDB ejecutada fuera de Amazon RDS que se configurará como instancia de origen. Si la configuración de la red incluye la replicación del puerto SSH que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

Cadena. ID de un usuario con permisos `REPLICATION SLAVE` en la instancia de base de datos de MariaDB que se va a configurar como réplica de lectura.

replication_user_password

Cadena. La contraseña del ID de usuario especificado en `replication_user_name`.

gtid

Cadena. El ID de transacción global de la instancia de origen desde el que debe comenzar la replicación.

Puede usar `@@gtid_current_pos` para obtener el GTID actual si la instancia de origen se ha bloqueado mientras se configura la replicación con el fin de que el registro binario no cambie entre los puntos en los que se obtiene el GTID y comienza la replicación.

De lo contrario, si usa `mysqldump` versión 10.0.13 o posterior para rellenar la instancia de réplica antes de comenzar la replicación, puede obtener la posición de GTID en la salida usando las opciones `--master-data` o `--dump-slave`. Si no usa `mysqldump` 10.0.13 o posterior, puede ejecutar `SHOW MASTER STATUS` o usar las mismas opciones de `mysqldump` para obtener el nombre y la posición del archivo de registro binario y convertirlos a continuación en un GTID ejecutando `BINLOG_GTID_POS` en la instancia de MariaDB externa:

```
SELECT BINLOG_GTID_POS('<binary log file name>', <binary log file position>);
```

Para obtener más información acerca de la implementación de los GTID en MariaDB, vaya a Global Transaction ID en la documentación de MariaDB.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `MASTER_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_master_gtid`. Se debe ejecutar en la instancia de base de datos de MariaDB que se está configurando como réplica de una instancia de MariaDB que se ejecuta fuera de Amazon RDS. Antes de ejecutar `mysql.rds_set_external_master_gtid`, debe haber configurado la instancia de MariaDB que se ejecuta fuera de Amazon RDS como instancia de origen. Para obtener más información, consulte Importación de datos en una instancia de base de datos de Amazon RDS para MariaDB.

> **Warning**
>
> No use `mysql.rds_set_external_master_gtid` para administrar la replicación entre dos instancias de base de datos de Amazon RDS. Úselo solo cuando replique con una instancia de MariaDB que se ejecute fuera de RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Después de llamar a `mysql.rds_set_external_master_gtid` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura, puede llamar a mysql.rds_start_replication en la réplica para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_master_gtid`, Amazon RDS registra la hora, el usuario y una acción "set master" en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MariaDB, el siguiente ejemplo la configura como réplica de una instancia de MariaDB que se ejecuta fuera de Amazon RDS.

```
call mysql.rds_set_external_master_gtid
 ('Sourcedb.some.com',3306,'ReplicationUser','SomePassW0rd','0-123-456',0);
```

mysql.rds_kill_query_id

Finaliza una consulta que se ejecuta en el servidor de MariaDB para finalizar consultas de larga duración o problemáticas. Puede identificar el ID de la consulta y detener de forma eficaz una consulta específica para abordar los problemas de rendimiento y mantener un funcionamiento óptimo de la base de datos.

Sintaxis

```
CALL mysql.rds_kill_query_id(queryID);
```

Parámetros

queryID

Entero. La identidad de la consulta que se va a finalizar.

Notas de uso

Para detener una consulta que se ejecute en el servidor de MariaDB, use el procedimiento `mysql.rds_kill_query_id` y transfiera el ID de esa consulta. Para obtener el ID de la consulta, consulte la Information Schema PROCESSLIST Table de MariaDB, como se muestra a continuación:

```
SELECT USER, HOST, COMMAND, TIME, STATE, INFO, QUERY_ID FROM
                INFORMATION_SCHEMA.PROCESSLIST WHERE USER = '<user name>';
```

La conexión al servidor de MariaDB se conserva.

Ejemplos

El siguiente ejemplo finaliza una consulta con el ID de consulta 230040:

```
call mysql.rds_kill_query_id(230040);
```

Zona horaria local para instancias de base de datos de MariaDB

De manera predeterminada, la zona horaria para una instancia de base de datos de MariaDB es el horario universal coordinado (UTC). En su lugar, puede definir la zona horaria de su instancia de base de datos en la zona horaria local de su aplicación.

Para definir la zona horaria local para una instancia de base de datos, configure el parámetro `time_zone` del grupo de parámetros de la instancia de base de datos en uno de los valores admitidos que se indican más adelante en esta sección. Al configurar el parámetro `time_zone` de un grupo de parámetros, todas las instancias de base de datos y réplicas de lectura que utilizan ese grupo de parámetros cambian para utilizar la nueva zona horaria local. Para obtener información acerca de cómo configurar los parámetros de un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.

Después de definir la zona horaria local, todas las conexiones nuevas con la base de datos reflejarán el cambio. Si tiene alguna conexión con la base de datos abierta al cambiar la zona horaria local, no verá la actualización de la zona horaria local hasta que cierre la conexión y abra una nueva conexión.

Puede definir una zona horaria local diferente para una instancia de base de datos y una o varias de sus réplicas de lectura. Para ello, utilice un grupo de parámetros diferente para la instancia de base de datos y para la réplica o las réplicas y establezca el parámetro `time_zone` de cada grupo de parámetros en una zona horaria local distinta.

Si se replica en las Regiones de AWS, la instancia de base de datos de origen y la réplica de lectura utilizan diferentes grupos de parámetros (los grupos de parámetros son exclusivos de una Región de AWS). Para usar la misma zona horaria local para cada instancia, debe configurar el parámetro `time_zone` en los grupos de parámetros de la instancia y de la réplica de lectura.

Cuando se restaura una instancia de base de datos desde una instantánea de base de datos, la zona horaria local se define como UTC. Podrá actualizar la zona horaria a su zona horaria local una vez que se haya completado la restauración. Si restaura una instancia de base de datos a un momento dado, la zona horaria local de la instancia de base de datos restaurada será el ajuste de zona horaria del grupo de parámetros de la instancia de base de datos restaurada.

Internet Assigned Numbers Authority (Autoridad de Números Asignados en Internet, IANA por sus siglas en inglés) publica nuevas zonas horarias en https://www.iana.org/time-zones varias veces al año. Cada vez que RDS publica una nueva versión secundaria de mantenimiento de MariaDB,

incluye los datos de zona horaria más recientes en el momento de la publicación. Cuando utiliza las versiones más recientes de RDS para MariaDB, dispone de datos de zona horaria recientes de RDS. Para garantizar que la instancia de base de datos tenga datos de zona horaria recientes, se recomienda actualizar a una versión posterior del motor de base de datos. Como alternativa, puede modificar las tablas de zonas horarias en las instancias de base de datos de MariaDB manualmente. Para ello, puede utilizar comandos SQL o ejecutar la herramienta mysql_tzinfo_to_sql en un cliente SQL. Tras actualizar los datos de la zona horaria de forma manual, reinicie la instancia de base de datos para que los cambios se apliquen. RDS no modifica ni restablece los datos de zona horaria de las instancias de base de datos en ejecución. Los nuevos datos de zona horaria solo se instalan cuando se actualiza la versión del motor de base de datos.

Puede definir su zona horaria local en uno de los valores siguientes.

Zona	Time zone (Zona horarioa)
África	África/El Cairo, África/Casablanca, África/Harare, África/Monrovia, África/Nairobi, África/Trípoli, África/Windhoek
América	América/Araguaína, América/Asunción, América/Bogotá, América/Buenos_Aires, América/Caracas, América/Chihuahua, América/Cuiabá, América/Denver, América/Fortaleza, América/Guatemala, América/Halifax, América/Manaos, América/Matamoros, América/Monterrey, América/Montevideo, América/Phoenix, América/Santiago, América/Tijuana
Asia	Asia/Amán, Asia/Asjabad, Asia/Bagdad, Asia/Bakú, Asia/Bangkok, Asia/Beirut, Asia/Calcuta, Asia/Daca, Asia/Damasco, Asia/Ereván, Asia/Irkutsk, Asia/Jerusalén, Asia/Kabul, Asia/Karachi, Asia/Katmandú, Asia/Krasnoyarsk, Asia/Magadán, Asia/Mascate, Asia/Novosibirsk, Asia/Riad, Asia/Seúl, Asia/Shanghái, Asia/Singapur, Asia/Taipéi, Asia/Teherán, Asia/Tokio, Asia/Ulán_Bator, Asia/Vladivostok, Asia/Yakutsk
Atlántico	Atlántico/Azores
Australia	Australia/Adelaida, Australia/Brisbane, Australia/Darwin, Australia/Hobart, Australia/Perth, Australia/Sídney
Brasil	Brasil/DeNoronha, Brasil/Este
Canadá	Canadá/Terranova, Canadá/Saskatchewan, Canadá/Yukón

Zona	Time zone (Zona horarioa)
Europa	Europa/Ámsterdam, Europa/Atenas, Europa/Dublín, Europa/Helsinki, Europa/Estambul, Europa/ Kaliningrado, Europa/Moscú, Europa/París, Europa/Praga, Europa/Sarajevo
Pacífico	Pacífico/Auckland, Pacífico/Fiyi, Pacífico/Guam, Pacífico/Honolulu, Pacífico/Samoa
EE. UU.	EE. UU./Alaska, EE. UU./Central, EE. UU./Indiana-Este, EE. UU./Este, EE. UU./Pacífico
UTC	UTC

Problemas conocidos y limitaciones de RDS para MariaDB

Los siguientes elementos son problemas conocidos y limitaciones al usar RDS para MariaDB.

> **Note**
>
> Esta lista no es exhaustiva.

Temas

- Límites de tamaño de archivo de MariaDB en Amazon RDS
- Palabra reservada InnoDB
- Puertos personalizados
- Performance Insights

Límites de tamaño de archivo de MariaDB en Amazon RDS

Para las instancias de base de datos MariaDB, el tamaño máximo de una tabla es de 16 TB cuando se usan espacios de tablas de archivos por tabla InnoDB. Este límite también restringe el espacio de tabla del sistema a un tamaño máximo de 16 TB. Los espacios de tabla de archivo por tabla de InnoDB (en los que las tablas están cada una en su propio espacio de tabla) se habilitan de forma predeterminada para las instancias de base de datos de MariaDB. Este límite no está relacionado con el límite máximo de almacenamiento para las instancias de base de datos MariaDB. Para más información sobre el límite de almacenamiento, consulte Almacenamiento de instancias de base de datos de Amazon RDS.

El uso de los espacios de tabla file-per-table de InnoDB tiene pros y contras en función de la aplicación. Para determinar el mejor método para su aplicación, consulte File-Per-Table Tablespaces en la documentación de MySQL.

No es recomendable permitir que las tablas crezcan hasta el tamaño de archivo máximo. En general, es preferible dividir los datos en tablas más pequeñas, que pueden mejorar el desempeño y los tiempos de recuperación.

Una opción que se puede usar para dividir una tabla grande en tablas más pequeñas es la creación de particiones. Las particiones distribuyen las porciones de una tabla grande en archivos independientes en función de las reglas que se hayan especificado. Por ejemplo, si almacena las

transacciones por fecha, puede crear reglas de partición que distribuyan las transacciones más antiguas entre distintos archivos por medio de la creación de particiones. Después, periódicamente, se pueden archivar los datos de transacciones históricos que no tengan que estar disponibles de forma inmediata para su aplicación. Para obtener información, consulte Partitioning en la documentación de MySQL.

Determinación del tamaño de todos los espacios de tablas de InnoDB

- Utilice el comando SQL siguiente para determinar si alguna de las tablas es demasiado grande y por lo tanto es candidata para particiones.

> **Note**
>
> Para MariaDB 10.6 y versiones posteriores, esta consulta también devuelve el tamaño del espacio de tablas del sistema InnoDB.
> En las versiones de MariaDB anteriores a la 10.6 no es posible determinar el tamaño del espacio de tablas del sistema InnoDB consultando las tablas del sistema. Se recomienda una actualización a una versión posterior de Python.

```
SELECT SPACE,NAME,ROUND((ALLOCATED_SIZE/1024/1024/1024), 2)
as "Tablespace Size (GB)"
FROM information_schema.INNODB_SYS_TABLESPACES ORDER BY 3 DESC;
```

Determinación del tamaño de las tablas de usuario distintas de InnoDB

- Utilice el siguiente comando SQL para determinar si alguna de las tablas distintas de InnoDB es demasiado grande.

```
SELECT TABLE_SCHEMA, TABLE_NAME, round(((DATA_LENGTH + INDEX_LENGTH+DATA_FREE)
/ 1024 / 1024/ 1024), 2) As "Approximate size (GB)" FROM information_schema.TABLES
WHERE TABLE_SCHEMA NOT IN ('mysql', 'information_schema', 'performance_schema')
and ENGINE<>'InnoDB';
```

Para habilitar espacios de tabla file-per-table de InnoDB

- Establezca el parámetro `innodb_file_per_table` en `1` el grupo de parámetros para la instancia de base de datos.

Para deshabilitar los espacios de tabla file-per-table de InnoDB

- Establezca el parámetro `innodb_file_per_table` en `0` el grupo de parámetros para la instancia de base de datos.

Para obtener más información acerca de la actualización de un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.

Cuando haya habilitado o deshabilitado los espacios de tabla file-per-table de InnoDB, puede ejecutar un comando `ALTER TABLE`. Puede utilizar este comando para mover una tabla desde el espacio de tabla global a su propio espacio de tabla. O bien, puede mover una tabla desde su propio espacio de tabla al espacio de tabla global. A continuación se muestra un ejemplo.

```
ALTER TABLE table_name ENGINE=InnoDB, ALGORITHM=COPY;
```

Palabra reservada InnoDB

`InnoDB` es una palabra reservada para RDS for MariaDB. No puede utilizar este nombre para una base de datos MariaDB.

Puertos personalizados

Amazon RDS bloquea las conexiones al puerto personalizado 33060 para el motor de MariaDB. Elija un puerto diferente para su motor de MariaDB.

Performance Insights

Los contadores de InnoDB no son visibles en Información de rendimiento para RDS para MariaDB 10.11 porque la comunidad de MariaDB ya no los admite.

Amazon RDS for Microsoft SQL Server

Amazon RDS admite varias versiones y ediciones de Microsoft SQL Server. En la siguiente tabla se muestra la versión secundaria compatible más reciente de cada versión principal. Para ver una lista completa de las versiones, ediciones y versiones del motor de RDS admitidas, consulte Versiones de Microsoft SQL Server en Amazon RDS.

Versión principal	Paquete de servicio / GDR	Actualización acumulativa	Versión secundaria	Artículo de la base de conocimientos	Fecha de lanzamiento
SQL Server 202	RDA	CU13	16.0.4131.2	KB5040939	12 de agosto de 2024
SQL Server 201	No aplicable	CU27	15.0.4382.1	KB5040948	12 de agosto de 2024
SQL Server 201	RDA	CU31	14.0.3471.2	KB5040940	12 de agosto de 2024
SQL Server 201	SP3 GDR	No aplicable	13.0.6441.1	KB5040946	12 de agosto de 2024

Para obtener información acerca de licencias para SQL Server, consulte Licencias de Microsoft SQL Server en Amazon RDS. Para obtener información sobre todas las compilaciones de SQL Server, consulte este artículo de soporte de Microsoft sobre dónde encontrar información sobre las últimas compilaciones de SQL Server.

Con Amazon RDS puede crear instancias de bases de datos e instantáneas de base de datos, restauraciones a un momento dado y copias de seguridad automatizadas o manuales. Las instancias de base de datos en las que se ejecuta SQL Server se pueden usar dentro de una VPC. También puede utilizar la capa de conexión segura (SSL) para conectarse a una instancia de base de datos en la que se ejecuta SQL Server y puede utilizar el cifrado de datos (TDE) transparente para cifrar los datos en reposo. Amazon RDS admite actualmente implementaciones Multi-AZ para SQL Server

mediante SQL Server Database Mirroring (DBM) o los grupos de disponibilidad AlwaysOn (AG) como solución de conmutación por error de alta disponibilidad.

Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso de shell a las instancias de base de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Amazon RDS permite el acceso a las bases de datos de una instancia de base de datos con cualquier aplicación cliente de SQL estándar. Amazon RDS no permite el acceso de anfitrión directo a una instancia de base de datos a través de Telnet, Secure Shell (SSH) o conexión a escritorio remoto de Windows. Cuando se crea una instancia de base de datos, el usuario maestro se asigna al rol db_owner para todas las bases de datos de usuario en esa instancia y tiene todos los permisos de nivel de base de datos excepto los que se utilizan para copias de seguridad. Amazon RDS administra las copias de seguridad por usted.

Antes de crear su primera instancia de base de datos, debe completar los pasos que se describen en la sección de configuración de esta guía. Para obtener más información, consulte Configuración del entorno para Amazon RDS.

Temas

- Tareas de administración frecuentes para Microsoft SQL Server en Amazon RDS
- Limitaciones para instancias de base de datos de Microsoft SQL Server
- Compatibilidad con clases de instancia de base de datos para Microsoft SQL Server
- Seguridad de Microsoft SQL Server
- Compatibilidad con el programa de conformidad de las instancias de base de datos de Microsoft SQL Server
- Compatibilidad con SSL para las instancias de base de datos de Microsoft SQL Server
- Versiones de Microsoft SQL Server en Amazon RDS
- Administración de versiones en Amazon RDS
- Características de Microsoft SQL Server en Amazon RDS
- Compatibilidad de captura de datos de cambio para instancias de base de datos de Microsoft SQL Server
- Características no compatibles y características con compatibilidad limitada
- Implementaciones Multi-AZ con creación de reflejos de base de datos de Microsoft SQL Server o grupos de disponibilidad Always On
- Uso del cifrado de datos transparente para cifrar los datos en reposo
- Funciones y procedimientos almacenados para Amazon RDS for Microsoft SQL Server

- Zona horaria local para las instancias de base de datos de Microsoft SQL Server
- Licencias de Microsoft SQL Server en Amazon RDS
- Conexión a la instancia de base de datos de Microsoft SQL Server
- Uso de Active Directory con RDS para SQL Server
- Actualización de aplicaciones para la conexión a las instancias de base de datos de Microsoft SQL Server con los nuevos certificados SSL/TLS
- Actualizaciones del motor de base de datos de Microsoft SQL Server
- Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas
- Uso de réplicas de lectura para Microsoft SQL Server en Amazon RDS
- Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server
- Características adicionales para Microsoft SQL Server en Amazon RDS
- Opciones para el motor de base de datos de Microsoft SQL Server
- Tareas comunes de administrador de bases de datos de Amazon RDS para Microsoft SQL Server

Tareas de administración frecuentes para Microsoft SQL Server en Amazon RDS

A continuación se detallan las tareas de administración frecuentes que se realizan instancia de base de datos de Amazon RDS for SQL Server, con enlaces a la documentación relativa a cada tarea.

Área de la tarea	Documentación relacionada
Clases de instancias, almacenamiento y PIOPS Si va a crear una instancia de base de datos con fines de producción, debe entender cómo funcionan en Amazon RDS las clases de instancia, los tipos de almacenamiento y las IOPS provisionadas.	Compatibilidad con clases de instancia de base de datos para Microsoft SQL Server Tipos de almacenamiento de Amazon RDS
Implementaciones Multi-AZ Una instancia de base de datos de producción debe usar implementaciones Multi-AZ. Las implementaciones Multi-AZ	Configuración y administración de una implementación multi-AZ para Amazon RDS

Área de la tarea	Documentación relacionada
proporcionan unos niveles superiores de disponibilidad, durabilidad de los datos y tolerancia a errores para las instancias de base de datos. Las implementaciones Multi-AZ de SQL Server se implementan con la tecnología de DBM o AG nativas de SQL Server.	Implementaciones Multi-AZ con creación de reflejos de base de datos de Microsoft SQL Server o grupos de disponibilidad Always On
Amazon Virtual Private Cloud (VPC) Si su cuenta de AWS tiene una VPC predeterminada, la instancia de base de datos se creará automáticamente dentro de la VPC predeterminada. Si su cuenta no tiene una VPC predeterminada y desea que la instancia de base de datos esté en una VPC, debe crear los grupos de VPC y de subredes antes de crear la instancia de base de datos.	Uso de una instancia de base de datos en una VPC
Grupos de seguridad De manera predeterminada, las instancias de base de datos se crean con un firewall que impide el acceso a ellas. Por ello, debe crear un grupo de seguridad con la dirección IP y la configuración de red correctas para obtener acceso a la instancia de base de datos.	Control de acceso con grupos de seguridad
Grupos de parámetros Si su instancia de base de datos va a requerir unos parámetros de base de datos concretos, debe crear un grupo de parámetros antes de crear la instancia de base de datos.	Grupos de parámetros para Amazon RDS
Grupos de opciones Si su instancia de base de datos va a requerir unas opciones de base de datos concretas, debe crear un grupo de opciones antes de crear la instancia de base de datos.	Opciones para el motor de base de datos de Microsoft SQL Server

Área de la tarea	Documentación relacionada
Conexión a la instancia de base de datos Después de crear un grupo de seguridad y de asociarlo a una instancia de base de datos, puede conectarse a la instancia de base de datos usando cualquier aplicación cliente de SQL estándar como Microsoft SQL Server Management Studio.	Conexión a la instancia de base de datos de Microsoft SQL Server
Copia de seguridad y restauración Cuando cree la instancia de base de datos, puede configurarla para que realice copias de seguridad automatizadas. También puede realizar copias de seguridad y restaurar las bases de datos manualmente utilizando archivos de copia de seguridad completos (archivos .bak).	Introducción a las copias de seguridad Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas
Supervisión Puede monitorizar la instancia de base de datos de SQL Server usando métricas, eventos y monitorización mejorada de Amazon RDS de CloudWatch.	Consulta de métricas en la consola de Amazon RDS Consulta de eventos de Amazon RDS
Archivos de registro Puede obtener acceso a los archivos de registro de su instancia de base de datos de SQL Server.	Supervisión de archivos de registro de Amazon RDS Archivos de registro de base de datos de Amazon RDS para Microsoft SQL Server

También hay tareas administrativas avanzadas para trabajar con las instancias de base de datos de SQL Server. Para obtener más información, consulte la documentación siguiente:

- Tareas comunes de administrador de bases de datos de Amazon RDS para Microsoft SQL Server.
- Uso de AWS Managed Active Directory con RDS para SQL Server
- Acceso a la base de datos tempdb

Limitaciones para instancias de base de datos de Microsoft SQL Server

La implementación con Amazon RDS de Microsoft SQL Server en una instancia de base de datos tiene algunas limitaciones que debe conocer:

- El número máximo de bases de datos compatibles en una instancia de base de datos depende del tipo de clase de instancia y el modo de disponibilidad: Creación de reflejos de bases de datos (DBM) Single-AZ y Multi-AZ, o grupos de disponibilidad Multi-AZ (AG). Las bases de datos del sistema de Microsoft SQL Server no cuentan para este límite.

  La siguiente tabla muestra el número máximo de bases de datos compatibles para cada tipo de clase de instancia y modo de disponibilidad. Utilice esta tabla para decidir si puede cambiar de un tipo de clase de instancia a otro, o desde un modo de disponibilidad a otro. Si su instancia de base de datos de origen dispone de más bases de datos de las que el tipo de clase de instancia de destino o el modo de disponibilidad puede soportar, se producirá un error al modificar la instancia de base de datos. Puede ver el estado de su solicitud en el panel Events (Eventos).

Tipo de clase de instancia	Single-AZ	Multi-AZ con DBM	Multi-AZ con grupos de disponibilidad siempre activos
db.*.micro a db.*.medium	30	N/A	N/A
db.*.large	30	30	30
db.*.xlarge a db.*.16xlarge	100	50	75
db.*.24xlarge	100	50	100

  * Representa los diferentes tipos de clase de instancia.

  Por ejemplo, supongamos que su instancia de base de datos se ejecuta en db.*.16xlarge con Single-AZ y que dispone de 76 bases de datos. Modifique la instancia de base de datos que actualizar mediante grupos de disponibilidad Always On Multi-AZ. Se producirá un error en la

actualización porque su instancia de base de datos contiene más bases de datos de las que su configuración de destino puede soportar. Si actualiza su tipo de clase de instancia a db.*.24xlarge, la modificación se realiza correctamente.

Si se produce un error en la actualización, verá eventos y mensajes similares al siguiente:

- No es posible modificar la clase de instancia de base de datos. La instancia tiene 76 bases de datos, pero después de la conversión solo admitirá 75.
- No es posible convertir la instancia de base de datos en Multi-AZ: la instancia dispone de 76 bases de datos, pero después de la conversión solo admitirá 75.

Si se produce un error en la restauración a un momento dado o la restauración de una instantánea, verá eventos y mensajes similares al siguiente:

- Instancia de base de datos puesta en una restauración incompatible. La instancia tiene 76 bases de datos, pero después de la conversión solo admitirá 75.

- Estos puertos están reservados para Amazon RDS y no se pueden usar al crear una instancia de base de datos: `1234, 1434, 3260, 3343, 3389, 47001,` y `49152-49156`.
- La conexiones de cliente desde direcciones IP en el rango 169.254.0.0/16 no están permitidas. Este es el rango de direccionamiento IP privado automático (APIPA), que se utiliza para direccionamiento de enlace local.
- SQL Server Standard Edition solo utiliza un subconjunto de los procesadores disponibles si la instancia de base de datos tiene más procesadores que los límites del software (24 núcleos, 4 sockets y 128 GB de RAM). Algunos ejemplos de esto son las clases de instancias db.m5.24xlarge y db.r5.24xlarge.

  Para obtener más información, consulte la tabla de límites de escala en Ediciones y características compatibles de SQL Server 2019 (15.x) en la documentación de Microsoft.
- Amazon RDS for SQL Server no admite la importación de datos en la base de datos de msdb.
- No se puede cambiar el nombre de las bases de datos de una instancia de base de datos en una implementación Multi-AZ de SQL Server.
- Asegúrese de utilizar estos lineamientos al configurar los siguientes parámetros de la base de datos en RDS for SQL Server:
  - `max server memory (mb)`256 MB
  - `max worker threads` >= (número de CPU lógicas * 7)

  Para obtener más información sobre la configuración de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.

- El tamaño máximo de almacenamiento para las instancias de base de datos de SQL Server es el siguiente:
  - Almacenamiento de uso general (SSD): 16 TiB para todas las ediciones
  - Almacenamiento de IOPS provisionadas: 16 TiB para todas las ediciones
  - Almacenamiento magnético: 1 TiB para todas las ediciones

  Si necesita una cantidad mayor de almacenamiento, puede usar la fragmentación entre varias instancias de base de datos para evitar este límite. Esta estrategia requiere una lógica de enrutamiento dependiente de los datos en las aplicaciones que se conectan con el sistema fragmentado. Puede usar un marco de fragmentación ya existente o escribir código personalizado para habilitarlo. Si usa un marco ya existente, este no podrá instalar ningún componente en el mismo servidor que la instancia de base de datos.
- El tamaño mínimo de almacenamiento para las instancias de base de datos de SQL Server es el siguiente:
  - Almacenamiento de uso general (SSD) – 20 GiB para ediciones Enterprise, Standard, Web y Express
  - Almacenamiento de IOPS provisionadas – 20 GiB para ediciones Enterprise, Standard, Web y Express
  - Almacenamiento magnético – 20 GiB para ediciones Enterprise, Standard, Web y Express
- Amazon RDS no admite la ejecución de estos servicios en el mismo servidor que la instancia de base de datos de RDS:
  - Data Quality Services
  - Master Data Services

  Para utilizar esas características, recomendamos que instale SQL Server en una instancia de Amazon EC2 o utilice una instancia de SQL Server local. En esos casos, la instancia de EC2 o SQL Server funciona como servidor de Master Data Services para su instancia de base de datos de SQL Server en Amazon RDS. Puede instalar SQL Server en una instancia Amazon EC2 con almacenamiento de Amazon EBS, de acuerdo con las políticas de licencias de Microsoft.
- A causa de las limitaciones de Microsoft SQL Server, restaurar a un momento dado antes de completar la ejecución de `DROP DATABASE` podría no reflejar el estado de la base de datos en ese momento. Por ejemplo, la base de datos abandonada se restaura normalmente a su estado hasta 5 minutos antes de que se ejecute el comando `DROP DATABASE`. Este tipo de restauración significa que no puede restaurar las transacciones realizadas durante esos minutos en su base de datos abandonada. Para resolver este inconveniente, puede volver a ejecutar el comando `DROP`

`DATABASE` después de que se complete la operación de restauración. Al eliminar una base de datos, se eliminan los registros de transacciones correspondientes.

- En SQL Server, las bases de datos se crean después de crear la instancia de base de datos. Los nombres de base de datos siguen las reglas de nomenclatura habituales en SQL Server con las siguientes diferencias.
  - Los nombres de la base de datos no pueden comenzar con `rdsadmin`.
  - No pueden comenzar ni terminar con un espacio o una tabulación.
  - No pueden contener ninguno de los caracteres que crean una nueva línea.
  - No pueden contener una comilla simple (`'`).
  - Actualmente, RDS para SQL Server no admite actualizaciones automáticas de versiones secundarias. Para obtener más información, consulte Administración de versiones en Amazon RDS.
- SQL Server Web Edition solo permite utilizar la plantilla Dev/Test al crear una nueva instancia de base de datos de RDS para SQL Server.

Compatibilidad con clases de instancia de base de datos para Microsoft SQL Server

La capacidad de cómputo y de memoria de la instancia de base de datos se determina mediante su clase de instancia de base de datos. La clase de instancia de base de datos que necesita depende de la potencia de procesamiento y de los requisitos de memoria. Para obtener más información, consulte Clases de instancia de base de datos de .

A continuación se muestra una lista de las clases de instancia de base de datos compatibles con Microsoft SQL Server. Para ver la lista más actualizada, consulte la consola de RDS: https://console.aws.amazon.com/rds/.

No todas las clases de instancia de base de datos están disponibles en todas las versiones secundarias de SQL Server compatibles. Por ejemplo, algunas clases de instancias de base de datos más recientes, como db.r6i, no están disponibles en versiones secundarias anteriores. Puede utilizar el comando describe-orderable-db-instancia de la AWS CLI para averiguar qué clases de instancias de base de datos están disponibles para la edición y versión de SQL Server.

Edición de SQL Server	Rango de compatibilidad de 2022	Rango de compatibilidad de 2019	Rango de compatibilidad de 2017 y 2016
Enterprise Edition	db.t3.xlarge –db.t3.2xlarge	db.t3.xlarge –db.t3.2xlarge	db.t3.xlarge –db.t3.2xlarge
	db.r5.large –db.r5.24xlarge	db.r5.xlarge –db.r5.24xlarge	db.r5.xlarge –db.r5.24xlarge
	db.r5b.large –db.r5b.24xlarge	db.r5b.xlarge –db.r5b.24xlarge	db.r5b.xlarge –db.r5b.24xlarge
	db.r5d.large –db.r5d.24xlarge	db.r5d.xlarge –db.r5d.24xlarge	db.r5d.xlarge –db.r5d.24xlarge
	db.r6i.large –db.r6i.32xlarge	db.r6i.xlarge –db.r6i.32xlarge	db.r6i.xlarge –db.r6i.32xlarge
	db.m5.large –db.m5.24xlarge	db.m5.xlarge –db.m5.24xlarge	db.m5.xlarge –db.m5.24xlarge
	db.m5d.large –db.m5d.24xlarge	db.m5d.xlarge –db.m5d.24xlarge	db.m5d.xlarge –db.m5d.24xlarge
	db.m6i.large –db.m6i.32xlarge	db.m6i.xlarge –db.m6i.32xlarge	db.m6i.xlarge –db.m6i.32xlarge
	db.x2iedn.xlarge –db.x2iedn.32xlarge	db.x1.16xlarge –db.x1.32xlarge	db.x1.16xlarge –db.x1.32xlarge

Edición de SQL Server	Rango de compatibilidad de 2022	Rango de compatibilidad de 2019	Rango de compatibilidad de 2017 y 2016
	db.z1d.large –db.z1d.12xlarge	db.x1e.xlarge –db.x1e.32xlarge db.x2iedn.xlarge –db.x2iedn.32xlarge db.z1d.xlarge –db.z1d.12xlarge	db.x1e.xlarge –db.x1e.32xlarge db.x2iedn.xlarge –db.x2iedn.32xlarge db.z1d.xlarge –db.z1d.12xlarge

Edición de SQL Server	Rango de compatibilidad de 2022	Rango de compatibilidad de 2019	Rango de compatibilidad de 2017 y 2016
Standarc Edition	db.t3.xlarge –db.t3.2xlarge db.r5.large –db.r5.24xlarge db.r5b.large –db.r5b.8xlarge db.r5d.large –db.r5d.24xlarge db.r6i.large –db.r6i.8xlarge db.m5.large –db.m5.24xlarge db.m5d.large –db.m5d.24xlarge db.m6i.large –db.m6i.8xlarge db.x2iedn.xlarge –db.x2iedn.8xlarge db.z1d.large –db.z1d.12xlarge	db.t3.xlarge –db.t3.2xlarge db.r5.large –db.r5.24xlarge db.r5b.large –db.r5b.24xlarge db.r5d.large –db.r5d.24xlarge db.r6i.large –db.r6i.8xlarge db.m5.large –db.m5.24xlarge db.m5d.large –db.m5d.24xlarge db.m6i.large –db.m6i.8xlarge db.x1.16xlarge –db.x1.32xlarge db.x1e.xlarge –db.x1e.32xlarge	db.t3.xlarge –db.t3.2xlarge db.r5.large –db.r5.24xlarge db.r5b.large –db.r5b.24xlarge db.r5d.large –db.r5d.24xlarge db.r6i.large –db.r6i.8xlarge db.m5.large –db.m5.24xlarge db.m5d.large –db.m5d.24xlarge db.m6i.large –db.m6i.8xlarge db.x1.16xlarge –db.x1.32xlarge db.x1e.xlarge –db.x1e.32xlarge

Edición de SQL Server	Rango de compatibilidad de 2022	Rango de compatibilidad de 2019	Rango de compatibilidad de 2017 y 2016
		db.x2iedn .xlarge –db.x2iedn .32xlarge db.z1d.la rge –db.z1d.12 xlarge	db.x2iedn .xlarge –db.x2iedn .32xlarge db.z1d.la rge –db.z1d.12 xlarge
Web Edition	db.t3.sma ll –db.t3.xlarge db.r5.lar ge –db.r5.4xlarge db.r5b.la rge –db.r5b.4xlarge db.r5d.la rge –db.r5d.4xlarge db.r6i.la rge –db.r6i.4xlarge db.m5.lar ge –db.m5.4xlarge db.m5d.la rge –db.m5d.4xlarge db.m6i.la rge –db.m6i.4xlarge db.z1d.la rge –db.z1d.13 xlarge	db.t3.sma ll –db.t3.2xlarge db.r5.lar ge –db.r5.4xlarge db.r5b.la rge –db.r5b.4xlarge db.r5d.la rge –db.r5d.4xlarge db.r6i.la rge –db.r6i.4xlarge db.m5.lar ge –db.m5.4xlarge db.m5d.la rge –db.m5d.4xlarge db.m6i.la rge –db.m6i.4xlarge db.z1d.la rge –db.z1d.3xlarge	db.t3.sma ll –db.t3.2xlarge db.r5.lar ge –db.r5.4xlarge db.r5b.la rge –db.r5b.4xlarge db.r5d.la rge –db.r5d.4xlarge db.r6i.la rge –db.r6i.4xlarge db.m5.lar ge –db.m5.4xlarge db.m5d.la rge –db.m5d.4xlarge db.m6i.la rge –db.m6i.4xlarge db.z1d.la rge –db.z1d.3xlarge

Edición de SQL Server	Rango de compatibilidad de 2022	Rango de compatibilidad de 2019	Rango de compatibilidad de 2017 y 2016
Express Edition	`db.t3.mic ro –db.t3.xlarge`	`db.t3.mic ro –db.t3.xlarge`	`db.t3.mic ro –db.t3.xlarge`

Seguridad de Microsoft SQL Server

El motor de base de datos de Microsoft SQL Server usa la seguridad basada en roles. El nombre de usuario maestro que especifica al crear una instancia de base de datos es un inicio de sesión de autenticación de SQL Server que es miembro de los roles de servidor fijos `processadmin`, `public`, `setupadmin`.

Cualquier usuario que crea una base de datos obtiene el rol db_owner para esa base de datos y todos los permisos de nivel de base de datos, excepto los empleados para las copias de seguridad. Amazon RDS administra las copias de seguridad por usted.

Los siguientes roles de nivel de servidor no están disponibles en Amazon RDS for SQL Server:

- bulkadmin
- dbcreator
- diskadmin
- securityadmin
- serveradmin
- sysadmin

Los siguientes permisos de nivel de servidor no están disponibles en instancias base de datos de RDS for SQL Server:

- ALTER ANY DATABASE
- ALTER ANY EVENT NOTIFICATION
- ALTER RESOURCES

- ALTER SETTINGS (puede usar las operaciones de la API del grupo de parámetros de base de datos para modificar parámetros; para obtener más información, consulte Grupos de parámetros para Amazon RDS)
- AUTHENTICATE SERVER
- CONTROL_SERVER
- CREATE DDL EVENT NOTIFICATION
- CREATE ENDPOINT
- CREACIÓN DEL ROL DE SERVIDOR
- CREATE TRACE EVENT NOTIFICATION
- ELIMINAR CUALQUIER BASE DE DATOS
- EXTERNAL ACCESS ASSEMBLY
- SHUTDOWN (puede usar como alternativa la opción de reinicio de RDS)
- UNSAFE ASSEMBLY
- ALTER ANY AVAILABILITY GROUP
- CREATE ANY AVAILABILITY GROUP

Compatibilidad con el programa de conformidad de las instancias de base de datos de Microsoft SQL Server

AWSLos servicios de en el ámbito de aplicación han sido evaluados íntegramente por un auditor externo y dan como resultado una certificación, acreditación de conformidad o autoridad para operar (ATO). Para obtener más información, consulte Servicios de AWS incluidos en el ámbito por programa de conformidad.

Compatibilidad de HIPAA con instancias de base de datos de Microsoft SQL Server

Puede utilizar una base de datos Amazon RDS for Microsoft SQL Server para crear aplicaciones conformes con HIPAA. Puede guardar información de contenido sanitario, incluida información sanitaria protegida (PHI), si ha firmado un Acuerdo para socio empresarial (BAA) de AWS. Para obtener más información, consulte Conformidad con HIPAA.

Amazon RDS for SQL Server admite HIPAA en las siguientes versiones y ediciones:

- SQL Server 2022: Ediciones Enterprise, Standard y Web
- SQL Server 2019: Ediciones Enterprise, Standard y Web
- SQL Server 2017: Ediciones Enterprise, Standard y Web
- SQL Server 2016: Ediciones Enterprise, Standard y Web

Para disponer de compatibilidad con HIPAA en la instancia de base de datos, configure los siguientes tres componentes.

Componente	Detalles
Auditoría	Para configurar la auditoría, establezca el parámetro `rds.sqlserver_audit` en el valor `fedramp_hipaa`. Si la instancia de base de datos no utiliza aún un grupo de parámetros de base de datos personalizado, debe crear uno y asociarlo a la instancia de base de datos para poder modificar el parámetro `rds.sqlserver_audit`. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
Cifrado en tránsito	Para configurar el cifrado en tránsito, fuerce el uso de la Capa de conexión segura (SSL) en todas las conexiones a la instancia de base de datos. Para obtener más información, consulte ???.
Cifrado en reposo	Para configurar el cifrado en reposo, dispone de dos opciones: 1. Si está ejecutando SQL Server 2016–2022 Enterprise Edition o 2022 Standard Edition, puede usar el cifrado de datos transparente (TDE) para lograr el cifrado en reposo. Para obtener más información, consulte Compatibilidad con el Cifrado de datos transparente en SQL Server. 2. Puede configurar el cifrado en reposo utilizando claves de cifrado de AWS Key Management Service (AWS KMS). Para obtener más información, consulte Cifrado de recursos de Amazon RDS.

Compatibilidad con SSL para las instancias de base de datos de Microsoft SQL Server

Puede usar SSL para cifrar las conexiones entre las aplicaciones y las instancias de base de datos Amazon RDS en las que se ejecuta Microsoft SQL Server. También puede obligar a todas las conexiones con su instancia de base de datos a usar SSL. Si obliga a las conexiones a usar SSL, esto sucede de modo transparente para el cliente, que no tiene que hacer nada para usar SSL.

SSL es compatible con todas las regiones de AWS y con todas las ediciones admitidas de SQL Server. Para obtener más información, consulte ???.

Versiones de Microsoft SQL Server en Amazon RDS

Puede especificar cualquier versión admitida actualmente de Microsoft SQL Server al crear una nueva instancia de base de datos. Puede especificar la versión principal de Microsoft SQL Server (como Microsoft SQL Server 14.00) y cualquier versión secundaria admitida para la versión principal especificada. Si no se especifica ninguna versión, Amazon RDS cambia de forma predeterminada a una versión admitida, normalmente la más reciente. Si se especifica una versión principal pero no una versión secundaria, Amazon RDS usa de manera predeterminada una versión reciente de la versión principal especificada.

En la siguiente tabla se muestran las versiones admitidas para todas las ediciones y todas las regiones de AWS, excepto donde se indique. Para ver una lista de las versiones admitidas, así como de las versiones predeterminadas para instancias de bases de datos recién creadas, utilice el comando `describe-db-engine-versions` de la AWS CLI. En la siguiente tabla, se muestran las versiones de SQL Server admitidas en RDS:

Versión principal	Versión secundaria	API de RDS **`EngineVersion`** y CLI **`engine-version`**
SQL Server 2022	16.00.4131.2 (CU13)	`16.00.4131.2.v1`
	16.00.4125.3 (CU13)	`16.00.4125.3.v1`
	16.00.4120.1 (CU12 GDR)	`16.00.4120.1.v1`
	16.00.4115.5 (CU12)	`16.00.4115.5.v1`
	16.00.4105.2 (CU11)	

Versión principal	Versión secundaria	API de RDS **EngineVersion** y CLI **engine-version**
	16.00.4095.4 (CU10)	16.00.4105.2.v1
	16.00.4085.2 (CU9)	16.00.4095.4.v1
		16.00.4085.2.v1
SQL Server 2019	15.00.4382.1 (CU27)	15.00.4382.1.v1
	15.00.4375.4 (CU27)	15.00.4375.4.v1
	15.00.4365.2 (CU26)	15.00.4365.2.v1
	15.00.4355.3 (CU25)	15.00.4355.3.v1
	15.00.4345.5 (CU24)	15.00.4345.5.v1
	15.00.4335.1 (CU23)	15.00.4335.1.v1
	15.00.4322.2 (CU22)	15.00.4322.2.v1
	15.00.4316.3 (CU21)	15.00.4316.3.v1
	15.00.4312.2 (CU20)	15.00.4312.2.v1
	15.00.4236.7 (CU16)	15.00.4236.7.v1
	15.00.4198.2 (CU15)	15.00.4198.2.v1
	15.00.4153.1 (CU12)	15.00.4153.1.v1
	15.00.4073.23 (CU8)	15.00.4073.23.v1
	15.00.4043.16 (CU5)	15.00.4043.16.v1

Versión principal	Versión secundaria	API de RDS **EngineVersion** y CLI **engine-version**
SQL Server 2017	14.00.3471.2 (CU31)	`14.00.3471.2.v1`
	14.00.3465.1 (CU31)	`14.00.3465.1.v1`
	14.00.3460.9 (CU31)	`14.00.3460.9.v1`
	14.00.3451.2 (CU30)	`14.00.3451.2.v1`
	14.00.3421.10 (CU27)	`14.00.3421.10.v1`
	14.00.3401.7 (CU25)	`14.00.3401.7.v1`
	14.00.3381.3 (CU23)	`14.00.3381.3.v1`
	14.00.3356.20 (CU22)	`14.00.3356.20.v1`
	14.00.3294.2 (CU20)	`14.00.3294.2.v1`
	14.00.3281.6 (CU19)	`14.00.3281.6.v1`
SQL Server 2016	13.00.6441.1 (GDR)	`13.00.6441.1.v1`
	13.00.6435.1 (GDR)	`13.00.6435.1.v1`
	13.00.6430.49 (GDR)	`13.00.6430.49.v1`
	13.00.6419.1 (SP3 + Hotfix)	`13.00.6419.1.v1`
	13.00.6300.2 (SP3)	`13.00.6300.2.v1`

Administración de versiones en Amazon RDS

Amazon RDS incluye la administración de versiones flexible que le permite controlar cuándo y dónde se aplica el parche a su instancia de base de datos o se actualiza. Esto le permite realizar las siguientes tareas en su motor de base de datos:

- Conservación de la compatibilidad con versiones de parche de motor de base de datos.

- Pruebe las nuevas versiones de parches para verificar que funcionan con la aplicación antes de implementarlas en producción.
- Planificación y realización de actualizaciones de versión para cumplir con los requisitos de tiempo y los acuerdos de nivel de servicio.

Aplicación de parches del motor de Microsoft SQL Server en Amazon RDS

Amazon RDS agrega periódicamente parches de base de datos de Microsoft SQL Server oficiales en una versión del motor de instancia de base de datos que es específica de Amazon RDS. Para obtener más información sobre los parches de Microsoft SQL Server en cada versión del motor, consulte Compatibilidad de versiones y características en Amazon RDS.

Actualmente, realiza manualmente todas las actualizaciones del motor en su instancia de base de datos. Para obtener más información, consulte Actualizaciones del motor de base de datos de Microsoft SQL Server.

Programación de obsolescencia para las versiones de motor principales de Microsoft SQL Server en Amazon RDS

La siguiente tabla muestra la programación establecida de las obsolencias para las versiones de motor principales de Microsoft SQL Server.

Date	Información
9 de julio de 2024	Microsoft detendrá las actualizaciones críticas de revisiones de SQL Server 2014. Pa información, consulte Microsoft SQL Server 2014 en la documentación de Microsoft.
1 de junio de 2024	Amazon RDS planea finalizar la compatibilidad con Microsoft SQL Server 2014 con F En ese momento, se programará la migración a SQL Server 2016 (la versión secund disponible) de las instancias restantes. Para obtener más información, consulte el an ión de la asistencia de Amazon RDS para SQL Server para las versiones principales Para evitar la actualización automática desde Microsoft SQL Server 2014, puede act momento que desee. Para obtener más información, consulte Actualización de una v instancia de base de datos.

Date	Información
12 de julio de 2022	Microsoft detendrá las actualizaciones críticas de parches para SQL Server 2012. Pa información, consulte Microsoft SQL Server 2012 en la documentación de Microsoft.
1 de junio de 2022	Amazon RDS planea finalizar la compatibilidad con Microsoft SQL Server 2012 en RI En ese momento, se programará la migración a SQL Server 2014 (la versión secund disponible). Para obtener más información, consulte Announcement: Amazon RDS fo support for SQL Server 2012 major versions. Para evitar la actualización automática desde Microsoft SQL Server 2012, puede actu momento que desee. Para obtener más información, consulte Actualización de una v instancia de base de datos.
1 de septiembre de 2021	Amazon RDS está empezando a deshabilitar la creación de nuevas instancias de bas para SQL Server mediante Microsoft SQL Server 2012. Para obtener más informació ent: Amazon RDS for SQL Server ending support for SQL Server 2012 major version
12 de julio de 2019	El equipo de Amazon RDS no ofrece compatibilidad con Microsoft SQL Server 2008 2019. Las instancias restantes de Microsoft SQL Server 2008 R2 se están migrando versión secundaria más reciente disponible). Para evitar la actualización automática desde Microsoft SQL Server 2008 R2, puede momento que desee. Para obtener más información, consulte Actualización de una v instancia de base de datos.
25 de abril de 2019	Antes de finales de abril de 2019, no podrá crear nuevas instancias de base de datos SQL Server mediante Microsoft SQL Server 2008R2.

Características de Microsoft SQL Server en Amazon RDS

Las versiones de SQL Server admitidas en Amazon RDS incluyen las siguientes características. En general, las versiones también incluyen funciones de versiones anteriores, a menos que se indique lo contrario en la documentación de Microsoft.

Temas

- Características de Microsoft SQL Server 2022
- Características de Microsoft SQL Server 2019

- Características de Microsoft SQL Server 2017
- Características de Microsoft SQL Server 2016
- Fin del soporte de Microsoft SQL Server 2014 en Amazon RDS
- Fin del soporte de Microsoft SQL Server 2012 en Amazon RDS
- Fin del soporte de Microsoft SQL Server 2008 R2 en Amazon RDS

Características de Microsoft SQL Server 2022

SQL Server 2022 incluye muchas características nuevas, como las siguientes:

- Optimización de planes sensible a los parámetros: permite almacenar varios planes en caché para una sola declaración parametrizada, lo que podría reducir los problemas relacionados con la detección de parámetros.
- SQL Server Ledger: permite demostrar criptográficamente que sus datos no se han modificado sin autorización.
- Inicialización instantánea de archivos para eventos de crecimiento de archivos de registro de transacciones: permite una ejecución más rápida de los eventos de crecimiento de registros de hasta 64 MB, incluso en el caso de bases de datos con el TDE activado.
- Mejoras en la simultaneidad del bloqueo de páginas en el sistema: reduce el bloqueo de páginas y, al mismo tiempo, asigna y desasigna páginas y extensiones de datos, lo que proporciona importantes mejoras de rendimiento para cargas de trabajo pesadas de `tempdb`.

Para obtener la lista completa de características de SQL Server 2022, consulte Novedades de SQL Server 2022 (16.x) en la documentación de Microsoft.

Para ver una lista de las características no admitidas, consulte Características no compatibles y características con compatibilidad limitada.

Características de Microsoft SQL Server 2019

SQL Server 2019 incluye muchas características nuevas, como las siguientes:

- Recuperación acelerada de bases de datos (ADR): reduce el tiempo de recuperación tras un reinicio o una restauración de transacciones de larga ejecución.
- Procesamiento inteligente de consultas (IQP):

  - Realimentación de concesión de memoria en modo de fila: corrige las concesiones excesivas automáticamente, que de otro modo provocarían una pérdida de memoria y una simultaneidad reducida.
  - Modo por lotes en almacén de filas: habilita la ejecución del modo por lotes para cargas de trabajo analíticas sin requerir índices de almacén de columnas.
  - Compilación diferida de variables de tabla: mejora la calidad del plan y el rendimiento general de las consultas que hacen referencia a variables de tabla.
- Rendimiento inteligente:
  - `OPTIMIZE_FOR_SEQUENTIAL_KEY`Opción de índice: mejora el rendimiento de las inserciones de alta simultaneidad en los índices.
  - Escalabilidad indirecta mejorada del punto de control: ayuda a las bases de datos con cargas de trabajo DML pesadas.
  - Actualizaciones de espacio libre de páginas simultáneas (PFS): permite la gestión como un bloqueo compartido en lugar de un bloqueo exclusivo.
- Mejoras en la monitorización:
  - `WAIT_ON_SYNC_STATISTICS_REFRESH`Tipo de espera: muestra el tiempo acumulado a nivel de instancia invertido en operaciones de actualización de estadísticas sincrónicas.
  - Configuraciones de ámbito de base de datos: Incluyen `LIGHTWEIGHT_QUERY_PROFILING` y `LAST_QUERY_PLAN_STATS`.
  - Funciones de administración dinámica (DMF): incluyen `sys.dm_exec_query_plan_stats` y `sys.dm_db_page_info`.
- Advertencias de truncamiento detallado: el mensaje de error de truncamiento de datos se establece de forma predeterminada para incluir nombres de tabla y columna y el valor truncado.
- Creación de índices en línea reanudable: en SQL Server 2017, solo se admite la reconstrucción de índices en línea reanudable.

Para obtener la lista completa de características de SQL Server 2019, consulte Novedades de SQL Server 2019 (15.x) en la documentación de Microsoft.

Para ver una lista de las características no admitidas, consulte Características no compatibles y características con compatibilidad limitada.

Características de Microsoft SQL Server 2017

SQL Server 2017 incluye muchas características nuevas, como las siguientes:

- Procesamiento de consultas adaptativas
- Corrección automática del plan (una característica de ajuste automático)
- GraphDB
- Reconstrucciones de índices que pueden reanudarse

Para obtener la lista completa de características de SQL Server 2017, consulte Novedades de SQL Server 2017 en la documentación de Microsoft.

Para ver una lista de las características no admitidas, consulte Características no compatibles y características con compatibilidad limitada.

Características de Microsoft SQL Server 2016

Amazon RDS es compatible con las siguientes características de SQL Server 2016:

- Cifrado en todo momento
- Compatibilidad con JSON
- Análisis operativo
- Almacén de consultas
- Tablas temporales

Para obtener la lista completa de características de SQL Server 2016, consulte Novedades de SQL Server 2016 en la documentación de Microsoft.

Fin del soporte de Microsoft SQL Server 2014 en Amazon RDS

SQL Server 2014 ha llegado al final del soporte en Amazon RDS.

RDS está actualizando todas las instancias de base de datos existentes que aún utilizan SQL Server 2014 a la última versión secundaria de SQL Server 2016. Para obtener más información, consulte Administración de versiones en Amazon RDS.

Fin del soporte de Microsoft SQL Server 2012 en Amazon RDS

SQL Server 2012 ha llegado al final del soporte en Amazon RDS.

RDS está actualizando todas las instancias de base de datos existentes que aún utilizan SQL Server 2012 a la última versión secundaria de SQL Server 2016. Para obtener más información, consulte Administración de versiones en Amazon RDS.

Fin del soporte de Microsoft SQL Server 2008 R2 en Amazon RDS

SQL Server 2008 R2 ha llegado al final del soporte en Amazon RDS.

RDS está actualizando todas las instancias de base de datos existentes que aún utilizan SQL Server 2008 R2 a la última versión secundaria de SQL Server 2012. Para obtener más información, consulte Administración de versiones en Amazon RDS.

Compatibilidad de captura de datos de cambio para instancias de base de datos de Microsoft SQL Server

Amazon RDS admite la captura de datos de cambios (CDC) para las instancias de base de datos que ejecutan Microsoft SQL Server. CDC captura cambios que se realizan a los datos de las tablas y almacena los metadatos sobre cada cambio a los que puede obtener acceso más tarde. Para obtener más información, consulte Captura de datos de cambio en la documentación de Microsoft.

Amazon RDS admite CDC para las siguientes ediciones y versiones de SQL Server:

- Microsoft SQL Server Enterprise Edition (todas las versiones)
- Microsoft SQL Server Standard Edition:
  - 2022
  - 2019
  - 2017
  - 2016, versión 13.00.4422.0 SP1 CU2 y posterior

Para usar CDC con las instancias de base de datos de Amazon RDS, primero habilite o deshabilite CDC en el nivel de base de datos mediante los procedimientos almacenados proporcionados por RDS. Tras ello, cualquier usuario que tenga el rol `db_owner` de esa base de datos puede usar los procedimientos almacenados de Microsoft nativos para controlar CDC en la base de datos. Para obtener más información, consulte Uso de la captura de datos de cambios de Amazon RDS para SQL Server.

Puede usar CDC y AWS Database Migration Service para habilitar la reproducción continua desde instancias de base de datos de SQL Server.

Características no compatibles y características con compatibilidad limitada

Las siguientes características de Microsoft SQL Server no son compatibles con Amazon RDS:

- Copia de seguridad en Almacenamiento de blobs de Microsoft Azure
- Extensión del grupo de búferes
- Políticas de contraseñas personalizadas
- Data Quality Services
- Trasvase de registros de bases de datos
- Instantáneas de base de datos (solo admite instantáneas de instancia de base de datos de Amazon RDS)
- Se han ampliado los procedimientos almacenados, incluido xp_cmdshell
- Compatibilidad con FILESTREAM
- Tablas de archivos
- Machine Learning y servicios R (requiere acceso al sistema operativo para la instalación)
- Planes de mantenimiento
- Recopilador de datos de desempeño
- Administración basada en políticas
- PolyBase
- Replicación
- Gobernador de recursos
- Desencadenadores de nivel de servidor
- Puntos de enlace de Service Broker
- Base de datos Stretch
- Propiedad de base de datos TRUSTWORTHY (requiere el rol de administrador del sistema)
- Puntos de enlace T-SQL (las operaciones que usan CREATE ENDPOINT no están disponibles)

- WCF Data Services

Las siguientes características de Microsoft SQL Server tienen compatibilidad limitada en Amazon RDS:

- Consultas distribuidas o servidores vinculados. Para obtener más información, consulte Implementación de servidores vinculados con Amazon RDS for Microsoft SQL Server.
- Common Runtime Language (CLR). En RDS for SQL Server 2016 y versiones anteriores, CLR es compatible en modo SAFE y solo cuando se utilizan bits de ensamblaje. CLR no es compatible con RDS for SQL Server 2017 y versiones posteriores. Para obtener más información, consulte Integración de Common Runtime Language en la documentación de Microsoft.
- Servidores enlazados con Oracle OLEDB en Amazon RDS para SQL Server. Para obtener más información, consulte Compatibilidad con servidores enlazados con Oracle OLEDB en Amazon RDS para SQL Server.

Las siguientes características no son compatibles en Amazon RDS con SQL Server 2022:

- Suspensión de la base de datos para instantánea
- Origen de datos externo
- Copia de seguridad y restauración en un almacenamiento de objetos compatible con S3
- Integración del almacén de objetos
- TLS 1.3 y MS-TDS 8.0
- Copia de seguridad, compresión y descarga con QAT
- SQL Server Analysis Services (SSAS)
- Duplicación de bases de datos con implementaciones multi-AZ SQL Server Always On es el único método compatible con implementaciones multi-AZ

Implementaciones Multi-AZ con creación de reflejos de base de datos de Microsoft SQL Server o grupos de disponibilidad Always On

Amazon RDS admite implementaciones Multi-AZ para instancias de base de datos en las que se ejecuta Microsoft SQL Server mediante el uso de la creación de reflejos de bases de datos

(DBM) de SQL Server o los grupos de disponibilidad (AG) Always On. Las implementaciones Multi-AZ proporcionan unos niveles superiores de disponibilidad, durabilidad de los datos y tolerancia a errores para las instancias de base de datos. Si se produce una interrupción del servicio no planificada o un mantenimiento planificado de la base de datos, Amazon RDS conmuta automáticamente a la réplica secundaria actualizada para que las operaciones de la base de datos puedan reanudarse rápidamente sin intervención manual. Las instancias principal y secundaria usan el mismo punto de enlace, cuya dirección de red física cambia a la réplica secundaria pasiva como parte del proceso de conmutación por error. No tiene que volver a configurar su aplicación cuando se produzca una conmutación por error.

Amazon RDS administra la conmutación por error monitorizando activamente el despliegue Multi-AZ e iniciando una conmutación por error cuando se produzca un problema en la instancia principal. La conmutación por error no ocurre, a menos que las instancias en espera y principal estén totalmente sincronizadas. Amazon RDS mantiene activamente su implementación Multi-AZ mediante la reparación automática de las instancias de base de datos con problemas y el restablecimiento de la reproducción síncrona. No es necesario que administre nada. Amazon RDS se encarga de la instancia principal, el testigo de creación de reflejo y la instancia en espera. Al configurar Multi-AZ de SQL Server, RDS configura instancias secundarias pasivas para todas las bases de datos de la instancia.

Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.

Uso del cifrado de datos transparente para cifrar los datos en reposo

Amazon RDS admite el cifrado de datos transparente (TDE) de Microsoft SQL Server, que cifra de forma transparente los datos almacenados. Amazon RDS utiliza grupos de opciones para habilitar y configurar estas características. Para obtener más información acerca de la opción TDE, consulte Compatibilidad con el Cifrado de datos transparente en SQL Server.

Funciones y procedimientos almacenados para Amazon RDS for Microsoft SQL Server

A continuación, encontrará una lista de los procedimientos almacenados y las funciones de Amazon RDS que ayudan a automatizar las tareas de SQL Server.

Tipo de tarea	Procedimiento o función	Dónde se utiliza
Tareas administrativas	`rds_drop_database`	Eliminación de una base de datos en una instancia de base de datos de Amazon RDS para Microsoft SQL Server
	`rds_failover_time`	Determinación de la hora de la última conmutación por error de Amazon RDS para SQL Server
	`rds_modify_db_name`	Cambio del nombre de una base de datos de Amazon RDS para Microsoft SQL Server en una implementación multi-AZ
	`rds_read_error_log`	Visualización de registros de agentes y errores
	`rds_set_configuration`	Esta operación se utiliza para establecer diversas configuraciones de instancia de base de datos: • Captura de datos de cambio para instancias Multi-AZ • Definición del periodo de retención para los archivos de seguimiento y volcado • Compresión de archivos de copia de seguridad
	`rds_set_database_online`	Transición de una base de datos de Amazon RDS para SQL Server de OFFLINE a ONLINE
	`rds_set_system_database_sync_objects`	Activación de la replicación de trabajos del agente de SQL Server

Tipo de tarea	Procedimiento o función	Dónde se utiliza

	`rds_fn_get_system_database_sync_objects`
	
	`rds_fn_server_object_last_sync_time`	

	`rds_show_configuration`	Para ver los valores que se configuran mediante `rds_set_configuration` , consulte estos temas: • Captura de datos de cambio para instancias Multi-AZ • Definición del periodo de retención para los archivos de seguimiento y volcado
	`rds_shrink_tempdbfile`	Reducción del tamaño de la base de datos tempdb
Captura de datos de cambio (CDC)	`rds_cdc_disable_db`	Desactivación de CDC
	`rds_cdc_enable_db`	Habilitación de CDC
Correo electrónico de base de datos	`rds_fn_sysmail_allitems`	Visualización de mensajes, registros y archivos adjuntos

Tipo de tarea	Procedimiento o función	Dónde se utiliza
	`rds_fn_sysmail_event_log`	Visualización de mensajes, registros y archivos adjuntos
	`rds_fn_sysmail_mailattachments`	Visualización de mensajes, registros y archivos adjuntos
	`rds_sysmail_control`	Esta operación se utiliza para iniciar y detener la cola de correo: • Inicio de la cola de correo • Detención de la cola de correo
	`rds_sysmail_delete_mailitems_sp`	Eliminación de mensajes
Copia de seguridad y restauración nativas	`rds_backup_database`	Realización de copia de seguridad de una base de datos
	`rds_cancel_task`	Cancelación de una tarea
	`rds_finish_restore`	Finalización de la restauración de una base de datos
	`rds_restore_database`	Restauración de una base de datos

Tipo de tarea	Procedimiento o función	Dónde se utiliza
	`rds_restore_log`	Restauración de un registro
Transferencia de archivos Amazon S3	`rds_delete_from_filesystem`	Eliminación de los archivos de la instancia de base de datos de RDS
	`rds_download_from_s3`	Descarga de archivos desde un bucket de Amazon S3 a una instancia de base de datos de SQL Server
	`rds_gather_file_details`	Descripción de los archivos de la instancia de base de datos de RDS
	`rds_upload_to_s3`	Carga de archivos desde una instancia de base de datos de SQL Server a un bucket de Amazon S3
Coordinador de transacciones distribuidas de Microsoft (MSDTC)	`rds_msdtc_transaction_tracing`	Uso del seguimiento de transacciones
SQL Server Audit	`rds_fn_get_audit_file`	Visualización de registros de auditoría

Tipo de tarea	Procedimiento o función	Dónde se utiliza

Cifrado de datos transparente	`rds_backup_tde_certificate`
	
	`rds_drop_tde_certificate`
	
	`rds_restore_tde_certificate`
	
	`rds_fn_list_user_tde_certificates`
		Compatibilidad con el Cifrado de datos transparente en SQL Server

Tipo de tarea	Procedimiento o función	Dónde se utiliza
Microsoft Business Intelligence (MSBI)	`rds_msbi_task`	Esta operación se utiliza con SQL Server Analysis Services (SSAS): • Implementación de proyectos SSAS en Amazon RDS • Agregar un usuario de dominio como administrador de bases de datos • Copia de seguridad de una base de datos SSAS • Restauración de una base de datos SSAS Esta operación también se utiliza con SQL Server Integration Services (SSIS): • Permisos administrativos en SSISDB • Implementación de un proyecto SSIS Esta operación también se utiliza con SQL Server Reporting Services (SSRS): • Concesión de acceso a usuarios de dominio • Revocación de permisos de nivel de sistema
	`rds_fn_task_status`	Esta operación muestra el estado de las tareas de MSBI: • SSAS: Monitoreo del estado de una tarea de implementación • SSIS: Monitoreo del estado de una tarea de implementación • SSRS: Monitoreo del estado de una tarea

Tipo de tarea	Procedimiento o función	Dónde se utiliza
SSIS	`rds_drop_ssis_database`	Borrado de la base de datos SSISDB
	`rds_sqlagent_proxy`	Creación de un proxy de SSIS
SSRS	`rds_drop_ssrs_databases`	Eliminación de las bases de datos SSRS

Zona horaria local para las instancias de base de datos de Microsoft SQL Server

La zona horaria de una instancia de base de datos de Amazon RDS en la que se ejecuta Microsoft SQL Server se define de forma predeterminada. El valor predeterminado actual es la Hora universal coordinada (UTC). Si lo prefiere, puede definir la zona horaria de su instancia de base de datos en una hora local para que coincida con la zona horaria de sus aplicaciones.

La zona horaria se define al crear inicialmente la instancia de base de datos. Puede crear su instancia de base de datos con la AWS Management Console, la acción CreateDBInstance de la API de Amazon RDS o con el comando de la AWS CLI create-db-instance.

Si su instancia de base de datos forma parte de una implementación Multi-AZ (que use la creación de reflejos de SQL Server o grupos de disponibilidad), al conmutar por error, la zona horaria seguirá siendo la zona horaria local que definió. Para obtener más información, consulte Implementaciones Multi-AZ con creación de reflejos de base de datos de Microsoft SQL Server o grupos de disponibilidad Always On.

Cuando solicite una restauración a un momento dado, debe especificar la hora a la que desea restaurar. La hora se muestra en la zona horaria local. Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

A continuación se indican las limitaciones de la definición de la hora local en una instancia de base de datos:

- No puede modificar la zona horaria de una instancia de base de datos de SQL Server.
- No puede restaurar una instantánea a partir de una instancia de base de datos de una zona horaria en una instancia de base de datos de una zona horaria diferente.
- Es recomendable que no restaure un archivo de copia de seguridad de una zona horaria en una zona horaria diferente. Si restaura un archivo de copia de seguridad de una zona horaria en otra zona horaria distinta, debe auditar las consultas y las aplicaciones para comprobar los efectos del cambio de zona horaria. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Zonas horarias admitidas

Puede definir su zona horaria local en uno de los valores que se muestran en la siguiente tabla.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Afganistán	(UTC+04:30)	Kabul	Esta zona horaria no aplica el horario de verano.
Hora estándar de Alaska	(UTC–09:00)	Alaska	
Hora estándar de las Islas Aleutianas	(UTC–10:00)	Islas Aleutianas	
Hora estándar de Altai	(UTC+07:00)	Barnaul, Gorno-Altaisk	
Hora estándar árabe	(UTC+03:00)	Kuwait, Riad	Esta zona horaria no aplica el horario de verano.
Hora estándar árabe	(UTC+04:00)	Abu Dabi, Muscat	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar arábica	(UTC+03:00)	Bagdad	Esta zona horaria no aplica el horario de verano.
Hora estándar de Argentina	(UTC–03:00)	Ciudad de Buenos Aires	Esta zona horaria no aplica el horario de verano.
Hora estándar de Astracán	(UTC+04:00)	Astracán, Uliánovsk	
Hora estándar del Atlántico	(UTC–04:00)	Hora del Atlántico (Canadá)	
Hora estándar central de Australia	(UTC+09:30)	Darwin	Esta zona horaria no aplica el horario de verano.
Hora estándar del centro-oeste de Australia	(UTC+08:45)	Eucla	
Hora estándar de Australia oriental	(UTC+10:00)	Canberra, Melbourne, Sídney	
Hora estándar de Azerbaiyán	(UTC+04:00)	Bakú	
Hora estándar de las Azores	(UTC–01:00)	Azores	
Hora estándar de Bahía	(UTC–03:00)	Salvador	
Hora estándar de Bangladesh	(UTC+06:00)	Dacca	Esta zona horaria no aplica el horario de verano.
Hora estándar de Bielorrusia	(UTC+03:00)	Minsk	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Bougainville	(UTC+11:00)	Isla Bougainville	
Hora estándar central de Canadá	(UTC–06:00)	Saskatchewan	Esta zona horaria no aplica el horario de verano.
Hora estándar de Cabo Verde	(UTC–01:00)	Archipiélago de Cabo Verde	Esta zona horaria no aplica el horario de verano.
Hora estándar del Cáucaso	(UTC+04:00)	Ereván	
Hora estándar de Australia central	(UTC+09:30)	Adelaida	
Hora estándar de América central	(UTC–06:00)	América Central	Esta zona horaria no aplica el horario de verano.
Hora estándar de Asia central	(UTC+06:00)	Astana	Esta zona horaria no aplica el horario de verano.
Hora estándar de Brasil central	(UTC–04:00)	Cuiaba	
Hora estándar de Europa central	(UTC+01:00)	Belgrado, Bratislava, Budapest, Liubliana, Praga	
Hora estándar europea central	(UTC+01:00)	Sarajevo, Skopie, Varsovia, Zagreb	
Hora estándar del Pacífico central	(UTC+11:00)	Islas Salomón, Nueva Caledonia	Esta zona horaria no aplica el horario de verano.

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar central	(UTC–06:00)	Hora central (Estados Unidos y Canadá)	
Hora estándar central (México)	(UTC–06:00)	Guadalajara, Ciudad de México, Monterrey	
Hora estándar de las islas Chatham	(UTC+12:45)	Islas Chatham	
Hora estándar de China	(UTC+08:00)	Pekín, Chongqing , Hong Kong, Urumchi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Cuba	(UTC–05:00)	Habana	
Hora estándar de línea de fecha	(UTC–12:00)	Línea internacional de cambio de fecha del oeste	Esta zona horaria no aplica el horario de verano.
Hora estándar de África oriental	(UTC+03:00)	Nairobi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Australia oriental	(UTC+10:00)	Brisbane	Esta zona horaria no aplica el horario de verano.
Hora estándar de Europa oriental	(UTC+02:00)	Chisinau	
Hora estándar de América del Sur oriental	(UTC–03:00)	Brasilia	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de la Isla de Pascua	(UTC–06:00)	Isla de Pascua	
Hora estándar oriental	(UTC–05:00)	Hora oriental (Estados Unidos y Canadá)	
Hora estándar oriental (México)	(UTC–05:00)	Chetumal	
Hora estándar de Egipto	(UTC+02:00)	El Cairo	
Hora estándar de Ekaterimburgo	(UTC+05:00)	Ekaterimburgo	
Hora estándar de Fiyi	(UTC+12:00)	Fiyi	
Hora estándar de FLE	(UTC+02:00)	Helsinki, Kiev, Riga, Sofía, Tallin, Vilna	
Hora estándar de Georgia	(UTC+04:00)	Tiflis	Esta zona horaria no aplica el horario de verano.
Hora estándar GMT	(UTC)	Dublín, Edimburgo, Lisboa, Londres	Esta zona horaria no es la misma que la hora media de Greenwich. Esta zona horaria aplica el horario de verano.
Hora estándar de Groenlandia	(UTC–03:00)	Groenlandia	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Greenwich	(UTC)	Monrovia, Reikiavik	Esta zona horaria no aplica el horario de verano.
Hora estándar GTB	(UTC+02:00)	Atenas, Bucarest	
Hora estándar de Haití	(UTC–05:00)	Haití	
Hora estándar de Hawái	(UTC–10:00)	Hawái	
Hora estándar de India	(UTC+05:30)	Chennai, Calcuta, Mumbai, Nueva Delhi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Irán	(UTC+03:30)	Teherán	
Hora estándar de Israel	(UTC+02:00)	Jerusalén	
Hora estándar de Jordania	(UTC+02:00)	Amán	
Hora estándar de Kaliningrado	(UTC+02:00)	Kaliningrado	
Hora estándar de Kamchatka	(UTC+12:00)	Petropavlovsk-Kamchatsky – Antiguo	
Hora estándar de Corea	(UTC+09:00)	Seúl	Esta zona horaria no aplica el horario de verano.
Hora estándar de Libia	(UTC+02:00)	Trípoli	
Hora estándar de las Islas de la Línea	(UTC+14:00)	Isla Kiritimati	
Hora estándar de Lord Howe	(UTC+10:30)	Isla Lord Howe	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Magadán	(UTC+11:00)	Magadán	Esta zona horaria no aplica el horario de verano.
Hora estándar de Magallanes	(UTC–03:00)	Punta Arenas	
Hora estándar de Marquesas	(UTC–09:30)	Islas Marquesas	
Hora estándar de Mauricio	(UTC+04:00)	Port-Louis	Esta zona horaria no aplica el horario de verano.
Hora estándar de Oriente Medio	(UTC+02:00)	Beirut	
Hora estándar de Montevideo	(UTC–03:00)	Montevideo	
Hora estándar de Marruecos	(UTC+01:00)	Casablanca	
Hora estándar de las montañas	(UTC–07:00)	Hora de las montañas (Estados Unidos y Canadá)	
Hora estándar de las montañas (México)	(UTC–07:00)	Chihuahua, La Paz, Mazatlán	
Hora estándar de Myanmar	(UTC+06:30)	Yangón (Rangún)	Esta zona horaria no aplica el horario de verano.
Hora estándar de Asia central norte	(UTC+07:00)	Novosibirsk	
Hora estándar de Namibia	(UTC+02:00)	Windhoek	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Nepal	(UTC+05:45)	Katmandú	Esta zona horaria no aplica el horario de verano.
Hora estándar de Nueva Zelanda	(UTC+12:00)	Auckland, Wellington	
Hora estándar de Terranova	(UTC–03:30)	Terranova	
Hora estándar de Norfolk	(UTC+11:00)	Isla Norfolk	
Hora estándar del este de Asia del Norte	(UTC+08:00)	Irkutsk	
Hora estándar del norte de Asia	(UTC+07:00)	Krasnoyarsk	
Hora estándar de Corea del Norte	(UTC+09:00)	Pyongyang	
Hora estándar de Omsk	(UTC+06:00)	Omsk	
Hora estándar de Sudamérica del Pacífico	(UTC–03:00)	Santiago	
Hora estándar del Pacífico	(UTC–08:00)	Hora del Pacífico (Estados Unidos y Canadá)	
Hora estándar del Pacífico (México)	(UTC–08:00)	Baja California	
Hora estándar de Pakistán	(UTC+05:00)	Islamabad, Karachi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Paraguay	(UTC–04:00)	Asunción	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar romance	(UTC+01:00)	Bruselas, Copenhague, Madrid, París	
Zona horaria 10 de Rusia	(UTC+11:00)	Chokurdakh	
Zona horaria 11 de Rusia	(UTC+12:00)	Anadyr, Petropavlovsk-Kamchatsky	
Zona horaria 3 de Rusia	(UTC+04:00)	Izhevsk, Samara	
Hora estándar de Rusia	(UTC+03:00)	Moscú, San Petersburgo, Volgogrado	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudamérica oriental	(UTC–03:00)	Cayena, Fortaleza	Esta zona horaria no aplica el horario de verano.
Hora estándar del Pacífico de Sudamérica	(UTC–05:00)	Bogotá, Lima, Quito, Río Branco	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudamérica occidental	(UTC–04:00)	Georgetown, La Paz, Manaos, San Juan	Esta zona horaria no aplica el horario de verano.
Hora estándar de San Pedro	(UTC–03:00)	San Pedro y Miquelón	
Hora estándar de Sajalín	(UTC+11:00)	Sajalín	
Hora estándar de Samoa	(UTC+13:00)	Samoa	
Hora estándar de Santo Tomé	(UTC+01:00)	Santo Tomé	
Hora estándar de Sarátov	(UTC+04:00)	Sarátov	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar del sureste de Asia	(UTC+07:00)	Bangkok, Hanói, Yakarta	Esta zona horaria no aplica el horario de verano.
Hora estándar de Singapur	(UTC+08:00)	Kuala Lumpur, Singapur	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudáfrica	(UTC+02:00)	Harare (Pretoria)	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sri Lanka	(UTC+05:30)	Sri Jayawarde nepura	Esta zona horaria no aplica el horario de verano.
Hora estándar de Sudán	(UTC+02:00)	Jartum	
Hora estándar de Siria	(UTC+02:00)	Damasco	
Hora estándar de Taipéi	(UTC+08:00)	Taipéi	Esta zona horaria no aplica el horario de verano.
Hora estándar de Tasmania	(UTC+10:00)	Hobart	
Hora estándar de Tocantins	(UTC–03:00)	Araguaina	
Hora estándar de Tokio	(UTC+09:00)	Osaka, Sapporo, Tokio	Esta zona horaria no aplica el horario de verano.
Hora estándar de Tomsk	(UTC+07:00)	Tomsk	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Tonga	(UTC+13:00)	Nuku'alofa	Esta zona horaria no aplica el horario de verano.
Hora estándar de Transbaikal	(UTC+09:00)	Chita	
Hora estándar de Turquía	(UTC+03:00)	Estambul	
Hora estándar de Islas Turcas y Caicos	(UTC–05:00)	Islas Turcas y Caicos	
Hora estándar de Ulán Bator	(UTC+08:00)	Ulán Bator	Esta zona horaria no aplica el horario de verano.
Hora estándar oriental de Estados Unidos	(UTC–05:00)	Indiana (Este)	
Hora estándar de las montañas (Estados Unidos)	(UTC–07:00)	Arizona	Esta zona horaria no aplica el horario de verano.
UTC	UTC	Horario universal coordinado	Esta zona horaria no aplica el horario de verano.
UTC–02	(UTC–02:00)	Horario universal coordinado–02	Esta zona horaria no aplica el horario de verano.
UTC–08	(UTC–08:00)	Horario universal coordinado–08	
UTC–09	(UTC–09:00)	Horario universal coordinado–09	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
UTC–11	(UTC–11:00)	Horario universal coordinado–11	Esta zona horaria no aplica el horario de verano.
UTC+12	(UTC+12:00)	Horario universal coordinado+12	Esta zona horaria no aplica el horario de verano.
UTC+13	(UTC+13:00)	Horario universal coordinado+13	
Hora estándar de Venezuela	(UTC–04:00)	Caracas	Esta zona horaria no aplica el horario de verano.
Hora estándar de Vladivostok	(UTC+10:00)	Vladivostok	
Hora estándar de Volgogrado	(UTC+04:00)	Volgogrado	
Hora estándar de Australia occidental	(UTC+08:00)	Perth	Esta zona horaria no aplica el horario de verano.
Hora estándar de África central occidental	(UTC+01:00)	África central occidental	Esta zona horaria no aplica el horario de verano.
Hora estándar de Europa occidental	(UTC+01:00)	Ámsterdam, Berlín, Berna, Roma, Estocolmo, Viena	
Hora estándar de Mongolia occidental	(UTC+07:00)	Hovd	

Zona horaria	Diferencia de hora estándar	Descripción	Notas
Hora estándar de Asia occidental	(UTC+05:00)	Ashgabat, Tashkent	Esta zona horaria no aplica el horario de verano.
Hora estándar de Cisjordania	(UTC+02:00)	Gaza, Hebrón	
Hora estándar del Pacífico occidental	(UTC+10:00)	Guam, Port Moresby	Esta zona horaria no aplica el horario de verano.
Hora estándar de Yakutsk	(UTC+09:00)	Yakutsk	

Licencias de Microsoft SQL Server en Amazon RDS

Al configurar una instancia de base de datos Amazon RDS para Microsoft SQL Server, se incluye la licencia de software.

Esto quiere decir que no es necesario que compre por su cuenta licencias de SQL Server. AWS ya es titular de la licencia del software de base de datos de SQL Server. Los precios de Amazon RDS incluyen la licencia de software, los recursos de hardware subyacentes y las funciones de administración de Amazon RDS.

Amazon RDS admite las siguientes ediciones de Microsoft SQL Server:

- Enterprise
- Standard
- Web
- Express

> **Note**
>
> Las licencias para SQL Server Web Edition solo admiten para páginas, sitios, aplicaciones y servicios web públicos y accesibles a través de Internet. Este nivel de compatibilidad es necesario para la conformidad de los derechos de uso de Microsoft. Para obtener más información, consulte las condiciones del servicio de AWS.

Amazon RDS admite implementaciones Multi-AZ para instancias de base de datos en las que se ejecuta Microsoft SQL Server mediante el uso de la creación de reflejos de bases de datos (DBM) de SQL Server o los grupos de disponibilidad (AG) Always On. No hay más requisitos de licencia adicionales para despliegues Multi-AZ. Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.

Restauración de instancias de base de datos con licencia caducada

Amazon RDS toma instantáneas de instancias de base de datos con licencia caducada. Si la instancia termina por problemas con la licencia, puede restaurarla a partir de la instantánea a una nueva instancia de base de datos. Las instancias de base de datos nuevas tienen una licencia incluida.

Para obtener más información, consulte Restauración de instancias de base de datos con licencia caducada de Amazon RDS para SQL Server.

Desarrollo y pruebas

Debido a los requisitos de las licencias, no podemos ofrecer la edición Developer de SQL Server en Amazon RDS. Puede utilizar la edición Express para muchas necesidades de desarrollo, pruebas y otras necesidades que no son de producción. Sin embargo, si necesita las capacidades completas de las características de una instalación empresarial de SQL Server para el desarrollo, puede descargar e instalar SQL Server Developer Edition en RDS Custom para SQL Server utilizando un CEV con BYOM. Para obtener más información, consulte Preparación de una CEV con Bring Your Own Media (BYOM). No se necesita una infraestructura dedicada para la edición Developer. Al usar su propio host, también obtiene acceso a otras características de programación a las que no se puede acceder en Amazon RDS. Para obtener más información sobre las diferencias entre las ediciones de SQL Server, consulte Ediciones y características admitidas de SQL Server 2019 en la documentación de Microsoft.

Conexión a la instancia de base de datos de Microsoft SQL Server

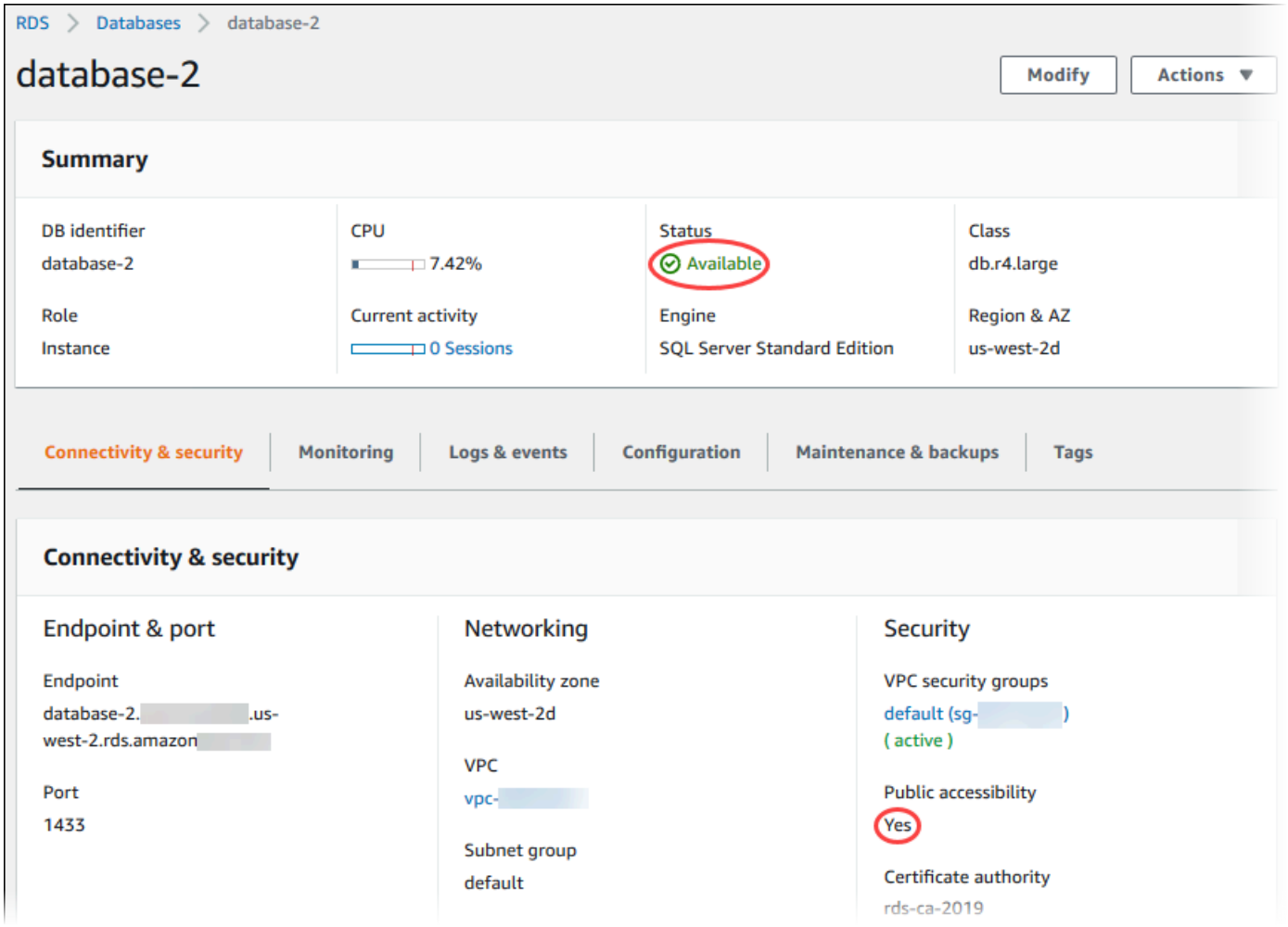
Después de que Amazon RDS aprovisione su instancia de base de datos, puede usar cualquier aplicación cliente de SQL estándar para conectarse a la instancia. En este tema, se conecta a la instancia de base de datos utilizando Microsoft SQL Server Management Studio (SSMS) o SQL Workbench/J.

Para ver un ejemplo que le enseña los procesos para crear y conectarse a una instancia de base de datos de muestra, consulte Creación de una instancia de base de datos de Microsoft SQL Server y conexión a ella.

Antes de conectarse

Para poder conectarse a su instancia de base de datos, tiene que estar disponible y accesible.

1. Asegúrese de que su estado sea `available`. Puede comprobarlo en la página de detalles de su instancia en la AWS Management Console o mediante el comando de la AWS CLI describe-db-instances.



2. Asegúrese de que su fuente pueda acceder a ella. Dependiendo de su situación, es posible que no sea necesario que sea de acceso público. Para obtener más información, consulte VPC de Amazon y Amazon RDS.
3. Asegúrese de que las reglas de entrada del grupo de seguridad de VPC permitan el acceso a la instancia de base de datos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Búsqueda del punto de enlace de instancia de base de datos y el número de puerto

Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.

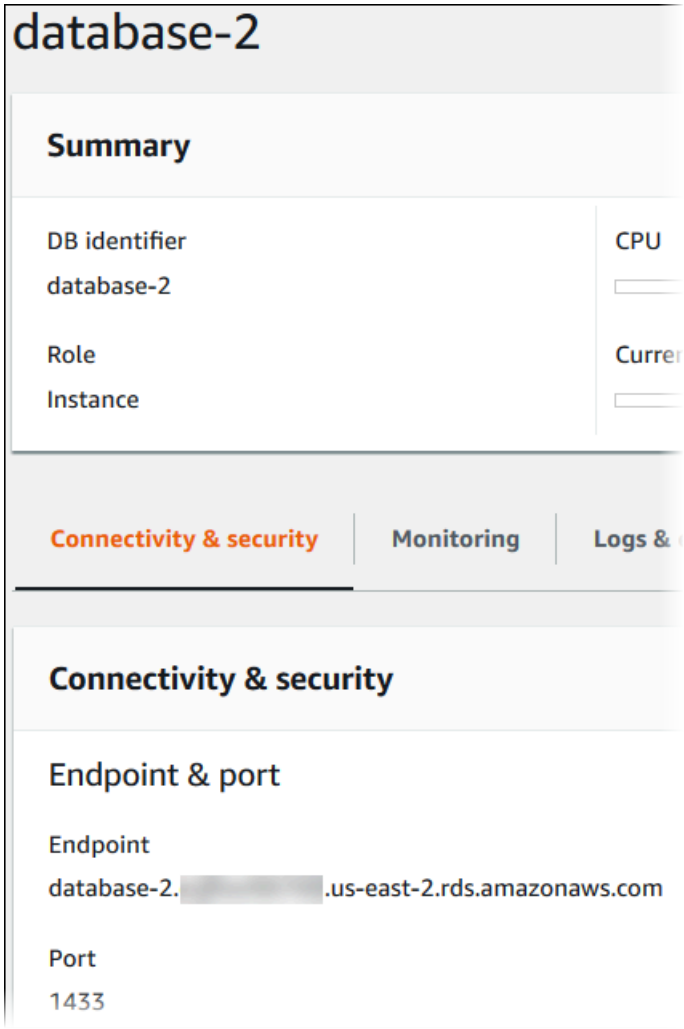
Para encontrar el punto de enlace y el puerto

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la región de AWS de la instancia de base de datos.
3. Busque el nombre del sistema de nombres de dominio (DNS) (punto de enlace) y el número de puerto para su instancia de base de datos:

   a. Abra la consola de RDS y, a continuación, elija Databases (Bases de datos) para mostrar una lista de las instancias de base de datos.

   b. Seleccione el nombre de la instancia de base de datos SQL Server para mostrar sus detalles.

   c. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace.



d. Anote el número de puerto.

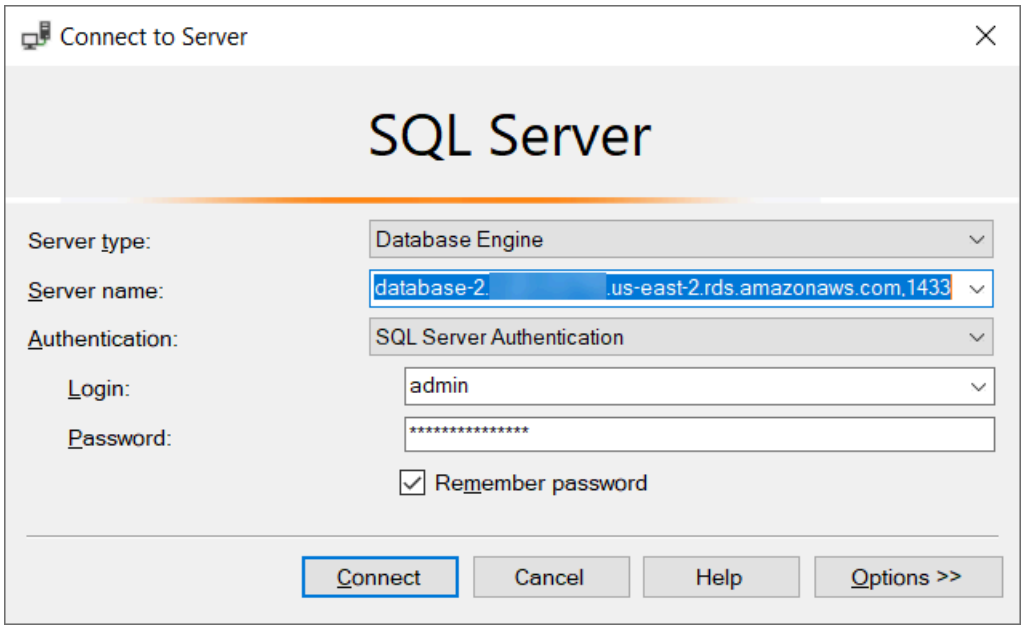
Conexión a su instancia de base de datos con Microsoft SQL Server Management Studio

En este procedimiento, puede conectarse a su instancia de base de datos de ejemplo utilizando Microsoft SQL Server Management Studio (SSMS). Para descargar una versión independiente de esta utilidad, consulte Descarga de SQL Server Management Studio (SSMS) en la documentación de Microsoft.

Para conectarse a una instancia de base de datos mediante SSMS

1. Inicie SQL Server Management Studio.

   Aparecerá el cuadro de diálogo Connect to Server.



2. Proporcione la información para la instancia de base de datos:

   a. En Server type, elija Database Engine.

   b. En Server name (Nombre del servidor), ingrese el nombre del DNS (punto de enlace) y el número de puerto de su instancia de base de datos, separados por una coma.

> **Important**
>
> Cambie los dos puntos entre el punto de enlace y el número de puerto por una coma.

El nombre del servidor debería tener el siguiente aspecto.

```
database-2.cg034itsfake.us-east-1.rds.amazonaws.com,1433
```

c. En Authentication, elija SQL Server Authentication.

d. En Login (Inicio de sesión), escriba el nombre de usuario maestro para la instancia de base de datos.

e. En Password (Contraseña), escriba la contraseña para la instancia de base de datos.

3. Elija Connect.

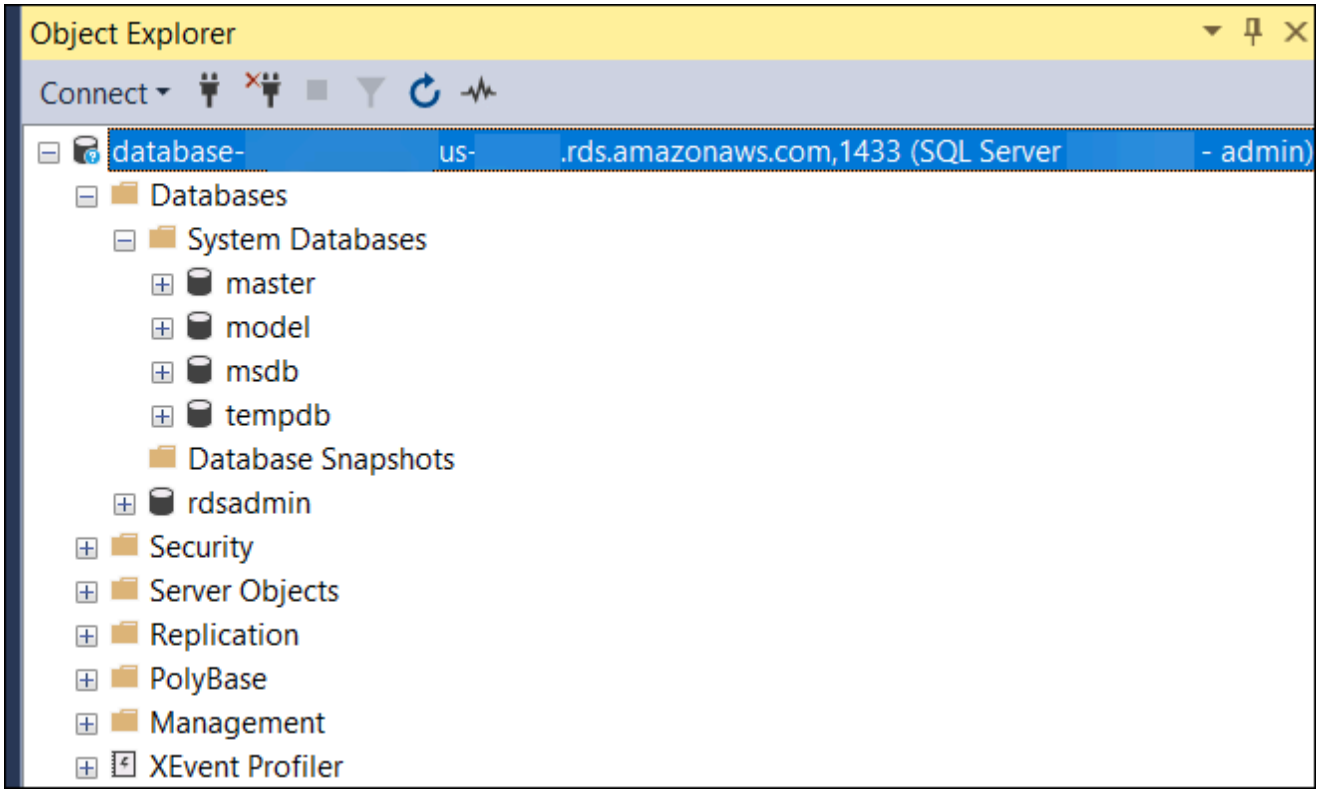
   Luego de unos instantes, SSMS se conecta a su instancia de base de datos.

   Si no puede conectarse a la instancia de base de datos, consulte Consideraciones relativas al grupo de seguridad y Solución de problemas de conexión a la instancia de base de datos de SQL Server.

4. Su instancia de base de datos de SQL Server incluye bases de datos de sistema estándar integradas de SQL Server (`master`, `model`, `msdb` y `tempdb`). Para explorar las bases de datos de sistema, haga lo siguiente:

   a. En SSMS, en el menú Ver elija Explorador de objetos.

   b. Amplíe la instancia de base de datos, amplíe Bases de datos y, a continuación, amplíe Bases de datos del sistema.



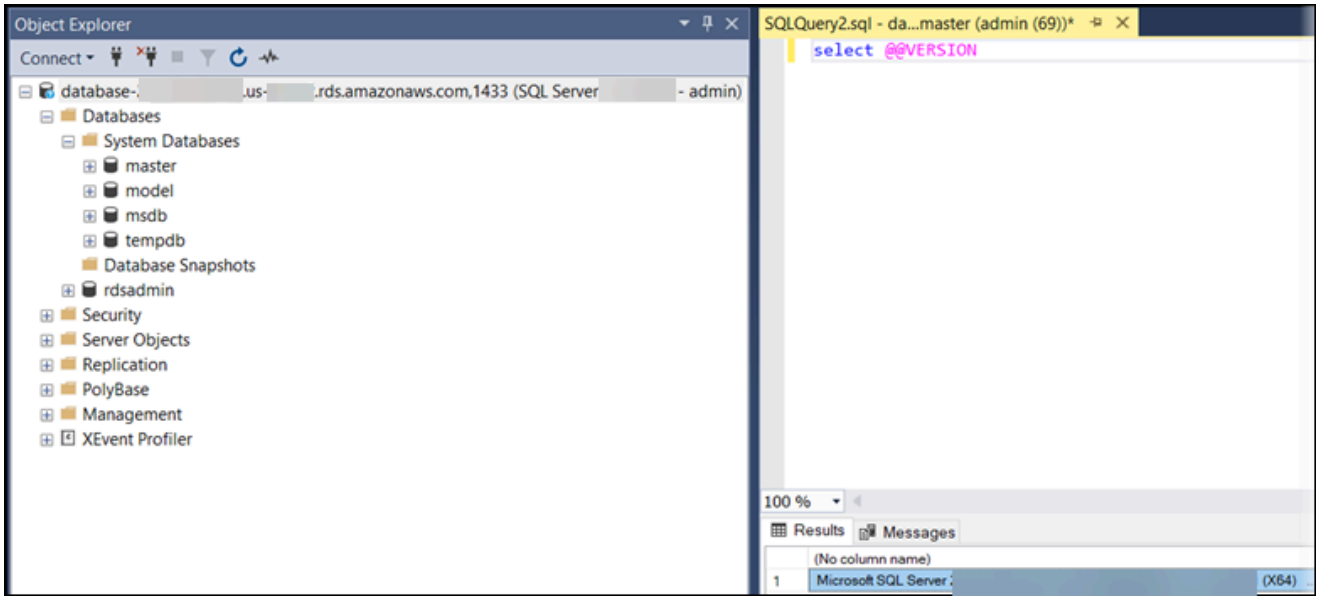
5. Su instancia de base de datos de SQL Server también viene con una base de datos llamada `rdsadmin`. Amazon RDS utiliza esta base de datos para almacenar los objetos que utiliza para administrar su base de datos. La base de datos `rdsadmin` también incluye procedimientos almacenados que puede ejecutar para realizar tareas avanzadas. Para obtener más información, consulte Tareas comunes de administrador de bases de datos de Amazon RDS para Microsoft SQL Server.
6. Ahora, puede comenzar a crear sus propias bases de datos y realizar consultas en la instancia de base de datos y bases de datos como siempre. Para ejecutar una consulta de prueba en la instancia de base de datos, haga lo siguiente:

   a. En SSMS, en el menú File, apunte a New y, a continuación, elija Query with Current Connection.

   b. Escriba la siguiente consulta de SQL.

   ```
   select @@VERSION
   ```

   c. Ejecute la consulta. SSMS devuelve la versión de SQL Server de su instancia de base de datos de Amazon RDS.



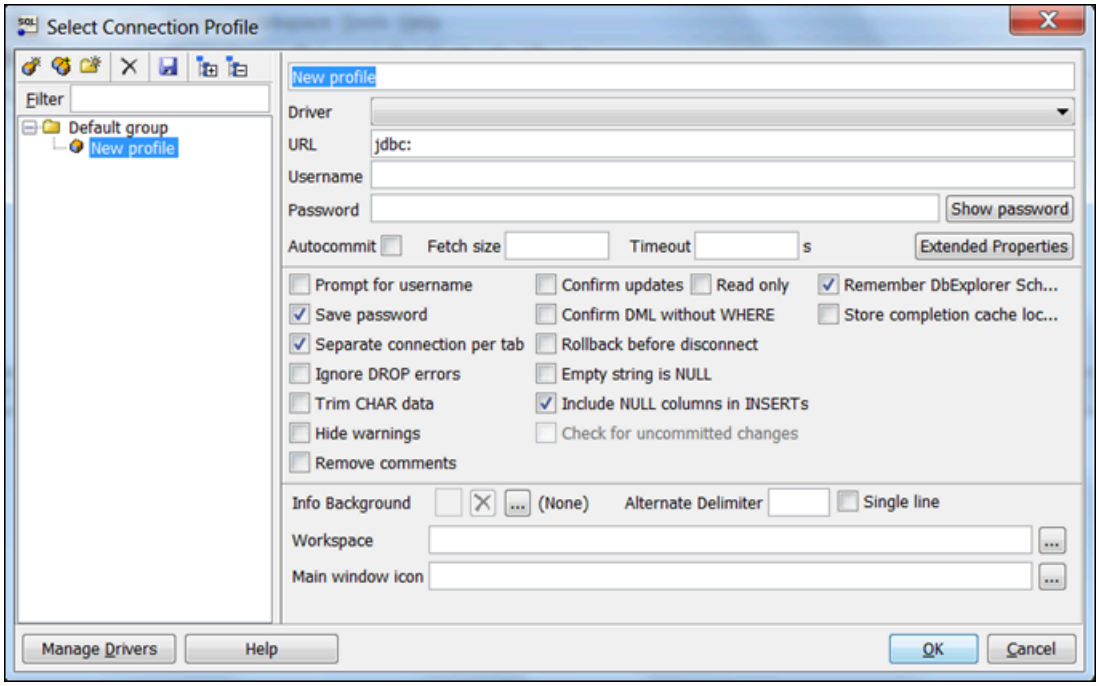
Conexión a la instancia de base de datos con SQL Workbench/J

Este ejemplo muestra cómo conectarse a una instancia de base de datos que ejecuta el motor de base de datos de Microsoft SQL Server mediante la herramienta de base de datos SQL Workbench/J. Para descargar SQL Workbench/J, consulte SQL Workbench/J.

SQL Workbench/J utiliza JDBC para conectarse a su instancia de base de datos. También necesita el controlador JDBC para SQL Server. Para descargar este controlador, consulte Descarga del controlador JDBC de Microsoft para SQL Server.

Para conectarse a una instancia de base de datos mediante SQL Workbench

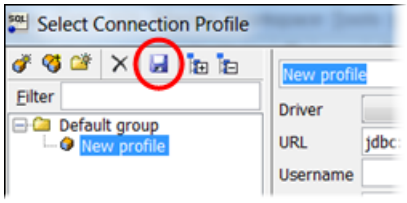
1. Abra SQL Workbench/J. Aparece el cuadro de diálogo Select Connection Profile (Seleccionar perfil de conexión) como se muestra a continuación.



2. En el primer cuadro en la parte superior del cuadro de diálogo, escriba un nombre para el perfil.
3. En Driver (Controlador), elija **`SQL JDBC 4.0`**.
4. En URL, escriba **`jdbc:sqlserver://`** y luego escriba el punto de enlace de su instancia de base de datos. Por ejemplo, el valor de la URL podría ser el siguiente.

```
jdbc:sqlserver://sqlsvr-pdz.abcd12340.us-west-2.rds.amazonaws.com:1433
```

5. En Username (Nombre de usuario), escriba el nombre de usuario maestro para la instancia de base de datos.
6. En Password (Contraseña), escriba la contraseña para el usuario maestro.
7. Elija el icono de guardar en la barra de herramientas del cuadro de diálogo, tal y como se muestra a continuación.

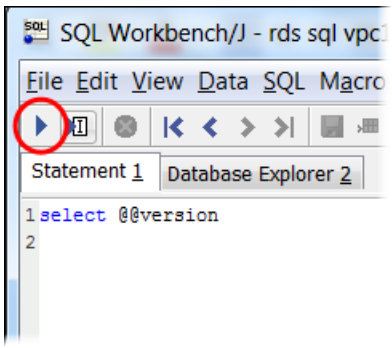


8. Seleccione OK. Luego de unos instantes, SQL Workbench/J se conecta a su instancia de base de datos. Si no puede conectarse a la instancia de base de datos, consulte Consideraciones relativas al grupo de seguridad y Solución de problemas de conexión a la instancia de base de datos de SQL Server.

9. En el panel de consultas, escriba la siguiente consulta SQL.

```
select @@VERSION
```

10. Elija el icono de `Execute` en la barra de herramientas, tal y como se muestra a continuación.



La consulta devuelve la información de versión de su instancia de base de datos, similar a la siguiente.

```
Microsoft SQL Server 2017 (RTM-CU22) (KB4577467) - 14.0.3356.20 (X64)
```

Consideraciones relativas al grupo de seguridad

Para conectarse a su instancia de base de datos, esta debe estar asociada a un grupo de seguridad. Este grupo de seguridad contiene las direcciones IP y la configuración de red que utiliza para tener acceso a la instancia de base de datos. Es posible que haya asociado la instancia de base de datos al grupo de seguridad apropiado cuando creó su instancia de base de datos. Si asignó un grupo de seguridad no configurado predeterminado cuando creó una instancia de base de datos, el firewall de la instancia de base datos impide las conexiones.

En algunos casos, es posible que necesite crear un nuevo grupo de seguridad para habilitar el acceso. Para obtener instrucciones sobre cómo crear grupos de seguridad nuevos, consulte Control de acceso con grupos de seguridad. Para encontrar un tema que le muestre el proceso de configuración de reglas para el grupo de seguridad de la VPC, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).

Después de haber creado el nuevo grupo de seguridad, modifique la instancia de base de datos para asociarla al grupo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Puede mejorar la seguridad utilizando SSL para cifrar conexiones a su instancia de base de datos. Para obtener más información, consulte ???.

Solución de problemas de conexión a la instancia de base de datos de SQL Server

En la tabla siguiente , se muestran los problemas que pueden presentarse cuando intenta conectarse a su instancia de base de datos de SQL Server.

Problema	Sugerencias para la solución de problemas
Could not open a connection to SQL Server – Microsoft SQL Server, Error: 53 (No se pudo abrir una conexión con SQL Server - Microsoft SQL Server, Error: 53)	Asegúrese de haber especificado el nombre del servidor correctamente. En Server name (Nombre del servidor), escriba el nombre DNS y el número de puerto de la instancia de base de datos de muestra, separados por una coma. **Important** Si tiene dos puntos entre el nombre DNS y el número de puerto, cambie los dos puntos por una coma. El nombre del servidor debería tener el siguiente aspecto. `sample-instance.cg034itsfake.us-east-1.rds.amazonaws.com,1433`
No connection could be made because the target machine actively refused it – Microsoft SQL Server, Error: 10061 (No se pudo establecer una conexión porque el equipo de destino la denegó expresamente - Microsoft SQL Server, Error: 10061)	Ha podido alcanzar la instancia de base de datos, pero se rechazó la conexión. Esto suele deberse a que se ha especificado incorrectamente el nombre de usuario o la contraseña. Compruebe el nombre de usuario y la contraseña, y, a continuación, vuelva a intentarlo.

Problema	Sugerencias para la solución de problemas
A network-related or instance-specific error occurred while establish ing a connection to SQL Server. The server was not found or was not accessible... The wait operation timed out – Microsoft SQL Server, Error: 258(Se produjo un error específico de la instancia o relacionado con la red al establecer una conexión con SQL Server. No se ha encontrado el servidor o no se pudo acceder a él. Se agotó el tiempo de la operación de espera - Microsoft SQL Server, Error: 258	Las reglas de acceso impuestas por el firewall local y las direccion es IP a las que autorizó el acceso a la instancia de base de datos podrían no coincidir. Lo más probable es que el problema se encuentre en las reglas de entrada de su grupo de seguridad. Para obtener más información, consulte Seguridad en Amazon RDS.
	La instancia de la base de datos debe ser accesible públicamente. Para conectarse a ella desde fuera de la VPC, la instancia debe tener asignada una dirección IP pública.

> **Note**
>
> Para obtener más información sobre problemas de conexión, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Uso de Active Directory con RDS para SQL Server

Puede unir una instancia de base de datos de RDS para SQL Server a un dominio de Microsoft Active Directory (AD). Su dominio de AD se puede alojar en un AD administrado de AWS dentro de AWS o en un AD autoadministrado en la ubicación que elija, incluidos los centros de datos corporativos, en AWS EC2 o con otros proveedores de nube.

Puede autenticar a los usuarios del dominio mediante la autenticación NTLM con Active Directory autoadministrado. Puede utilizar la autenticación Kerberos y NTLM con AWS Managed Active Directory.

En las siguientes secciones, encontrará información sobre cómo utilizar Active Directory autoadministrado y AWS Managed Active Directory para Microsoft SQL Server en Amazon RDS.

Temas

- Uso de Active Directory autoadministado con una instancia de base de datos de Amazon RDS para SQL Server
- Uso de AWS Managed Active Directory con RDS para SQL Server

Uso de Active Directory autoadministrado con una instancia de base de datos de Amazon RDS para SQL Server

Puede unir sus instancias de base de datos de RDS para SQL Server directamente a su dominio autoadministrado de Active Directory (AD), independientemente de dónde esté alojado su AD: en centros de datos corporativos, en AWS EC2 o con otros proveedores de nube. Con AD autoadministrado, utiliza la autenticación NTLM para controlar directamente la autenticación de los usuarios y los servicios en sus instancias de base de datos de RDS para SQL Server sin utilizar dominios intermediarios ni relaciones de confianza entre bosques. Cuando los usuarios se autentican con una instancia de base de datos de RDS para SQL Server unida a su dominio de AD autoadministrado, las solicitudes de autenticación se reenvían al dominio de AD autoadministrado que usted especifique.

Temas

- Disponibilidad en regiones y versiones
- Requisitos
- Limitaciones
- Descripción general de la configuración de Active Directory autoadministrado
- Configuración de Active Directory autoadministrado
- Administración de una instancia de base de datos en un dominio de Active Directory autoadministrado
- Descripción de la suscripción a un dominio de Active Directory autoadministrado
- Solución de problemas de Active Directory autoadministrado
- Restauración de una instancia de base de datos de SQL Server y adición de esta a un dominio de Active Directory autoadministrado

Disponibilidad en regiones y versiones

Amazon RDS admite AD autoadministrado para SQL Server mediante NTLM en todas las Regiones de AWS.

Requisitos

Asegúrese de cumplir los siguientes requisitos antes de unir una instancia de base de datos de RDS para SQL Server a su dominio de AD autoadministrado.

Temas

- Configure su AD en las instalaciones
- Configure la conectividad de red
- Configure su cuenta de servicio de dominio de AD

Configure su AD en las instalaciones

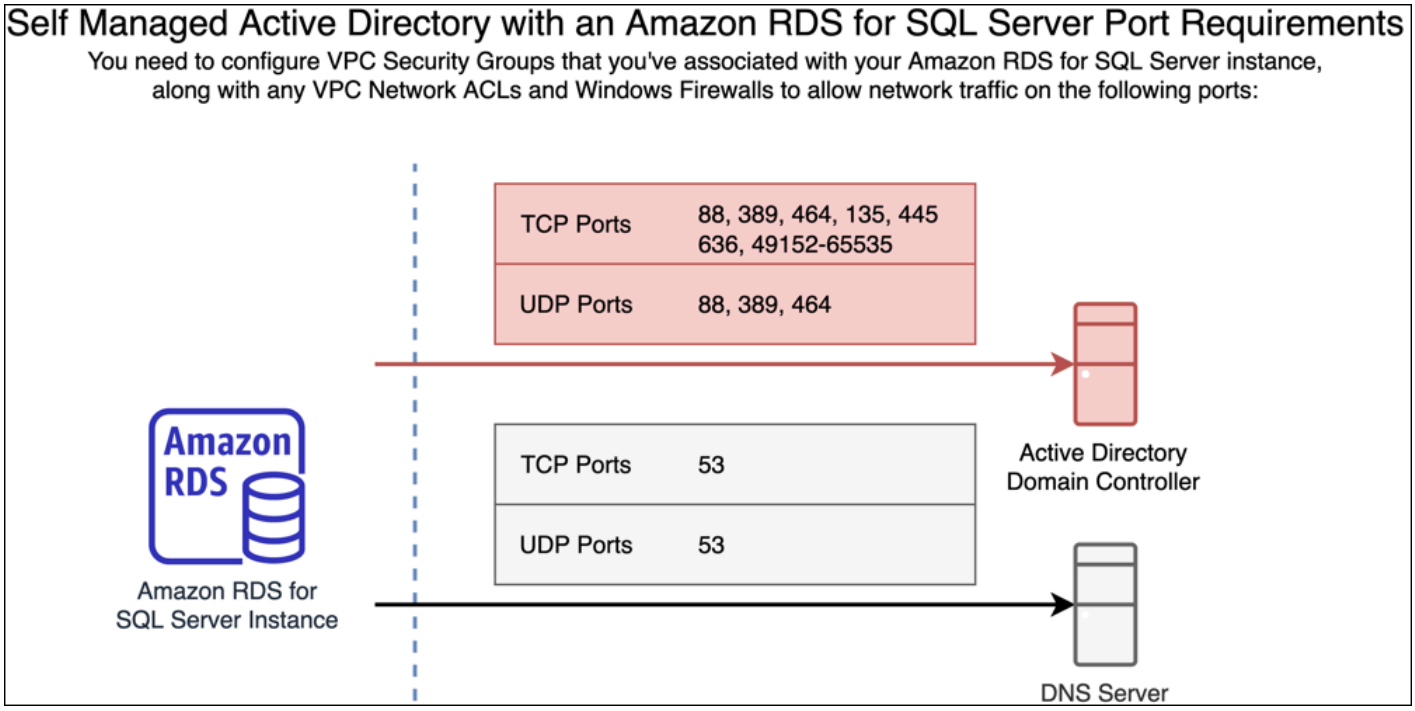
Asegúrese de tener un Microsoft AD en las instalaciones o de otro tipo autoadministrado al que pueda unirse a la instancia de Amazon RDS para SQL Server. Su AD en las instalaciones debe tener la siguiente configuración:

- Si tiene sitios definidos de Active Directory, asegúrese de que las subredes de la VPC asociadas a su instancia de base de datos de RDS para SQL Server estén definidas en su sitio de Active Directory. Confirme que no haya ningún conflicto entre las subredes de la VPC y las subredes de sus otros sitios de AD.
- El controlador de dominio de AD tiene un nivel funcional de dominio de Windows Server 2008 R2 o superior.
- El nombre de dominio de AD no puede estar en formato de dominio de etiqueta única (SLD). RDS para SQL Server no admite dominios de SLD.
- El nombre de dominio completo (FQDN) y su AD no pueden superar los 47 caracteres.

Configure la conectividad de red

Asegúrese de cumplir las siguientes configuraciones de red:

- Conectividad configurada entre la Amazon VPC donde desea crear la instancia de base de datos de RDS para SQL Server y su Active Directory autoadministrado. Puede configurar la conectividad mediante AWS Direct Connect, AWS VPN, emparejamiento de VPC o AWS Transit Gateway.
- En el caso de los grupos de seguridad de VPC, el grupo de seguridad predeterminado de la Amazon VPC predeterminada ya está agregado a la instancia de base de datos de RDS para SQL Server en la consola. Asegúrese de que el grupo de seguridad y las ACL de red de VPC de las subredes en las que va a crear su instancia de base de datos de RDS para SQL Server permitan el tráfico en los puertos y en las direcciones que se muestran en el siguiente diagrama.



En la siguiente tabla se identifica la función de cada puerto.

Protocolo	Puertos	Rol
TCP/UDP	53	Sistema de nombres de dominio (DNS)
TCP/UDP	88	Autenticación de Kerberos
TCP/UDP	464	Cambiar/establecer contraseña
TCP/UDP	389	Protocolo ligero de acceso a directorios (LDAP)
TCP	135	Entorno de computación distribuido/asignador de puntos de conexión (DCE/EPMAP)
TCP	445	Uso compartido de archivos SMB de Directory Services

Protocolo	Puertos	Rol
TCP	636	Protocolo ligero de acceso a directorios sobre TLS/ SSL (LDAP)
TCP	49152 - 65535	Puertos efímeros para RPC

- Por lo general, los servidores DNS de dominio se encuentran en los controladores de dominio de AD. No es necesario configurar el conjunto de opciones de DHCP de VPC para utilizar esta característica. Para obtener más información, consulte Conjuntos de opciones de DHCP en la Guía del usuario de Amazon VPC.

> **Important**
>
> Si utiliza ACL de red de VPC, también debe permitir el tráfico saliente en los puertos dinámicos (49152-65535) desde su instancia de base de datos de RDS para SQL Server. Asegúrese de que estas reglas de tráfico también se reflejen en los firewalls que se aplican a cada uno de los controladores de dominio de AD, los servidores DNS y las instancias de base de datos de RDS para SQL Server.
> Si bien los grupos de seguridad de VPC requieren que los puertos se abran solo en la dirección en la que se inicia el tráfico de red, la mayoría de los firewalls de Windows y las ACL de red de VPC requieren que los puertos estén abiertos en ambas direcciones.

Configure su cuenta de servicio de dominio de AD

Asegúrese de cumplir los siguientes requisitos para la cuenta de servicio de dominio de AD:

- Asegúrese de tener una cuenta de servicio en su dominio de AD autoadministrado con permisos delegados para unir equipos al dominio. Una cuenta de servicio de dominio es una cuenta de usuario de su AD autoadministrado a la que se le ha delegado permiso para realizar determinadas tareas.
- Los siguientes permisos se deben delegar en la cuenta de servicio de dominio en la unidad organizativa (OU) a la que va a unir su instancia de base de datos de RDS para SQL Server:
  - Capacidad validada para escribir en el nombre de host DNS
  - Capacidad validada para escribir en el nombre de entidad principal del servicio

- Crear y eliminar objetos de equipo

Estos representan el conjunto mínimo de permisos necesarios para unir objetos de equipo a su Active Directory autoadministrado. Para obtener más información, consulte Errors when attempting to join computers to a domain en la documentación de Microsoft Windows Server.

> **Important**
>
> No mueva los objetos de equipo que RDS para SQL Server cree en la unidad organizativa después de crear la instancia de base de datos. Si mueve los objetos asociados, la instancia de base de datos de RDS para SQL Server se configurará mal. Si necesita mover los objetos de equipo creados por Amazon RDS, utilice la operación de API de RDS ModifyDBInstance para modificar los parámetros del dominio con la ubicación deseada de los objetos del equipo.

Limitaciones

Se aplican las siguientes limitaciones al AD autoadministrado para SQL Server.

- NTLM es el único tipo de autenticación admitido. No se admite la autenticación Kerberos. Si necesita usar la autenticación Kerberos, puede usar AWS Managed AD en lugar de AD autoadministrado.
- No se admite el servicio Coordinador de transacciones distribuidas (MSDTC) de Microsoft, ya que requiere la autenticación Kerberos.
- Sus instancias de base de datos de RDS para SQL Server no utilizan el servidor de Network Time Protocol (NTP) de su dominio de AD autoadministrado. En cambio, utilizan un servicio NTP de AWS.
- Los servidores enlazados de SQL Server deben usar la autenticación SQL para conectarse a otras instancias de base de datos de RDS para SQL Server unidas a su dominio de AD autoadministrado.
- La configuración del objeto de política de grupo (GPO) de Microsoft de su dominio de AD autoadministrado no se aplica a las instancias de base de datos de RDS de SQL Server.

Descripción general de la configuración de Active Directory autoadministrado

Para configurar AD autoadministrado para una instancia de base de datos de RDS para SQL Server, siga los siguientes pasos, que se explican con más detalle en Configuración de Active Directory autoadministrado:

En el dominio de AD:

- Cree una unidad organizativa (OU).
- Crear un usuario de dominio de AD.
- Delegue el control al usuario del dominio de AD.

Desde la AWS Management Console o la API:

- Crea una clave de AWS KMS.
- Cree un secreto con AWS Secrets Manager.
- Cree o modifique una instancia de base de datos de RDS para SQL Server y únala a su dominio de AD autoadministrado.

Configuración de Active Directory autoadministrado

Para configurar un AD autoadministrado, siga estos pasos.

Temas

- Paso 1: Crear una unidad organizativa en el AD
- Paso 2: Crear un usuario de dominio de AD en su AD
- Paso 3: Delegar el control al usuario de AD
- Paso 4: Crear una clave de AWS KMS
- Paso 5: Crear un secreto de AWS
- Paso 6: Crear o modificar una instancia de base de datos de SQL Server
- Paso 7: Crear inicios de sesión de SQL Server de autenticación de Windows

Paso 1: Crear una unidad organizativa en el AD

> **Important**
>
> Se recomienda crear una credencial de servicio y una OU dedicadas a esa unidad organizativa para todas las cuentas de AWS que posean una instancia de base de datos de RDS para SQL Server que se haya unido a su dominio de AD autoadministrado. Al crear credenciales de servicio u OU dedicadas, puede evitar conflictos de permisos y seguir el principio de privilegio mínimo.

Para crear una OU en su AD

1. Conéctese a su dominio de AD como administrador de dominio.
2. Abra Usuarios y equipos de Active Directory y seleccione el dominio en el que desea crear la OU.
3. Haga clic con el botón derecho en el dominio y seleccione Nuevo y, a continuación, Unidad organizativa.
4. Escriba un nombre para la OU.
5. Mantenga la casilla seleccionada para Proteger el contenedor contra la eliminación accidental.
6. Haga clic en OK (Aceptar). La nueva OU aparecerá en su dominio.

Paso 2: Crear un usuario de dominio de AD en su AD

Las credenciales de usuario del dominio se utilizarán para el secreto en AWS Secrets Manager.

Para crear un usuario de dominio de AD en su AD

1. Abra Usuarios y equipos de Active Directory y seleccione el dominio y la OU en los que desea crear el usuario.
2. Haga clic con el botón derecho en el objeto Usuarios y seleccione Nuevo y, a continuación, Usuario.
3. Introduzca el nombre, los apellidos y el nombre de inicio de sesión del usuario. Haga clic en Next (Siguiente).
4. Introduzca una contraseña para el usuario. No seleccione El usuario debe cambiar la contraseña en el próximo inicio de sesión. No seleccione La cuenta está deshabilitada. Haga clic en Next (Siguiente).

5. Haga clic en OK (Aceptar). El nuevo usuario aparecerá en su dominio.

Paso 3: Delegar el control al usuario de AD

Para delegar el control al usuario del dominio AD de su dominio

1. Abra el complemento MMC Usuarios y equipos de Active Directory y seleccione el dominio en el que desea crear el usuario.
2. Haga clic con el botón derecho en la OU que creó anteriormente y seleccione Delegar control.
3. En Asistente para delegación de control, haga clic en Siguiente.
4. En la sección Usuarios o grupos, haga clic en Agregar.
5. En la sección Seleccionar usuarios, equipos o grupos, introduzca el usuario de AD que creó y haga clic en Verificar nombres. Si la comprobación de usuario de AD se ha realizado correctamente, haga clic en Aceptar.
6. En la sección Usuarios o grupos, confirme que ha añadido el usuario de AD y haga clic en Siguiente.
7. En la página Tareas que se delegarán, seleccione Crear una tarea personalizada para delegar y haga clic en Siguiente.
8. En la sección Tipo de objeto de Active Directory:
    a. Elija Solo los siguientes objetos de la carpeta.
    b. Seleccione Objetos computacionales.
    c. Seleccione Crear objetos seleccionados en esta carpeta.
    d. Seleccione Eliminar los objetos seleccionados en esta carpeta y haga clic en Siguiente.
9. En la sección Permisos:
    a. Mantenga seleccionada la opción General.
    b. Seleccione Escritura validada en el nombre de host DNS.
    c. Seleccione Escritura validada en el nombre de la entidad de servicio y haga clic en Siguiente.
10. Para Completar el asistente para delegación de control, revise y confirme la configuración y haga clic en Finalizar.

Paso 4: Crear una clave de AWS KMS

La clave de KMS se utiliza para cifrar el secreto de AWS.

Para crear una clave de AWS KMS

> **Note**
>
> En Clave de cifrado, no utilice la clave de KMS predeterminada de AWS. Asegúrese de crear la clave de AWS KMS en la misma cuenta de AWS que contiene la instancia de base de datos de RDS para SQL Server que desea unir a su AD autoadministrado.

1. En la consola de AWS KMS, elija Crear API.
2. En Tipo de clave, elija Simétrica.
3. Para Uso de claves, elija Cifrar y descifrar.
4. Para Advanced options (Opciones avanzadas):
   a. En Origen del material de claves, elija Externo.
   b. Para Regionalidad, elija Clave de región única y haga clic en Siguiente.
5. Para Alias, proporcione un nombre para la clave de KMS.
6. (Opcional) En Description, proporcione una descripción de la clave de KMS.
7. (Opcional) En etiquetas, introduzca una etiqueta para la clave KMS, y haga clic en Siguiente.
8. En Administradores de claves, proporcione el nombre de un usuario de IAM y selecciónelo.
9. En Eliminación de la clave, mantenga seleccionada la casilla Permitir que los administradores de claves eliminen esta clave y haga clic en Siguiente.
10. En Usuarios de clave, proporcione el mismo usuario de IAM del paso anterior y selecciónelo. Haga clic en Next (Siguiente).
11. Revise la configuración.
12. Para Política de claves, incluya lo siguiente en la política Instrucción:

```
{
    "Sid": "Allow use of the KMS key on behalf of RDS",
    "Effect": "Allow",
    "Principal": {
        "Service": [
```

```
            "rds.amazonaws.com"
        ]
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

13. Haga clic en Finish (Finalizar).

Paso 5: Crear un secreto de AWS

Creación de un secreto

> **Note**
>
> Asegúrese de crear la clave de en la misma cuenta de AWS que contiene la instancia de base de datos de RDS para SQL Server que desea unir a su AD autoadministrado.

1. En AWS Secrets Manager, elija Almacenar un nuevo secreto.
2. En Secret type (Tipo de secreto), elija Other type of secret (Otro tipo de secreto).
3. En los pares clave/valor, añada sus dos claves:
    a. Para la primera clave, introduzca `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`.
    b. Para el valor de la primera clave, ingrese solo el nombre de usuario (sin el prefijo de dominio) del usuario de AD. No incluya el nombre de dominio, ya que esto provocará un error en la creación de la instancia.
    c. Para la segunda clave, introduzca `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`.
    d. Para el valor de la segunda clave, introduzca la contraseña que creó para el usuario de AD en su dominio.
4. Para la Clave de cifrado, introduzca la clave de KMS que creó en el paso anterior y haga clic en Siguiente.
5. En Nombre de secreto, introduzca un nombre descriptivo que le ayude a buscar el secreto más adelante.
6. (Opcional) En Descripción, escriba una descripción del nombre del secreto.
7. En Permisos de recursos, haga clic en Editar.
8. Añada la siguiente política a la política de permisos:

> **Note**
>
> Le recomendamos que utilice la `aws:sourceAccount` y las condiciones `aws:sourceArn` de la política para evitar el problema del suplente confuso. Utilice su Cuenta de AWS para `aws:sourceAccount` y el ARN de la instancia de base de datos de RDS para SQL Server para `aws:sourceArn`. Para obtener más información, consulte Prevención de los problemas del suplente confuso entre servicios.

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "rds.amazonaws.com"
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*",
            "Condition":
            {
                "StringEquals":
                {
                    "aws:sourceAccount": "123456789012"
                },
                "ArnLike":
                {
                    "aws:sourceArn": "arn:aws:rds:us-
west-2:123456789012:db:*"
                }
            }
        }
    ]
}
```

9. Haz clic en Guardar y, a continuación, en Siguiente.

10. En Configurar los ajustes de rotación, mantenga los valores predeterminados y seleccione Siguiente.
11. Revise la configuración del secreto y haga clic en Guardar.
12. Elija el secreto que creó y copie el valor del ARN del secreto. Esto se utilizará en el siguiente paso para configurar Active Directory autoadministrado.

Paso 6: Crear o modificar una instancia de base de datos de SQL Server

Puede utilizar la consola, la CLI o la API de RDS para asociar una instancia de base de datos de RDS para SQL Server a un dominio de AD autoadministrado. Puedes hacerlo de una de las siguientes formas:

- Cree una nueva instancia de base de datos de SQL Server mediante la consola, el comando de la CLI create-db-instance o la operación CreateDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de SQL Server existente mediante la consola, el comando de la CLI modify-db-instance o la operación ModifyDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Restaure una instancia de base de datos de SQL Server a partir de una instantánea de base de datos mediante la consola, el comando de la CLI restore-db-instance-from-db-snapshot o la operación RestoreDBInstanceFromDBSnapshot de la API de RDS.

  Para obtener instrucciones, consulte Restauración a una instancia de base de datos.
- Restaure una instancia de base de datos de SQL Server a un punto en el tiempo mediante la consola, el comando de la CLI restore-db-instance-to-point-in-time o la operación RestoreDBInstanceToPointInTime de la API de RDS.

  Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Si utiliza la AWS CLI, necesitará los siguientes parámetros para que la instancia de base de datos pueda usar el dominio de Active Directory autoadministrado que ha creado:

- Para el parámetro `--domain-fqdn`, utilice el nombre de dominio completo (FQDN) de su Active Directory autoadministrado.
- Para el parámetro `--domain-ou`, utilice la OU que creó en su AD autoadministrado.
- Para el parámetro `--domain-auth-secret-arn`, utilice el valor del ARN del secreto que creó en un paso anterior.
- Para el parámetro `--domain-dns-ips`, utilice las direcciones IPv4 principal y secundaria de los servidores DNS de su AD autoadministrado. Si no tiene una dirección IP de servidor DNS secundaria, introduzca la dirección IP principal dos veces.

Los siguientes comandos de CLI de ejemplo muestran cómo crear, modificar y eliminar una instancia de base de datos de RDS para SQL Server con un dominio de AD autoadministrado.

> **Important**
>
> Si modifica una instancia de base de datos para unirla a un dominio de AD autoadministrado o eliminarla de él, es necesario reiniciar la instancia de base de datos para que la modificación surta efecto. Puede optar por aplicar los cambios inmediatamente o esperar hasta el próximo período de mantenimiento. Si opta por Aplicar inmediatamente, provocará un tiempo de inactividad para las instancias de base de datos Single-AZ. Las instancias de base de datos Multi-AZ realizarán una conmutación por error antes de completar el reinicio. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.

El siguiente comando de CLI crea una nueva instancia de base de datos de RDS para SQL Server y la une a un dominio de AD autoadministrado.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier my-DB-instance \
    --db-instance-class db.m5.xlarge \
    --allocated-storage 50 \
    --engine sqlserver-se \
    --engine-version 15.00.4043.16.v1 \
    --license-model license-included \
    --master-username my-master-username \
    --master-user-password my-master-password \
```

```
    --domain-fqdn my_AD_domain.my_AD.my_domain \
    --domain-ou OU=my-AD-test-OU,DC=my-AD-test,DC=my-AD,DC=my-domain \
    --domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:my-
AD-test-secret-123456" \
    --domain-dns-ips "10.11.12.13" "10.11.12.14"
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier my-DB-instance ^
    --db-instance-class db.m5.xlarge ^
    --allocated-storage 50 ^
    --engine sqlserver-se ^
    --engine-version 15.00.4043.16.v1 ^
    --license-model license-included ^
    --master-username my-master-username ^
    --master-user-password my-master-password ^
    --domain-fqdn my-AD-test.my-AD.mydomain ^
    --domain-ou OU=my-AD-test-OU,DC=my-AD-test,DC=my-AD,DC=my-domain ^
    --domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:my-
AD-test-secret-123456" \ ^
    --domain-dns-ips "10.11.12.13" "10.11.12.14"
```

El siguiente comando de CLI modifica una instancia de base de datos de RDS para SQL Server existente para que utilice un dominio de Active Directory autoadministrado.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-DB-instance \
    --domain-fqdn my_AD_domain.my_AD.my_domain \
    --domain-ou OU=my-AD-test-OU,DC=my-AD-test,DC=my-AD,DC=my-domain \
    --domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:my-
AD-test-secret-123456" \
    --domain-dns-ips "10.11.12.13" "10.11.12.14"
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-DBinstance ^
    --domain-fqdn my_AD_domain.my_AD.my_domain ^
    --domain-ou OU=my-AD-test-OU,DC=my-AD-test,DC=my-AD,DC=my-domain ^
```

```
    --domain-auth-secret-arn "arn:aws:secretsmanager:region:account-number:secret:my-
AD-test-secret-123456" ^
    --domain-dns-ips "10.11.12.13" "10.11.12.14"
```

El siguiente comando de CLI elimina una instancia de base de datos de RDS para SQL Server de un dominio de Active Directory autoadministrado.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-DB-instance \
    --disable-domain
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-DB-instance ^
    --disable-domain
```

Paso 7: Crear inicios de sesión de SQL Server de autenticación de Windows

Use las credenciales del usuario maestro de Amazon RDS para conectarse a la instancia de base de datos de SQL Server como lo haría con cualquier otra instancia de base de datos. Como la instancia de base de datos está unida al dominio de AD autoadministrado, puede aprovisionar inicios de sesión y usuarios de SQL Server. Para ello, utilice la utilidad de usuarios y grupos de AD de su dominio de AD autoadministrado. Los permisos de bases de datos se administran a través de los permisos de SQL Server estándar otorgados y revocados para estos inicios de sesión de Windows.

Para que un usuario de AD autoadministrado se autentique con SQL Server, debe existir un inicio de sesión de Windows de SQL Server para el usuario de AD autoadministrado o para un grupo de Active Directory autoadministrado del que el usuario sea miembro. El control detallado del acceso se gestiona mediante la concesión y la revocación de permisos en estos inicios de sesión de SQL Server. Un usuario de AD autoadministrado que no tenga un inicio de sesión de SQL Server o no pertenezca a un grupo de AD autoadministrado con dicho inicio de sesión no puede tener acceso a la instancia de base de datos de SQL Server.

El permiso ALTER ANY LOGIN es necesario para crear un inicio de sesión de SQL Server de AD autoadministrado. Si todavía no ha creado ningún inicio de sesión con este permiso, conéctese como usuario maestro de la instancia de base de datos usando la autenticación de SQL Server y cree sus inicios de sesión de SQL Server de AD autoadministrado bajo el contexto del usuario maestro.

Puede ejecutar un comando de lenguaje de definición de datos (DDL), como el siguiente, para crear un inicio de sesión de SQL Server para un usuario o grupo de AD autoadministrado.

> **Note**
>
> Especifique usuarios y grupos con el nombre de inicio de sesión anterior a Windows 2000 en el formato *my_AD_domain**my_AD_domain_user*. No puede usar un nombre principal del usuario (UPN) en el formato *my_AD_domain_user*@*my_AD_domain*.

```
USE [master]
GO
CREATE LOGIN [my_AD_domain\my_AD_domain_user] FROM WINDOWS WITH DEFAULT_DATABASE =
 [master], DEFAULT_LANGUAGE = [us_english];
GO
```

Para obtener más información, consulte CREATE LOGIN (Transact-SQL) (Crear inicio de sesión [Transact-SQL]) en la documentación de Microsoft Developer Network.

Los usuarios (tanto humanos como aplicaciones) del dominio pueden conectarse ahora a la instancia de RDS para SQL Server desde un equipo cliente unido al dominio de AD autoadministrado utilizando la autenticación de Windows.

Administración de una instancia de base de datos en un dominio de Active Directory autoadministrado

Puede usar la consola, la AWS CLI o la API de Amazon RDS para administrar la instancia de base de datos y la relación con su dominio de AD autoadministrado. Por ejemplo, puede mover la instancia de base de datos dentro, fuera o entre dominios.

Por ejemplo, con la API de Amazon RDS puede hacer lo siguiente:

- Para volver a intentar una unión de dominio autoadministrado por una suscripción fallida, utilice la operación de API ModifyDBInstance y especifique el mismo conjunto de parámetros:
  - `--domain-fqdn`
  - `--domain-dns-ips`
  - `--domain-ou`
  - `--domain-auth-secret-arn`

- Para eliminar una instancia de base de datos de un dominio autoadministrado, use la operación `ModifyDBInstance` de la API y especifique `--disable-domain` como parámetro del dominio.
- Para mover una instancia de base de datos de un dominio autoadministrado a otro, use la operación `ModifyDBInstance` de la API y especifique los parámetros para el nuevo dominio.
  - `--domain-fqdn`
  - `--domain-dns-ips`
  - `--domain-ou`
  - `--domain-auth-secret-arn`
- Para ver la suscripción de dominio de AD autoadministrado para cada instancia de base de datos, use la operación DescribeDBInstances de la API.

Descripción de la suscripción a un dominio de Active Directory autoadministrado

Una vez que haya creado o modificado una instancia de base de datos, esta se convierte en miembro del dominio de AD autoadministrado. La consola de AWS indica el estado de la suscripción del dominio de Active Directory autoadministrado para la instancia de base de datos. El estado de la instancia de base de datos puede ser uno de los siguientes:

- joined: la instancia es miembro del dominio de AD.
- joining: la instancia está en el proceso de convertirse en miembro del dominio de AD.
- pending-join: la suscripción de la instancia está pendiente.
- pending-maintenance-join: AWS intentará convertir la instancia en miembro del dominio de AD durante el próximo período de mantenimiento programado.
- pending-removal: la eliminación de la instancia del dominio de AD está pendiente.
- pending-maintenance-removal: AWS intentará eliminar la instancia del dominio de AD durante el próximo período de mantenimiento programado.
- error: un problema de configuración ha impedido que la instancia se una al dominio de AD. Compruebe y corrija la configuración antes de volver a ejecutar el comando para modificar la instancia.
- removing: la instancia se está eliminando del dominio de AD autoadministrado.

Una solicitud para convertirse en miembro de un dominio de AD autoadministrado puede generar un error a causa de un problema de conectividad de la red. Por ejemplo, puede crear una instancia de base de datos o modificar una instancia existente y que se produzca un error al intentar que la

instancia de base de datos se convierta en miembro de un dominio de AD autoadministrado. En este caso, vuelva a emitir el comando para crear o modificar la instancia de base de datos o modificar la instancia recién creada para unirse al dominio de AD autoadministrado.

Solución de problemas de Active Directory autoadministrado

Los siguientes son los problemas que pueden surgir al configurar o modificar el AD autoadministrado.

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
Error 2 / 0x2	El sistema no puede encontrar el archivo especificado.	El formato o la ubicación de la unidad organizativa (OU) especificados con el parámetro `–domain-ou` no es válido. La cuenta de servicio de dominio especificada mediante AWS Secrets Manager carece de los permisos necesarios para unirse a la OU.	Revise el parámetro `–domain-ou` . Asegúrese de que la cuenta de servicio de dominio tenga los permisos correctos para la OU. Para obtener más información, consulte Configure su cuenta de servicio de dominio de AD.
Error 5 / 0x5	Se deniega el acceso.	Los permisos de la cuenta de servicio del dominio están mal configurados o la cuenta del equipo ya existe en el dominio.	Revise los permisos de la cuenta de servicio del dominio y compruebe que la cuenta del equipo de RDS no esté duplicada en el dominio. Para comprobar el nombre de la cuenta del equipo de RDS, ejecute `SELECT @@SERVERNAME` en su instancia de base de datos de RDS para SQL Server. Si utiliza Multi-AZ, intente reiniciar con conmutación por error y, a

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
			continuación, compruebe de nuevo la cuenta del equipo de RDS. Para obtener más información, consulte Reinicio de una instancia de base de datos.
Error 87 / 0x57	El parámetro es incorrecto.	La cuenta de servicio de dominio especificada mediante AWS Secrets Manager no tiene los permisos correctos. El perfil de usuario también podría estar dañado.	Revise los requisitos de la cuenta de servicio de dominio. Para obtener más información, consulte Configure su cuenta de servicio de dominio de AD.
Error 234 / 0xEA	La unidad organizativa (OU) especificada no existe.	La unidad organizativa especificada con el parámetro `–domain-ou` no existe en su AD autoadministrado.	Revise el parámetro `–domain-ou` y asegúrese de que la unidad organizativa especificada exista en su AD autoadministrado.

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
Error 1326 / 0x52E	El nombre de usuario o la contraseña es incorrecto.	Las credenciales de la cuenta de servicio de dominio proporcionadas en AWS Secrets Manager contienen un nombre de usuario desconocido o una contraseña incorrecta. La cuenta de dominio también podría estar deshabilitada en su AD autoadministrado.	Asegúrese de que las credenciales proporcionadas en AWS Secrets Manager sean correctas y de que la cuenta de dominio esté habilitada en su Active Directory autoadministrado.
Error 1355 / 0x54B	El dominio especificado no existe o no se pudo contactar con él.	El dominio está inactivo, no se puede acceder al conjunto especificado de IP de DNS o no se puede acceder al FQDN especificado.	Revise los parámetros `–domain-dns-ips` y `–domain-fqdn` para asegurarse de que son correctos. Revise la configuración de red de su instancia de base de datos de RDS para SQL Server y asegúrese de que sea posible acceder a su AD autoadministrado. Para obtener más información, consulte Configure la conectividad de red.

Código de error	Descripción	Causas habituales	Sugerencias para la solución de problemas
Error 1772/0x6BA	El servidor RPC no está disponible.	Se ha producido un problema al acceder al servicio de RPC de su dominio de AD. Puede deberse a un problema de red o de servicio.	Valide que el servicio de RPC se esté ejecutando en sus controladores de dominio y que se pueda acceder a los puertos de TCP `135` y `49152-65535` en su dominio desde su instancia de base de datos de RDS para SQL Server.
Error 2224 / 0x8B0	La cuenta de usuario ya existe.	La cuenta de equipo que se intenta añadir al AD autoadministrado ya existe.	Para identificar la cuenta del equipo, ejecute `SELECT @@SERVERNAME` en su instancia de base de datos de RDS para SQL Server y, a continuación, elimínela cuidadosamente de su AD autoadministrado.
Error 2242 / 0x8c2	La contraseña de este usuario ha caducado.	La contraseña de la cuenta de servicio de dominio especificada a través de AWS Secrets Manager ha caducado.	Actualice la contraseña de la cuenta de servicio de dominio utilizada para unir su instancia de base de datos de RDS para SQL Server a su AD autoadministrado.

Restauración de una instancia de base de datos de SQL Server y adición de esta a un dominio de Active Directory autoadministrado

Puede restaurar una instantánea de base de datos o realizar una recuperación en un momento dado (PITR) para una instancia de base de datos de SQL Server y, a continuación, añadirla a un dominio de Active Directory autoadministrado. Una vez que la instancia de base de datos se haya restaurado, modifíquela con el proceso que se explica en Paso 6: Crear o modificar una instancia de base de datos de SQL Server para agregar la instancia de base de datos a un dominio de AD autoadministrado.

Uso de AWS Managed Active Directory con RDS para SQL Server

Puede usar AWS Managed Microsoft AD para autenticar a los usuarios con autenticación de Windows cuando se conecten a su instancia de base de datos de RDS para SQL Server. La instancia de base de datos funciona con AWS Directory Service for Microsoft Active Directory, también denominado AWS Managed Microsoft AD, para habilitar la autenticación de Windows. Cuando los usuarios se autentican con una instancia de base de datos de SQL Server unida al dominio de confianza, las solicitudes de autenticación se reenvían al directorio de dominio que se ha creado con AWS Directory Service.

Disponibilidad en regiones y versiones

Amazon RDS solo admite el uso de AWS Managed Microsoft AD para la autenticación de Windows. RDS no admite el uso de AD Connector. Para obtener más información, consulte los siguientes temas:

- Política de compatibilidad de las aplicaciones para AWS Managed Microsoft AD
- Política de compatibilidad de las aplicaciones para AD Connector

Para obtener información sobre la disponibilidad en versiones y regiones, consulte Autenticación Kerberos con RDS para SQL Server.

Información sobre la configuración de la autenticación de Windows

Amazon RDS usa el modo mixto para la autenticación de Windows. Este método significa que el usuario principal (el nombre y la contraseña que se han utilizado para crear la instancia de base de datos de SQL Server) usa la autenticación de SQL. Dado que la cuenta de usuario maestro es una credencial privilegiada, debe restringir el acceso a esta cuenta.

Para realizar la autenticación de Windows con un Microsoft Active Directory en las instalaciones o autoalojado, cree una relación de confianza entre bosques. La confianza puede ser unidireccional o bidireccional. Para obtener más información acerca de la configuración de relaciones de confianza entre bosques con AWS Directory Service, consulte Cuándo crear una relación de confianza en la Guía de administración de AWS Directory Service.

Para configurar la autenticación de Windows para una instancia de base de datos de SQL Server, lleve a cabo los siguientes pasos, que se explican con más detalle e Configuración de la autenticación de Windows para las instancias de base de datos de SQL Server:

1. Use AWS Managed Microsoft AD, desde la AWS Management Console o la API de AWS Directory Service, para crear un directorio AWS Managed Microsoft AD.
2. Si usa la AWS CLI o la API de Amazon RDS para crear la instancia de base de datos de SQL Server, cree un rol de AWS Identity and Access Management (IAM). Este rol utiliza la política de IAM administrada `AmazonRDSDirectoryServiceAccess` y permite a Amazon RDS realizar llamadas a su directorio. Si usa la consola para crear la instancia de base de datos de SQL Server, AWS crea el rol de IAM automáticamente.

   Para que el rol permita el acceso, el punto de enlace AWS Security Token Service (AWS STS) debe activarse en la región AWS para su cuenta AWS. Los puntos de enlace de AWS STS están activos de forma predeterminada en todas las regiones AWS y puede usarlos sin ninguna acción posterior. Para obtener más información, consulte Administración de AWS STS en una Región de AWS en la guía del usuario de IAM.
3. Cree y configure usuarios y grupos en el directorio de AWS Managed Microsoft AD usando las herramientas de Microsoft Active Directory. Para obtener más información sobre la creación de usuarios en su Active Directory, consulte Administrar usuarios y grupos en AWS Managed Microsoft AD en la guía de administración de AWS Directory Service.
4. Si tiene previsto ubicar el directorio y la instancia de base de datos en diferentes VPC, habilite el tráfico entre VPC.
5. Utilice Amazon RDS para crear una nueva instancia de base de datos de SQL Server desde la consola, la AWS CLI o la API de Amazon RDS. En la solicitud de creación, proporcione el identificador de dominio (identificador «`d-*`») que se generó cuando creó el directorio y el nombre del rol. También puede modificar una instancia de base de datos de SQL Server existente para usar la autenticación de Windows mediante la configuración de los parámetros dominio y rol de IAM para la instancia de base de datos.
6. Use las credenciales del usuario maestro de Amazon RDS para conectarse a la instancia de base de datos de SQL Server como lo haría con cualquier otra instancia de base de datos. Como la instancia de base de datos está unida al dominio AWS Managed Microsoft AD, puede aprovisionar inicios de sesión y usuarios de SQL Server desde los usuarios y grupos de Active Directory de su dominio. (Estos se conocen como inicios de sesión de SQL Server «Windows»). Los permisos de bases de datos se administran a través de los permisos de SQL Server estándar otorgados y revocados para estos inicios de sesión de Windows.

Al crear una instancia de base de datos de RDS para SQL Server conectada a un dominio mediante la consola de Amazon RDS, AWS crea automáticamente el rol de IAM `rds-directoryservice-`

`access-role`. Este rol es esencial para administrar las instancias conectadas a un dominio y es necesario para las siguientes operaciones:

- Realización de cambios de configuración en las instancias de SQL Server conectadas a un dominio
- Administración de la configuración de la integración de Active Directory
- Realización de operaciones de mantenimiento en instancias unidas a un dominio

> **Important**
>
> Si elimina el rol de IAM `rds-directoryservice-access-role`, no puede realizar cambios en la instancia de SQL Server conectada al dominio a través de la consola o la API de Amazon RDS. Al intentar modificar la instancia, aparece un mensaje de error que indica: No tiene permiso para iam:CreateRole. Para solicitar acceso, copie el siguiente texto y envíelo al administrador de AWS.
> Este error se produce porque Amazon RDS necesita volver a crear el rol para administrar la conexión del dominio, pero carece de los permisos necesarios. Además, este error no se registra en CloudTrail, lo que puede dificultar la solución de problemas.

Si elimina accidentalmente `rds-directoryservice-access-role`, debe tener permisos `iam:CreateRole` para volver a crearlo antes de poder realizar cambios en la instancia de SQL Server conectada al dominio. Para volver a crear el rol manualmente, asegúrese de que tenga la política administrada `AmazonRDSDirectoryServiceAccess` asociada y la relación de confianza adecuada que permita que el servicio de RDS asuma el rol.

Creación del punto de enlace para la autenticación Kerberos

La autenticación basada en Kerberos requiere que el punto de enlace sea el nombre de host especificado por el cliente, un punto y, a continuación, el nombre de dominio completo (FQDN). Por ejemplo, el siguiente ejemplo muestra un punto de enlace que se podría usarse con la autenticación basada en Kerberos. En este ejemplo, el nombre de host de la instancia de base de datos de SQL Server es `ad-test` y el nombre de dominio es `corp-ad.company.com`.

```
ad-test.corp-ad.company.com
```

Si desea asegurarse de que su conexión use Kerberos, ejecute la siguiente consulta:

```
SELECT net_transport, auth_scheme
  FROM sys.dm_exec_connections
 WHERE session_id = @@SPID;
```

Configuración de la autenticación de Windows para las instancias de base de datos de SQL Server

Debe usar AWS Directory Service for Microsoft Active Directory, también llamado AWS Managed Microsoft AD, para configurar la autenticación de Windows para una instancia de base de datos de SQL Server. Para configurar la autenticación de Windows, lleve a cabo los siguientes pasos.

Paso 1: crear un directorio con AWS Directory Service for Microsoft Active Directory

AWS Directory Service crea un directorio de Microsoft Active Directory totalmente gestionado en la nube de AWS. Cuando crea un directorio AWS Managed Microsoft AD, AWS Directory Service crea dos controladores de dominio y servidores del Servicio de nombres de dominio (DNS) en su nombre. Los servidores de directorio se crean en dos subredes en dos zonas de disponibilidad diferentes dentro de una VPC. Esta redundancia ayuda a garantizar que su directorio permanezca accesible incluso si ocurre un fallo.

Cuando crea un directorio de AWS Managed Microsoft AD, AWS Directory Service realiza en su nombre las siguientes tareas:

- Configura un Microsoft Active Directory dentro de la VPC.
- Crea una cuenta de administrador para el directorio con el nombre de usuario Admin y la contraseña especificada. Esta cuenta le permite administrar el directorio.
- Crea un grupo de seguridad para los controladores del directorio.

Al lanzar AWS Directory Service for Microsoft Active Directory, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa, que tiene el nombre de NetBIOS que escribió al crear el directorio, se encuentra en la raíz del dominio. La raíz del dominio es propiedad de , que también se encarga de su administració AWS.

La cuenta admin que se creó con el directorio de AWS Managed Microsoft AD dispone de permisos para realizar las actividades administrativas más habituales para la unidad organizativa:

- Cree, actualice o elimine usuarios, grupos y equipos.

- Añadir recursos a su dominio, como servidores de archivos o de impresión y, a continuación, asignar permisos para esos recursos a usuarios y grupos dentro de la unidad organizativa.
- Crear unidades organizativas y contenedores adicionales.
- Delegar autoridad.
- Crear y enlazar políticas de grupo.
- Restaurar objetos eliminados de la papelera de reciclaje de Active Directory.
- Ejecutar módulos de AD y DNS de Windows PowerShell en el servicio web de Active Directory.

La cuenta admin también tiene derechos para realizar las siguientes actividades en todo el dominio:

- Administrar configuraciones DNS (agregar, quitar o actualizar registros, zonas y programas de envío).
- Ver logs de eventos DNS.
- Ver logs de eventos de seguridad.

Para crear un directorio con AWS Managed Microsoft AD

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios) y, a continuación, elija Set up Directory (Configurar directorio).
2. Elija AWS Managed Microsoft AD. Es la única opción que se admite actualmente para el uso con Amazon RDS.
3. Elija Siguiente.
4. En la página Enter directory information (Especifique la información del directorio), facilite la siguiente información:

   Edición

   Elija la edición que se adapte a sus necesidades.

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo `corp.example.com`. SQL Server no admite nombres de más de 47 caracteres.

   Nombre NetBIOS del directorio

   Un nombre abreviado del directorio opcional, como COR `CORP`.

Descripción del directorio

Descripción opcional del directorio.

Contraseña de administrador

Contraseña del administrador del directorio. El proceso de creación de directorios crea una cuenta de administrador con el nombre de usuario Admin y esta contraseña.

La contraseña del administrador del directorio no puede contener la palabra `admin`. La contraseña distingue entre mayúsculas y minúsculas y debe tener un mínimo de 864 caracteres y un máximo de 64. También debe contener al menos un carácter de tres de las siguientes categorías:

- Letras minúsculas (a-z)
- Letras mayúsculas (A-Z)
- Números (0-9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password

Vuelva a escribir la contraseña de administrador.

5. Elija Siguiente.
6. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la información siguiente:

VPC

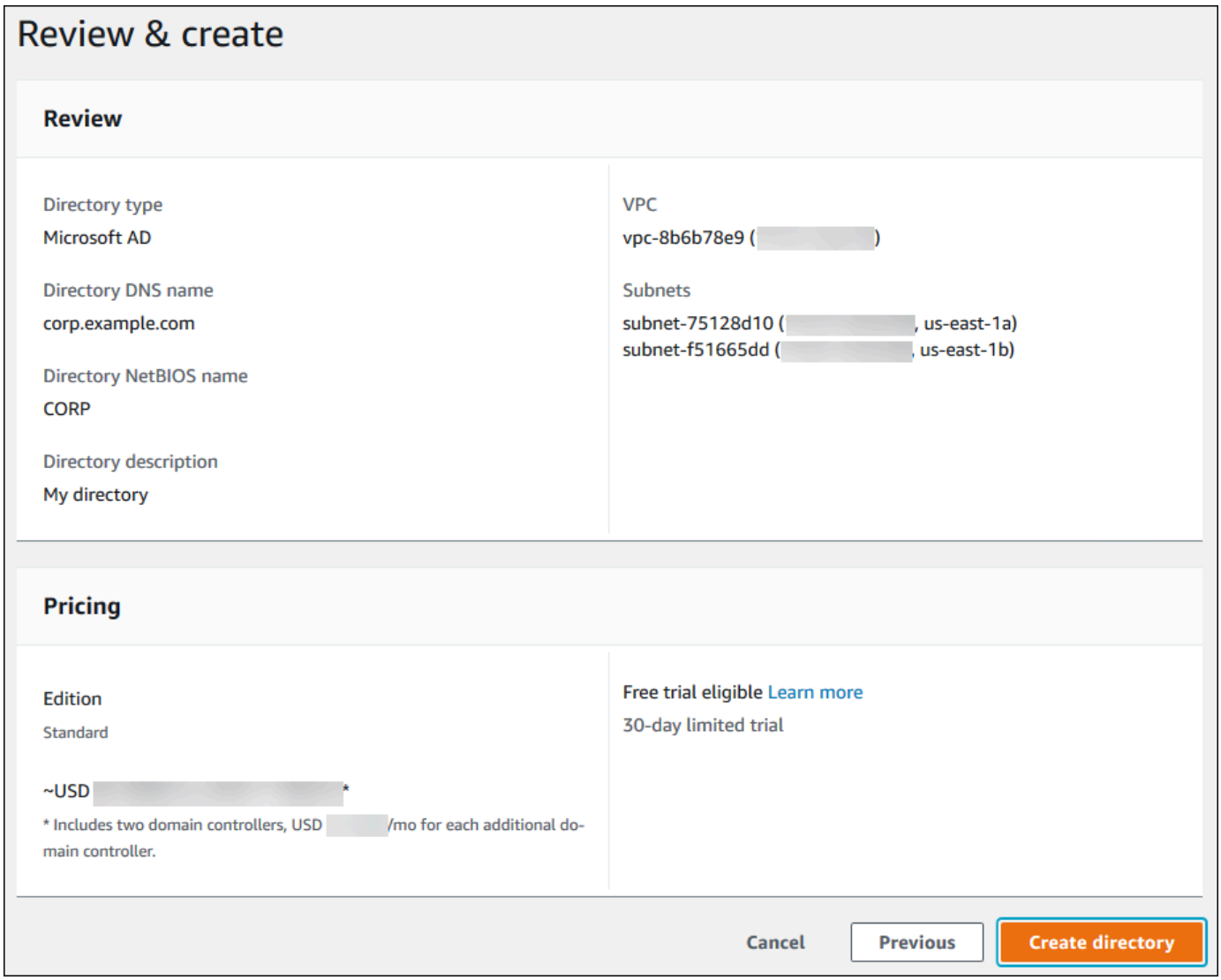
Elija la VPC del directorio.

> **Note**
>
> Puede ubicar el directorio y la instancia de base de datos en diferentes VPC pero, si lo hace así, habilite el tráfico entre VPC. Para obtener más información, consulte Paso 4: habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos.

Subredes

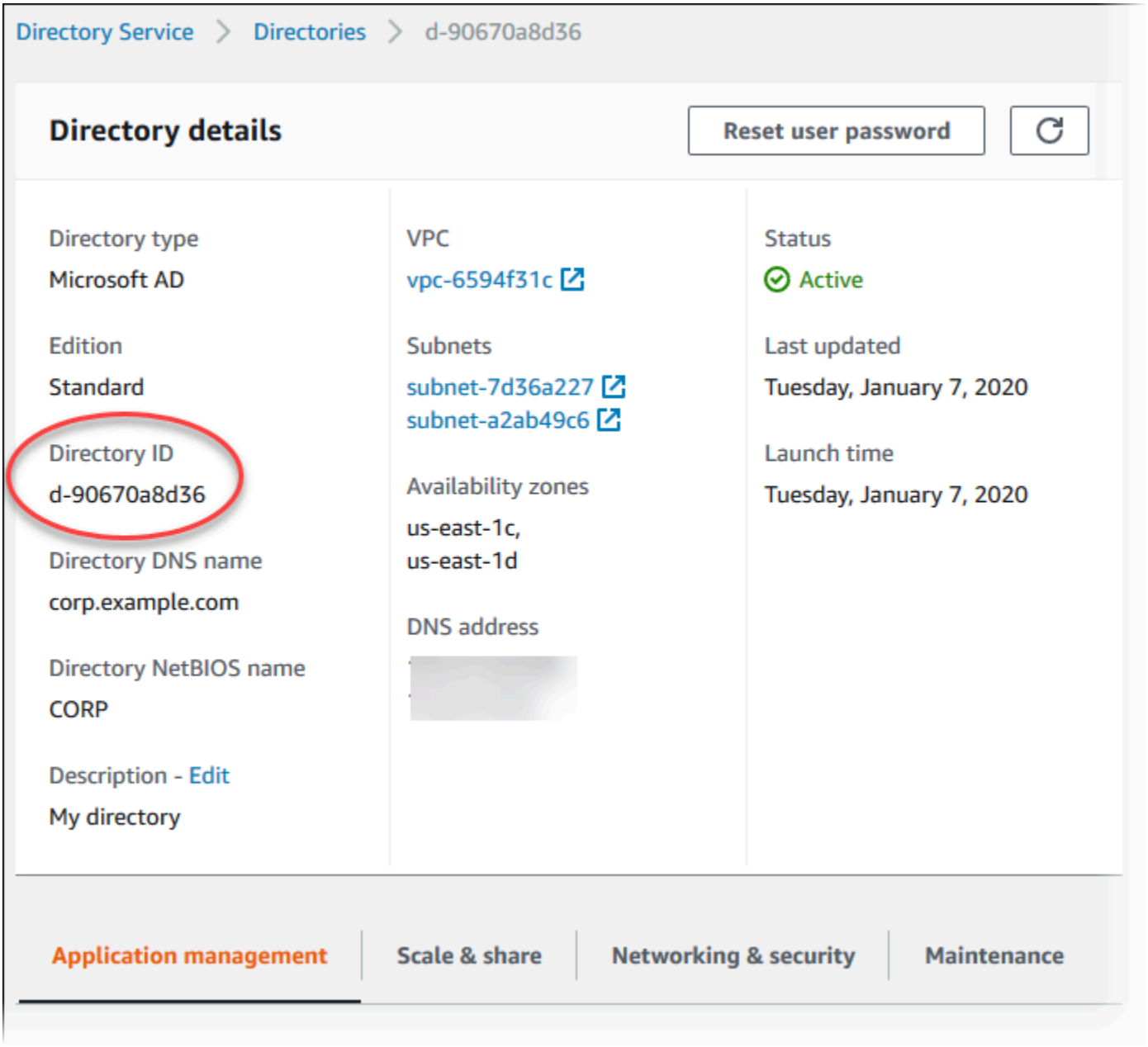
Elija las subredes de los servidores del directorio. Las dos subredes deben estar en diferentes zonas de disponibilidad.

7. Elija Siguiente.
8. Revise la información del directorio. Si es necesario realizar algún cambio, seleccione Privous (Anterior). Cuando la información sea correcta, seleccione Create directory (Crear directorio).



La creación del directorio tarda varios minutos. Cuando se haya creado correctamente, el valor de Status (Estado) cambiará a Active (Activo).

Para ver información acerca de su directorio, seleccione el ID del directorio en la lista de directorios. Anote el valor de Directory ID (ID de directorio). Necesitará este valor cuando cree o modifique la instancia de base de datos de SQL Server.



Paso 2: crear el rol de IAM que usará Amazon RDS

Si usa la consola para crear la instancia de base de datos de SQL Server, puede omitir este paso. Si usa la CLI o la API de RDS para crear su propia instancia de base de datos de SQL Server, debe crear un rol de IAM que use la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. Este rol permite a Amazon RDS realizar llamadas a AWS Directory Service en su nombre.

Si usa una política personalizada para unirse a un dominio en lugar de usar la política AWS administrada por `AmazonRDSDirectoryServiceAccess`, debe permitir la acción `ds:GetAuthorizedApplicationDetails`. Este requisito entrará en vigor a partir de julio de 2019, debido a un cambio en la API de AWS Directory Service.

La siguiente política de IAM, `AmazonRDSDirectoryServiceAccess`, proporciona acceso a AWS Directory Service.

Example Política de IAM para proporcionar acceso a AWS Directory Service

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
            "ds:DescribeDirectories",
            "ds:AuthorizeApplication",
            "ds:UnauthorizeApplication",
            "ds:GetAuthorizedApplicationDetails"
        ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Le recomendamos que utilice las claves de contexto de condición globales de `aws:SourceArn` y `aws:SourceAccount` en las relaciones de confianza basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

Puede utilizar claves de contexto de condición globales y hacer que el valor de `aws:SourceArn` contenga el ID de cuenta. En estos casos, el valor de `aws:SourceAccount` y la cuenta del valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilizan en la misma instrucción.

- Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.

- Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En la relación de confianza, asegúrese de utilizar la clave de contexto de condición global `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo de los recursos que acceden al rol. Para la autenticación de Windows, asegúrese de incluir las instancias de base de datos, tal y como se muestra en el siguiente ejemplo.

Example relación de confianza con la clave de contexto de condición global para la autenticación de Windows

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier"
                    ]
                }
            }
        }
    ]
}
```

Cree un rol de IAM con esta política de IAM y su relación de confianza. Para obtener más información acerca de la creación de roles de IAM, consulte Creación de políticas administradas por el cliente en la Guía del usuario de IAM.

Paso 3: crear y configurar usuarios y grupos

Puede crear usuarios y grupos con la herramienta Usuarios y equipos de Active Directory. Esta herramienta es una de las herramientas Active Directory Domain Services y Active Directory Lightweight Directory Services. Los usuarios representan a las personas físicas o entidades que tienen acceso al directorio. Los grupos resultan muy útiles para conceder o denegar privilegios a un conjunto de usuarios en lugar de asignar esos privilegios a cada usuario por separado.

Para crear usuarios y grupos en un directorio de AWS Directory Service, debe estar conectado a una instancia EC2 de Windows que sea miembro del directorio de AWS Directory Service. También debe haber iniciado sesión como usuario con privilegios para crear usuarios. Para obtener más información, consulte la sección para agregar usuarios y grupos (Simple AD yAWS Managed Microsoft AD) en la guía de administraciónde AWS Directory Service.

Paso 4: habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos

Si tiene previsto ubicar el directorio y la instancia de base de datos en la misma VPC, omita este paso y continúe con Paso 5: crear o modificar una instancia de base de datos de SQL Server.

Si tiene previsto ubicar el directorio y la instancia de base de datos en diferentes VPC, configure el tráfico entre VPC mediante la interconexión de VPC o AWSTransit Gateway.

El siguiente procedimiento permite el tráfico entre VPC mediante la interconexión de VPC. Siga las instrucciones de ¿Qué es una interconexión de VPC? en la Guía de interconexión de Amazon Virtual Private Cloud.

Para habilitar el tráfico entre VPC mediante la interconexión de VPC

1. Configure las reglas de enrutamiento de VPC adecuadas para garantizar que el tráfico de red pueda fluir en ambos sentidos.
2. Asegúrese de que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico de entrada del grupo de seguridad del directorio.
3. Asegúrese de que no haya una regla de lista de control de acceso (ACL) a la red para bloquear el tráfico.

Si una cuenta de AWS distinta es la propietaria del directorio, debe compartirlo.

Para compartir el directorio entre cuentas de AWS

1. Comience a compartir el directorio con la cuenta AWS en la que se creará la instancia de base de datos siguiendo las instrucciones de Tutorial: Uso compartido del directorio de AWS Managed Microsoft AD para realizar la unión al dominio fluida de EC2 en la AWS Directory ServiceGuía de administración.
2. Inicie sesión en la consola de AWS Directory Service utilizando la cuenta para la instancia de base de datos y asegúrese de que el dominio tiene el estado `SHARED` antes de continuar.
3. Una vez iniciada sesión en la consola de AWS Directory Service utilizando la cuenta de la instancia de base de datos, anote el valor de Directory ID (ID de directorio). Utilice este identificador de directorio para unir la instancia de base de datos al dominio.

Paso 5: crear o modificar una instancia de base de datos de SQL Server

Cree o modifique una instancia de base de datos de SQL Server para usarla con su directorio. Puede utilizar la consola, CLI, o la API de RDS para asociar una instancia de base de datos con un directorio. Puede hacerlo de una de las siguientes formas:

- Cree una nueva instancia de base de datos de SQL Server mediante la consola, el comando de la CLI create-db-instance o la operación CreateDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de SQL Server existente mediante la consola, el comando de la CLI modify-db-instance o la operación ModifyDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Restaure una instancia de base de datos de SQL Server a partir de una instantánea de base de datos mediante la consola, el comando de la CLI restore-db-instance-from-db-snapshot o la operación RestoreDBInstanceFromDBSnapshot de la API de RDS.

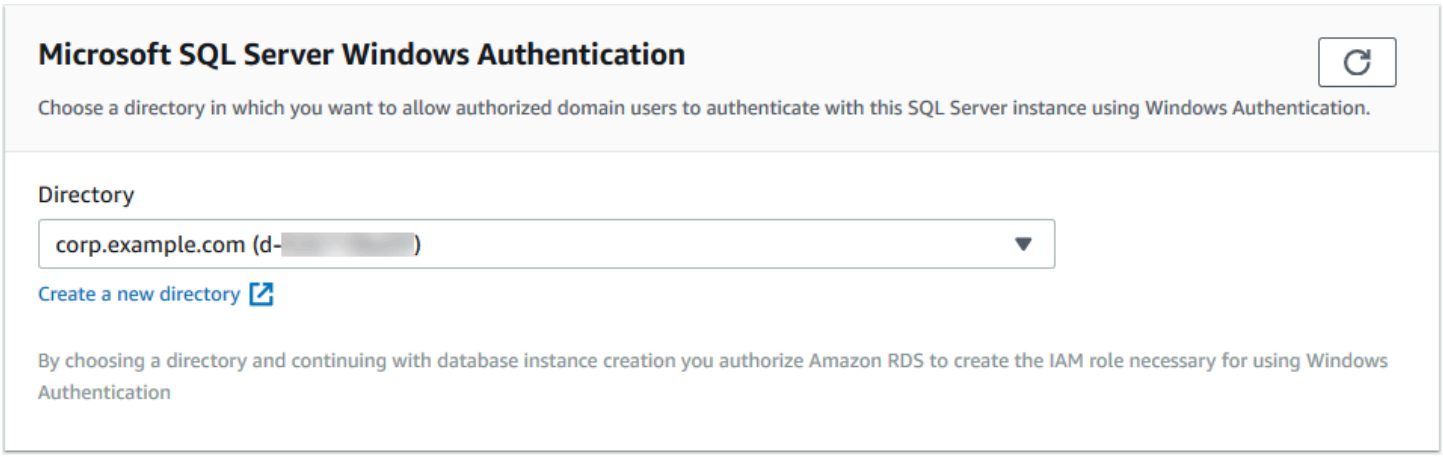
  Para obtener instrucciones, consulte Restauración a una instancia de base de datos.
- Restaure una instancia de base de datos de SQL Server a un punto en el tiempo mediante la consola, el comando de la CLI restore-db-instance-to-point-in-time o la operación RestoreDBInstanceToPointInTime de la API de RDS.

  Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

La autenticación Windows solo es compatible con instancias de base de datos de SQL Server en una VPC.

Para que la instancia de base de datos pueda usar el directorio de dominio que ha creado, se precisa lo siguiente:

- Para Directory (Directorio), elija el identificador de dominio (d-*ID*) que se generó cuando creó el directorio.
- Asegúrese de que el grupo de seguridad de VPC tiene una regla de salida que permita a la instancia de base de datos comunicarse con el directorio.



Cuando utilice la AWS CLI, se necesitan los siguientes parámetros para que la instancia de base de datos pueda usar el directorio que ha creado:

- Para el parámetro `--domain`, utilice el identificador de dominio (identificador «d-*ID*») que se generó cuando creó el directorio.
- Para el parámetro `--domain-iam-role-name`, utilice el rol que creó que usa la política `AmazonRDSDirectoryServiceAccess` de IAM administrada.

Por ejemplo, el siguiente comando de CLI modifica una instancia de base de datos para usar un directorio.

Para Linux, macOS, o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --domain d-ID \
```

```
    --domain-iam-role-name role-name
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

> **Important**
>
> Si modifica una instancia de base de datos para habilitar la autenticación Kerberos, reinicie la instancia de base de datos después de realizar el cambio.

Paso 6: crear inicios de sesión de SQL Server de autenticación de Windows

Use las credenciales del usuario maestro de Amazon RDS para conectarse a la instancia de base de datos de SQL Server como lo haría con cualquier otra instancia de base de datos. Como la instancia de base de datos está unida al dominio AWS Managed Microsoft AD, puede aprovisionar inicios de sesión y usuarios de SQL Server. Esto se realiza desde los usuarios y grupos de Active Directory de su dominio. Los permisos de bases de datos se administran a través de los permisos de SQL Server estándar otorgados y revocados para estos inicios de sesión de Windows.

Para que un usuario de Active Directory se autentique con SQL Server, debe existir un inicio de sesión de Windows de SQL Server para el usuario o para un grupo del que el usuario sea miembro. El control detallado del acceso se gestiona mediante la concesión y la revocación de permisos en estos inicios de sesión de SQL Server. Un usuario que no tenga un inicio de sesión de SQL Server o no pertenezca a un grupo con dicho inicio de sesión no puede tener acceso a la instancia de base de datos de SQL Server.

El permiso ALTER ANY LOGIN es necesario para crear un inicio de sesión de SQL Server de Active Directory. Si todavía no ha creado ningún inicio de sesión con este permiso, conéctese como usuario maestro de la instancia de base de datos usando la autenticación de SQL Server.

Ejecute el comando de lenguaje de definición de datos (DDL), como en el siguiente ejemplo, para crear un inicio de sesión de SQL Server para el usuario o el grupo de Active Directory.

> **Note**
>
> Especifique usuarios y grupos con el nombre de inicio de sesión anterior a Windows 2000 en el formato *domainName**login_name*. No puede usar un nombre principal del usuario (UPN) en el formato *login_name*@*DomainName*.
> Solo puede crear un inicio de sesión de autenticación de Windows en una instancia de RDS para SQL Server mediante instrucciones T-SQL. No puede usar SQL Server Management Studio para crear un inicio de sesión de autenticación de Windows.

```
USE [master]
GO
CREATE LOGIN [mydomain\myuser] FROM WINDOWS WITH DEFAULT_DATABASE = [master],
 DEFAULT_LANGUAGE = [us_english];
GO
```

Para obtener más información, consulte CREATE LOGIN (Transact-SQL) (Crear inicio de sesión [Transact-SQL]) en la documentación de Microsoft Developer Network.

Los usuarios (tanto humanos como aplicaciones) del dominio pueden conectarse ahora a la instancia de RDS for SQL Server desde un equipo cliente unido al dominio utilizando la autenticación de Windows.

Administración de una instancia de base de datos en un dominio

Puede usar la consola, la AWS CLI o la API de Amazon RDS para administrar la instancia de base de datos y la relación con su dominio. Por ejemplo, puede mover la instancia de base de datos dentro, fuera o entre dominios.

Por ejemplo, con la API de Amazon RDS puede hacer lo siguiente:

- Para volver a intentar una unión de dominio para una suscripción que haya generado un error, use la operación ModifyDBInstance de la API y especifique el ID del directorio de suscripción actual.
- Para actualizar el nombre del rol de IAM para la suscripción, use la operación `ModifyDBInstance` de la API y especifique el ID del directorio de la suscripción actual y el nuevo rol de IAM.
- Para eliminar una instancia de base de datos de un dominio, use la operación `ModifyDBInstance` de la API y especifique `none` como parámetro del dominio.

- Para mover una instancia de base de datos de un dominio a otro, use la operación `ModifyDBInstance` de la API y especifique el identificador del nuevo dominio como parámetro del dominio.
- Para ver la suscripción de cada instancia de base de datos, use la operación DescribeDBInstances de la API.

Descripción de la pertenencia a los dominios

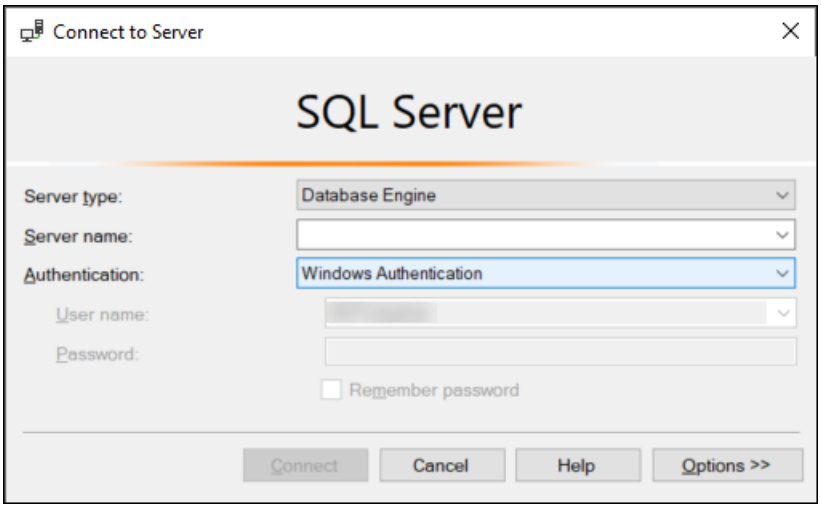
Una vez que haya creado o modificado una instancia de base de datos, esta se convierte en miembro del dominio. La consola AWS indica el estado de la pertenencia del dominio para la instancia de base de datos. El estado de la instancia de base de datos puede ser uno de los siguientes:

- joined: la instancia es miembro del dominio.
- joining: la instancia está en el proceso de convertirse en miembro del dominio.
- pending-join: la suscripción de la instancia está pendiente.
- pending-maintenance-join: AWS intentará convertir la instancia en miembro del dominio durante el próximo periodo de mantenimiento programado.
- pending-removal: la eliminación de la instancia del dominio está pendiente.
- pending-maintenance-removal: AWS intentará eliminar la instancia del dominio durante el próximo periodo de mantenimiento programado.
- error: un problema de configuración ha impedido que la instancia se una al dominio. Compruebe y corrija la configuración antes de volver a ejecutar el comando para modificar la instancia.
- removing: la instancia se está eliminando del dominio.

Una solicitud para convertirse en miembro de un dominio puede generar un error a causa de un problema de conectividad de la red o de un rol de IAM incorrecto. Por ejemplo, puede crear una instancia de base de datos o modificar una instancia existente y que se produzca un error al intentar que la instancia de base de datos se convierta en miembro de un dominio. En este caso, vuelva a emitir el comando para crear o modificar la instancia de base de datos o modificar la instancia recién creada para unirse al dominio.

Conexión a SQL Server con la autenticación de Windows

Para conectarse a SQL Server con la autenticación de Windows, debe haber iniciado sesión en un equipo unido al dominio como usuario del dominio. Después de lanzar SQL Server Management Studio, elija Windows Authentication como tipo de autenticación, como se puede ver a continuación.



Restauración de una instancia de base de datos de SQL Server y adición de esta a un dominio

Puede restaurar una instantánea de base de datos o realizar una restauración a un momento dado (PITR) para una instancia de base de datos de SQL Server y, a continuación, añadirla a un dominio. Una vez que la instancia de base de datos se haya restaurado, modifíquela usando el proceso que se explica en la sección Paso 5: crear o modificar una instancia de base de datos de SQL Server para agregar la instancia de base de datos a un dominio.

Actualización de aplicaciones para la conexión a las instancias de base de datos de Microsoft SQL Server con los nuevos certificados SSL/TLS

El 13 de enero de 2023, Amazon RDS publicó nuevos certificados de entidades de certificación (CA) para la conexión a sus instancias de base de datos de RDS mediante la capa de sockets seguros o seguridad de la capa de transporte (SSL/TLS). Después, puede encontrar la información sobre la actualización de sus aplicaciones para utilizar los nuevos certificados.

Este tema puede ayudarle a determinar si las aplicaciones de cualquier cliente utilizan SSL/TLS para conectarse a sus instancias de base de datos. Si lo hacen, puede comprobar de manera adicional si esas aplicaciones precisan una verificación de certificados para conectarse.

> **Note**
>
> Algunas aplicaciones están configuradas para conectarse a las instancias de base de datos de SQL Server solo si pueden verificar con éxito el certificado del servidor.
> Para esas aplicaciones, debe actualizar los almacenes de confianza de la aplicación de su cliente para incluir los nuevos certificados de CA.

Después actualizar sus certificados de CA en los almacenes de confianza de la aplicación de su cliente, puede rotar los certificados en sus instancias de base de datos. Recomendamos encarecidamente probar estos procedimientos en un entorno de desarrollo o ensayo antes de implementarlos en sus entornos de producción.

Para obtener más información acerca de la rotación de certificados, consulte Rotar certificados SSL/TLS. Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener información sobre el uso de SSL/TLS con las instancias de base de datos de Microsoft SQL Server, consulte ???.

Temas

- Determinación de si alguna aplicación se conecta a su instancia de base de datos de Microsoft SQL Server mediante SSL
- Determinación de si un cliente necesita una verificación de certificados para conectarse
- Actualización del almacén de confianza de su aplicación

Determinación de si alguna aplicación se conecta a su instancia de base de datos de Microsoft SQL Server mediante SSL

Compruebe la configuración de la instancia de base de datos para obtener el valor del parámetro de `rds.force_ssl`. De forma predeterminada, el parámetro `rds.force_ssl` tiene el valor 0 (desactivado). Si el parámetro `rds.force_ssl` está configurado como 1 (activado), se precisa que los clientes utilicen SSL/TLS para las conexiones. Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

Ejecute la siguiente consulta para tener acceso a la opción de cifrado actual para todas las conexiones abiertas de la instancia de base de datos. La columna `ENCRYPT_OPTION` devuelve `TRUE` si la conexión está cifrada.

```
select SESSION_ID,
    ENCRYPT_OPTION,
    NET_TRANSPORT,
    AUTH_SCHEME
    from SYS.DM_EXEC_CONNECTIONS
```

Esta consulta muestra solo las conexiones actuales. No muestra si las aplicaciones que se han conectado y desconectado anteriormente han utilizado SSL.

Determinación de si un cliente necesita una verificación de certificados para conectarse

Puede comprobar si diferentes tipos de clientes precisan la verificación de certificados para conectarse.

> **Note**
>
> Si utiliza conectores distintos a los enumerados, consulte la documentación del conector específico para obtener información sobre cómo aplica las conexiones cifradas. Para obtener más información, consulte Módulos de conexión para las bases de datos de Microsoft SQL en la documentación de Microsoft SQL Server.

SQL Server Management Studio

Compruebe si el cifrado se aplica para las conexiones de SQL Server Management Studio:

1. Lance SQL Server Management Studio.
2. En Connect to server (Conectar al servidor), introduzca la información del servidor, el nombre de usuario de inicio de sesión y la contraseña.
3. Elija Options.
4. Compruebe si Encrypt connection (Cifrar conexión) se ha seleccionado en la página de conexión.

Para obtener más información acerca de SQL Server Management Studio, consulte SQL Server Management Studio.

Sqlcmd

En el siguiente ejemplo con el cliente de `sqlcmd` se muestra cómo comprobar la conexión a SQL Server de un script para determinar si las conexiones realizadas correctamente precisan un certificado válido. Para obtener más información, consulte Conexión con sqlcmd en la documentación de Microsoft SQL Server.

Al utilizar `sqlcmd`, una conexión SSL precisa una verificación frente al certificado del servidor si utiliza el argumento del comando `-N` para cifrar conexiones, como en el siguiente ejemplo.

```
$ sqlcmd -N -S dbinstance.rds.amazon.com -d ExampleDB
```

> **Note**
>
> Si se invoca `sqlcmd` con la opción `-C`, confía en el certificado del servidor, incluso si no coincide con el almacén de confianza del lado del cliente.

ADO.NET

En el siguiente ejemplo, la aplicación se conecta utilizando SSL y el certificado del servidor se debe verificar.

```
using SQLC = Microsoft.Data.SqlClient;

...

    static public void Main()
    {
        using (var connection = new SQLC.SqlConnection(
            "Server=tcp:dbinstance.rds.amazon.com;" +
            "Database=ExampleDB;User ID=LOGIN_NAME;" +
            "Password=YOUR_PASSWORD;" +
            "Encrypt=True;TrustServerCertificate=False;"
            ))
        {
            connection.Open();
            ...
        }
```

Java

En el siguiente ejemplo, la aplicación se conecta utilizando SSL y el certificado del servidor se debe verificar.

```
String connectionUrl =
    "jdbc:sqlserver://dbinstance.rds.amazon.com;" +
    "databaseName=ExampleDB;integratedSecurity=true;" +
    "encrypt=true;trustServerCertificate=false";
```

Para habilitar el cifrado SSL para los clientes que se conectan usando JDBC, puede ser necesario añadir el certificado de Amazon RDS al almacén de certificados de CA de Java. Para obtener instrucciones, consulte Configuración del cliente para el cifrado en la documentación de Microsoft SQL Server. También puede proporcionar el nombre del archivo del certificado de CA de confianza directamente añadiendo `trustStore=`*`path-to-certificate-trust-store-file`* a la cadena de conexión.

> **Note**
>
> SI utiliza `TrustServerCertificate=true` (o su equivalente) en la cadena de conexión, el proceso de conexión omite la validación de la cadena de confianza. En este

caso, la aplicación se conecta incluso si el certificado no se puede verificar. El uso de `TrustServerCertificate=false` aplica la validación del certificado y es una práctica recomendada.

Actualización del almacén de confianza de su aplicación

Puede actualizar el almacén de confianza para las aplicaciones que utilizan Microsoft SQL Server. Para obtener instrucciones, consulte ???. Además, consulte Configuración del cliente para el cifrado en la documentación de Microsoft SQL Server.

Si utiliza un sistema operativo distinto a Microsoft Windows, consulte la documentación de distribución de software para conseguir la implementación de SSL/TLS para obtener información sobre la adición de un nuevo certificado de CA de raíz. Por ejemplo, OpenSSL y GnuTLS son opciones populares. Utilice el método de implementación para añadir confianza al certificado de CA de raíz de RDS. Microsoft proporciona instrucciones para configurar certificados en algunos sistemas.

Para obtener información sobre la descarga del certificado raíz, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Para obtener secuencias de comandos de ejemplo que importan certificados, consulte Script de muestra para la importación de certificados en su almacén de confianza.

> **Note**
>
> Cuando actualice el almacén de confianza, puede retener certificados antiguos además de añadir los nuevos certificados.

Actualizaciones del motor de base de datos de Microsoft SQL Server

Cuando Amazon RDS admita una nueva versión de un motor de base de datos, podrá actualizar sus instancias de base de datos a la nueva versión. Hay dos tipos de actualizaciones para las instancias de base de datos de SQL Server: actualizaciones de versiones principales y actualizaciones de versiones secundarias.

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de las aplicaciones. Por lo tanto, debe realizar manualmente las actualizaciones de versiones principales de sus instancias de base de datos. Puede iniciar una actualización de versión principal modificando su instancia de base de datos. Sin embargo, antes de realizar una actualización de versión principal, recomendamos que pruebe la actualización siguiendo los pasos descritos en Prueba de una actualización de RDS para SQL Server.

Las actualizaciones de versiones secundarias solo contienen cambios compatibles con las versiones anteriores de las aplicaciones existentes. Puede actualizar la versión secundaria de la instancia de base de datos de dos maneras:

- Manualmente: modifique la instancia de base de datos para iniciar la actualización
- Automáticamente: habilite las actualizaciones automáticas de versiones secundarias para la instancia de base de datos

Al habilitar las actualizaciones automáticas de las versiones secundarias, RDS para SQL Server actualiza automáticamente la instancia de base de datos durante los periodos de mantenimiento programados cuando hay actualizaciones de seguridad críticas disponibles en una versión secundaria más reciente.

Para las versiones secundarias del motor posteriores a `16.00.4120.1`, `15.00.4365.2`, `14.00.3465.1`, `13.00.6435.1`, los siguientes protocolos de seguridad están desactivados de forma predeterminada:

- `rds.tls10` (protocolo TLS 1.0)
- `rds.tls11` (protocolo TLS 1.1)
- `rds.rc4` (cifrado RC4)
- `rds.curve25519` (cifrado Curve25519)

- `rds.3des168` (cifrado Triple DES)

Para versiones anteriores del motor, Amazon RDS habilita estos protocolos de seguridad de forma predeterminada.

```
...

"ValidUpgradeTarget": [
    {
        "Engine": "sqlserver-se",
        "EngineVersion": "14.00.3281.6.v1",
        "Description": "SQL Server 2017 14.00.3281.6.v1",
        "AutoUpgrade": false,
        "IsMajorVersionUpgrade": false
    }
...
```

Para obtener más información acerca de cómo realizar actualizaciones, consulte Actualización de una instancia de base de datos de SQL Server. Para obtener información acerca de las versiones de SQL Server disponibles en Amazon RDS, consulte Amazon RDS for Microsoft SQL Server.

Temas

- Actualizaciones de versiones principales de RDS para SQL Server
- Aspectos a tener en cuenta sobre las actualizaciones de SQL Server
- Prueba de una actualización de RDS para SQL Server
- Actualización de una instancia de base de datos de SQL Server
- Actualización de instancias de base de datos obsoletas antes de finalizar el soporte técnico

Actualizaciones de versiones principales de RDS para SQL Server

Amazon RDS admite actualmente las siguientes actualizaciones de la versión principal para una instancia de base de datos de Microsoft SQL Server.

Puede actualizar su instancia de base de datos existente a SQL Server 2017 o 2019 desde cualquier versión salvo SQL Server 2008. Para actualizar desde SQL Server 2008, primero actualice a una de las otras versiones.

Versión actual	Versiones de actualización admitidas
SQL Server 2019	SQL Server 2022
SQL Server 2017	SQL Server 2022 SQL Server 2019
SQL Server 2016	SQL Server 2022 SQL Server 2019 SQL Server 2017

Puede utilizar una consulta de AWS CLI, como el ejemplo siguiente, para buscar las actualizaciones disponibles para una versión concreta del motor de base de datos.

Example

Para Linux, macOS o:Unix

```
aws rds describe-db-engine-versions \
    --engine sqlserver-se \
    --engine-version 14.00.3281.6.v1 \
    --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" \
    --output table
```

En:Windows

```
aws rds describe-db-engine-versions ^
    --engine sqlserver-se ^
    --engine-version 14.00.3281.6.v1 ^
    --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" ^
    --output table
```

El resultado muestra que puede actualizar la versión 14.00.3281.6 a las versiones más recientes disponibles de SQL Server 2017 o 2019.

```
--------------------------
```

```
|DescribeDBEngineVersions|
+------------------------+
|      EngineVersion     |
+------------------------+
|  14.00.3294.2.v1       |
|  14.00.3356.20.v1      |
|  14.00.3381.3.v1       |
|  14.00.3401.7.v1       |
|  14.00.3421.10.v1      |
|  14.00.3451.2.v1       |
|  15.00.4043.16.v1      |
|  15.00.4073.23.v1      |
|  15.00.4153.1.v1       |
|  15.00.4198.2.v1       |
|  15.00.4236.7.v1       |
+------------------------+
```

Nivel de compatibilidad de la base de datos

Puede utilizar los niveles de compatibilidad de la base de datos de Microsoft SQL Server para ajustar algunos comportamientos de la base de datos con objeto de imitar versiones anteriores de SQL Server. Para obtener más información, consulte Niveles de compatibilidad en la documentación de Microsoft. Al actualizar la instancia de base de datos, todas las bases de datos existentes conservan su nivel de compatibilidad original.

Puede cambiar el nivel de compatibilidad de una base de datos mediante el comando ALTER DATABASE. Por ejemplo, para cambiar una base de datos llamada `customeracct` de modo que sea compatible con SQL Server 2016, utilice el siguiente comando:

```
ALTER DATABASE customeracct SET COMPATIBILITY_LEVEL = 130
```

Aspectos a tener en cuenta sobre las actualizaciones de SQL Server

Amazon RDS toma dos instantáneas de base de datos durante el proceso de actualización. La primera instantánea de base de datos es la de la instancia de base de datos antes de que se haya llevado a cabo ningún cambio. La segunda instantánea de base de datos se crea cuando termina la actualización.

> **Note**
>
> Amazon RDS solo realiza instantáneas de base de datos si ha definido el periodo de retención de copia de seguridad de su instancia de base de datos en un número mayor que 0. Para cambiar el periodo de retención de copia de seguridad, consulte Modificación de una instancia de base de datos de Amazon RDS.

Después de completar la actualización, no puede volver a la versión anterior del motor de base de datos. Si desea volver a la versión anterior, restaure desde la instantánea de base de datos que se realizó antes de la actualización para crear una nueva instancia de base de datos.

Durante la actualización de una versión principal o secundaria de SQL Server, las métricas Free Storage Space y Disk Queue Depth mostrarán el valor `-1`. Una vez finalizada la actualización, las dos métricas recuperarán sus valores normales.

Antes de actualizar la instancia de SQL Server, lea la siguiente información.

Temas

- Prácticas recomendadas antes de iniciar una actualización
- Consideraciones de Multi-AZ
- Consideraciones sobre las réplicas de lectura
- Consideraciones relativas al grupo de opciones
- Consideraciones relativas al grupo de parámetros

Prácticas recomendadas antes de iniciar una actualización

Antes de iniciar el proceso de actualización, implemente los siguientes pasos preparatorios para lograr un rendimiento óptimo de la actualización y minimizar los posibles problemas:

Administración de tiempos y carga de trabajo

- Programe las actualizaciones durante los periodos de bajo volumen de transacciones.
- Minimice las operaciones de escritura durante el periodo de actualización.

  Esto permite a Amazon RDS completar las actualizaciones con mayor rapidez al reducir la cantidad de archivos de copia de seguridad del registro de transacciones que RDS necesita restaurar durante el emparejamiento entre el secundario y el primario.

Administración de transacciones

- Identifique y supervise transacciones de larga duración.
- Asegúrese de que todas las transacciones críticas estén confirmadas antes de iniciar la actualización.
- Evite las transacciones de larga duración durante el periodo de actualización.

Optimización de archivos de registro

Revise y optimice los archivos de registro de transacciones:

- Reduzca los archivos de registro de gran tamaño.
- Reduzca los patrones de alto consumo de registros.
- Administre los archivos de registro virtuales (VLF).
- Mantenga un espacio libre adecuado para las operaciones normales.

Consideraciones de Multi-AZ

Amazon RDS admite implementaciones Multi-AZ para instancias de base de datos en las que se ejecuta Microsoft SQL Server mediante el uso de la creación de reflejos de bases de datos (DBM) de SQL Server o los grupos de disponibilidad (AG) Always On. Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.

En una implementación multi-AZ (reflejo/AlwaysOn), cuando se solicita una actualización, RDS sigue una estrategia de actualización progresiva para las instancias principal y secundaria. Las actualizaciones progresivas garantizan que al menos una instancia esté disponible para las transacciones mientras se actualiza la instancia secundaria. Se espera que la interrupción solo dure lo que la conmutación por error.

Durante la actualización, RDS elimina la instancia secundaria de la configuración Multi-AZ, actualiza la instancia secundaria y restaura las copias de seguridad de registros de transacciones de la principal realizadas durante la desconexión. Una vez restauradas todas las copias de seguridad del registro, RDS une la secundaria actualizada a la principal. Cuando todas las bases de datos se encuentran en estado sincronizado, RDS realiza una conmutación por error a la instancia secundaria actualizada. Una vez completada la conmutación por error, RDS continúa con la actualización de la instancia principal anterior, restaura las copias de seguridad del registro de transacciones y la empareja con la nueva principal.

Para minimizar la duración de esta conmutación por error, recomendamos utilizar el punto de conexión del oyente del grupo de disponibilidad AlwaysOn AG cuando se utilizan bibliotecas de

clientes que admiten la opción de conexión `MultiSubnetFailover` en la cadena de conexión. Cuando se utiliza el punto de conexión del oyente del grupo de disponibilidad, los tiempos de conmutación por error suelen ser inferiores a 10 segundos; no obstante, esta duración no incluye ningún tiempo adicional de recuperación tras un bloqueo.

Consideraciones sobre las réplicas de lectura

Durante una actualización de la versión de la base de datos, Amazon RDS actualiza todas las réplicas de lectura junto con la instancia de base de datos principal. Amazon RDS no admite actualizaciones de versiones de bases de datos en las réplicas de lectura por separado. Para obtener más información acerca de las réplicas de lectura, consulte Uso de réplicas de lectura para Microsoft SQL Server en Amazon RDS.

Al actualizar la versión de la base de datos de la instancia de base de datos principal, todas las réplicas de lectura también se actualizan automáticamente. Amazon RDS actualiza todas las réplicas de lectura de forma simultánea antes de actualizar la instancia de base de datos principal. Es posible que las réplicas de lectura no estén disponibles hasta que se complete la actualización de la versión de la base de datos en la instancia de base de datos principal.

Consideraciones relativas al grupo de opciones

Si la instancia de base de datos utiliza un grupo de opciones de base de datos personalizado, en algunos casos Amazon RDS no puede asignar automáticamente a la instancia de base de datos un grupo de opciones nuevo. Por ejemplo, cuando se actualiza a una nueva versión principal, se debe especificar un grupo de opciones nuevo. Recomendamos que cree un grupo de opciones nuevo y que le añada las mismas opciones que tiene el grupo de opciones personalizado existente.

Para obtener más información, consulte Creación de un grupo de opciones o Copia de un grupo de opciones.

Consideraciones relativas al grupo de parámetros

Si su instancia de base de datos utiliza un grupo de parámetro de base de datos personalizado:

- Amazon RDS reinicia automáticamente la instancia de base de datos después de una actualización.
- En algunos casos, RDS no puede asignar automáticamente un grupo de parámetro nuevo a su instancia de base de datos.

Por ejemplo, cuando se actualiza a una versión principal nueva, se debe especificar un grupo de parámetro nuevo. Recomendamos que cree un grupo de parámetros nuevo y que configure en él los mismos parámetros que tiene el grupo de parámetros personalizado existente.

Para obtener más información, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS o Copia de un grupo de parámetros de base de datos en Amazon RDS.

Prueba de una actualización de RDS para SQL Server

Antes de realizar una actualización de versión principal en su instancia de base de datos, deberá realizar una comprobación exhaustiva de su base de datos y de todas las aplicaciones que tienen acceso a ella, para determinar la compatibilidad con la versión nueva. Le recomendamos que utilice el siguiente procedimiento.

Para probar una actualización de versión principal

1. Revise Actualizar SQL Server en la documentación de actualización relativa a la nueva versión del motor de base de datos para ver si hubiera problemas de compatibilidad que pudieran afectar a su base de datos o aplicaciones:
2. Si la instancia de base de datos utiliza un grupo de opciones personalizado, cree un grupo de opciones nuevo compatible con la versión nueva a la que va a actualizar. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.
3. Si la instancia de base de datos utiliza un grupo de parámetros personalizado, cree un grupo de parámetros nuevo compatible con la versión nueva a la que va a actualizar. Para obtener más información, consulte Consideraciones relativas al grupo de parámetros.
4. Cree una instantánea de base de datos de la instancia de base de datos que se va a actualizar. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
5. Restaure la instantánea de base de datos para crear una nueva instancia de base de datos de prueba. Para obtener más información, consulte Restauración a una instancia de base de datos.
6. Modifique esta instancia de base de datos de prueba nueva para actualizarla a la nueva versión, utilizando uno de los siguientes métodos:

   - Consola
   - AWS CLI
   - API de RDS

7. Evalúe el almacenamiento utilizado por la instancia actualizada para determinar si la actualización necesita almacenamiento adicional.
8. Ejecute tantas pruebas de control de calidad en la instancia de base de datos actualizada como necesite para asegurarse de que la base de datos y la aplicación funcionan correctamente con la versión nueva. Implemente las pruebas nuevas necesarias para evaluar el impacto de cualquier problema de compatibilidad identificado en el paso 1. Pruebe todas las funciones y los procedimientos almacenados. Dirija las versiones de prueba de sus aplicaciones a la instancia de base de datos actualizada.
9. Si se superan todas las pruebas, realice la actualización de la instancia de base de datos de producción. Recomendamos que no permita operaciones de escritura en la instancia de base de datos hasta haber confirmado que todo funciona correctamente.

Actualización de una instancia de base de datos de SQL Server

Para obtener más información acerca de la actualización automática o manual de una instancia de base de datos de SQL Server, consulte lo siguiente:

- Actualización de una versión del motor de una instancia de base de datos
- Procedimientos recomendados para actualizar SQL Server 2008 R2 a SQL Server 2016 en Amazon RDS for SQL Server

> **Important**
>
> Si tiene instantáneas cifradas con AWS KMS, es recomendable que inicie una actualización antes de que finalice el soporte técnico.

Actualización de instancias de base de datos obsoletas antes de finalizar el soporte técnico

Una vez que queda obsoleta una versión principal, no puede instalarla en instancias de base de datos nuevas. RDS intentará actualizar automáticamente todas las instancias de base de datos existentes.

Si necesita restaurar una instancia de base de datos obsoleta, puede realizar una recuperación a un momento dado (PITR) o restaurar una instantánea. De este modo se le concederá acceso

temporal a una instancia de base de datos que use la versión obsoleta. No obstante, una vez que una versión principal haya quedado totalmente obsoleta, estas instancias de base de datos también se actualizarán automáticamente a una versión compatible.

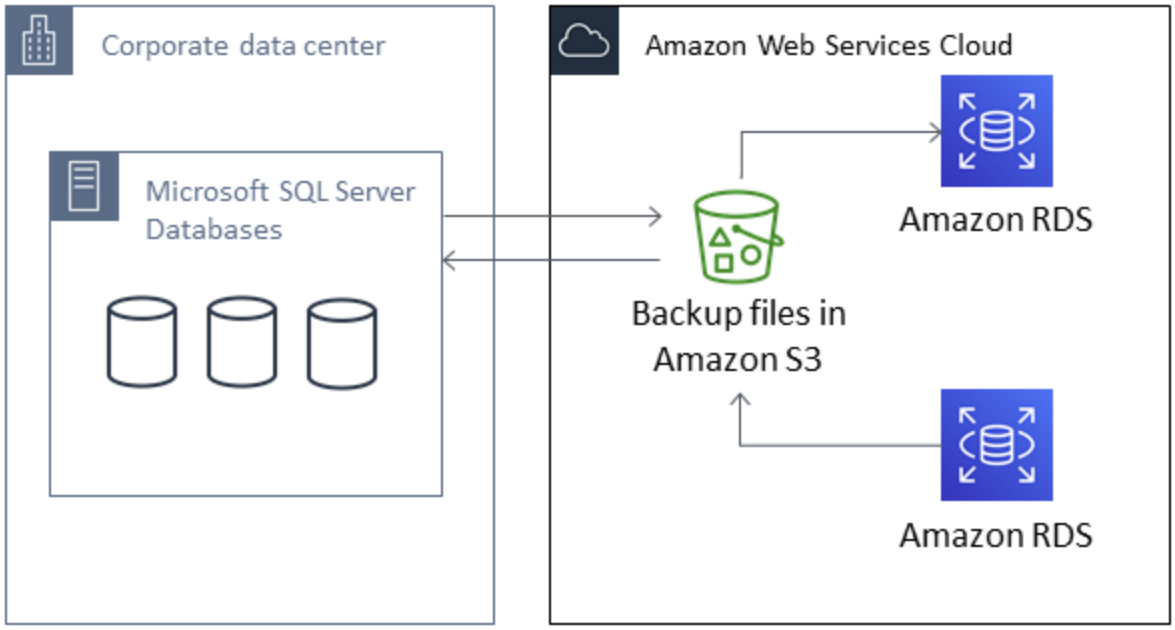
Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas

Amazon RDS admite la copia de seguridad y la restauración nativas de bases de datos de Microsoft SQL Server mediante los archivos de copia de seguridad completos (archivos .bak). Al utilizar RDS, accede a archivos almacenados en Amazon S3 en lugar de usar el sistema de archivos local en el servidor de base de datos.

Por ejemplo, puede crear una copia de seguridad completa desde su servidor local, almacenarlo en S3 y restaurarlo en una instancia de base de datos de Amazon RDS. También puede realizar copias de seguridad desde RDS, almacenarlas en S3 y restaurarlas siempre que quiera.

La copia de seguridad y la restauración nativas están disponibles en todas las regiones AWS para instancias de base de datos Single-AZ y Multi-AZ, incluidas las instancias de base de datos Multi-AZ con réplicas de lectura. La copia de seguridad y la restauración nativas están disponibles para todas las ediciones de Microsoft SQL Server compatibles con Amazon RDS.

En el siguiente diagrama se muestran los escenarios admitidos.



El uso de archivos .bak nativos para realizar copias de seguridad y restaurar bases de datos suele ser la forma más rápida de realizar copias de seguridad y de restaurar bases de datos. El uso de la copia de seguridad y la restauración nativas ofrece muchos beneficios adicionales. Por ejemplo, puede hacer lo siguiente:

- Migrar bases de datos a o desde Amazon RDS.
- Mover bases de datos entre instancias de bases de datos de RDS para SQL Server.
- Migrar datos, esquemas, procedimientos almacenados, disparadores y otro tipo de código de base de datos dentro de los archivos .bak.
- Realizar una copia de seguridad y restaurar bases de datos únicas, en lugar de instancias de base de datos completas.
- Crear copias de bases de datos para desarrollo, pruebas, sesiones de formación y demostraciones.
- Almacenar y transferir archivos de copia de seguridad con Amazon S3 para capa de protección adicional para la recuperación de desastres.
- Cree copias de seguridad nativas de bases de datos que tengan activado el cifrado de datos transparente (TDE) y restaure esas copias de seguridad en bases de datos en las instalaciones. Para obtener más información, consulte Compatibilidad con el Cifrado de datos transparente en SQL Server.
- Restaure copias de seguridad nativas de bases de datos en las instalaciones que tengan TDE activado en instancias de base de datos de RDS para SQL Server. Para obtener más información, consulte Compatibilidad con el Cifrado de datos transparente en SQL Server.

Contenido

- Limitaciones y recomendaciones
- Configuración de la copia de seguridad y la restauración nativas
  - Creación manual de un rol de IAM para la copia de seguridad y la restauración nativas
- Uso de la copia de seguridad y la restauración nativas
  - Realización de copia de seguridad de una base de datos
    - Uso
    - Ejemplos
  - Restauración de una base de datos
    - Uso
    - Ejemplos
  - Restauración de un registro
    - Uso
    - Ejemplos

- Finalización de la restauración de una base de datos
  - Uso
- Uso de bases de datos parcialmente restauradas
  - Eliminación de una base de datos parcialmente restaurada
  - Comportamiento de la restauración de instantáneas y la recuperación en un momento dado en bases de datos parcialmente restauradas
- Cancelación de una tarea
  - Uso
- Seguimiento del estado de las tareas
  - Uso
  - Ejemplos
  - Respuesta
- Compresión de archivos de copia de seguridad
- Solución de problemas
- Importación y exportación de datos de SQL Server por otros métodos
  - Importación de datos a RDS para SQL Server utilizando una instantánea
    - Importación de los datos
      - Asistente Generar y publicar scripts
      - Asistente para importación y exportación
      - Copia masiva
  - Exportación de datos de RDS para SQL Server
    - Asistente para importación y exportación de SQL Server
    - Asistente Generar y publicar scripts de SQL Server y utilidad bcp
- Uso de la utilidad BCP de Linux para importar y exportar datos
  - Requisitos previos
  - Instalación de las herramientas de línea de comandos de SQL Server en Linux
  - Exportación de datos de RDS para SQL Server
    - Sintaxis básica de exportación
    - Ejemplo de exportación
  - Importación de datos a RDS para SQL Server

    - Sintaxis básica de importación
    - Ejemplo de importación
  - Opciones de BCP comunes
  - Prácticas recomendadas y consideraciones
  - Solución de problemas comunes de

Limitaciones y recomendaciones

El uso de la copia de seguridad y la restauración nativas tiene limitaciones como las siguientes:

- No se puede realizar una copia de seguridad desde un bucket de Amazon S3 situado en una región de AWS que no coincida con la de la instancia de base de datos de Amazon RDS.
- No puede restaurar una base de datos si ya existe una base de datos SSAS con el mismo nombre. Los nombres de base de datos son únicos.
- Recomendamos encarecidamente que no restaure copias de seguridad de una zona horaria en una zona horaria diferente. Si restaura copias de seguridad de una zona horaria a otra zona horaria distinta, debe auditar las consultas y aplicaciones para comprobar los efectos del cambio de zona horaria.
- Amazon S3 tiene un límite de 5 TB por archivo. Para las copias de seguridad nativas de bases de datos más grandes, puede utilizar la copia de seguridad de varios archivos.
- El tamaño máximo de la base de datos del que se puede realizar una copia de seguridad en S3 depende de la memoria, la CPU, la E/S y los recursos de red disponibles en la instancia de base de datos. Cuanto mayor sea la base de datos, más memoria consume el agente de copia de seguridad.
- No puede realizar copias de seguridad ni restaurar de más de 10 archivos de copia de seguridad al mismo tiempo.
- Una copia de seguridad diferencial se basa en la copia de seguridad completa. Para que funcionen los backups diferenciales, no puede crear una instantánea entre el último backup completo y la copia de seguridad diferencial. Si desea una copia de seguridad diferencial, pero existe una instantánea manual o automatizada, haga otra copia de seguridad completa antes de continuar con la copia de seguridad diferencial.
- Las restauraciones de registros y diferenciales no son compatibles con bases de datos con archivos que tienen su file_guid (identificador único) establecido en `NULL`.
- Puede ejecutar hasta dos tareas de copia de seguridad o restauración al mismo tiempo.

- No puede realizar copias de seguridad del registro nativas desde SQL Server en Amazon RDS.
- RDS admite restauraciones nativas de bases de datos de hasta 64 TiB. Las restauraciones nativas de bases de datos en SQL Server Express Edition están limitadas a 10 GB.
- No se puede realizar una copia de seguridad nativa durante el periodo de mantenimiento ni mientras Amazon RDS esté creando una instantánea de la base de datos. Si una tarea de copia de seguridad nativa se superpone a la ventana de copia de seguridad diaria de RDS, la tarea de copia de seguridad nativa se cancela.
- En las instancias de base de datos Multi-AZ, solo puede restaurar de forma nativa las bases de datos a las que se haya realizado una copia de seguridad en el modelo de recuperación completa.
- No se admite la restauración desde copias de seguridad diferenciales en instancias Multi-AZ.
- La llamada a los procedimientos RDS para la copia de seguridad y la restauración nativas no es compatible.
- Utilice una AWS KMS key de cifrado simétrica para cifrar las copias de seguridad. Amazon RDS no admite las claves de KMS asimétricas. Para obtener más información, consulte Creación de claves KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service.
- Los archivos de copia de seguridad nativos están cifrados con la clave de KMS especificada con el modo criptográfico "Solo cifrado". Al restaurar archivos de copia de seguridad cifrados, tenga en cuenta que estaban cifrados con el modo criptográfico "Solo cifrado".
- No se puede restaurar una base de datos que contenga un grupo de archivos FILESTREAM.
- Actualmente, no se admite el cifrado del servidor de Amazon S3 con AWS KMS (SSE-KMS). Al proporcionar una clave de KMS a un procedimiento almacenado, todas las copias de seguridad y restauraciones nativas se cifran y descifran en el cliente con la clave de KMS. AWS almacena las copias de seguridad en el bucket S3 con SSE-S3.

Si la base de datos puede estar sin conexión mientras se crea, se copia y se restaura el archivo de copia de seguridad, recomendamos utilizar la copia de seguridad y la restauración nativas para migrarla a RDS. Si la base de datos en las instalaciones no puede estar sin conexión, recomendamos utilizar AWS Database Migration Service para migrar la base de datos a Amazon RDS. Para obtener más información, consulte ¿Qué es AWS Database Migration Service?

La copia de seguridad y la restauración nativas no se han diseñado para reemplazar las capacidades de recuperación de datos de la característica de copia de instantáneas entre regiones. Recomendamos utilizar la función de copia de instantáneas para copiar la instantánea de base de datos en otra región de AWS para la recuperación de desastres entre regiones en Amazon RDS.

Para obtener más información, consulte Copia de una instantánea de base de datos para Amazon RDS.

Configuración de la copia de seguridad y la restauración nativas

Para configurar la copia de seguridad y la restauración nativas, son necesarios tres componentes:

1. Un bucket de Amazon S3 para almacenar los archivos de copia de seguridad.

   Debe tener un bucket S3 para utilizar con sus archivos de copia de seguridad y después cargar las copias de seguridad que quiera migrar a RDS. Si ya tiene un bucket de Amazon S3, puede utilizarlo. Si no dispone de un bucket, puede crear un bucket. También puede hacer que se cree automáticamente un bucket cuando añada la opción `SQLSERVER_BACKUP_RESTORE` mediante la AWS Management Console.

   Para obtener más información sobre el uso de S3, consulte la Guía del usuario de Amazon Simple Storage Service.
2. Un rol de AWS Identity and Access Management (IAM) para acceder al bucket.

   Si ya tiene un rol de IAM, puede utilizarlo. También puede elegir que un nuevo rol de IAM se cree en su nombre cuando se agregue la opción `SQLSERVER_BACKUP_RESTORE` mediante la AWS Management Console. Si lo desea, puede crear uno nuevo manualmente.

   Si desea crear un nuevo rol de IAM manualmente, siga las indicaciones de la siguiente sección. Haga lo mismo si desea asociar relaciones de confianza y directivas de permisos a un rol de IAM existente.
3. La opción `SQLSERVER_BACKUP_RESTORE` añadida a un grupo de opciones en la instancia de base de datos.

   Para activar la copia de seguridad y la restauración nativas en la instancia de base de datos, añada la opción `SQLSERVER_BACKUP_RESTORE` a un grupo de opciones en la instancia de base de datos. Para obtener más información e instrucciones, consulte Compatibilidad con copia de seguridad y restauración nativas en SQL Server.

Creación manual de un rol de IAM para la copia de seguridad y la restauración nativas

Si desea crear manualmente un nuevo rol de IAM para utilizarlo con la copia de seguridad y la restauración nativas, puede hacerlo. En este caso, se crea un rol para delegar los permisos desde el servicio de Amazon RDS a su bucket de Amazon S3. Cuando cree un rol de IAM, asocie una

relación de confianza y una política de permisos. La relación de confianza permite que RDS adopte este rol. La política de permisos define las acciones que puede realizar este rol. Para obtener más información acerca de cómo crear un rol, consulte Crear un rol para delegar permisos a un servicio AWS.

En el caso de la copia de seguridad y la restauración nativas, utilice relacione de confianza y políticas de permisos similares a las de los ejemplos de esta sección. En el ejemplo siguiente, vamos a usar el nombre de la entidad principal de servicio, `rds.amazonaws.com`, como alias de todas las cuentas del servicio. En los otros ejemplos, especificamos un Nombre de recurso de Amazon (ARN) para identificar otra cuenta, usuario o función con acceso a la política de confianza.

Le recomendamos que utilice las claves de contexto de condición globales de `aws:SourceArn` y `aws:SourceAccount` en las relaciones de confianza basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

Puede utilizar claves de contexto de condición globales y hacer que el valor de `aws:SourceArn` contenga el ID de cuenta. En estos casos, el valor de `aws:SourceAccount` y la cuenta del valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilizan en la misma instrucción.

- Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
- Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En la relación de confianza, asegúrese de utilizar la clave de contexto de condición global `aws:SourceArn` con el ARN completo de los recursos que acceden al rol. Para la restauración y la copia de seguridad nativa, asegúrese de incluir tanto el grupo de opciones de base de datos como las instancias de base de datos, como se muestra en el siguiente ejemplo.

Example Ejemplo de relación de confianza con la clave de contexto de condición global para la restauración y la copia de seguridad nativa

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:rds:Region:0123456789:db:db_instance_identifier",
                        "arn:aws:rds:Region:0123456789:og:option_group_name",
                  "arn:aws:s3:::amzn-s3-demo-bucket"
                    ],
                    "aws:SourceAccount": "0123456789"
                }
            }
        }
    ]
}
```

En el siguiente ejemplo se utiliza un ARN para especificar un recurso. Para obtener más información sobre cómo usar ARN, consulte Nombres de recursos de Amazon (ARN).

Example Ejemplo de política de permisos para la restauración y copia de seguridad nativa sin cifrado

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
        "Effect": "Allow",
```

```
        "Action":
            [
                "s3:GetObjectAttributes",
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Example política de permisos para la restauración y copia de seguridad nativa con cifrado

Si desea cifrar los archivos de copia de seguridad, incluya una clave de cifrado en la política de permisos. Para obtener más información acerca de las claves de cifrado, consulte la introducción en la guía para desarrolladores de AWS Key Management Service.

> **Note**
>
> Debe utilizar una clave de cifrado de KMS simétrica para cifrar las copias de seguridad. Amazon RDS no admite las claves de KMS asimétricas. Para obtener más información, consulte Creación de claves KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service.
> El rol de IAM también debe ser un usuario de claves y un administrador de claves de la clave de KMS; es decir, debe estar especificado en la política de claves. Para obtener más información, consulte Creación de claves KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service.

JSON

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
        "Effect": "Allow",
```

```
        "Action":
            [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Encrypt",
                "kms:Decrypt"
            ],
        "Resource": "arn:aws:kms:region:account-id:key/key-id"
        },
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:GetObjectAttributes",
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Uso de la copia de seguridad y la restauración nativas

Una vez que haya activado y configurado la copia de seguridad y la restauración nativas, puede empezar a utilizarlos. En primer lugar, conéctese a la base de datos de Microsoft SQL Server y, a continuación, llame a un procedimiento almacenado de Amazon RDS para que haga el trabajo. Para obtener instrucciones acerca de cómo conectarse a la base de datos, consulte Conexión a la instancia de base de datos de Microsoft SQL Server.

Algunos procedimientos almacenados necesitan que asigne un nombre de recurso de Amazon (ARN) al bucket de Amazon S3 y al archivo. El formato del ARN es `arn:aws:s3:::bucket_name/file_name.extension`. Amazon S3 no requiere un número de cuenta ni una región de AWS en los ARN.

Si también proporciona una clave de KMS opcional, el formato para el ARN de la clave es `arn:aws:kms:region:account-id:key/key-id`. Para obtener más información, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios AWS. Debe utilizar una clave de cifrado de KMS simétrica para cifrar las copias de seguridad. Amazon RDS no admite las claves de KMS asimétricas. Para obtener más información, consulte Creación de claves KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service.

> **Note**
>
> Independientemente de que utilice o no una clave de KMS, de forma predeterminada, las tareas nativas de copia de seguridad y restauración habilitan el cifrado de 256 bits del estándar de cifrado avanzado (AES) del servidor en los archivos cargados en S3.

Para obtener instrucciones acerca de cómo llamar a cada procedimiento almacenado, consulte los siguientes temas:

- Realización de copia de seguridad de una base de datos
- Restauración de una base de datos
- Restauración de un registro
- Finalización de la restauración de una base de datos
- Uso de bases de datos parcialmente restauradas
- Cancelación de una tarea
- Seguimiento del estado de las tareas

Realización de copia de seguridad de una base de datos

Para realizar una copia de seguridad de una base de datos, use el procedimiento almacenado `rds_backup_database`.

> **Note**
>
> No se puede realizar una copia de seguridad de una base de datos durante el periodo de mantenimiento ni mientras Amazon RDS esté tomando una instantánea.

Uso

```
exec msdb.dbo.rds_backup_database
 @source_db_name='database_name',
 @s3_arn_to_backup_to='arn:aws:s3:::bucket_name/file_name.extension',
 [@kms_master_key_arn='arn:aws:kms:region:account-id:key/key-id'],
 [@overwrite_s3_backup_file=0|1],
 [@block_size=512|1024|2048|4096|8192|16384|32768|65536],
        [@max_transfer_size=n],
        [@buffer_count=n],
 [@type='DIFFERENTIAL|FULL'],
 [@number_of_files=n];
```

Se requieren los siguientes parámetros:

- `@source_db_name`: nombre de la base de datos de la que se va a realizar la copia de seguridad.
- `@s3_arn_to_backup_to`: el ARN que indica el bucket de Amazon S3 que se usará para la copia de seguridad, además del nombre del archivo de copia de seguridad.

  El archivo puede tener cualquier extensión, pero se suele utilizar `.bak`.

Los siguientes parámetros son opcionales:

- `@kms_master_key_arn`: ARN de la clave de cifrado de KMS simétrica que se va a utilizar para cifrar el elemento.
  - No puede usar la clave de cifrado predeterminada. Si utiliza la clave predeterminada, no se realizará una copia de seguridad de la base de datos.

  - Si no especifica un identificador de clave KMS, el archivo de copia de seguridad no se cifrará. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
  - Cuando se especifica una clave de KMS, se utiliza el cifrado del lado del cliente.
  - Amazon RDS no admite las claves de KMS asimétricas. Para obtener más información, consulte Creación de claves KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service.
- `@overwrite_s3_backup_file`: un valor que indica si se va a sobrescribir un archivo de copia de seguridad existente.
  - `0`: no se sobrescribe el archivo existente. Este valor es el valor predeterminado.

    Al establecer `@overwrite_s3_backup_file` en 0, se devuelve un error si ya existe el archivo.
  - `1`: se sobrescribe un archivo existente que tenga el nombre especificado, aunque no sea un archivo de copia de seguridad.
- `@type`: el tipo de copia de seguridad.
  - `DIFFERENTIAL`: se crea una copia de seguridad diferencial.
  - `FULL`: se crea una copia de seguridad completa. Este valor es el valor predeterminado.

  Una copia de seguridad diferencial se basa en la copia de seguridad completa. Para que funcionen los backups diferenciales, no puede crear una instantánea entre el último backup completo y la copia de seguridad diferencial. Si desea una copia de seguridad diferencial, pero existe una instantánea, haga otra copia de seguridad completa antes de continuar con la copia de seguridad diferencial.

  Puede buscar la última copia de seguridad completa o instantánea con la siguiente consulta de SQL de ejemplo:

```
select top 1
database_name
,  backup_start_date
,  backup_finish_date
from    msdb.dbo.backupset
where   database_name='mydatabase'
and     type = 'D'
order by backup_start_date desc;
```

- `@number_of_files`: el número de archivos en los que se dividirá la copia de seguridad (fragmentada). El número máximo es 10.

- La copia de seguridad de varios archivos es compatible tanto para copias de seguridad completas como diferenciales.
- Si introduce un valor de 1 u omite el parámetro, se creará un único archivo de copia de seguridad.

Proporcione el prefijo que comparten los archivos y, a continuación, agregue un asterisco () como suf (*). El asterisco puede estar en cualquier parte de *nombre_archivo* del ARN de S3. El asterisco se sustituye por una serie de cadenas alfanuméricas en los archivos generados, empezando por `1-of-`*`number_of_files`*.

Por ejemplo, si los nombres de archivo en el ARN de S3 son `backup*.bak` y establece `@number_of_files=4`, los archivos de copia de seguridad generados son `backup1-of-4.bak`, `backup2-of-4.bak`, `backup3-of-4.bak` y `backup4-of-4.bak`.

- Si ya existe alguno de los nombres de archivo y `@overwrite_s3_backup_file` es 0, se devuelve un error.
- Las copias de seguridad de varios archivos solo pueden tener un asterisco en la parte *nombre_archivo* del ARN de S3.
- Las copias de seguridad de un solo archivo pueden tener cualquier número de asteriscos en la parte *nombre_archivo* del ARN de S3. Los asteriscos no se eliminan del nombre de archivo generado.

- `@block_size`: tamaño del bloque (en bytes) que especifica el tamaño del bloque físico para las operaciones de copia de seguridad. Los valores válidos son 512, 1024, 2048, 4096, 8192, 16 384, 32 768 y 65 536.
- `@max_transfer_size`: el tamaño máximo de transferencia indica el límite superior del volumen de datos (en bytes) transmitidos por operación de E/S durante el proceso de copia de seguridad. Los valores válidos son múltiplos de 65 536 bytes (64 KB) hasta 4 194 304 bytes (4 MB).
- `@buffer_count`: número total de búferes de E/S que se utilizarán para el proceso de copia de seguridad.

Ejemplos

Example de copia de seguridad diferencial

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup1.bak',
```

```
@overwrite_s3_backup_file=1,
@type='DIFFERENTIAL';
```

Example de copia de seguridad completa con cifrado

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup1.bak',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE',
@overwrite_s3_backup_file=1,
@type='FULL';
```

Example de copia de seguridad de varios archivos

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@number_of_files=4;
```

Example de copia de seguridad diferencial de varios múltiples

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@type='DIFFERENTIAL',
@number_of_files=4;
```

Example de copia de seguridad de varios archivos con cifrado

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE',
@number_of_files=4;
```

Example de copia de seguridad de varios archivos con sobrescritura de S3

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@overwrite_s3_backup_file=1,
```

```
@number_of_files=4;
```

Example de respaldo con tamaño de bloque

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@block_size=512;
```

Example de copia de seguridad de varios archivos con **`@max_transfer_size`** y **`@buffer_count`**

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@number_of_files=4,
@max_transfer_size=4194304,
@buffer_count=10;
```

Example de copia de seguridad de un solo archivo con el parámetro @number_of_files

En este ejemplo se genera un archivo de copia de seguridad denominado `backup*.bak`.

```
exec msdb.dbo.rds_backup_database
@source_db_name='mydatabase',
@s3_arn_to_backup_to='arn:aws:s3:::mybucket/backup*.bak',
@number_of_files=1;
```

Restauración de una base de datos

Para restaurar la base de datos, llame al procedimiento almacenado `rds_restore_database`. Amazon RDS crea una instantánea inicial de la base de datos una vez que finalice la tarea de restauración y se abra la base de datos.

Uso

```
exec msdb.dbo.rds_restore_database
 @restore_db_name='database_name',
 @s3_arn_to_restore_from='arn:aws:s3:::bucket_name/file_name.extension',
 @with_norecovery=0|1,
 [@kms_master_key_arn='arn:aws:kms:region:account-id:key/key-id'],
        [@block_size=512|1024|2048|4096|8192|16384|32768|65536],
```

```
        [@max_transfer_size=n],
        [@buffer_count=n],
[@type='DIFFERENTIAL|FULL'];
```

Se requieren los siguientes parámetros:

- `@restore_db_name`: nombre de la base de datos que se va a restaurar. Los nombres de base de datos son únicos. No puede restaurar una base de datos si ya existe una base de datos SSAS con el mismo nombre.
- `@s3_arn_to_restore_from` – el ARN que indica el prefijo de Amazon S3 y los nombres de los archivos de copia de seguridad utilizados para restaurar la base de datos.
  - Para una copia de seguridad de un solo archivo, proporcione todo el nombre del archivo.
  - Para una copia de seguridad de varios archivos, proporcione el prefijo que comparten los archivos y, a continuación, agregue un asterisco () como suf (*).
  - Si `@s3_arn_to_restore_from` está vacío, se devolverá el siguiente mensaje de error: S3 ARN prefix cannot be empty.

El siguiente parámetro es obligatorio para las restauraciones diferenciales, pero opcional para las restauraciones completas:

- `@with_norecovery`: la cláusula de recuperación que se utilizará para la operación de restauración.
  - Establezca esta opción en `0` para la restauración con RECOVERY. En este caso, la base de datos está online tras la restauración.
  - Establezca esta opción en 1 para la restauración con NORECOVERY. En este caso, la base de datos permanece en estado RESTORING una vez finalizada la tarea de restauración. Con este método, puede realizar restauraciones diferenciales posteriores.
  - En las restauraciones DIFFERENTIAL, especifique `0` o 1.
  - En las restauraciones `FULL`, este valor se establece de forma predeterminada en `0`.

Los siguientes parámetros son opcionales:

- `@kms_master_key_arn`: si cifró el archivo de copia de seguridad, se trata de la clave de KMS que se va a utilizar para descifrar el archivo.

  Cuando se especifica una clave de KMS, se utiliza el cifrado del lado del cliente.

- `@type`: el tipo de restauración. Los tipos válidos son `DIFFERENTIAL` y `FULL`. El valor predeterminado es `FULL`.
- `@block_size`: tamaño del bloque (en bytes) que especifica el tamaño del bloque físico para las operaciones de copia de seguridad. Los valores válidos son 512, 1024, 2048, 4096, 8192, 16 384, 32 768 y 65 536.
- `@max_transfer_size`: el tamaño máximo de transferencia indica el límite superior del volumen de datos (en bytes) transmitidos por operación de E/S durante el proceso de copia de seguridad. Los valores válidos son múltiplos de 65 536 bytes (64 KB) hasta 4 194 304 bytes (4 MB).
- `@buffer_count`: número total de búferes de E/S que se utilizarán para el proceso de copia de seguridad.

> **Note**
>
> En las restauraciones diferenciales, la base de datos debe tener el estado RESTORING o debe existir previamente una tarea que restaure con NORECOVERY.
> No puede restaurar copias de seguridad diferenciales posteriores mientras la base de datos esté online.
> No puede enviar una tarea de restauración para una base de datos que ya tenga una tarea de restauración pendiente con RECOVERY.
> No se admiten las restauraciones completas con NORECOVERY ni las restauraciones diferenciales en instancias Multi-AZ.
> La restauración de una base de datos en una instancia Multi-AZ con réplicas de lectura es similar a la restauración de una base de datos en una instancia Multi-AZ. No es necesario realizar ninguna acción adicional para restaurar una base de datos en una réplica.

Ejemplos

Example de restauración de un solo archivo

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak';
```

Example de restauración de múltiples archivos

Para evitar errores al restaurar varios archivos, asegúrese de que todos los archivos de copia de seguridad tienen el mismo prefijo y que ningún otro archivo lo utiliza.

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup*';
```

Example de restauración completa de una base de datos con RECOVERY

En los tres ejemplos siguientes, se realiza la misma tarea, una restauración completa con RECOVERY.

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak';
```

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
[@type='DIFFERENTIAL|FULL'];
```

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='FULL',
@with_norecovery=0;
```

Example de restauración completa de una base de datos con cifrado

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE';
```

Example de restauración con tamaño de bloque

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
```

```
@block_size=512;
```

Example de restaurar varios archivos con @max_transfer_size y @buffer_count

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup*',
@max_transfer_size=4194304,
@buffer_count=10;
```

Example de restauración completa de una base de datos con NORECOVERY

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='FULL',
@with_norecovery=1;
```

Example de restauración diferencial con NORECOVERY

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='DIFFERENTIAL',
@with_norecovery=1;
```

Example de restauración diferencial con RECOVERY

```
exec msdb.dbo.rds_restore_database
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/backup1.bak',
@type='DIFFERENTIAL',
@with_norecovery=0;
```

Restauración de un registro

Para restaurar el registro, llame al procedimiento almacenado `rds_restore_log`.

Uso

```
exec msdb.dbo.rds_restore_log
```

```
@restore_db_name='database_name',
@s3_arn_to_restore_from='arn:aws:s3:::bucket_name/log_file_name.extension',
[@kms_master_key_arn='arn:aws:kms:region:account-id:key/key-id'],
[@with_norecovery=0|1],
[@stopat='datetime'],
[@block_size=512|1024|2048|4096|8192|16384|32768|65536],
       [@max_transfer_size=n],
       [@buffer_count=n];
```

Se requieren los siguientes parámetros:

- `@restore_db_name`: nombre de la base de datos cuyo registro se va a restaurar.
- `@s3_arn_to_restore_from`: el ARN que indica el prefijo de Amazon S3 y el nombre del archivo de registro utilizado para restaurarlo. El archivo puede tener cualquier extensión, pero se suele utilizar `.trn`.

  Si `@s3_arn_to_restore_from` está vacío, se devolverá el siguiente mensaje de error: S3 ARN prefix cannot be empty.

Los siguientes parámetros son opcionales:

- `@kms_master_key_arn`: si cifró el registro, se trata de la clave de KMS que se va a utilizar para descifrar el registro.
- `@with_norecovery`: la cláusula de recuperación que se utilizará para la operación de restauración. Este valor se establece de forma predeterminada en 1.
  - Establezca esta opción en `0` para la restauración con RECOVERY. En este caso, la base de datos está online tras la restauración. No puede restaurar más copias de seguridad de registros mientras la base de datos esté online.
  - Establezca esta opción en 1 para la restauración con NORECOVERY. En este caso, la base de datos permanece en estado RESTORING una vez finalizada la tarea de restauración. Con este método, puede realizar restauraciones de registros posteriores.
- `@stopat`: un valor que especifica que la base de datos se restaura al estado que presentaba en la fecha y la hora especificadas (en formato fechahora). Solo se aplican a la base de datos los registros de transacciones escritos antes de la fecha y la hora especificadas.

  Si no se especifica este parámetro (es NULL), se restaura el registro completo.

- `@block_size`: tamaño del bloque (en bytes) que especifica el tamaño del bloque físico para las operaciones de copia de seguridad. Los valores válidos son 512, 1024, 2048, 4096, 8192, 16 384, 32 768 y 65 536.
- `@max_transfer_size`: el tamaño máximo de transferencia indica el límite superior del volumen de datos (en bytes) transmitidos por operación de E/S durante el proceso de copia de seguridad. Los valores válidos son múltiplos de 65 536 bytes (64 KB) hasta 4 194 304 bytes (4 MB).
- `@buffer_count`: número total de búferes de E/S que se utilizarán para el proceso de copia de seguridad.

> **Note**
>
> En las restauraciones de registros, la base de datos debe tener un estado de restauración o debe existir previamente una tarea que restaure con NORECOVERY.
> No puede restaurar copias de seguridad de registros mientras la base de datos esté online.
> No puede enviar una tarea de restauración de registros en una base de datos que ya tenga una tarea de restauración pendiente con RECOVERY.
> No se admiten las restauraciones de registros en instancias Multi-AZ.

Ejemplos

Example de restauración de registros

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn';
```

Example de restauración de registros con cifrado

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@kms_master_key_arn='arn:aws:kms:us-east-1:123456789012:key/AKIAIOSFODNN7EXAMPLE';
```

Example de restauración de registros con NORECOVERY

En los dos ejemplos siguientes, se realiza la misma tarea, una restauración de registros con NORECOVERY.

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@with_norecovery=1;
```

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn';
```

Example de restauración con tamaño de bloque

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@block_size=512;
```

Example de restauración de registros con RECOVERY

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@with_norecovery=0;
```

Example de restauración de registros con la cláusula STOPAT

```
exec msdb.dbo.rds_restore_log
@restore_db_name='mydatabase',
@s3_arn_to_restore_from='arn:aws:s3:::mybucket/mylog.trn',
@with_norecovery=0,
@stopat='2019-12-01 03:57:09';
```

Finalización de la restauración de una base de datos

Si la última tarea de restauración de la base de datos se ha realizado con `@with_norecovery=1`, la base de datos tiene ahora el estado RESTORING. Abra esta base de datos para el uso normal mediante el procedimiento almacenado `rds_finish_restore`.

Uso

```
exec msdb.dbo.rds_finish_restore @db_name='database_name';
```

> **Note**
>
> Para utilizar este método, la base de datos debe tener el estado RESTORING sin ninguna tarea de restauración pendiente.
> No se admite el procedimiento `rds_finish_restore` en instancias Multi-AZ.
> Para finalizar la restauración de la base de datos, utilice el inicio de sesión maestro. O utilice el inicio de sesión del usuario que restauró la base de datos más recientemente o inicie sesióncon NORECOVERY.

Uso de bases de datos parcialmente restauradas

Eliminación de una base de datos parcialmente restaurada

Para eliminar una base de datos parcialmente restaurada (que se ha quedado en el estado RESTORING), utilice el procedimiento almacenado `rds_drop_database`.

```
exec msdb.dbo.rds_drop_database @db_name='database_name';
```

> **Note**
>
> No puede enviar una solicitud DROP para una base de datos que ya tenga una tarea de restauración pendiente o una tarea de restauración finalizada.
> Para eliminar la base de datos, utilice el inicio de sesión maestro. O utilice el inicio de sesión del usuario que restauró la base de datos más recientemente o inicie sesióncon NORECOVERY.

Comportamiento de la restauración de instantáneas y la recuperación en un momento dado en bases de datos parcialmente restauradas

Las bases de datos parcialmente restauradas de la instancia de origen (que se ha quedado en el estado RESTORING) se eliminan de la instancia de destino durante la recuperación en un momento dado y la restauración de una instantánea.

Cancelación de una tarea

Para cancelar una tarea de copia de seguridad o de restauración, llame al procedimiento almacenado `rds_cancel_task`.

> **Note**
>
> No se puede cancelar una tarea FINISH_RESTORE.

Uso

```
exec msdb.dbo.rds_cancel_task @task_id=ID_number;
```

El siguiente parámetro es obligatorio:

- `@task_id`: ID de la tarea que se va a cancelar. Puede obtener el ID de la tarea llamando a `rds_task_status`.

Seguimiento del estado de las tareas

Para realizar un seguimiento del estado de las tareas de copia de seguridad o de restauración, llame al procedimiento almacenado `rds_task_status`. Si no proporciona ningún parámetro, el procedimiento almacenado devuelve el estado de todas las tareas. El estado de las tareas se actualiza cada dos minutos aproximadamente. El historial de tareas se conserva durante 36 días.

Uso

```
exec msdb.dbo.rds_task_status
 [@db_name='database_name'],
 [@task_id=ID_number];
```

Los siguientes parámetros son opcionales:

- `@db_name`: nombre de la base de datos para la que se desea mostrar el estado de una tarea.
- `@task_id`: ID de la tarea cuyo estado se desea mostrar.

Ejemplos

Example de descripción del estado de una tarea específica

```
exec msdb.dbo.rds_task_status @task_id=5;
```

Example de descripción del estado de una tarea y una base de datos específicas

```
exec msdb.dbo.rds_task_status
@db_name='my_database',
@task_id=5;
```

Example de descripción de todas las tareas y sus estados en una base de datos específica

```
exec msdb.dbo.rds_task_status @db_name='my_database';
```

Example de descripción de todas las tareas y sus estados en la instancia actual

```
exec msdb.dbo.rds_task_status;
```

Respuesta

El procedimiento almacenado `rds_task_status` devuelve las siguientes columnas.

Columna	Descripción
`task_id`	El ID de la tarea.

`task_type`	El tipo de tarea que depende de los parámetros de entrada, como se indica a continuación:
	• Para tareas de copia de seguridad:
	  • BACKUP_DB: copia de seguridad completa de una base de datos
	  • BACKUP_DB_DIFFERENTIAL: copia de seguridad diferencial de una base de datos
	• Para tareas de restauración:
	  • RESTORE_DB: restauración completa de una base de datos con RECOVERY
	  •

Columna	Descripción
	RESTORE_DB_NORECOVERY: restauración completa de una base de datos con NORECOVERY • RESTORE_DB_DIFFERENTIAL: restauración diferencial de una base de datos con RECOVERY • RESTORE_DB_DIFFERENTIAL_NORECOVERY: restauración diferencial de una base de datos con NORECOVERY • RESTORE_DB_LOG: restauración de registros con RECOVERY • RESTORE_DB_LOG_NORECOVERY: restauración de registros con NORECOVERY • Para tareas que finalizan una restauración: • FINISH_RESTORE: se finaliza una restauración y se abre una base de datos Amazon RDS crea una instantánea inicial de la base de datos después de que esta se abra tras la finalización de las siguientes tareas de restauración: • RESTORE_DB • RESTORE_DB_DIFFERENTIAL • RESTORE_DB_LOG • FINISH_RESTORE
`database_name`	El nombre de la base de datos a la que está asociada la tarea.
`% complete`	El valor porcentual de progreso de la tarea.

Columna	Descripción
`duration (mins)`	El tiempo empleado en la tarea, en minutos.
`lifecycle`	El estado de la tarea. Los posibles estados son los siguientes: • `CREATED`: en el momento en que se llama a `rds_backup_database` o a `rds_restore_database`, se crea una tarea y se establece su estado en `CREATED`. • `IN_PROGRESS` – después de que comienza una tarea de copia de seguridad o de restauración, se establece su estado en `IN_PROGRESS`. El estado puede tardar hasta cinco minutos en cambiar de `CREATED` a `IN_PROGRESS`. • `SUCCESS` – después de que finaliza una tarea de copia de seguridad o de restauración, se establece su estado en `SUCCESS`. • `ERROR` – si se produce un error en una tarea de copia de seguridad o de restauración, se establece su estado en `ERROR`. Para obtener más información acerca del error, consulte la columna `task_info`. • `CANCEL_REQUESTED`: en el momento en que se llama a `rds_cancel_task`, se establece el estado de la tarea en `CANCEL_REQUESTED`. • `CANCELLED` – después de que se cancela una tarea correctamente, se establece su estado en `CANCELLED`.
`task_info`	Información adicional acerca de la tarea. Si ocurre un error al realizar una copia de seguridad o al restaurar una base de datos, esta columna contiene información acerca del error. Para obtener una lista de posibles errores y estrategias de mitigación, consulte Solución de problemas.
`last_updated`	La fecha y hora en que se actualizó por última vez el estado de la tarea. El estado se actualiza cada vez que la tarea progresa un 5 %.

Columna	Descripción
`created_at`	La fecha y hora en que se creó la tarea.
`S3_object_arn`	El ARN que indica el prefijo de Amazon S3 y el nombre del archivo que se está restaurando o del que se está realizando una copia de seguridad.
`overwrite_s3_backup_file`	El valor del parámetro `@overwrite_s3_backup_file` especificado al llamar a una tarea de backup. Para obtener más información, consulte Realización de copia de seguridad de una base de datos.
`KMS_master_key_arn`	El ARN de la clave de KMS que se utilizó para el cifrado (para la copia de seguridad) y el descifrado (para la restauración).
`filepath`	No se aplica a las tareas de copia de seguridad y restauración nativas.
`overwrite_file`	No se aplica a las tareas de copia de seguridad y restauración nativas.

Compresión de archivos de copia de seguridad

Para ahorrar espacio en el bucket de Amazon S3 puede comprimir los archivos de backup. Para obtener más información acerca de cómo comprimir archivos de backup, consulte Compresión de copia de seguridad en la documentación de Microsoft.

La compresión de archivos de backup se admite para las siguientes ediciones de base de datos:

- Microsoft SQL Server Enterprise Edition
- Microsoft SQL Server Standard Edition

Para activar la compresión de los archivos de backup, ejecute el código siguiente:

```
exec rdsadmin.dbo.rds_set_configuration 'S3 backup compression', 'true';
```

Para desactivar la compresión de los archivos de backup, ejecute el código siguiente:

```
exec rdsadmin.dbo.rds_set_configuration 'S3 backup compression', 'false';
```

Solución de problemas

A continuación se muestran los problemas que pueden presentarse al utilizar la copia de seguridad y la restauración nativas.

Problema	Sugerencias para la solución de problemas
La opción de copia de seguridad y restauración de base de datos aún no está habilitada o está en proceso de habilitarse. Inténtelo de nuevo más tarde.	Asegúrese de haber agregado la opción `SQLSERVER_BACKUP_RESTORE` al grupo de opciones de base de datos asociado a la instancia de base de datos. Para obtener más información, consulte Adición de opciones de copia de seguridad y restauración nativas.
Se ha denegado el permiso EXECUTE en el objeto “*rds_backup_database*”, base de datos “msdb”, esquema “dbo”.	Asegúrese de que está utilizando el usuario maestro al ejecutar el procedimiento almacenado. Si encuentra este error incluso después de iniciar sesión como usuario principal, puede deberse a que los permisos de usuario administrador no están alineados correctamente. Para restablecer el usuario maestro, utilice la AWS Management Console. Consulte Restablecimiento de la pertenencia al rol db_owner para el usuario maestro de Amazon RDS para SQL Server.
Se ha denegado el permiso EXECUTE en el objeto “*rds_restore_database*”, base de datos “msdb”, esquema “dbo”.	Asegúrese de que está utilizando el usuario maestro al ejecutar el procedimiento almacenado. Si encuentra este error incluso después de iniciar sesión como usuario principal, puede deberse a que los permisos de usuario administrador no están alineados correctamente. Para restablecer el usuario maestro, utilice la AWS Management Console. Consulte Restablecimiento de la pertenencia al rol db_owner para el usuario maestro de Amazon RDS para SQL Server.
Acceso denegado	El proceso de copia de seguridad o restauración no puede acceder al archivo de copia de seguridad. Normalmente, esto se suele debe a problemas como el siguiente: •

Problema	Sugerencias para la solución de problemas
	Hacer referencia a un bucket incorrecto. Hacer referencia a un bucket utilizando un formato incorrecto. Hacer referencia a un nombre de archivo sin utilizar el ARN. • Permisos incorrectos en el archivo de bucket. Por ejemplo, si se crea mediante una cuenta distinta que está intentando acceder ahora, añada los permisos correctos. • Una política IAM que es incorrecta o incompleta. Su función IAM debe incluir todos los elementos necesarios, incluyendo, por ejemplo, la versión correcta. Estas se destacan en Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.
BACKUP BASE DE DATOS CON COMPRESIÓN no es compatible con la edición<edition_name>	La compresión de los archivos de copia de seguridad solo se admite para las ediciones Enterprise y Standard de Microsoft SQL Server. Para obtener más información, consulte Compresión de archivos de copia de seguridad.
La clave no existe<ARN>	Ha intentado restaurar una copia de seguridad cifrada, pero no ha proporcionado una clave de cifrado válida. Compruebe la clave de cifrado y vuelva a intentarlo. Para obtener más información, consulte Restauración de una base de datos.

Problema	Sugerencias para la solución de problemas
Vuelva a emitir la tarea con el tipo correcto y sobrescribir la propiedad	Si intenta realizar una copia de seguridad de la base de datos e indica un nombre de archivo que ya existe, pero no ha establecido en 1 la propiedad de sobrescribir, la operación falla al guardar el archivo. Para solucionar este error, indique un nombre de archivo que no exista o establezca en 1 la propiedad de sobrescribir. Para obtener más información, consulte Realización de copia de seguridad de una base de datos. También es posible que pretendiese restaurar la base de datos, pero que haya llamado al procedimiento almacenado `rds_backup_database` por error. En ese caso, llame al procedimiento almacenado `rds_restore_database` en su lugar. Para obtener más información, consulte Restauración de una base de datos. Si pretendía restaurar la base de datos y ha llamado al procedimiento almacenado `rds_restore_database`, asegúrese de que ha indicado un nombre de archivo de backup válido. Para obtener más información, consulte Uso de la copia de seguridad y la restauración nativas.
Especifique un depósito que se encuentra en la misma región que la instancia de RDS	No se puede realizar una copia de seguridad desde un bucket de Amazon S3 situado en una región de AWS que no coincida con la de la instancia de base de datos de Amazon RDS. Puede utilizar la reproducción de Amazon S3 para copiar el archivo de copia de seguridad en la región de AWS correcta. Para obtener más información, consulte Replicación entre regiones en la documentación de Amazon S3.

Problema	Sugerencias para la solución de problemas
El bucket especificado no existe	Compruebe que ha proporcionado el ARN correcto para el bucket y el archivo, y que el formato es correcto. Para obtener más información, consulte Uso de la copia de seguridad y la restauración nativas.
El usuario no está autorizado a realizar en el recurso<ARN> <kms action> <ARN>	Ha solicitado una operación cifrada, pero no ha proporcionado los permisos de AWS KMS correctos. Compruebe que tiene los permisos correctos o añádalos. Para obtener más información, consulte Configuración de la copia de seguridad y la restauración nativas.
La tarea Restaurar no puede restaurar desde más de 10 archivos de copia de seguridad). Reduzca el número de archivos coincidentes e inténtelo de nuevo.	Reduzca el número de archivos a partir de los cuales está intentand o llevar a cabo la restauración. Puede agrandar cada archivo individual si es necesario.
La base de datos "*database_name* " ya existe. No se permiten dos bases de datos que difieren solo por caso o acento. Elija un nombre de base de datos diferente.	No puede restaurar una base de datos si ya existe una base de datos SSAS con el mismo nombre. Los nombres de base de datos son únicos.

Importación y exportación de datos de SQL Server por otros métodos

A continuación, puede encontrar información acerca del uso de instantáneas para importar sus datos de Microsoft SQL Server a Amazon RDS. También puede encontrar información sobre el uso de instantáneas para exportar sus datos desde una instancia de base de datos de RDS que ejecuta SQL Server.

Si es posible en su situación concreta, lo más sencillo es importar y exportar los datos de Amazon RDS utilizando las funciones de backup y restauración nativas. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

> **Note**
>
> Amazon RDS para Microsoft SQL Server no admite la importación de datos en la base de datos `msdb`.

Importación de datos a RDS para SQL Server utilizando una instantánea

Para importar datos a una instancia de base de datos SQL Server utilizando una instantánea

1. Cree una instancia de base de datos. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
2. Detenga el acceso de las aplicaciones a la instancia de base de datos de destino.

   Si impide el acceso a la instancia de base de datos durante la importación, la transferencia de datos será más rápida. Además no tiene que preocuparse por que se produzcan conflictos durante la carga de datos si otras aplicaciones no pueden escribir al mismo tiempo en la instancia de base de datos. Si hay algún problema y es necesario volver a una instantánea anterior de la base de datos, los únicos cambios que se perderán serán los datos importados. Puede volver a importar estos datos tras resolver el problema.

   Para obtener más información sobre el control del acceso a la instancia de base de datos, consulte Control de acceso con grupos de seguridad.
3. Cree una instantánea de la base de datos de destino.

   Si la base de datos de destino ya contiene datos, es recomendable obtener una instantánea de ella antes de importar nuevos datos. Si hay algún problema en la importación o desea descartar

los cambios, podrá utilizar la instantánea para devolver a la base de datos su estado anterior. Para obtener más información acerca de la creación de instantáneas de base de datos, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

> **Note**
>
> Al obtener una instantánea de base de datos, las operaciones de E/S de la base de datos se suspenden durante un momento (milisegundos), mientras se efectúa una copia de seguridad.

4. Deshabilite los backups automatizados en la base de datos de destino.

   La deshabilitación de los backups automatizados en la base de datos de destino mejora el rendimiento de la importación de datos, ya que con los backups automáticos deshabilitados Amazon RDS no registra las transacciones. Sin embargo, hay algunos aspectos que se deben considerar. Se precisa que las copias de seguridad automatizadas realicen una recuperación en un momento dado. Por lo tanto, no puede restaurar la base de datos a un momento específico mientras importa los datos. Además, las copias de seguridad automatizadas creadas en la instancia de base de datos se borran a no ser que elija conservarlos.

   Optar por retener las copias de seguridad automatizadas puede ayudarlo a protegerse contra la eliminación accidental de datos. Amazon RDS también guarda las propiedades de instancia de base de datos junto con cada copia de seguridad automatizada para facilitar la recuperación. Esta opción le permite restaurar una instancia de base de datos eliminada a un momento específico dentro del periodo de retención de la copia de seguridad, incluso después de haberla eliminado. Las copias de seguridad automáticas, al igual que las de una instancia de base de datos activa, se eliminan automáticamente al final del período especificado.

   También puede usar instantáneas anteriores para recuperar la base de datos, y las instantáneas que haya obtenido continúan disponibles. Para obtener información acerca de los backups automatizados, consulte Introducción a las copias de seguridad.

5. Deshabilite las restricciones de clave externa, en su caso.

   Si es necesario deshabilitar las restricciones de clave externa, puede hacerlo con el script siguiente.

```
--Disable foreign keys on all tables
```

```
    DECLARE @table_name SYSNAME;
    DECLARE @cmd NVARCHAR(MAX);
    DECLARE table_cursor CURSOR FOR SELECT name FROM sys.tables;

    OPEN table_cursor;
    FETCH NEXT FROM table_cursor INTO @table_name;

    WHILE @@FETCH_STATUS = 0 BEGIN
      SELECT @cmd = 'ALTER TABLE '+QUOTENAME(@table_name)+' NOCHECK CONSTRAINT
 ALL';
      EXEC (@cmd);
      FETCH NEXT FROM table_cursor INTO @table_name;
    END

    CLOSE table_cursor;
    DEALLOCATE table_cursor;

    GO
```

6. Elimine los índices, en su caso.
7. Deshabilite los disparadores, en su caso.

   Si es necesario deshabilitar los disparadores, puede hacerlo con el script siguiente.

```
--Disable triggers on all tables
    DECLARE @enable BIT = 0;
    DECLARE @trigger SYSNAME;
    DECLARE @table SYSNAME;
    DECLARE @cmd NVARCHAR(MAX);
    DECLARE trigger_cursor CURSOR FOR SELECT trigger_object.name trigger_name,
     table_object.name table_name
    FROM sysobjects trigger_object
    JOIN sysobjects table_object ON trigger_object.parent_obj = table_object.id
    WHERE trigger_object.type = 'TR';

    OPEN trigger_cursor;
    FETCH NEXT FROM trigger_cursor INTO @trigger, @table;

    WHILE @@FETCH_STATUS = 0 BEGIN
      IF @enable = 1
         SET @cmd = 'ENABLE ';
      ELSE
         SET @cmd = 'DISABLE ';
```

```
      SET @cmd = @cmd + ' TRIGGER dbo.'+QUOTENAME(@trigger)+' ON
dbo.'+QUOTENAME(@table)+' ';
      EXEC (@cmd);
      FETCH NEXT FROM trigger_cursor INTO @trigger, @table;
   END

   CLOSE trigger_cursor;
   DEALLOCATE trigger_cursor;

   GO
```

8. Consulte la instancia SQL Server de origen para determinar los nombres de inicio de sesión que desea importar a la instancia de base de datos de destino.

   SQL Server almacena los nombres y contraseñas de inicio de sesión en la base de datos `master`. Amazon RDS no permite el acceso a la base de datos `master`, por lo que no es posible importar directamente los nombres y contraseñas de inicio de sesión en la instancia de base de datos de destino. En su lugar, debe consultar la base de datos `master` en la instancia SQL Server de origen para generar un archivo de lenguaje de definición de datos (DDL). Este archivo debería incluir todos los inicios de sesión y las contraseñas que desee añadir a la instancia de base de datos de destino. Este archivo también debería incluir las suscripciones y permisos de rol que desea transferir.

   Para obtener información acerca de cómo consultar la base de datos `master`, consulte Transferir inicios de sesión y contraseñas entre servidores SQL Server en Microsoft Knowledge Base.

   La salida del script es otro script que puede ejecutar en la instancia de base de datos de destino. El script del artículo de Knowledge Base contiene el código siguiente:

   ```
   p.type IN
   ```

   En todos los lugares donde aparezca `p.type`, sustitúyalo por el código siguiente:

   ```
   p.type = 'S'
   ```

9. Importe los datos siguiendo el método indicado en Importación de los datos.
10. Conceda a las aplicaciones acceso a la instancia de base de datos de destino.

Cuando termine la importación de los datos, puede conceder acceso a la instancia de base de datos a las aplicaciones que bloqueó antes de la importación. Para obtener más información sobre el control del acceso a la instancia de base de datos, consulte Control de acceso con grupos de seguridad.

11. Habilite los backups automatizados para la instancia de base de datos de destino.

    Para obtener información acerca de los backups automatizados, consulte Introducción a las copias de seguridad.

12. Habilite las restricciones de clave externa.

    Si antes deshabilitó las restricciones de clave externa, puede habilitarlas ahora con el script siguiente.

```
--Enable foreign keys on all tables
    DECLARE @table_name SYSNAME;
    DECLARE @cmd NVARCHAR(MAX);
    DECLARE table_cursor CURSOR FOR SELECT name FROM sys.tables;

    OPEN table_cursor;
    FETCH NEXT FROM table_cursor INTO @table_name;

    WHILE @@FETCH_STATUS = 0 BEGIN
      SELECT @cmd = 'ALTER TABLE '+QUOTENAME(@table_name)+' CHECK CONSTRAINT ALL';
      EXEC (@cmd);
      FETCH NEXT FROM table_cursor INTO @table_name;
    END

    CLOSE table_cursor;
    DEALLOCATE table_cursor;
```

13. Habilite los índices, en su caso.
14. Habilite los disparadores, en su caso.

    Si antes deshabilitó los disparadores, puede habilitarlos ahora con el script siguiente.

```
--Enable triggers on all tables
    DECLARE @enable BIT = 1;
    DECLARE @trigger SYSNAME;
    DECLARE @table SYSNAME;
    DECLARE @cmd NVARCHAR(MAX);
```

```
    DECLARE trigger_cursor CURSOR FOR SELECT trigger_object.name trigger_name,
     table_object.name table_name
    FROM sysobjects trigger_object
    JOIN sysobjects table_object ON trigger_object.parent_obj = table_object.id
    WHERE trigger_object.type = 'TR';

    OPEN trigger_cursor;
    FETCH NEXT FROM trigger_cursor INTO @trigger, @table;

    WHILE @@FETCH_STATUS = 0 BEGIN
      IF @enable = 1
         SET @cmd = 'ENABLE ';
      ELSE
         SET @cmd = 'DISABLE ';

      SET @cmd = @cmd + ' TRIGGER dbo.'+QUOTENAME(@trigger)+' ON
dbo.'+QUOTENAME(@table)+' ';
      EXEC (@cmd);
      FETCH NEXT FROM trigger_cursor INTO @trigger, @table;
    END

    CLOSE trigger_cursor;
    DEALLOCATE trigger_cursor;
```

Importación de los datos

Microsoft SQL Server Management Studio es un cliente SQL Server gráfico incluido en todas las ediciones de Microsoft SQL Server excepto Express Edition. Microsoft ofrece SQL Server Management Studio Express como descarga gratuita. Encontrará esta descarga en el sitio web de Microsoft.

> **Note**
>
> SQL Server Management Studio solo está disponible como aplicación basada en Windows.

SQL Server Management Studio incluye herramientas que resultan útiles para importar datos a una instancia de base de datos SQL Server:

- Asistente Generar y publicar scripts
- Asistente para importación y exportación

- Copia masiva

Asistente Generar y publicar scripts

El asistente Generar y publicar scripts crea un script que contiene el esquema de una base de datos, los datos en sí, o ambos. Puede generar un script para una base de datos en su implementación SQL Server local. Puede ejecutar el script para que transfiera la información que contiene a una instancia de base de datos de Amazon RDS.

> **Note**
>
> Para las bases de datos de 1 GiB o más, es más eficiente generar scripts solo para el esquema de la base de datos. Puede utilizar el asistente para la Importación y Exportación o la característica de copia masiva de SQL Server para transferir los datos.

Para obtener información detallada acerca del asistente Generar y publicar scripts, consulte la documentación de Microsoft SQL Server.

En el asistente, ponga especial atención en las opciones avanzadas de la página Establecer opciones de scripting para asegurarse de que esté seleccionado todo lo que desea incluir en el script. Por ejemplo, por defecto los disparadores de base de datos no se incluyen en el script.

Una vez generado y guardado el script, puede usar SQL Server Management Studio para conectar con la instancia de base de datos y ejecutarlo.

Asistente para importación y exportación

El Asistente para importación y exportación crea un paquete especial de servicios de integración que puede usar para copiar datos de la base de datos SQL Server local a la instancia de base de datos de destino. El asistente puede filtrar las tablas e incluso las tuplas de una tabla que se copian a la instancia de base de datos de destino.

> **Note**
>
> El Asistente para importación y exportación funciona bien con conjuntos de datos grandes, pero puede no ser el modo más rápido para exportar datos desde una instalación local. Para conseguir una velocidad incluso mayor, considere utilizar la función de copia masiva de SQL Server.

Para obtener información detallada acerca del Asistente para importación y exportación, consulte la documentación de Microsoft SQL Server.

En el asistente, en la página Elegir un destino, haga lo siguiente:

- En Nombre del servidor, escriba el nombre del punto de conexión de la instancia de base de datos.
- Elija Utilizar autenticación de SQL Server como modo de autenticación del servidor.
- En Nombre de usuario y Contraseña, escriba las credenciales del usuario maestro que ha creado para la instancia de base de datos.

Copia masiva

La función de copia masiva de SQL Server es un modo eficiente de copiar datos de una base de datos de origen a una instancia de base de datos. La copia masiva escribe los datos que especifique en un archivo de datos, por ejemplo un archivo ASCII. A continuación puede ejecutar de nuevo la copia masiva para escribir el contenido del archivo en la instancia de base de datos de destino.

En esta sección se utiliza la herramienta bcp, que se incluye en todas las ediciones de SQL Server. Para obtener información detallada acerca las operaciones de importación y exportación masivas, consulte la documentación de Microsoft SQL Server.

> **Note**
>
> Antes de usar la copia masiva, debe importar el esquema de base de datos en la instancia de base de datos de destino. El asistente Generar y publicar scripts, descrito anteriormente en este tema, es una herramienta excelente para hacerlo.

El siguiente comando se conecta a la instancia SQL Server local. Genera un archivo delimitado por tabuladores a partir de una tabla especificada en el directorio C:\root de la instalación de SQL Server existente. La tabla se especifica por su nombre completo y el archivo de texto tiene el mismo nombre que la tabla que se copia.

```
bcp dbname.schema_name.table_name out C:\table_name.txt -n -S localhost -U username -
P password -b 10000
```

En el código anterior se incluyen las opciones siguientes:

- `-n` especifica que la copia masiva utiliza los tipos de datos nativos de los datos que se copian.

- `-S` especifica la instancia SQL Server con la que conecta la utilidad bcp.
- `-U` especifica el nombre de usuario de la cuenta que inicia sesión en la instancia de SQL Server.
- `-P` especifica la contraseña del usuario indicado con `-U`.
- `-b` especifica el número de filas en cada lote de datos importados.

> **Note**
>
> Puede haber otros parámetros importantes para cada caso de importación. Por ejemplo, puede ser necesario el parámetro `-E`, que se refiere a los valores de identidad. Para obtener más información, consulte la descripción completa de la sintaxis de línea de comandos de la utilidad bcp en la documentación de Microsoft SQL Server.

Por ejemplo, supongamos que una base de datos llamada `store` usa el esquema predeterminado dbo y contiene una tabla llamada `customers`. La cuenta de usuario `admin`, con la contraseña `insecure`, copia 10 000 filas de la tabla `customers` en un archivo llamado `customers.txt`.

```
bcp store.dbo.customers out C:\customers.txt -n -S localhost -U admin -P insecure -b
 10000
```

Después de generar el archivo de datos, puede cargar los datos en su instancia de base de datos utilizando un comando similar. Previamente, cree la base de datos y el esquema en la instancia de base de datos de destino. Utilice el argumento `in` para especificar un archivo de entrada en lugar de `out` para especificar un archivo de salida. En lugar de especificar localhost para indicar la instancia SQL Server local, especifique el punto de conexión de la instancia de base de datos. Si usa un puerto distinto del 1433, también debe especificarlo. El nombre de usuario y la contraseña son los del usuario maestro de la instancia de base de datos. La sintaxis es la siguiente:

```
bcp dbname.schema_name.table_name
     in C:\table_name.txt -n -S endpoint,port -U master_user_name -
P master_user_password -b 10000
```

Para continuar con el ejemplo anterior, supongamos que el nombre del usuario maestro es `admin` y que la contraseña es `insecure`. El punto de conexión de la instancia de base de datos es `rds.ckz2kqd4qsn1.us-east-1.rds.amazonaws.com` y se usa el puerto 4080. El comando es el siguiente:

```
bcp store.dbo.customers in C:\customers.txt -n -S rds.ckz2kqd4qsn1.us-
east-1.rds.amazonaws.com,4080 -U admin -P insecure -b 10000
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Exportación de datos de RDS para SQL Server

Se puede elegir una de las siguientes opciones para exportar datos desde una instancia de base de datos de RDS para SQL Server:

- Copia de seguridad de base de datos nativo con un archivo de copia de seguridad completo (.bak): el uso de archivos .bak para la copia de seguridad de bases de datos está muy optimizado y normalmente es la forma más rápida de exportar datos. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.
- Asistente para importación y exportación de SQL Server: para obtener más información, consulte Asistente para importación y exportación de SQL Server.
- Asistente Generar y publicar scripts y utilidad bcp de SQL Server: para obtener más información, consulte Asistente Generar y publicar scripts de SQL Server y utilidad bcp.

Asistente para importación y exportación de SQL Server

Se puede utilizar el asistente para importación y exportación de SQL Server para copiar una o varias tablas, vistas o consultas de una instancia de base de datos RDS para SQL Server a otro almacén de datos. Esta es la mejor opción cuando el almacén de datos de destino no es SQL Server. Para obtener más información, consulte Asistente para importación y exportación de SQL Server en la documentación de SQL Server.

El asistente para importación y exportación de SQL Server está disponible como parte de SQL Server Management Studio. Es un cliente SQL Server gráfico incluido en todas las ediciones de Microsoft SQL Server excepto Express Edition. SQL Server Management Studio solo está disponible como aplicación basada en Windows. Microsoft ofrece SQL Server Management Studio Express como descarga gratuita. Encontrará esta descarga en el sitio web de Microsoft.

Para usar el Asistente para importación y exportación de SQL Server para exportar datos

1. En SQL Server Management Studio, conéctese con la instancia de base de datos RDS para SQL Server. Para obtener más detalles sobre cómo hacerlo, consulte Conexión a la instancia de base de datos de Microsoft SQL Server.
2. En el Explorador de objetos, expanda Bases de datos, abra el menú contextual (clic con el botón derecho) para la base de datos de origen, elija Tareas y, a continuación, elija Exportar datos. Aparecerá el asistente.
3. En la página Elija un origen de datos, haga lo siguiente:
   a. Para Origen de datos, elija **`SQL Server Native Client 11.0`**.
   b. Asegúrese de que el cuadro Nombre del servidor muestre el punto de conexión de la instancia de base de datos RDS para SQL Server.
   c. Seleccione Utilizar autenticación de SQL Server. En Nombre de usuario y Contraseña, escriba el nombre y la contraseña del usuario maestro de la instancia de la base de datos.
   d. Compruebe que en el cuadro Base de datos aparece la base de datos desde la que desea exportar datos.
   e. Elija Siguiente.
4. En la página Elija un destino, haga lo siguiente:
   a. Para Destino: elija **`SQL Server Native Client 11.0`**.

      > **Note**
      >
      > Hay disponibles otros orígenes de datos de destino disponibles. Estos incluyen .NET Framework, clientes nativos SQL Server, ADO.NET, Microsoft Office Excel, Microsoft Office Access y el origen Archivo sin formato. Si elige como destino uno de estos orígenes de datos, omita el recordatorio del paso 4. Para obtener detalles la siguiente información de conexión que proporcionar, consulte Elija un destino en la documentación de SQL Server.

   b. En Nombre del servidor, escriba el nombre del servidor de la instancia de base de datos SQL de destino.
   c. Elija el tipo de autenticación adecuado. Escriba un nombre de usuario y una contraseña si es necesario.

d. En Base de datos, elija el nombre de la base de datos de destino, o bien elija Nueva para crear una base de datos nueva para contener los datos exportados.

   Si elige Nueva, consulte Crear base de datos en la documentación de SQL Server para obtener detalles sobre la información de base de datos que debe proporcionar.

e. Elija Siguiente.

5. En la página Copia de tabla o consulta, elija Copiar los datos de una o más tablas o vistas o Escribir una consulta para especificar los datos que se van a transferir. Elija Siguiente.
6. Si elige Escribir una consulta para especificar los datos que se van a transferir, aparecerá la página Proporcionar una consulta de origen. Escriba o pegue una consulta SQL y, a continuación, elija Analizar para comprobarla. Una vez validada la consulta, elija Siguiente.
7. En la página Seleccionar tablas y vistas de origen, haga lo siguiente:

   a. Seleccione las tablas y vistas que desea exportar o compruebe que está seleccionada la consulta que ha especificado.

   b. Elija Editar asignaciones y especifique la información de la base de datos y de asignación de columnas. Para obtener más información, consulte Mapeos de columnas en la documentación de SQL Server.

   c. (Opcional) Para ver una vista previa de los datos que se van a exportar, seleccione la tabla, vista o consulta y elija Vista previa.

   d. Elija Siguiente.

8. En la página Ejecutar paquete, compruebe que está seleccionado Ejecutar inmediatamente. Elija Siguiente.
9. En la página Finalización del asistente, compruebe que los detalles de la exportación de datos son los que espera. Seleccione Finalizar.
10. En la página Ejecución completada con éxito, elija Cerrar.

Asistente Generar y publicar scripts de SQL Server y utilidad bcp

Puede usar el asistente Generar y publicar scripts de SQL Server para crear scripts referidos a toda una base de datos o solo a objetos seleccionados. A continuación puede ejecutar esos scripts en una instancia de base de datos SQL Server de destino para volver a crear los objetos especificados. Entonces puede usar la herramienta bcp para una exportación masiva de los datos de los objetos seleccionados a la instancia de base de datos de destino, Esta es la mejor opción cuando se desea transferir una base de datos completa (incluyendo los objetos que no son tablas)

o grandes cantidades de datos entre dos instancias de base de datos SQL Server. Para obtener una descripción completa de la sintaxis de línea de comandos de bcp, consulte bcp (utilidad) en la documentación de Microsoft SQL Server.

El asistente Generar y publicar scripts de SQL Server está disponible como parte de SQL Server Management Studio. Es un cliente SQL Server gráfico incluido en todas las ediciones de Microsoft SQL Server excepto Express Edition. SQL Server Management Studio solo está disponible como aplicación basada en Windows. Microsoft ofrece SQL Server Management Studio Express como descarga gratuita.

Para usar el asistente Generar y publicar scripts y la utilidad bcp de SQL Server para exportar datos

1. En SQL Server Management Studio, conéctese con la instancia de base de datos RDS para SQL Server. Para obtener más detalles sobre cómo hacerlo, consulte Conexión a la instancia de base de datos de Microsoft SQL Server.
2. En el Explorador de objetos, expanda el nodo Bases de datos y seleccione la base de datos que desee incluir en el script.
3. Siga las instrucciones indicadas en Asistente Generar y publicar scripts en la documentación de SQL Server para crear un archivo de script.
4. En SQL Server Management Studio, conecte con la instancia de base de datos SQL Server de destino.
5. Con la instancia de base de datos de SQL Server de destino seleccionada en Object Explorer (Explorador de objetos), elija Open (Abrir) en el menú File (Archivo), elija File (Archivo) y, luego, abra el archivo de script.
6. Si ha realizado scripts en toda la base de datos, revise la instrucción CREATE DATABASE en el scripts. Asegúrese de que la base de datos se crea en la ubicación y con los parámetros que desea, Para obtener más información, consulte CREATE DATABASE en la documentación de SQL Server.
7. Si va a crear usuarios de base de datos con el script, compruebe si los nombres de inicio de sesión en el servidor existen para esos usuarios en la instancia de base de datos. Si no existen, cree nombres de inicio de sesión para los usuarios. De no hacerlo, los comandos del script que crean los usuarios de base de datos generan un error. Para obtener más información, consulte Crear un inicio de sesión en la documentación de SQL Server.
8. Elija !Ejecutar en el menú del Editor SQL para ejecutar el archivo de script y crear los objetos de base de datos. Cuando termine el script, compruebe que existen todos los objetos de base de datos que esperaba.

9. Use la utilidad BCP para exportar datos de la instancia de base de datos RDS para SQL Server a archivos. Abra un símbolo del sistema y escriba el comando siguiente:

```
bcp database_name.schema_name.table_name out data_file -n -S aws_rds_sql_endpoint -
U username -P password
```

En el código anterior se incluyen las opciones siguientes:

- table_name es el nombre de una de las tablas que ha creado en la base de datos de destino y que ahora quiere rellenar con datos.
- data_file es la ruta completa y el nombre del archivo de datos que se va a crear.
- `-n` especifica que la copia masiva utiliza los tipos de datos nativos de los datos que se copian.
- `-S` especifica la instancia de base de datos SQL Server desde la que se exporta.
- `-U` especifica el nombre de usuario empleado al conectar con la instancia de base de datos SQL Server.
- `-P` especifica la contraseña del usuario indicado con `-U`.

El siguiente es un ejemplo del comando .

```
bcp world.dbo.city out C:\Users\JohnDoe\city.dat -n -S sql-jdoe.1234abcd.us-
west-2.rds.amazonaws.com,1433 -U JohnDoe -P ClearTextPassword
```

Repita este paso hasta tener archivos de datos para todas las tablas que desea exportar.

10. Prepare la instancia de base de datos de destino para la importación masiva de datos siguiendo las instrucciones indicadas en Prepararse para importar datos de forma masiva en la documentación de SQL Server.
11. Para decidir el método de importación masiva a emplear, tenga en cuenta las consideraciones y aspectos expuestos en Acerca de las operaciones de importación y exportación masivas en la documentación de SQL Server.
12. Importe de forma masiva los datos de los archivos de datos que ha creado utilizando la utilidad bcp. Para hacerlo, siga las instrucciones facilitadas en Importar y exportar datos de forma masiva con la utilidad bcp o en Importar de forma masiva datos mediante BULK INSERT u OPENROWSET(BULK...) en la documentación de SQL Server, dependiendo de lo que haya decidido en el paso 11.

Uso de la utilidad BCP de Linux para importar y exportar datos

La utilidad BCP (Programa de copia masiva) proporciona una forma eficaz de transferir grandes cantidades de datos entre la instancia de base de datos de RDS para SQL Server y los archivos de datos. Puede utilizar BCP desde entornos de Linux para realizar operaciones de datos masivos, lo que lo hace útil para la migración de datos, los procesos de ETL y las transferencias de datos periódicas.

El BCP permite importar datos de archivos a tablas de SQL Server y exportar datos de tablas de SQL Server a archivos. Esto resulta especialmente eficaz para transferir datos estructurados en varios formatos, incluidos archivos de texto delimitado.

Requisitos previos

Antes de usar BCP con la instancia de base de datos de RDS para SQL Server desde Linux, asegúrese de tener lo siguiente:

- Un entorno de Linux con conectividad de red con la instancia de base de datos de RDS para SQL Server
- Herramientas de línea de comandos de Microsoft SQL Server instaladas en el sistema Linux, que incluyen:
  - sqlcmd: herramienta de consulta de línea de comandos de SQL Server
  - bcp: utilidad del programa de copia masiva
- Credenciales válidas para la instancia de base de datos de RDS para SQL Server
- El acceso a la red se configura mediante grupos de seguridad para permitir las conexiones en el puerto de SQL Server (normalmente el 1433)
- Permisos de base de datos adecuados para las operaciones que desea realizar

Instalación de las herramientas de línea de comandos de SQL Server en Linux

Para usar BCP desde Linux, debe instalar las herramientas de la línea de comandos de Microsoft SQL Server. Para obtener instrucciones de instalación detalladas para su distribución de Linux específica, consulte la siguiente documentación de Microsoft:

- Instalación de sqlcmd y bcp, las herramientas de línea de comandos de SQL Server, en Linux
- utilidad bcp: referencia completa de la utilidad BCP

Tras la instalación, asegúrese de que las herramientas estén disponibles en su PATH ejecutando:

```
bcp -v
sqlcmd -?
```

Exportación de datos de RDS para SQL Server

Puede usar BCP para exportar datos de la instancia de base de datos de RDS para SQL Server a archivos en el sistema Linux. Esto resulta útil para crear copias de seguridad, analizar datos o preparar datos para la migración.

Sintaxis básica de exportación

La sintaxis básica para exportar datos mediante BCP es:

```
bcp database.schema.table out output_file -S server_name -U username -P password
 [options]
```

Donde:

- `database.schema.table`: el nombre de la tabla cualificada completo
- `output_file`: la ruta y el nombre del archivo de salida
- `server_name`: el punto de conexión de RDS para SQL Server
- `username`: el nombre de usuario de la base de datos
- `password`: la contraseña de la base de datos

Ejemplo de exportación

En el siguiente ejemplo, se exportan datos de una tabla denominada `customers` en la base de datos de `sales`:

```
bcp sales.dbo.customers out /home/user/customers.txt \
    -S mydb.cluster-abc123.us-east-1.rds.amazonaws.com \
    -U admin \
    -P mypassword \
    -c \
    -t "|" \
```

```
    -r "\n"
```

Este comando:

- Exporta datos de la tabla de `customers`
- Guarda el resultado en `/home/user/customers.txt`
- Utiliza el formato de caracteres (`-c`)
- Utiliza una barra vertical (|) como delimitador de campo (`-t "|"`)
- Utiliza una nueva línea como delimitador de filas (`-r "\n"`)

Importación de datos a RDS para SQL Server

Puede usar BCP para importar datos de los archivos en el sistema Linux en la instancia de base de datos de RDS para SQL Server. Esto resulta útil para la migración de datos, la carga de datos de prueba o las actualizaciones de datos periódicas.

Sintaxis básica de importación

La sintaxis básica para importar datos mediante BCP es:

```
bcp database.schema.table in input_file -S server_name -U username -P password
 [options]
```

Donde:

- `database.schema.table`: el nombre completo de la tabla de destino cualificada
- `input_file`: la ruta y el nombre del archivo de entrada
- `server_name`: el punto de conexión de RDS para SQL Server
- `username`: el nombre de usuario de la base de datos
- `password`: la contraseña de la base de datos

Ejemplo de importación

En el siguiente ejemplo, se importan datos de un archivo a una tabla denominada `customers`:

```
bcp sales.dbo.customers in /home/user/customers.txt \
```

```
    -S mydb.cluster-abc123.us-east-1.rds.amazonaws.com \
    -U admin \
    -P mypassword \
    -c \
    -t "|" \
    -r "\n" \
    -b 1000
```

Este comando:

- Importa datos en una tabla de `customers`
- Lee datos de `/home/user/customers.txt`
- Utiliza el formato de caracteres (`-c`)
- Utiliza una barra vertical (|) como delimitador de campo (`-t "|"`)
- Utiliza una nueva línea como delimitador de filas (`-r "\n"`)
- Procesa los datos en lotes de 1000 filas (`-b 1000`)

Opciones de BCP comunes

El BCP ofrece numerosas opciones para controlar el formato de los datos y el comportamiento de transferencia. En la tabla siguiente, se describen las opciones que suelen utilizarse:

Opción	Descripción
`-c`	Utiliza el tipo de datos de caracteres para todas las columnas
`-n`	Utiliza los tipos de datos de bases de datos nativos
`-t`	Especifica el delimitador de campo (el predeterminado es pestaña)
`-r`	Especifica el delimitador de filas (el predeterminado es nueva línea)
`-b`	Especifica el tamaño del lote para las operaciones masivas
`-F`	Especifica la primera fila para exportar o importar
`-L`	Especifica la última fila para exportar o importar
`-e`	Especifica un archivo de errores para capturar las filas rechazadas

Opción	Descripción
`-f`	Especifica un archivo de formato para dar formato a los datos
`-q`	Utiliza identificadores entre comillas para los nombres de los objetos

Prácticas recomendadas y consideraciones

Al usar BCP con RDS para SQL Server desde Linux, tenga en cuenta las siguientes prácticas recomendadas:

- Use el procesamiento por lotes: para conjuntos de datos grandes, utilice la `-b` opción para procesar los datos en lotes. Esto mejora el rendimiento y permite una mejor recuperación de errores.
- Gestione los errores sin problemas: utilice la opción `-e` para capturar la información sobre los errores y las filas rechazadas en un archivo independiente para su análisis.
- Elija los formatos de datos adecuados: utilice el formato de caracteres (`-c`) para garantizar la compatibilidad multiplataforma o el formato nativo (`-n`) para mejorar el rendimiento cuando el origen y el destino son SQL Server.
- Proteja sus credenciales: evite poner las contraseñas directamente en las líneas de comandos. Considere la posibilidad de utilizar variables de entorno o archivos de configuración con los permisos adecuados.
- Realice pruebas con conjuntos de datos pequeños: antes de procesar grandes cantidades de datos, pruebe los comandos de BCP con conjuntos de datos más pequeños para comprobar el formato y la conectividad.
- Supervise la conectividad de la red: garantice conexiones de red estables, especialmente para transferencias de datos de gran tamaño. Considere la posibilidad de utilizar herramientas como `screen` o `tmux` para operaciones de larga duración.
- Valide la integridad de los datos: después de la transferencia de datos, verifique el recuento de filas y los datos de ejemplo para garantizar que la operación se haya completado correctamente.

Solución de problemas comunes de

En la siguiente tabla se describen los problemas más comunes que puede encontrar al utilizar BCP desde Linux y sus soluciones:

Problema	Solución
Tiempo de espera de conexión o errores de red	Compruebe el punto de conexión de Amazon RDS, la configuración del grupo de seguridad y la conectividad de red. Asegúrese de que el puerto de SQL Server (normalmente 1433) sea accesible desde el sistema Linux.
Errores de autenticación	Verifique el nombre de usuario y la contraseña. Asegúrese de que el usuario de la base de datos tenga los permisos adecuados para las operaciones que está realizando.
Errores de formato de datos	Compruebe los delimitadores de campos y filas. Asegúrese de que el formato de los datos coincida con lo que BCP espera. Utilice archivos de formato para estructuras de datos complejas.
Errores de permiso denegado	Asegúrese de que el usuario de la base de datos tenga permisos `INSERT` para importaciones o permisos `SELECT` para exportaciones en las tablas de destino.
Problemas de gestión de archivos grandes	Utilice el procesamiento por lotes con la opción `-b`. Considere la posibilidad de dividir los archivos grandes en fragmentos más pequeños para mejorar el rendimiento y la recuperación de errores.
Problemas con la codificación de caracteres	Asegúrese de que los archivos de datos utilicen una codificación de caracteres compatible. Utilice la opción `-c` para el formato de caracteres o especifique las páginas de códigos adecuadas.

Uso de réplicas de lectura para Microsoft SQL Server en Amazon RDS

Normalmente se utilizan réplicas de lectura para configurar la replicación entre instancias de base de datos de Amazon RDS. Para obtener información general acerca de las réplicas de lectura, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Esta sección contiene información específica acerca de cómo utilizar las réplicas de lectura en Amazon RDS for SQL Server.

- Sincronización de los usuarios y objetos de la base de datos con una réplica de lectura de SQL Server
- Solución de problemas de réplicas de lectura de SQL Server

Configuración de réplicas de lectura para SQL Server

Para que una instancia de base de datos pueda servir como instancia de origen para la replicación, debe habilitar las copias de seguridad automáticas en la instancia de base de datos de origen. Para ello, debe establecer el periodo de retención de copia de seguridad en un valor distinto de 0. Al establecer este tipo de implementación también se exige que estén habilitadas las copias de seguridad automáticas.

Para crear una réplica de lectura de SQL Server no se requiere una interrupción de la instancia de base de datos primaria. Amazon RDS establece los parámetros y permisos necesarios para la instancia de base de datos de origen y la réplica de lectura sin interrupción del servicio. Se toma una instantánea de la instancia de base de datos de origen, y esta instantánea se convierte en la réplica de lectura. No se produce ninguna interrupción cuando se elimina una réplica de lectura.

Puede crear hasta 15 réplicas de lectura a partir de una instancia de base de datos de origen. Para que la replicación resulte eficaz, recomendamos que configure cada réplica de lectura con la misma cantidad de recursos de computación y de almacenamiento que la instancia de base de datos de origen. Si modifica la escala de la instancia de base de datos de origen, debe ajustar también la escala de las réplicas de lectura.

La versión del motor de base de datos de SQL Server de la instancia de base de datos de origen y todas sus réplicas de lectura deben ser iguales. Amazon RDS actualiza la primaria inmediatamente después de actualizar las réplicas de lectura, independientemente del periodo de mantenimiento.

Para obtener más información acerca de cómo actualizar la versión del motor de base de datos, consulte Actualizaciones del motor de base de datos de Microsoft SQL Server.

Para que una réplica de lectura reciba y aplique los cambios desde el origen, debe tener suficientes recursos de almacenamiento e informáticos. Si una réplica de lectura llega a su capacidad en materia de recursos de almacenamiento, de red o informáticos, dejará de recibir o aplicar los cambios desde su origen. Puede modificar los recursos de CPU y almacenamiento de una réplica de lectura independientemente de su origen y otras réplicas de lectura.

Para obtener más información sobre cómo crear una réplica de lectura, consulte Creación de una réplica de lectura.

Limitaciones de las réplicas de lectura con SQL Server

Se aplican las siguientes limitaciones a las réplicas de lectura de SQL Server en Amazon RDS:

- Las réplicas de lectura solo están disponibles en el motor de SQL Server Enterprise Edition (EE).
- Las réplicas de lectura están disponibles para las versiones 2016–2022 de SQL Server.
- Puede crear hasta 15 réplicas de lectura a partir de una instancia de base de datos de origen. La replicación puede retrasarse si la instancia de base de datos de origen tiene más de 5 réplicas de lectura.
- Además, solo están disponibles para las instancias de base de datos que se ejecutan en clases de instancia de base de datos con cuatro o más vCPU.
- Una réplica de lectura admite hasta 100 bases de datos, según el tipo de clase de instancia y el modo de disponibilidad. Debe crear bases de datos en la instancia de base de datos de origen para replicarlas automáticamente en las réplicas de lectura. No puede elegir bases de datos individuales para replicar. Para obtener más información, consulte Limitaciones para instancias de base de datos de Microsoft SQL Server.
- No se puede eliminar una base de datos de una réplica de lectura. Para eliminar una base de datos, elimínela de la instancia de base de datos de origen con el procedimiento almacenado `rds_drop_database`. Para obtener más información, consulte Eliminación de una base de datos en una instancia de base de datos de Amazon RDS para Microsoft SQL Server.
- Si la instancia de base de datos de origen utiliza Cifrado de datos transparente (TDE) para cifrar los datos, la réplica de lectura también configura el TDE de forma automática.

  Si la instancia de base de datos de origen utiliza una clave KMS para cifrar los datos, las réplicas de lectura de la misma región utilizan la misma clave KMS. Para las réplicas de lectura entre

regiones, debe especificar una clave KMS de la región de la réplica de lectura al crear la réplica de lectura. No puede cambiar la clave KMS de una réplica de lectura.

- Las réplicas de lectura tienen la misma zona horaria y la misma intercalación que la instancia de base de datos de origen, independientemente de la zona de disponibilidad en la que se hayan creado.
- Lo siguiente no es compatible con Amazon RDS for SQL Server:
  - Retención de copias de seguridad de réplicas de lectura
  - Recuperación a un momento dado de réplicas de lectura
  - Instantáneas manuales de réplicas de lectura
  - Réplicas de lectura Multi-AZ
  - Creación de réplicas de lectura a partir de otras réplicas de lectura
  - Sincronización de inicios de sesión de usuario para leer réplicas
- Amazon RDS for SQL Server no interviene para mitigar el retraso de réplica elevado entre una instancia de base de datos de origen y sus réplicas de lectura. Asegúrese de que la instancia de base de datos de origen y sus réplicas de lectura tienen el tamaño adecuado, en términos de potencia informática y almacenamiento, para adaptarse a su carga operativa.
- Puede reproducir entre las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (US-West), pero no dentro ni fuera de AWS GovCloud (US) Regions.

Consideraciones relativas a opciones para réplicas de RDS para SQL Server

Antes de crear una réplica de RDS para SQL Server, tenga en cuenta los siguientes requisitos, restricciones y recomendaciones:

- Si la réplica de SQL Server se encuentra en la misma región que su instancia de base de datos de origen, asegúrese de que pertenezca al mismo grupo de opciones que la instancia de base de datos de origen. Las modificaciones en el grupo de opciones de origen o en la suscripción a grupos de opciones de origen se propagan a las réplicas. Estos cambios se aplican a las réplicas inmediatamente después de su aplicación a la instancia de base de datos de origen, con independencia del periodo de mantenimiento de la réplica.

  Para obtener más información acerca de los grupos de opciones, consulte Trabajo con grupos de opciones.

- Cuando crea una réplica entre regiones de SQL Server, Amazon RDS crea un grupo de opciones dedicado para ella.

  No puede eliminar una réplica entre regiones de SQL Server desde su grupo de opciones dedicado. Ninguna otra instancia de base de datos puede utilizar el grupo de opciones dedicado para una réplica entre regiones de SQL Server.

  Las siguientes opciones son opciones replicadas. Para agregar otras opciones a una réplica de lectura entre regiones de Oracle, agréguelas al grupo de opciones de la instancia de base de datos de origen. La opción también está instalada en todas las réplicas de la instancia de base de datos de origen.

  - `TDE`

  Las siguientes opciones son opciones no replicadas. Solo puede agregar o quitar opciones no replicadas de un grupo de opciones dedicado.

  - `MSDTC`
  - `SQLSERVER_AUDIT`
  - Para habilitar la opción `SQLSERVER_AUDIT` en la réplica de lectura entre regiones, añada la opción `SQLSERVER_AUDIT` al grupo de opciones dedicado de la réplica de lectura entre regiones y al grupo de opciones de la instancia de origen. Al agregar la opción `SQLSERVER_AUDIT` a la instancia de origen de la réplica de lectura entre regiones de SQL Server, puede crear un objeto de auditoría de nivel de servidor y especificaciones de auditoría de nivel de servidor en cada una de las réplicas de lectura entre regiones de la instancia de origen. Para permitir el acceso a las réplicas de lectura entre regiones para cargar los registros de auditoría completos en un bucket de Amazon S3, añada la opción `SQLSERVER_AUDIT` al grupo de opciones dedicado y configure los ajustes de las opciones. El bucket de Amazon S3 que usa como destino para los archivos de auditoría debe estar en la misma región que la réplica de lectura entre regiones. Puede modificar la configuración de la opción `SQLSERVER_AUDIT` para cada réplica de lectura entre regiones de forma independiente de manera que cada una pueda acceder a un bucket de Amazon S3 en su región respectiva.

  Las siguientes opciones no son compatibles con réplicas de lectura.

  - `SSRS`
  - `SSAS`
  - `SSIS`

  Las siguientes opciones no compatibles parcialmente con réplicas de lectura entre regiones.

- SQLSERVER_BACKUP_RESTORE
- La instancia de base de datos de origen de una réplica entre regiones de SQL Server puede tener la opción SQLSERVER_BACKUP_RESTORE, pero no podrá realizar restauraciones nativas en la instancia de base de datos de origen hasta que elimine todas sus réplicas entre regiones. Todas las tareas de restauración nativas existentes se cancelarán durante la creación de una réplica entre regiones. No puedes añadir la opción SQLSERVER_BACKUP_RESTORE a un grupo de opciones dedicado.

  Para obtener más información acerca de la copia de seguridad y la restauración nativas, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Al promocionar una réplica de lectura entre regiones de SQL Server, la réplica de lectura promocionada se comporta igual que las otras instancias de base de datos de SQL Server, incluida la administración de sus opciones. Para obtener más información sobre los grupos de opciones, consulte Trabajo con grupos de opciones.

Sincronización de los usuarios y objetos de la base de datos con una réplica de lectura de SQL Server

Se espera que todos los inicios de sesión, los roles de servidor personalizados, las tareas del agente SQL u otros objetos de nivel de servidor que existan en la instancia de base de datos principal en el momento de crear una réplica de lectura estén presentes en la réplica de lectura recién creada. Sin embargo, los objetos de nivel de servidor que se creen en la instancia de base de datos principal tras la creación de la réplica de lectura no se replicarán automáticamente y deberá crearlos manualmente en la réplica de lectura.

Los usuarios de la base de datos se replican automáticamente de la instancia de base de datos principal a la réplica de lectura. Como la base de datos de réplica de lectura está en modo de solo lectura, el identificador de seguridad (SID) del usuario de la base de datos no se puede actualizar en la base de datos. Por lo tanto, al crear inicios de sesión de SQL en la réplica de lectura, es fundamental asegurarse de que el SID de ese inicio de sesión coincida con el SID del inicio de sesión de SQL correspondiente en la instancia de base de datos principal. Si no sincroniza los SID de los inicios de sesión de SQL, no podrán acceder a la base de datos en la réplica de lectura. Los inicios de sesión autenticados de Windows Active Directory (AD) no presentan este problema porque el SQL Server obtiene el SID de Active Directory.

Sincronización de un inicio de sesión de SQL de la instancia de base de datos principal con la réplica de lectura

1. Conéctese a la instancia de base de datos principal.
2. Cree un nuevo inicio de sesión de SQL en la instancia de base de datos principal.

```
USE [master]
GO
CREATE LOGIN TestLogin1
WITH PASSWORD = 'REPLACE WITH PASSWORD';
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

3. Cree un nuevo usuario de base de datos para el inicio de sesión de SQL en la base de datos.

```
USE [REPLACE WITH YOUR DB NAME]
GO
CREATE USER TestLogin1 FOR LOGIN TestLogin1;
GO
```

4. Compruebe el SID del inicio de sesión de SQL que se acaba de crear en la instancia de base de datos principal.

```
SELECT name, sid FROM sys.server_principals WHERE name =  TestLogin1;
```

5. Conéctese a la réplica de lectura. Cree el nuevo inicio de sesión de SQL.

```
CREATE LOGIN TestLogin1 WITH PASSWORD = 'REPLACE WITH PASSWORD', SID=[REPLACE WITH
 sid FROM STEP #4];
```

Como alternativa, si tiene acceso a la base de datos de réplica de lectura, puede corregir el usuario huérfano de la siguiente manera:

1. Conéctese a la réplica de lectura.
2. Identifique los usuarios huérfanos de la base de datos.

```
USE [REPLACE WITH YOUR DB NAME]
GO
EXEC sp_change_users_login 'Report';
GO
```

3. Cree un nuevo inicio de sesión de SQL para el usuario huérfano de la base de datos.

```
CREATE LOGIN TestLogin1 WITH PASSWORD = 'REPLACE WITH PASSWORD', SID=[REPLACE WITH
 sid FROM STEP #2];
```

Ejemplo:

```
CREATE LOGIN TestLogin1 WITH PASSWORD = 'TestPa$$word#1',
 SID=[0x1A2B3C4D5E6F7G8H9I0J1K2L3M4N5O6P];
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Solución de problemas de réplicas de lectura de SQL Server

Puede monitorizar el retardo de replicación en Amazon CloudWatch mediante la visualización de la métrica `ReplicaLag` de Amazon RDS. Para obtener información sobre el retardo de replicación, consulte Monitoreo de la replicación de lectura.

Si el retraso de replicación es demasiado largo, puede usar la siguiente consulta para obtener información acerca de este.

```
SELECT AR.replica_server_name
     , DB_NAME (ARS.database_id) 'database_name'
     , AR.availability_mode_desc
     , ARS.synchronization_health_desc
     , ARS.last_hardened_lsn
     , ARS.last_redone_lsn
     , ARS.secondary_lag_seconds
FROM sys.dm_hadr_database_replica_states ARS
INNER JOIN sys.availability_replicas AR ON ARS.replica_id = AR.replica_id
```

```
--WHERE DB_NAME(ARS.database_id) = 'database_name'
ORDER BY AR.replica_server_name;
```

Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server

Las implementaciones Multi-AZ proporcionan unos niveles superiores de disponibilidad, durabilidad de los datos y tolerancia a errores para las instancias de base de datos. Si se produce una interrupción del servicio no planificada o un mantenimiento planificado de la base de datos, Amazon RDS conmuta automáticamente a la instancia de base de datos secundaria. Esta funcionalidad permite que las operaciones de base de datos se reanuden rápidamente sin intervención manual. Las instancias principal y en espera usan el mismo punto de enlace, cuya dirección de red física cambia a la réplica secundaria como parte del proceso de conmutación por error. No tiene que volver a configurar su aplicación cuando se produzca una conmutación por error.

Amazon RDS admite implementaciones Multi-AZ para instancias de base de datos en las que se ejecuta Microsoft SQL Server mediante el uso de la creación de reflejos de bases de datos (DBM) de SQL Server o los grupos de disponibilidad (AG) AlwaysOn. Amazon RDS monitorea y mantiene el estado de la implementación Multi-AZ. Si se produce algún problema, RDS reparará automáticamente las instancias de base de datos con problemas, restablecerá la sincronización e iniciará las conmutaciones por error. La conmutación por error solo ocurre si las instancias en espera y principal están totalmente sincronizadas. No es necesario que administre nada.

Al configurar Multi-AZ en SQL Server, RDS configura automáticamente todas las bases de datos en la instancia para utilizar DBM o AG. Amazon RDS se encarga de la instancia principal, el testigo de creación de reflejo y la instancia de base de datos secundaria en su nombre. Debido a que la configuración es automática, RDS selecciona DBM o AG siempre en función de la versión de SQL Server que implemente.

Amazon RDS admite Multi-AZ con los AG Always On para las siguientes versiones y ediciones de SQL Server:

- SQL Server 2022
  - Standard Edition
  - Enterprise Edition
- SQL Server 2019:
  - Standard Edition 15.00.4073.23 y posteriores
  - Enterprise Edition
- SQL Server 2017:

  - Standard Edition 14.00.3401.7 y posteriores
  - Enterprise Edition 14.00.3049.1 y posteriores
- SQL Server 2016: Enterprise Edition 13.00.5216.0 o posterior

Amazon RDS es compatible con Multi-AZ con DBM para las siguientes versiones y ediciones de SQL Server, salvo para las versiones mencionadas anteriormente:

- SQL Server 2019: Standard Edition 15.00.4043.16
- SQL Server 2017: Standard y Enterprise Editions
- SQL Server 2016: Standard y Enterprise Editions

Puede utilizar la siguiente consulta SQL para determinar si su instancia de base de datos de SQL Server es Single-AZ, Multi-AZ con DBM o Multi-AZ con AG Always On.

```
SELECT CASE WHEN dm.mirroring_state_desc IS NOT NULL THEN 'Multi-AZ (Mirroring)'
    WHEN dhdrs.group_database_id IS NOT NULL THEN 'Multi-AZ (AlwaysOn)'
    ELSE 'Single-AZ'
    END 'high_availability'
FROM sys.databases sd
LEFT JOIN sys.database_mirroring dm ON sd.database_id = dm.database_id
LEFT JOIN sys.dm_hadr_database_replica_states dhdrs ON sd.database_id =
 dhdrs.database_id AND dhdrs.is_local = 1
WHERE DB_NAME(sd.database_id) = 'rdsadmin';
```

La salida se parece a la siguiente:

```
high_availability
Multi-AZ (AlwaysOn)
```

Adición de implementaciones Multi-AZ a una instancia de base de datos de Microsoft SQL Server

Al crear una nueva instancia de base de datos de SQL Server utilizando la AWS Management Console, puede añadir Multi-AZ con creación de reflejos (DBM) o AG Always On. Para ello, elija Yes (Mirroring / Always On) (Sí [Creación de reflejos / Always On]) en la Multi-AZ Deployment (Implementación Multi-AZ) . Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

Cuando modifique una instancia de base de datos de SQL Server existente con la consola, puede añadir Multi-AZ con DBM o AG al seleccionar Yes (Mirroring/Always On) (Sí [Replicación/Siempre activada]) en Multi-AZ Deployment (Implementación multi-AZ) en la página Modify DB Instance (Modificar instancia de base de datos). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Note**
>
> Si la instancia de base de datos ejecuta la creación de reflejos de base de datos (DBM) —no grupos de disponibilidad (AG) Always On— deshabilite la optimización en memoria antes de agregar Multi-AZ. Deshabilite la optimización en memoria con DBM antes de agregar Multi-AZ si su instancia de base de datos ejecuta SQL Server 2016 o 2017 Enterprise Edition y está habilitada la optimización en memoria.
> Si la instancia de base de datos está ejecutando AG, este paso no es necesario.

Eliminación de Multi-AZ de una instancia de base de datos de Microsoft SQL Server

Al modificar una instancia de base de datos de SQL Server existente mediante AWS Management Console, se pueden eliminar implementaciones Multi-AZ con DBM o AG. Para hacerlo, elija No (Mirroring / Always On) (No [Replicación/Siempre activada) en Multi-AZ deployment (Implementación Multi-AZ) en la página Modify DB Instance (Modificar instancia de base de datos). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Limitaciones, notas y recomendaciones relativas a las implementaciones Multi-AZ de Microsoft SQL Server

Las siguientes limitaciones se aplican al trabajar con implementaciones Multi-AZ en RDS para instancias de base de datos de SQL Server:

- No se admite Multi-AZ entre regiones.
- No se puede detener una instancia de base de datos de Amazon RDS para SQL Server que esté en una implementación Multi-AZ.
- No puede configurar la instancia de base de datos secundaria de modo que acepte la actividad de lectura de bases de datos.

- Multi-AZ con grupos de disponibilidad (AG) Always On es compatible con la optimización en memoria.
- Multi-AZ con grupos de disponibilidad (AG) Always On no admite la autenticación Kerberos para el agente de escucha del grupo de disponibilidad. Esto se debe a que el agente de escucha no tiene nombre principal de servicio (SPN).
- No se puede cambiar el nombre de una base de datos de una instancia de base de datos de SQL Server que esté en una implementación Multi-AZ de SQL Server. Si tiene que cambiar el nombre de una base de datos en una instancia de este tipo, desactive primero la implementación Multi-AZ para la instancia de base de datos, cambie el nombre de la base de datos. Por último, vuelva a activar la implementación Multi-AZ en la instancia de base de datos.
- Solo puede restaurar las instancias de base de datos Multi-AZ a las que se haya realizado una copia de seguridad usando el modelo de recuperación completa.
- Las implementaciones multi-AZ tienen un límite de 10 000 trabajos del Agente SQL Server.

  Si se necesitan límites más altos, solicite un aumento; para ello, contáctese con Soporte. Abra la página del centro de AWS Support, inicie sesión si es preciso y, luego, elija Create Case (Crear caso). Seleccione Service limit increase (Aumento del límite de servicio). Rellene y envíe el formulario.
- No puede tener una base de datos sin conexión en una instancia de base de datos de SQL Server que se encuentre en una implementación Multi-AZ de SQL Server.
- RDS para SQL Server no replica los permisos de la base de datos MSDB en la instancia secundaria. Si necesita estos permisos en la instancia secundaria, debe recrearlos manualmente.

En las siguientes notas se describe el trabajo con implementaciones Multi-AZ en RDS para instancias de base de datos de SQL Server:

- Amazon RDS expone el punto de enlace del agente de escucha del grupo de disponibilidad de los AG Always On. El punto de conexión está visible en la consola, y lo devuelve la operación de API `DescribeDBInstances` como entrada en el campo de puntos de conexión.
- Amazon RDS es compatible con las conmutaciones por error multisubred de grupos de disponibilidad.
- Para usar las implementaciones Multi-AZ con una instancia de base de datos de SQL Server en una nube privada virtual (VPC), debe crear primero un grupo de subredes de base de datos que tenga subredes en al menos dos zonas de disponibilidad diferentes. A continuación, asigne el grupo de subredes de la réplica principal de la instancia de base de datos de SQL Server.

- Cuando una instancia de base de datos se modifica para convertirla en una implementación Multi-AZ, durante la modificación tiene el estado modifying (modificando). Amazon RDS crea el modo de espera y realiza una copia de seguridad de la instancia de base de datos primaria. Una vez que el proceso se haya completado, el estado de la instancia de base de datos principal pasará a ser available (disponible).
- Las implementaciones Multi-AZ mantienen todas las bases de datos en el mismo nodo. Si una base de datos del anfitrión principal experimenta una conmutación por error, todas las bases de datos de SQL Server conmutarán por error como una unidad atómica al anfitrión en espera. Amazon RDS aprovisiona un nuevo anfitrión en buen estado y reemplaza al anfitrión que no está en buen estado.
- Las implementaciones Multi-AZ con DBM o AG son compatibles con una única réplica en espera.
- Los usuarios, los inicios de sesión y los permisos se replican automáticamente en la secundaria. No tiene que volver a crearlos. Los roles de servidor definidos por los usuarios solo se replican en instancias de base de datos que utilizan Always On AGs para implementaciones multi-AZ.
- En las implementaciones multi-AZ, RDS para SQL Server crea inicios de sesión de SQL Server para permitir grupos de disponibilidad (AG) Always On o la creación de reflejos de bases de datos. RDS crea inicios de sesión con el siguiente patrón: `db_<dbiResourceId>_node1_login`, `db_<dbiResourceId>_node2_login` y `db_<dbiResourceId>_witness_login`.
- RDS para SQL Server crea un inicio de sesión de SQL Server para permitir el acceso a las réplicas de lectura. RDS crea inicios de sesión con el siguiente patrón: `db_<readreplica_dbiResourceId>_node_login`.
- En las implementaciones Multi-AZ, los trabajos de SQL Server Agent se replican desde el host principal al host secundario cuando la función de replicación de trabajos está activada. Para obtener más información, consulte Activación de la replicación de trabajos del agente de SQL Server.
- Pueden producirse latencias elevadas comparadas con una implementación de instancia de base de datos estándar (en una única zona de disponibilidad) debido a la replicación de datos síncrona.
- Los tiempos de conmutación por error se ven afectados por el tiempo necesario para completar el proceso de recuperación. Las transacciones grandes aumentan el tiempo de conmutación por error.
- En las implementaciones Multi-AZ de SQL Server, el reinicio con conmutación por error reinicia sólo la instancia de base de datos principal. Después de la conmutación por error, la instancia de base de datos principal se convierte en la nueva instancia de base de datos secundaria. Puede que no se actualicen los parámetros para instancias Multi-AZ. Para el reinicio sin conmutación

por error, las instancias de base de datos primaria y secundaria se reinician y los parámetros se actualizan después del reinicio. Si la instancia de base de datos no responde, se recomienda reiniciar sin conmutación por error.

Las siguientes recomendaciones están indicadas al trabajar con implementaciones Multi-AZ en RDS para instancias de base de datos de Microsoft SQL Server:

- Para conocer las bases de datos utilizadas en el proceso de producción y preproducción, le recomendamos las siguientes opciones:
  - Implementaciones Multi-AZ para alta disponibilidad
  - "IOPS provisionadas" para un rendimiento rápido y coherente
  - "Optimizada para memoria" en lugar de "Uso general"
- No se puede seleccionar la zona de disponibilidad (AZ) para la instancia secundaria, así que al implementar los hosts de las aplicaciones, tenga esto en cuenta. Su base de datos podría experimentar una conmutación por error a otra zona de disponibilidad y los hosts de las aplicaciones podrían no estar en la misma zona de disponibilidad que la base de datos. Por este motivo, le recomendamos equilibrar los hosts de aplicaciones entre todas las zonas de disponibilidad de la región de AWS dada.
- Para obtener el máximo rendimiento, no habilite la creación de reflejos ni AG Always On durante una operación grande de carga de datos. Si desea que la carga de datos sea lo más rápida posible, termínela antes de convertir la instancia de base de datos en una implementación Multi-AZ.
- Las aplicaciones que obtienen acceso a las bases de datos de SQL Server deben tener un tratamiento de las excepciones que detecte los errores de conexión. En la siguiente muestra de código, un bloque try/catch detecta un error de comunicación. En este ejemplo, la instrucción `break` sale del bucle `while` si la conexión es correcta, pero vuelve a intentarlo hasta 10 veces si se produce una excepción.

```
int RetryMaxAttempts = 10;
int RetryIntervalPeriodInSeconds = 1;
int iRetryCount = 0;
while (iRetryCount < RetryMaxAttempts)
{
   using (SqlConnection connection = new SqlConnection(DatabaseConnString))
   {
      using (SqlCommand command = connection.CreateCommand())
      {
```

```
         command.CommandText = "INSERT INTO SOME_TABLE VALUES ('SomeValue');";
         try
         {
            connection.Open();
            command.ExecuteNonQuery();
            break;
         }
         catch (Exception ex)
         {
            Logger(ex.Message);
            iRetryCount++;
         }
         finally {
            connection.Close();
         }
      }
   }
   Thread.Sleep(RetryIntervalPeriodInSeconds * 1000);
}
```

- No use el comando `Set Partner Off` cuando se trabaja con instancias Multi-AZ. Por ejemplo, no haga lo siguiente.

```
--Don't do this
ALTER DATABASE db1 SET PARTNER off
```

- No establezca el modo de recuperación en `simple`. Por ejemplo, no haga lo siguiente.

```
--Don't do this
ALTER DATABASE db1 SET RECOVERY simple
```

- No use el parámetro `DEFAULT_DATABASE` cuando cree nuevos inicios de sesión en instancias de base de datos Multi-AZ, ya que esta configuración no se puede aplicar en el reflejo en espera. Por ejemplo, no haga lo siguiente.

```
--Don't do this
CREATE LOGIN [test_dba] WITH PASSWORD=foo, DEFAULT_DATABASE=[db2]
```

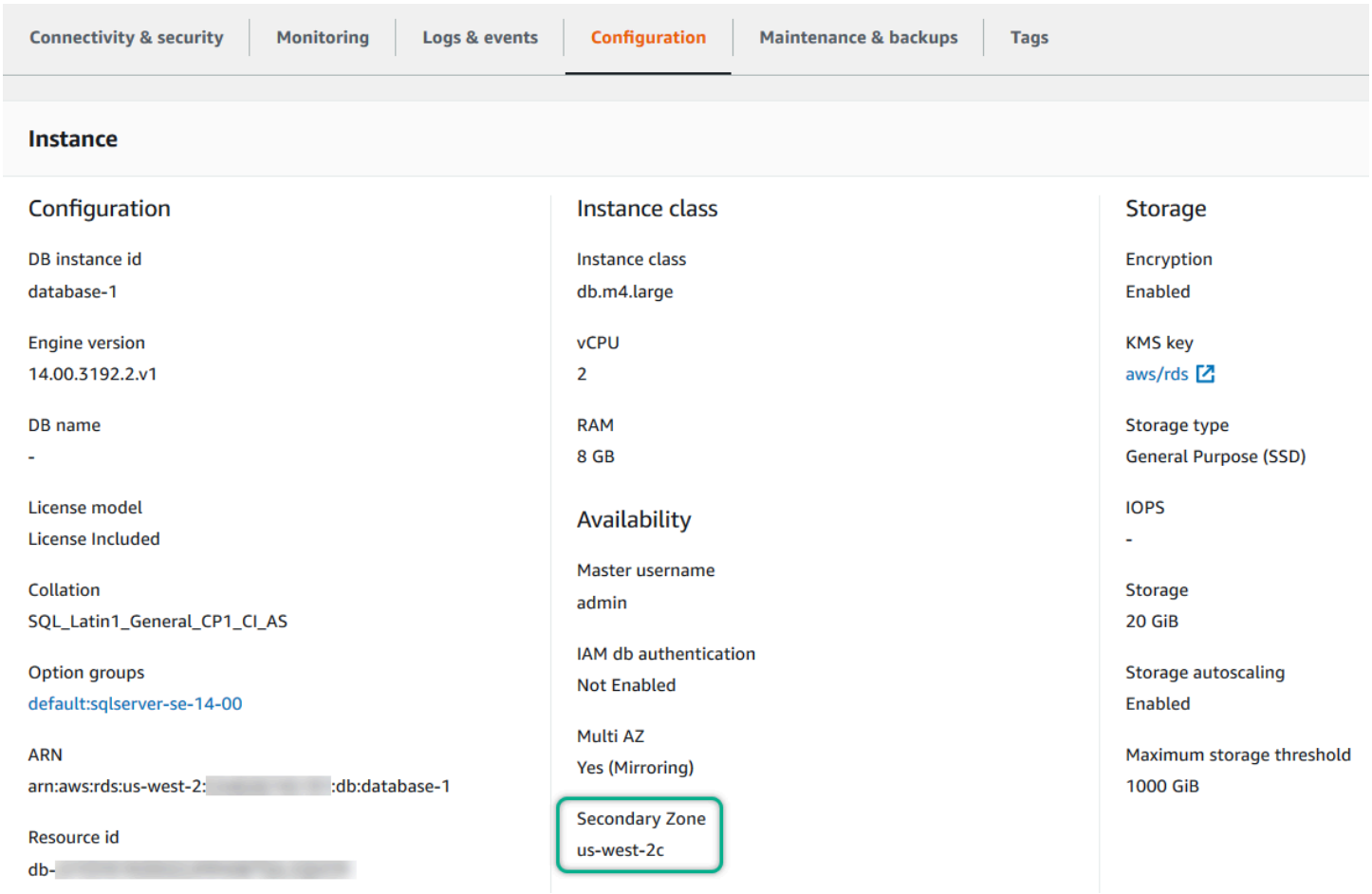
  Tampoco haga lo siguiente.

```
--Don't do this
```

```
ALTER LOGIN [test_dba] WITH DEFAULT_DATABASE=[db3]
```

Determinar la ubicación de la secundaria

Puede determinar la ubicación de la réplica secundaria usando la AWS Management Console. Debe conocer la ubicación de la secundaria si va a configurar la instancia de base de datos principal en una VPC.



También puede ver la zona de disponibilidad de la secundaria usando el comando AWS CLI de la `describe-db-instances` o la operación `DescribeDBInstances` de la API de RDS. La salida muestra la zona de disponibilidad secundaria en la que se encuentra el reflejo en espera.

Migración desde la creación de reflejos de base de datos a grupos de disponibilidad Always On

En la versión 14.00.3049.1 de Microsoft SQL Server Enterprise Edition, los grupos de disponibilidad (AG) Always On están habilitados de forma predeterminada.

Para migrar desde la creación de reflejos de base de datos (DBM) a AG, compruebe su versión antes. Si está utilizando una instancia de base de datos con una versión anterior a Enterprise Edition 13.00.5216.0, modifique la instancia para parchearla a la versión 13.00.5216.0 o posterior. Si está utilizando una instancia de base de datos con una versión anterior a Enterprise Edition 14.00.3049.1, modifique la instancia para parchearla a la versión 14.00.3049.1 o posterior.

Si desea actualizar una instancia de base de datos de la que se ha creado el reflejo para usar AG, ejecute la actualización primero, modifique la instancia para eliminar Multi-AZ y, a continuación, vuelva a modificarla para añadir Multi-AZ. Esto convierte su instancia para usar AG Always On.

Características adicionales para Microsoft SQL Server en Amazon RDS

En las secciones siguientes, puede encontrar información acerca de cómo aumentar las instancias de Amazon RDS que ejecutan el motor de base de datos de Microsoft SQL Server.

Temas

- Uso de la política de contraseñas para inicios de sesión de SQL Server en RDS para SQL Server
- Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3
- Uso de Database Mail en Amazon RDS for SQL Server
- Soporte del almacén de instancias para la base de datos tempdb en Amazon RDS for SQL Server
- Uso de eventos extendidos con Amazon RDS for Microsoft SQL Server
- Acceso a las copias de seguridad del registro de transacciones con RDS para SQL Server

Uso de la política de contraseñas para inicios de sesión de SQL Server en RDS para SQL Server

Amazon RDS le permite configurar la política de contraseñas de su instancia de base de datos de Amazon RDS en la que se ejecuta Microsoft SQL Server. Utilícela para establecer los requisitos de complejidad, longitud y bloqueo para los inicios de sesión que utilizan la autenticación de SQL Server para autenticarse en su instancia de base de datos.

Términos clave

Login (Iniciar sesión)

: En SQL Server, una entidad principal de servidor que puede autenticarse en una instancia de base de datos se denomina inicio de sesión. Otros motores de bases de datos pueden denominar esta entidad principal como usuario. En RDS para SQL Server, un inicio de sesión puede autenticarse mediante la autenticación de SQL Server o la autenticación de Windows.

Inicio de sesión de SQL Server

: Un inicio de sesión que utiliza un nombre de usuario y una contraseña para autenticarse mediante la autenticación de SQL Server es un inicio de sesión de SQL Server. La política de contraseñas que se configura mediante los parámetros de base de datos solo se aplica a los inicios de sesión de SQL Server.

Inicio de sesión de Windows

: Un inicio de sesión que se basa en una entidad principal de Windows y se autentica mediante la autenticación de Windows es un inicio de sesión de Windows. Puede configurar la política de contraseñas para los inicios de sesión de Windows en Active Directory. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.

Habilitación y deshabilitación de política para cada inicio de sesión

Cada inicio de sesión de SQL Server tiene marcadores para `CHECK_POLICY` y `CHECK_EXPIRATION`. De forma predeterminada, los nuevos inicios de sesión se crean con `CHECK_POLICY` establecido en `ON` y `CHECK_EXPIRATION` establecido en `OFF`.

Si `CHECK_POLICY` está habilitada para un inicio de sesión, RDS para SQL Server valida la contraseña comparándola con los requisitos de complejidad y longitud mínima. También se aplican

políticas de bloqueo. Un ejemplo de una instrucción de T-SQL para habilitar `CHECK_POLICY` y `CHECK_EXPIRATION`:

```
ALTER LOGIN [master_user] WITH CHECK_POLICY = ON, CHECK_EXPIRATION = ON;
```

Si `CHECK_EXPIRATION` está habilitada, las contraseñas están sujetas a las políticas de antigüedad de las contraseñas. La instrucción de T-SQL para comprobar si `CHECK_POLICY` y `CHECK_EXPIRATION` están configuradas:

```
SELECT name, is_policy_checked, is_expiration_checked FROM sys.sql_logins;
```

Parámetros de las políticas de contraseñas

Todos los parámetros de la política de contraseñas son dinámicos y no requieren que se reinicie la base de datos para que surtan efecto. La siguiente tabla muestra los parámetros de base de datos que puede configurar para modificar la política de contraseñas para los inicios de sesión de SQL Server:

Parámetro de base de datos	Descripción	Valores permitidos	Valor predeterminado	
rds.password_complexity_enabled	Se deben cumplir los requisitos de complejidad de las contraseñas al crear o cambiar las contraseñas para los inicios de sesión de SQL Server. Se deben cumplir las siguientes restricciones: • La contraseña debe incluir	0,1	0	

Parámetro de base de datos	Descripción	Valores permitidos	Valor predeterminado	
	caracteres de tres de las siguientes categorías: • Letra latina minúscula (de la a a la z) • Letra latina mayúscula (de la A a la Z) • Caracteres no alfanuméricos como: signo de exclamación (!), signo de dólar ($), almohadilla (#) o porcentaje (%). • La contraseña no contiene el nombre de la cuenta del usuario.			

Parámetro de base de datos	Descripción	Valores permitidos	Valor predeterminado	
rds.password_min_length	El número mínimo de caracteres que debe tener una contraseña para un inicio de sesión de SQL Server.	0-14	0	
rds.password_min_age	El número mínimo de días que debe utilizarse una contraseña de inicio de sesión de SQL Server antes de que el usuario pueda cambiarla. Las contraseñas se pueden cambiar inmediatamente si se establece en 0.	0-998	0	

Parámetro de base de datos	Descripción	Valores permitidos	Valor predeterminado	
rds.password_max_age	El número máximo de días que se puede usar una contraseña de inicio de sesión de SQL Server tras los cuales el usuario debe cambiarla. Las contraseñas nunca caducan cuando se establece en 0.	0-999	42	
rds.password_lockout_threshold	El número de intentos de inicio de sesión fallidos consecutivos que provocan el bloqueo de un inicio de sesión de SQL Server.	0-999	0	
rds.password_lockout_duration	El número de minutos que debe esperar un inicio de sesión de SQL Server bloqueado antes de desbloquearse.	1-60	10	

Parámetro de base de datos	Descripción	Valores permitidos	Valor predeterminado	
rds.password_lockout_reset_counter_after	El número de minutos que deben transcurrir después de un intento de inicio de sesión fallido antes de que el contador de intentos de inicio de sesión fallidos se restablezca a 0.	1-60	10	

> **Note**
>
> Para obtener más información sobre la política de contraseñas de SQL Server, consulte Política de contraseñas.
> Las políticas de complejidad y longitud mínima de las contraseñas también se aplican a los usuarios de bases de datos en bases de datos independientes. Para obtener más información, consulte Bases de datos independientes.

Se aplican las siguientes limitaciones a los parámetros de las políticas de contraseñas:

- El parámetro `rds.password_min_age` debe ser menor que `rds.password_max_age parameter`, a menos que `rds.password_max_age` esté establecido en 0
- El parámetro `rds.password_lockout_reset_counter_after` debe ser igual o menor que el parámetro `rds.password_lockout_duration`.
- Si `rds.password_lockout_threshold` está establecido en 0, `rds.password_lockout_duration` y `rds.password_lockout_reset_counter_after` no se aplican.

Consideraciones sobre inicios de sesión existentes

Tras modificar la política de contraseñas en una instancia, las contraseñas existentes para los inicios de sesión no se evalúan retroactivamente en función de los nuevos requisitos de complejidad y longitud de las contraseñas. Solo las contraseñas nuevas se validan según la nueva política.

SQL Server evalúa las contraseñas existentes en función de los requisitos de antigüedad.

Es posible que las contraseñas caduquen inmediatamente una vez que se modifique la política de contraseñas. Por ejemplo, si un inicio de sesión tiene habilitado `CHECK_EXPIRATION` y su contraseña se modificó por última vez hace 100 días, y establece el parámetro `rds.password_max_age` en 5 días, la contraseña caducará inmediatamente y el inicio de sesión tendrá que cambiar la contraseña la próxima vez que intente iniciar sesión.

> **Note**
>
> RDS para SQL Server no admite políticas de historial de contraseñas. Las políticas de historial impiden que los inicios de sesión reutilicen las contraseñas que ya han utilizado anteriormente.

Consideraciones para implementaciones Multi-AZ

El contador de intentos de inicio de sesión fallidos y el estado de bloqueo de las instancias multi-AZ no se replican entre nodos. En caso de que se bloquee un inicio de sesión debido a una conmutación por error en una instancia multi-AZ, es posible que el inicio de sesión ya esté desbloqueado en el nuevo nodo.

Consideraciones sobre la contraseña para el inicio de sesión maestro

Cuando se crea una instancia de base de datos de RDS para SQL Server, la contraseña del usuario maestro no se evalúa con respecto a la política sobre contraseñas. Una nueva contraseña maestra tampoco se evalúa con respecto a la contraseña al realizar operaciones con el usuario maestro, específicamente al configurar `MasterUserPassword` en el comando `ModifyDBInstance`. En ambos casos, puede establecer una contraseña para el usuario maestro que no cumpla su política de contraseñas y la operación seguirá realizándose correctamente. Si no se cumple la política, RDS intenta generar un evento de RDS con la recomendación de establecer una contraseña segura. Tenga cuidado y use solo contraseñas seguras para el usuario maestro.

RDS intenta generar los siguientes mensajes de eventos cuando la contraseña del usuario maestro no cumple los requisitos de la política de contraseñas:

- Se creó el usuario maestro, pero la contraseña no cumple el requisito de longitud mínima de su política de contraseñas. Plantéese utilizar una contraseña más segura.
- Se creó el usuario maestro, pero la contraseña no cumple el requisito de complejidad de su política de contraseñas. Plantéese utilizar una contraseña más segura.
- Se restableció el usuario maestro, pero la contraseña no cumple el requisito de longitud mínima de su política de contraseñas. Plantéese utilizar una contraseña más segura.
- Se restableció el usuario maestro, pero la contraseña no cumple con el requisito de complejidad de su política de contraseñas. Plantéese utilizar una contraseña más segura.

De forma predeterminada, el usuario maestro se crea con `CHECK_POLICY` y `CHECK_EXPIRATION` ajustado en `OFF`. Para aplicar la política de contraseñas al usuario maestro, debe habilitar manualmente estos marcadores para el usuario maestro tras la creación de la instancia de base de datos. Tras habilitar estos marcadores, modifique la contraseña del usuario maestro directamente en SQL Server (por ejemplo, mediante instrucciones T-SQL o SSMS) para validar la nueva contraseña con respecto a la política de contraseñas.

> **Note**
>
> Si el usuario maestro queda bloqueado, puede desbloquearlo restableciendo su contraseña mediante el comando `ModifyDBInstance`.

Modificación de la contraseña del usuario principal

Puede modificar la contraseña del usuario maestro mediante el comando ModifyDBInstance.

> **Note**
>
> Al restablecer la contraseña del usuario maestro, RDS restablece varios permisos para el usuario maestro y este puede perder algunos permisos. Si se restablece la contraseña del usuario maestro, también se desbloquea al usuario maestro si estaba bloqueado.

RDS valida la nueva contraseña del usuario maestro e intenta emitir un evento de RDS si la contraseña no cumple la política. RDS establece la contraseña incluso si no cumple la política de contraseñas.

Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3

Puede transferir archivos entre una instancia de base de datos que se ejecuta en Amazon RDS for SQL Server y un bucket de Amazon S3. Al hacer esto, puede utilizar Amazon S3 con las características de SQL Server, por ejemplo, INSERCIÓN MASIVA. Por ejemplo, puede descargar archivos .csv, .xml, .txt y de otro tipo desde Amazon S3 al host de la instancia de base de datos e importar los datos desde `D:\S3\` a la base de datos. Todos los archivos se almacenan en `D:\S3\` en la instancia de base de datos.

Se aplican las siguientes restricciones:

> **Note**
>
> El tráfico entre el host de RDS y S3 se enruta a través de los puntos de conexión de VPC en las VPC internas de RDS para todas las características de SQL Server que utilizan S3. Este tráfico no utiliza el ENI del punto de conexión de la instancia de RDS. Las políticas de bucket de S3 no pueden restringir el tráfico de RDS según las condiciones de la red.

- Los archivos de la carpeta `D:\S3` se eliminan en la réplica en espera después de una conmutación por error en instancias multi-AZ. Para obtener más información, consulte Limitaciones multi-AZ para la integración S3.
- La instancia de base de datos y el bucket de S3 deben estar en la misma región de AWS.
- Si ejecuta más de una tarea de integración de S3 a la vez, las tareas se ejecutan secuencialmente, no en paralelo.

  > **Note**
  >
  > Las tareas de integración de S3 comparten la misma cola que las tareas nativas de copia de seguridad y restauración. Como máximo, solo puede tener dos tareas en curso en cualquier momento en esta cola. Por lo tanto, dos tareas nativas de copia de seguridad y restauración bloquearán cualquier tarea de integración de S3.

- Tiene que volver a habilitar la característica de integración de S3 en las instancias restauradas. La integración de S3 no se propaga desde la instancia de origen a la instancia restaurada. Los archivos en `D:\S3` se eliminan en una instancia restaurada.

- Las descargas a la instancia de base de datos tienen un límite de 100 archivos. En otras palabras, no puede haber más de 100 archivos en `D:\S3\`.
- Sólo se admiten archivos sin extensiones de archivo o con las siguientes extensiones de archivo: .abf, .asdatabase, .bcp, .configsettings, .csv, .dat, .deploymentoptions, .deploymenttargets, .fmt, .i
  y .xmla.
- El propietario del bucket de S3 debe ser el mismo que el del rol relacionado de AWS Identity and Access Management (IAM). Por lo tanto, no se admite la integración de S3 entre cuentas.
- Además, el bucket de S3 no puede estar abierto al público.
- El tamaño de archivo para cargas de RDS a S3 está limitado a 50 GB por archivo.
- El tamaño de archivo para las descargas de S3 a RDS está limitado al máximo admitido por S3.

Temas

- Requisitos previos para la integración de RDS for SQL Server con S3
- Habilitación de la integración de RDS for SQL Server con S3
- Transferencia de archivos entre RDS for SQL Server y Amazon S3
- Descripción de los archivos de la instancia de base de datos de RDS
- Eliminación de los archivos de la instancia de base de datos de RDS
- Monitoreo del estado de una tarea de transferencia de archivos
- Cancelación de una tarea
- Limitaciones multi-AZ para la integración S3
- Desactivación de la integración de RDS for SQL Server con S3

Para obtener más información sobre cómo trabajar con archivos en Amazon S3, consulte Introducción a Amazon Simple Storage Service.

Requisitos previos para la integración de RDS for SQL Server con S3

Antes de comenzar, busque o cree el bucket de S3 que desea utilizar. También tiene que añadir los permisos para que la instancia de base de datos de RDS pueda acceder al bucket de S3. Para configurar este acceso, cree una política de IAM y un rol de IAM.

Consola

Para crear una política de IAM para acceder a Amazon S3

1. En la IAM Management Console, seleccione Policies (Políticas) en el panel de navegación.
2. Cree una nueva política y utilice la pestaña Visual editor (Editor visual) para los siguientes pasos.
3. En Service (Servicio), introduzca **S3** y, a continuación, seleccione el servicio de S3.
4. En Actions (Acciones), seleccione los siguientes elementos para conceder el acceso que requiere la instancia de base de datos:

   - `ListAllMyBuckets`: obligatorio
   - `ListBucket`: obligatorio
   - `GetBucketAcl`: obligatorio
   - `GetBucketLocation`: obligatorio
   - `GetObject` – obligatorio para descargar archivos desde S3 a `D:\S3\`
   - `PutObject`: obligatorio para cargar archivos desde `D:\S3\` a S3
   - `ListMultipartUploadParts`: obligatorio para cargar archivos desde `D:\S3\` a S3
   - `AbortMultipartUpload`: obligatorio para cargar archivos desde `D:\S3\` a S3
5. En Resources (Recursos), las opciones que aparecen varían en función de las acciones que seleccione en el paso anterior. Es posible que vea opciones para bucket, object (objeto) o para ambos. En cada una de ellas, añada el nombre de recurso de Amazon (ARN) adecuado.

   En bucket, añada el ARN del bucket que desea utilizar. Por ejemplo, si el bucket se denomina *`amzn-s3-demo-bucket`*, establezca el ARN en `arn:aws:s3:::`*`amzn-s3-demo-bucket`*.

   En object (objeto), introduzca el ARN del bucket y, a continuación, seleccione una de las siguientes opciones:

   - Para conceder acceso a todos los archivos del bucket especificado, seleccione Any (Cualquiera) en Bucket name (Nombre de bucket) y Object name (Nombre de objeto).
   - Para conceder acceso a carpetas o archivos específicos del bucket, facilite los ARN de los objetos y buckets específicos a los que desea que SQL Server acceda.
6. Siga las instrucciones de la consola hasta que termine de crear la política.

Se trata de una guía resumida para configurar una política. Para obtener instrucciones más detalladas acerca de la creación de políticas de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para crear un rol de IAM que utiliza la política de IAM del procedimiento anterior

1. En la IAM Management Console, seleccione Roles en el panel de navegación.
2. Cree un rol de IAM nuevo y seleccione las siguientes opciones a medida que aparecen en la consola:

   - Servicio de AWS
   - RDS
   - RDS – Add Role to Database (RDS: Añadir rol a la base de datos)

   A continuación, seleccione Next:Permissions (Siguiente:Permisos) en la parte inferior.
3. En Attach permissions policies (Asociar políticas de permisos), introduzca el nombre de la política de IAM que ha creado previamente. A continuación, seleccione la política de la lista.
4. Siga las instrucciones de la consola hasta que termine de crear el rol.

   Se trata de una guía resumida para configurar un rol. Si desea obtener instrucciones más detalladas acerca de la creación de roles, consulte Roles de IAM en la Guía del usuario de IAM.

AWS CLI

Para conceder a Amazon RDS acceso a un bucket de Simple Storage Service (Amazon S3), utilice el siguiente proceso:

1. Cree una política de IAM que conceda a Amazon RDS acceso a un bucket de S3.
2. Cree un rol de IAM que Amazon RDS pueda asumir en su nombre para acceder a los buckets de S3.

   Para obtener más información, vea Crear un rol para delegar permisos a un usuario de IAM en Guía del usuario de IAM.
3. Asocie la política de IAM que creó al rol de IAM creado.

Creación de la política de IAM

Incluya las acciones adecuadas para conceder el acceso que requiere la instancia de base de datos:

- `ListAllMyBuckets`: obligatorio
- `ListBucket`: obligatorio
- `GetBucketAcl`: obligatorio
- `GetBucketLocation`: obligatorio
- `GetObject` – obligatorio para descargar archivos desde S3 a `D:\S3\`
- `PutObject`: obligatorio para cargar archivos desde `D:\S3\` a S3
- `ListMultipartUploadParts`: obligatorio para cargar archivos desde `D:\S3\` a S3
- `AbortMultipartUpload`: obligatorio para cargar archivos desde `D:\S3\` a S3

1. El siguiente comando de la AWS CLI crea una política de IAM denominada `rds-s3-integration-policy` con estas opciones. Otorga acceso a un bucket denominado *`amzn-s3-demo-bucket`*.

   Example

   Para Linux, macOS o Unix:

```
aws iam create-policy \
  --policy-name rds-s3-integration-policy \
  --policy-document '{
         "Version": "2012-10-17",
         "Statement": [
             {
                 "Effect": "Allow",
                 "Action": "s3:ListAllMyBuckets",
                 "Resource": "*"
             },
             {
                 "Effect": "Allow",
                 "Action": [
                     "s3:ListBucket",
                     "s3:GetBucketAcl",
                     "s3:GetBucketLocation"
                 ],
                 "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
```

```
            },
            {
                "Effect": "Allow",
                "Action": [
                    "s3:GetObject",
                    "s3:PutObject",
                    "s3:ListMultipartUploadParts",
                    "s3:AbortMultipartUpload"
                ],
                "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/key_prefix/*"
            }
        ]
    }'
```

Para Windows:

Asegúrese de cambiar las terminaciones de las líneas a las que son compatibles con la interfaz (^ en lugar de \). Además, en Windows, tiene que escapar todas las comillas dobles con \. Para evitar tener que escapar las comillas del JSON, puede guardarlo en un archivo y transferirlo como un parámetro.

En primer lugar, cree el archivo `policy.json` con la siguiente política de permisos:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketACL",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/key_prefix/*"
        }
    ]
}
```

A continuación, utilice el siguiente comando para crear la política:

```
aws iam create-policy ^
     --policy-name rds-s3-integration-policy ^
     --policy-document file://file_path/assume_role_policy.json
```

2. Después de crear la política, anote el Nombre de recurso de Amazon (ARN) de la política. Necesita el ARN para un paso posterior.

Creación del rol de IAM

- El siguiente comando de la AWS CLI crea el rol de IAM `rds-s3-integration-role` con este fin.

  Example

  Para Linux, macOS o Unix:

```
aws iam create-role \
    --role-name rds-s3-integration-role \
    --assume-role-policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
             "Service": "rds.amazonaws.com"
           },
```

```
          "Action": "sts:AssumeRole"
        }
      ]
    }'
```

Para Windows:

Asegúrese de cambiar las terminaciones de las líneas a las que son compatibles con la interfaz (^ en lugar de \). Además, en Windows, tiene que escapar todas las comillas dobles con \. Para evitar tener que escapar las comillas del JSON, puede guardarlo en un archivo y transferirlo como un parámetro.

En primer lugar, cree el archivo `assume_role_policy.json` con la siguiente política:

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "rds.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

A continuación, utilice el siguiente comando para crear el rol de IAM:

```
aws iam create-role ^
     --role-name rds-s3-integration-role ^
     --assume-role-policy-document file://file_path/assume_role_policy.json
```

Example de utilizar la clave de contexto de condición global para crear el rol de IAM

Le recomendamos que utilice las claves de contexto de condición globales `aws:SourceArn` y `aws:SourceAccount` en las políticas basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

Puede utilizar claves de contexto de condición globales y hacer que el valor de `aws:SourceArn` contenga el ID de cuenta. En estos casos, el valor de `aws:SourceAccount` y la cuenta del valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilizan en la misma instrucción de política.

- Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
- Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En la política, asegúrese de utilizar la clave de contexto de condición global `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo de los recursos que acceden al rol. Para la integración de S3, asegúrese de incluir los ARN de la instancia de base de datos, tal y como se muestra en el siguiente ejemplo.

Para Linux, macOS o Unix:

```
aws iam create-role \
    --role-name rds-s3-integration-role \
    --assume-role-policy-document '{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
             "Service": "rds.amazonaws.com"
           },
          "Action": "sts:AssumeRole",
                "Condition": {
                    "StringEquals": {

 "aws:SourceArn":"arn:aws:rds:Region:my_account_ID:db:db_instance_identifier"
                    }
```

```
                }
            }
        ]
    }'
```

Para Windows:

Agregue la clave de contexto de condición global a `assume_role_policy.json`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "rds.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {

 "aws:SourceArn":"arn:aws:rds:Region:my_account_ID:db:db_instance_identifier"
                }
            }
        }
    ]
}
```

Para adjuntar la política de IAM al rol de IAM

- El siguiente comando de la AWS CLI asocia la política al rol denominado `rds-s3-integration-role`. Sustituya *`your-policy-arn`* por el ARN de la política anotado en el paso anterior.

  Example

  Para Linux, macOS o Unix:

```
aws iam attach-role-policy \
    --policy-arn your-policy-arn \
    --role-name rds-s3-integration-role
```

Para Windows:

```
aws iam attach-role-policy ^
    --policy-arn your-policy-arn ^
    --role-name rds-s3-integration-role
```

Habilitación de la integración de RDS for SQL Server con S3

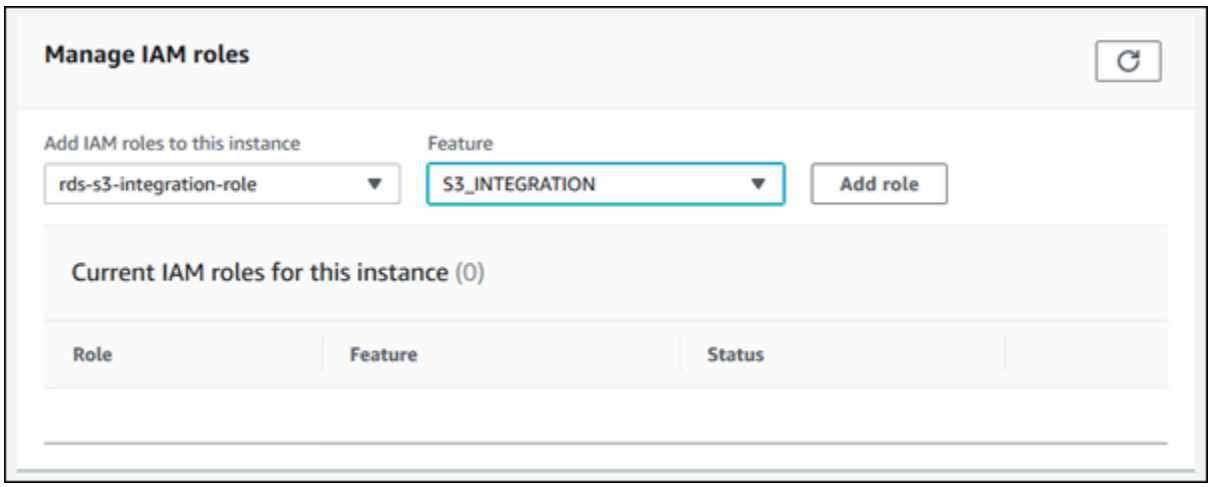
En la siguiente sección, puede encontrar cómo habilitar la integración de Amazon S3 con Amazon RDS for SQL Server. Para trabajar con la integración de S3, la instancia de base de datos debe estar asociada al rol de IAM que ha creado previamente antes de utilizar el parámetro feature-name de `S3_INTEGRATION`.

> **Note**
>
> Para añadir un rol de IAM a una instancia de base de datos, el estado de la instancia de base de datos debe ser available (disponible).

Consola

Para asociar su rol de IAM a su instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione el nombre de la instancia de base de datos de RDS for SQL Server para mostrar los detalles.
3. En la pestaña Connectivity & security (Conectividad y seguridad), en la sección Manage IAM roles (Administrar roles de IAM), seleccione el rol de IAM que desea añadir en Add IAM roles to this instance (Añadir roles de IAM a esta instancia).
4. En Feature (Característica), elija S3_INTEGRATION.



5. Seleccione Add role (Añadir rol).

AWS CLI

Para añadir el rol de IAM a la instancia de base de datos de RDS for SQL Server

- El siguiente comando AWS CLI agrega el rol de IAM a una instancia de base de datos de RDS for SQL Server denominada *mydbinstance*.

  Example

  Para Linux, macOS o:Unix

```
aws rds add-role-to-db-instance \
    --db-instance-identifier mydbinstance \
    --feature-name S3_INTEGRATION \
    --role-arn your-role-arn
```

  En:Windows

```
aws rds add-role-to-db-instance ^
    --db-instance-identifier mydbinstance ^
    --feature-name S3_INTEGRATION ^
    --role-arn your-role-arn
```

  Sustituya *your-role-arn* por el ARN del rol anotado en el paso anterior. `S3_INTEGRATION` debe especificarse para la opción `--feature-name`.

Transferencia de archivos entre RDS for SQL Server y Amazon S3

Puede utilizar los procedimientos almacenados de Amazon RDS para descargar y cargar archivos entre Amazon S3 y su instancia de base de datos de RDS. También puede utilizar los procedimientos almacenados de Amazon RDS para visualizar y eliminar los archivos de la instancia de RDS.

Los archivos que descarga desde y carga a S3 se almacenan en la carpeta `D:\S3`. Esta es la única carpeta que puede utilizar para acceder a los archivos. Puede organizar los archivos en subcarpetas, que se crean cuando incluye la carpeta de destino durante la descarga.

Algunos procedimientos almacenados necesitan que asigne un nombre de recurso de Amazon (ARN) al bucket de S3 y al archivo. El formato del ARN es `arn:aws:s3:::`*`amzn-s3-demo-bucket`*`/file_name`. Amazon S3 no requiere un número de cuenta ni una región de AWS en los ARN.

Las tareas de integración de S3 se ejecutan de forma secuencial y comparten la misma cola que las tareas de restauración y copia de seguridad nativas. Como máximo, solo puede tener dos tareas en curso en cualquier momento en esta cola. La tarea puede tardar hasta cinco minutos en comenzar a procesarse.

Descarga de archivos desde un bucket de Amazon S3 a una instancia de base de datos de SQL Server

Para descargar archivos desde un bucket de S3 a una instancia de base de datos de RDS for SQL Server, utilice el Amazon RDS procedimiento almacenado `msdb.dbo.rds_download_from_s3` con los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`@s3_arn_of_file`	NVARCHAR	–	Obligatorio	El ARN de S3 del archivo que desea descargar, por ejemplo: `arn:aws:s3::: amzn-s3-demo-bucket /mydata.csv`
`@rds_file_path`	NVARCHAR	–	Opcional	La ruta del archivo de la instancia de RDS.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				Si no se especifica, la ruta del archivo es `D:\S3\<filename in s3>`. RDS admite rutas absolutas y relativas . Si desea crear una subcarpeta, inclúyala en la ruta del archivo.
`@overwrite_file`	INT	0	Opcional	Sobrescribir el archivo existente: 0 = No sobrescribir 1 = Sobrescribir

Puede descargar archivos sin una extensión de archivo y archivos con las siguientes extensiones de archivo: .bcp, .csv, .dat, .fmt, .info, .lst, .tbl, .txt y .xml.

> **Note**
>
> Los archivos con la extensión de archivo .ispac se pueden descargar cuando SQL Server Integration Services está habilitado. Para obtener más información sobre la habilitación de SSIS, consulte SQL Server Integration Services.
> Los archivos con las siguientes extensiones de archivo se pueden descargar cuando SQL Server Analysis Services está habilitado: .abf, .asdatabase, .configsettings, .deploymentoptions, .deploymenttargets y .xmla. Para obtener más información sobre cómo habilitar SSAS, consulte SQL Server Analysis Services.

En el siguiente ejemplo se muestra el procedimiento almacenado para descargar archivos desde S3.

```
exec msdb.dbo.rds_download_from_s3
```

```
    @s3_arn_of_file='arn:aws:s3:::amzn-s3-demo-bucket/bulk_data.csv',
    @rds_file_path='D:\S3\seed_data\data.csv',
    @overwrite_file=1;
```

La operación de ejemplo `rds_download_from_s3` crea una carpeta denominada `seed_data` en `D:\S3\`, si la carpeta no existe. A continuación, el ejemplo descarga el archivo de origen `bulk_data.csv` desde S3 a un nuevo archivo denominado `data.csv` en la instancia de base de datos. Si el archivo existía previamente, se sobrescribe porque el parámetro `@overwrite_file` está establecido en 1.

Carga de archivos desde una instancia de base de datos de SQL Server a un bucket de Amazon S3

Para cargar archivos desde una instancia de base de datos de RDS for SQL Server en un bucket de S3, utilice el el Amazon RDS procedimiento almacenado `msdb.dbo.rds_upload_to_s3` con los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`@s3_arn_of_file`	NVARCHAR	–	Obligatorio	El ARN de S3 del archivo que desea crear en S3, por ejemplo: `arn:aws:s3::: amzn-s3-demo-bucket /mydata.csv`
`@rds_file_path`	NVARCHAR	–	Obligatorio	La ruta del archivo que desea cargar en S3. Se admiten rutas relativas y absolutas.
`@overwrite_file`	INT	–	Opcional	Sobrescribir el archivo existente: 0 = No sobrescribir 1 = Sobrescribir

En el siguiente ejemplo se carga el archivo denominado `data.csv` desde la ubicación especificada en `D:\S3\seed_data\` al archivo `new_data.csv` del bucket de S3 que especifica el ARN.

```
exec msdb.dbo.rds_upload_to_s3
  @rds_file_path='D:\S3\seed_data\data.csv',
  @s3_arn_of_file='arn:aws:s3:::amzn-s3-demo-bucket/new_data.csv',
  @overwrite_file=1;
```

Si el archivo existía previamente en S3, se sobrescribe porque el parámetro @overwrite_file está establecido en 1.

Descripción de los archivos de la instancia de base de datos de RDS

Para visualizar los archivos disponibles en la instancia de base de datos, utilice una función y un procedimiento almacenado. En primer lugar, ejecute el siguiente procedimiento almacenado para recopilar los detalles de los archivos que se encuentran en `D:\S3\`.

```
exec msdb.dbo.rds_gather_file_details;
```

El procedimiento almacenado devuelve el ID de la tarea. Al igual que con las otras tareas, este procedimiento almacenado se ejecuta de forma asíncrona. Cuando el estado de la tarea sea `SUCCESS`, puede utilizar el ID de la tarea en la función `rds_fn_list_file_details` para visualizar los directorios y los archivos existentes que se encuentran en D:\S3\, como se muestra a continuación.

```
SELECT * FROM msdb.dbo.rds_fn_list_file_details(TASK_ID);
```

La función `rds_fn_list_file_details` devuelve una tabla con las siguientes columnas.

Parámetro de salida	Descripción
`filepath`	Ruta absoluta del archivo (por ejemplo, `D:\S3\mydata.csv`)
`size_in_bytes`	Tamaño del archivo (en bytes)
`last_modified_utc`	Fecha y hora en formato UTC de la última modificación

Parámetro de salida	Descripción
`is_directory`	Opción que indica si el elemento es un directorio (`true`/`false`)

Eliminación de los archivos de la instancia de base de datos de RDS

Para eliminar los archivos disponibles en la instancia de base de datos, utilice el procedimiento almacenado de Amazon RDS `msdb.dbo.rds_delete_from_filesystem` con los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`@rds_file_path`	NVARCHAR	–	Obligatorio	La ruta del archivo que desea eliminar. Se admiten rutas relativas y absolutas.
`@force_delete`	INT	0	Opcional	Para eliminar un directorio, se debe incluir este indicador y establecerlo en 1. 1 = Eliminar directorio Este parámetro se ignora si va a eliminar un archivo.

Para eliminar un directorio, `@rds_file_path` debe terminar con una barra invertida (\) y `@force_delete` se debe establecer en 1.

En el siguiente ejemplo se elimina el archivo `D:\S3\delete_me.txt`.

```
exec msdb.dbo.rds_delete_from_filesystem
```

```
    @rds_file_path='D:\S3\delete_me.txt';
```

En el siguiente archivo se elimina el directorio `D:\S3\example_folder\`.

```
exec msdb.dbo.rds_delete_from_filesystem
    @rds_file_path='D:\S3\example_folder\',
    @force_delete=1;
```

Monitoreo del estado de una tarea de transferencia de archivos

Para realizar un seguimiento del estado de la tarea de integración de S3, llame a la función `rds_fn_task_status`. Tiene dos parámetros. El primer parámetro siempre debe ser `NULL` porque no se aplica a la integración de S3. El segundo parámetro acepta un ID de tarea.

Para obtener una lista de todas las tareas, establezca el primer parámetro en `NULL` y el segundo en `0`, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Para obtener una tarea específica, establezca el primer parámetro en `NULL` y el segundo en el ID de la tarea, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La función `rds_fn_task_status` devuelve la siguiente información.

Parámetro de salida	Descripción
`task_id`	El ID de la tarea.
`task_type`	En la integración de S3, las tareas pueden ser de los siguientes tipos: • `DOWNLOAD_FROM_S3` • `UPLOAD_TO_S3` • `LIST_FILES_ON_DISK` • `DELETE_FILES_ON_DISK`
`database_name`	No se aplica a las tareas de integración de S3.

Parámetro de salida	Descripción
`% complete`	El porcentaje de progreso de la tarea.
`duration(mins)`	El tiempo empleado en la tarea, en minutos.
`lifecycle`	El estado de la tarea. Los posibles estados son los siguientes: • `CREATED` – después de llamar a uno de los procedimientos almacenados de la integración de S3, se crea una tarea y el estado se establece en `CREATED`. • `IN_PROGRESS` – cuando una tarea comienza, el estado se establece en `IN_PROGRESS`. Pueden pasar hasta cinco minutos hasta que el estado cambie de `CREATED` a `IN_PROGRESS`. • `SUCCESS` – cuando una tarea se completa, el estado se establece en `SUCCESS`. • `ERROR` – si se produce un error con una tarea, el estado se establece en `ERROR`. Para obtener más información acerca del error, consulte la columna `task_info`. • `CANCEL_REQUESTED`: después de llamar a `rds_cancel_task`, el estado de la tarea se establece en `CANCEL_REQUESTED`. • `CANCELLED` – después de que se cancela una tarea correctamente, se establece su estado en `CANCELLED`.
`task_info`	Información adicional acerca de la tarea. Si se produce un error durante el procesamiento, esta columna contiene información acerca del error.

Parámetro de salida	Descripción
`last_updated`	La fecha y hora en que se actualizó por última vez el estado de la tarea.
`created_at`	La fecha y hora en que se creó la tarea.
`S3_object_arn`	El ARN del objeto de S3 desde el que se descarga o al que se carga.
`overwrite_S3_backup_file`	No se aplica a las tareas de integración de S3.
`KMS_master_key_arn`	No se aplica a las tareas de integración de S3.
`filepath`	La ruta del archivo de la instancia de base de datos de RDS.
`overwrite_file`	Una opción que indica si un archivo existente se sobrescribe.
`task_metadata`	No se aplica a las tareas de integración de S3.

Cancelación de una tarea

Para cancelar las tareas de integración de S3, utilice el procedimiento almacenado `msdb.dbo.rds_cancel_task` con el parámetro `task_id`. La eliminación y la visualización de las tareas que están en curso no se pueden cancelar. En el siguiente ejemplo se muestra una solicitud para cancelar una tarea.

```
exec msdb.dbo.rds_cancel_task @task_id = 1234;
```

Para obtener información general acerca de todas las tareas y sus ID de tarea, utilice la función `rds_fn_task_status` como se describe en Monitoreo del estado de una tarea de transferencia de archivos.

Limitaciones multi-AZ para la integración S3

En las instancias multi-AZ, los archivos de la carpeta `D:\S3` se eliminan en la réplica en espera después de una conmutación por error. Se puede planificar una conmutación por error, por ejemplo,

durante las modificaciones de instancia de base de datos, como cambiar la clase de instancia o actualizar la versión del motor. O una conmutación por error puede no estar planificada, durante una interrupción del servicio principal.

> **Note**
>
> No recomendamos usar la carpeta `D:\S3` para el almacenamiento de archivos. La práctica recomendada consiste en cargar archivos creados en Amazon S3 para hacerlos duraderos y descargar archivos cuando tenga que importar datos.

Para determinar la hora de la última conmutación por error, puede utilizar el procedimiento almacenado `msdb.dbo.rds_failover_time`. Para obtener más información, consulte Determinación de la hora de la última conmutación por error de Amazon RDS para SQL Server.

Example de No hay conmutación por error reciente

Este ejemplo muestra el resultado cuando no hay conmutación por error reciente en los registros de errores. No se ha producido ninguna conmutación por error desde 2020-04-29 23:59:00 .01.

Por lo tanto, todos los archivos descargados después de esa hora que no se hayan eliminado mediante el procedimiento almacenado `rds_delete_from_filesystem` siguen siendo accesibles en el alojamiento actual. Los archivos descargados antes de esa hora también pueden estar disponibles.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	null

Example de Conmutación por error reciente

Este ejemplo muestra el resultado cuando hay una conmutación por error en los registros de errores. La conmutación por error más reciente fue en 2020-05-05 18:57:51 .89.

Todos los archivos descargados después de esa hora que no se hayan eliminado mediante el procedimiento almacenado `rds_delete_from_filesystem` siguen siendo accesibles en el alojamiento actual.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	2020-05-05 18:57:51.8900000

Desactivación de la integración de RDS for SQL Server con S3

A continuación puede encontrar cómo deshabilitar la integración de Amazon S3 con Amazon RDS for SQL Server. Los archivos de `D:\S3\` no se eliminan al deshabilitar la integración de S3.

> **Note**
>
> Para eliminar un rol de IAM de una instancia de base de datos, el estado de la instancia de base de datos debe ser `available`.

Consola

Para desvincular el rol de IAM de la instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione el nombre de la instancia de base de datos de RDS for SQL Server para mostrar los detalles.
3. En la pestaña Connectivity & security (Conectividad y seguridad), en la sección Manage IAM roles (Administrar roles de IAM), seleccione el rol de IAM que desea eliminar.
4. Elija Eliminar.

AWS CLI

Para eliminar el rol de IAM de la instancia de base de datos de RDS for SQL Server

- El siguiente comando AWS CLI elimina el rol de IAM de una instancia de base de datos RDS for SQL Server denominada *mydbinstance*.

  Example

  Para Linux, macOS o:Unix

```
aws rds remove-role-from-db-instance \
    --db-instance-identifier mydbinstance \
    --feature-name S3_INTEGRATION \
    --role-arn your-role-arn
```

En:Windows

```
aws rds remove-role-from-db-instance ^
    --db-instance-identifier mydbinstance ^
    --feature-name S3_INTEGRATION ^
    --role-arn your-role-arn
```

Sustituya *your-role-arn* por el ARN del rol de IAM adecuado en la opción `--feature-name`.

Uso de Database Mail en Amazon RDS for SQL Server

Puede utilizar Database Mail para enviar mensajes de correo electrónico a los usuarios desde su instancia de base de datos Amazon RDS en SQL Server. Los mensajes pueden contener archivos y resultados de consulta. Database Mail incluye los siguientes componentes:

- Objetos de configuración y seguridad – Estos objetos crean perfiles y cuentas y se almacenan en la base de datos `msdb`.
- Objetos de mensajería – Estos objetos incluyen el procedimiento almacenado sp_send_dbmail utilizado para enviar mensajes y estructuras de datos que contienen información sobre los mensajes. Están almacenados en la base de datos `msdb`.
- Objetos de registro y auditoría – Database Mail escribe información de registro en la base de datos `msdb` y en el registro de eventos de aplicación de Microsoft Windows.
- El ejecutable de Database Mail – `DatabaseMail.exe` lee desde una cola en la base de datos `msdb` y envía mensajes de correo electrónico.

RDS es compatible con Database Mail para todas las versiones de SQL Server en las ediciones Web, Estándar y Enterprise.

Limitaciones

Las siguientes limitaciones se aplican al uso de Database Mail en su instancia de base de datos de SQL Server:

- Database Mail no es compatible con la edición SQL Server Express.
- La modificación de los parámetros de la configuración de Database Mail no es compatible. Para ver los valores preestablecidos (predeterminados), utilice el procedimiento almacenado sysmail_help_configure_sp.
- Los archivos adjuntos no son totalmente compatibles. Para obtener más información, consulte Trabajar con archivos adjuntos.
- El tamaño máximo del archivo adjunto es de 1 MB.
- Database Mail requiere configuración adicional en las instancias de base de datos Multi-AZ. Para obtener más información, consulte Consideraciones para implementaciones Multi-AZ.
- La configuración del Agente SQL Server para enviar mensajes de correo electrónico a operadores predefinidos no es compatible.

Habilitación de Database Mail

Utilice el siguiente proceso para habilitar Database Mail para su instancia de base de datos:

1. Cree un nuevo grupo de parámetros.
2. Modifique el grupo de parámetros para establecer el parámetro `database mail xps` en 1.
3. Asocie el nuevo grupo de parámetros a la instancia de base de datos.

Creación del grupo de parámetros para Database Mail

Cree un grupo de parámetros para el parámetro `database mail xps` que corresponde a la edición y versión de SQL Server de su instancia de base de datos.

> **Note**
>
> También puede modificar un grupo de parámetros existente. Siga el procedimiento indicado en Modificación del parámetro que habilita Database Mail.

Consola

En el ejemplo siguiente se crea un grupo de parámetros para SQL Server Standard Edition 2016.

Para crear el grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija Create parameter group.
4. En el panel Create parameter group (Crear grupo de parámetros), haga lo siguiente:
   a. En Familia de grupos de parámetros, elija sqlserver-se-13.0.
   b. En Nombre de grupo, escriba un identificador para el grupo de parámetros, como **`dbmail-sqlserver-se-13`**.
   c. En Descripción, escriba **`Database Mail XPs`**.
5. Elija Create (Crear).

CLI

En el ejemplo siguiente se crea un grupo de parámetros para SQL Server Standard Edition 2016.

Para crear el grupo de parámetros

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-db-parameter-group \
    --db-parameter-group-name dbmail-sqlserver-se-13 \
    --db-parameter-group-family "sqlserver-se-13.0" \
    --description "Database Mail XPs"
```

  En:Windows

```
aws rds create-db-parameter-group ^
    --db-parameter-group-name dbmail-sqlserver-se-13 ^
    --db-parameter-group-family "sqlserver-se-13.0" ^
    --description "Database Mail XPs"
```

Modificación del parámetro que habilita Database Mail

Modifique el parámetro `database mail xps` en el grupo de parámetros que corresponde a la edición y la versión de SQL Server de su instancia de base de datos.

Para habilitar Database Mail, establezca el parámetro `database mail xps` en 1.

Consola

En el ejemplo siguiente se modifica el grupo de parámetros que ha creado para SQL Server Standard Edition 2016.

Para modificar el grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).

3. Elija el grupo de parámetros, como ssis-sqlserver-se-13.
4. En Parámetros, filtre la lista de parámetros para **`mail`**.
5. Elija database mail xps (procedimientos almacenados extendidos [XP] de Database Mail).
6. Elija Edit parameters (Editar parámetros).
7. Escriba **1**.
8. Elija Guardar cambios.

CLI

En el ejemplo siguiente se modifica el grupo de parámetros que ha creado para SQL Server Standard Edition 2016.

Para modificar el grupo de parámetros

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name dbmail-sqlserver-se-13 \
    --parameters "ParameterName='database mail
 xps',ParameterValue=1,ApplyMethod=immediate"
```

  En:Windows

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name dbmail-sqlserver-se-13 ^
    --parameters "ParameterName='database mail
 xps',ParameterValue=1,ApplyMethod=immediate"
```

Asociación del grupo de parámetros con la instancia de base de datos

Puede utilizar la AWS Management Console o la AWS CLI para asociar el grupo de parámetros de Database Mail con la instancia de base de datos.

Consola

Puede asociar el grupo de parámetros de Database Mail con una instancia de base de datos nueva o existente.

- Para una nueva instancia de base de datos, asóciela cuando lance la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, asóciela modificando la instancia. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

CLI

Puede asociar el grupo de parámetros de Database Mail con una instancia de base de datos nueva o existente.

Para crear una instancia de base de datos con el grupo de parámetros de Database Mail

- Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de parámetros.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 13.00.5426.0.v1 \
    --allocated-storage 100 \
    --manage-master-user-password \
    --master-username admin \
    --storage-type gp2 \
    --license-model li
    --db-parameter-group-name dbmail-sqlserver-se-13
```

  En:Windows

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-instance-class db.m5.2xlarge ^
```

```
    --engine sqlserver-se ^
    --engine-version 13.00.5426.0.v1 ^
    --allocated-storage 100 ^
    --manage-master-user-password ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --db-parameter-group-name dbmail-sqlserver-se-13
```

Para modificar una instancia de base de datos y asociar el grupo de parámetros de Database Mail

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --db-parameter-group-name dbmail-sqlserver-se-13 \
    --apply-immediately
```

  En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-parameter-group-name dbmail-sqlserver-se-13 ^
    --apply-immediately
```

Configuración de Database Mail

Realice las siguientes tareas para configurar Database Mail:

1. Cree el perfil de Database Mail.
2. Cree la cuenta de Database Mail.
3. Agregue la cuenta de Database Mail al perfil de Database Mail.
4. Agregue usuarios al perfil de Database Mail.

> **Note**
>
> Para configurar Database Mail, asegúrese de que tenga permiso `execute` sobre los procedimientos almacenados en la base de datos `msdb`.

Creación del perfil de Database Mail

Para crear el perfil de Database Mail, utilice el procedimiento almacenado sysmail_add_profile_sp. En el ejemplo siguiente se crea un perfil denominado `Notifications`.

Para crear el perfil

- Utilice la siguiente instrucción SQL.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_profile_sp
    @profile_name         = 'Notifications',
    @description          = 'Profile used for sending outgoing notifications using
 Amazon SES.';
GO
```

Creación de la cuenta de Database Mail

Para crear la cuenta de Database Mail, utilice el procedimiento almacenado sysmail_add_account_sp. En el ejemplo siguiente, se crea una cuenta denominada SES en una instancia de base de datos de RDS para SQL Server en una VPC privada mediante Amazon Simple Email Service.

Para utilizar Amazon SES se requieren los siguientes parámetros:

- `@email_address`: Una identidad verificada de Amazon SES. Para obtener más información, consulte Verificación de identidades en Amazon SES.
- `@mailserver_name`: Un punto de enlace SMTP de Amazon SES. Para obtener más información, consulte Conexión a un punto de enlace SMTP de Amazon SES.
- `@username`: Un nombre de usuario de SMTP de Amazon SES. Para obtener más información, consulte Obtención de las credenciales SMTP de Amazon SES.

No utilice un nombre de usuario AWS Identity and Access Management.

- `@password`: Una contraseña SMTP de Amazon SES. Para obtener más información, consulte Obtención de las credenciales SMTP de Amazon SES.

Para crear la cuenta

- Utilice la siguiente instrucción SQL.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_account_sp
    @account_name        = 'SES',
    @description         = 'Mail account for sending outgoing notifications.',
    @email_address       = 'nobody@example.com',
    @display_name        = 'Automated Mailer',
    @mailserver_name     = 'vpce-0a1b2c3d4e5f-01234567.email-smtp.us-
west-2.vpce.amazonaws.com',
    @port                = 587,
    @enable_ssl          = 1,
    @username            = 'Smtp_Username',
    @password            = 'Smtp_Password';
GO
```

> **Note**
>
> Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

Adición de la cuenta de Database Mail al perfil de Database Mail

Para agregar la cuenta de Database Mail al perfil de Database Mail, utilice el procedimiento almacenado sysmail_add_profileaccount_sp. En el ejemplo siguiente se agrega la cuenta SES al perfil `Notifications`.

Para agregar la cuenta al perfil

- Utilice la siguiente instrucción SQL.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_profileaccount_sp
    @profile_name        = 'Notifications',
    @account_name        = 'SES',
    @sequence_number     = 1;
GO
```

Adición de usuarios al perfil de Database Mail

Para conceder permiso a una entidad principal de base de datos `msdb` para utilizar un perfil de Database Mail, utilice el procedimiento almacenado sysmail_add_principalprofile_sp. Una entidad principal es una entidad que puede solicitar recursos de SQL Server. La entidad principal de base de datos debe asignarse a un usuario de autenticación de SQL Server, un usuario de autenticación de Windows o un grupo de autenticación de Windows.

En el ejemplo siguiente se concede acceso público al perfil `Notifications`.

Para agregar un usuario al perfil

- Utilice la siguiente instrucción SQL.

```
USE msdb
GO

EXECUTE msdb.dbo.sysmail_add_principalprofile_sp
    @profile_name       = 'Notifications',
    @principal_name     = 'public',
    @is_default         = 1;
GO
```

Procedimientos y funciones almacenados de Amazon RDS para Database Mail

Microsoft proporciona procedimientos almacenados para usar Database Mail, como crear, enumerar, actualizar y eliminar cuentas y perfiles. Además, RDS provee los procedimientos almacenados y las funciones almacenadas para Database Mail que se muestran en la tabla siguiente.

Procedimiento/Función	Descripción
rds_fn_sysmail_allitems	Muestra los mensajes enviados, incluidos los enviados por otros usuarios.
rds_fn_sysmail_event_log	Muestra eventos, incluidos los de mensajes enviados por otros usuarios.
rds_fn_sysmail_mailattachments	Muestra archivos adjuntos, incluidos los de los mensajes enviados por otros usuarios.
rds_sysmail_control	Inicia y detiene la cola de correo (proceso DatabaseMail.exe).
rds_sysmail_delete_mailitems_sp	Elimina los mensajes de correo electrónico enviados por todos los usuarios de las tablas internas de Database Mail.

Envío de mensajes de correo electrónico con Database Mail

Utilice el procedimiento almacenado sp_send_dbmail para enviar mensajes de correo electrónico mediante Database Mail.

Uso

```
EXEC msdb.dbo.sp_send_dbmail
@profile_name = 'profile_name',
@recipients = 'recipient1@example.com[; recipient2; ... recipientn]',
@subject = 'subject',
@body = 'message_body',
[@body_format = 'HTML'],
[@file_attachments = 'file_path1; file_path2; ... file_pathn'],
[@query = 'SQL_query'],
[@attach_query_result_as_file = 0|1]';
```

Se requieren los siguientes parámetros:

- `@profile_name` – El nombre del perfil de Database Mail desde el que se va a enviar el mensaje.
- `@recipients` – La lista delimitada por punto y coma de direcciones de correo electrónico a las que enviar el mensaje.
- `@subject` – El asunto del mensaje.

- `@body` – El cuerpo del mensaje. También puede usar una variable declarada como cuerpo.

Los siguientes parámetros son opcionales:

- `@body_format` – Este parámetro se utiliza con una variable declarada para enviar un correo electrónico en formato HTML.
- `@file_attachments` – La lista delimitada por punto y coma de archivos adjuntos de mensajes. Las rutas de archivo deben ser rutas absolutas.
- `@query` – Una consulta SQL que se va a ejecutar. Los resultados de la consulta se pueden adjuntar como un archivo o incluirse en el cuerpo del mensaje.
- `@attach_query_result_as_file` – Si se debe adjuntar el resultado de la consulta como un archivo. Establezca en 0 para no, 1 para sí. El valor predeterminado es 0.

Ejemplos

Los ejemplos siguientes muestran cómo enviar mensajes de correo electrónico.

Example de enviar un mensaje a un único destinatario

```
USE msdb
GO

EXEC msdb.dbo.sp_send_dbmail
     @profile_name       = 'Notifications',
     @recipients         = 'nobody@example.com',
     @subject            = 'Automated DBMail message - 1',
     @body               = 'Database Mail configuration was successful.';
GO
```

Example de enviar un mensaje a varios destinatarios

```
USE msdb
GO

EXEC msdb.dbo.sp_send_dbmail
     @profile_name       = 'Notifications',
     @recipients         = 'recipient1@example.com;recipient2@example.com',
     @subject            = 'Automated DBMail message - 2',
     @body               = 'This is a message.';
```

```
GO
```

Example de enviar un resultado de consulta SQL como un archivo adjunto

```
USE msdb
GO

EXEC msdb.dbo.sp_send_dbmail
     @profile_name       = 'Notifications',
     @recipients         = 'nobody@example.com',
     @subject            = 'Test SQL query',
     @body               = 'This is a SQL query test.',
     @query              = 'SELECT * FROM abc.dbo.test',
     @attach_query_result_as_file = 1;
GO
```

Example de enviar un mensaje en formato HTML

```
USE msdb
GO

DECLARE @HTML_Body as NVARCHAR(500) = 'Hi, <h4> Heading </h4> </br> See the report. <b>
 Regards </b>';

EXEC msdb.dbo.sp_send_dbmail
     @profile_name       = 'Notifications',
     @recipients         = 'nobody@example.com',
     @subject            = 'Test HTML message',
     @body               = @HTML_Body,
     @body_format        = 'HTML';
GO
```

Example de enviar un mensaje mediante un desencadenador cuando se produce un evento específico en la base de datos

```
USE AdventureWorks2017
GO
IF OBJECT_ID ('Production.iProductNotification', 'TR') IS NOT NULL
DROP TRIGGER Purchasing.iProductNotification
GO
```

```
CREATE TRIGGER iProductNotification ON Production.Product
   FOR INSERT
   AS
   DECLARE @ProductInformation nvarchar(255);
   SELECT
   @ProductInformation = 'A new product, ' + Name + ', is now available for $' +
 CAST(StandardCost AS nvarchar(20)) + '!'
   FROM INSERTED i;

EXEC msdb.dbo.sp_send_dbmail
     @profile_name       = 'Notifications',
     @recipients         = 'nobody@example.com',
     @subject            = 'New product information',
     @body               = @ProductInformation;
GO
```

Visualización de mensajes, registros y archivos adjuntos

Utilice procedimientos almacenados de RDS para ver mensajes, registros de eventos y archivos adjuntos.

Para ver todos los mensajes de correo electrónico

- Utilice la siguiente consulta SQL.

```
SELECT * FROM msdb.dbo.rds_fn_sysmail_allitems(); --WHERE sent_status='sent' or
 'failed' or 'unsent'
```

Para ver todos los registros de eventos de correo electrónico

- Utilice la siguiente consulta SQL.

```
SELECT * FROM msdb.dbo.rds_fn_sysmail_event_log();
```

Para ver todos los archivos adjuntos de correo electrónico

- Utilice la siguiente consulta SQL.

```
SELECT * FROM msdb.dbo.rds_fn_sysmail_mailattachments();
```

Eliminación de mensajes

Utilice el procedimiento almacenado `rds_sysmail_delete_mailitems_sp` para eliminar mensajes.

> **Note**
>
> RDS elimina automáticamente los elementos de la tabla de correo cuando los datos del historial de DBMail alcanzan un tamaño de 1 GB, con un periodo de retención de al menos 24 horas.
> Si desea conservar los elementos de correo durante un periodo más largo, puede archivarlos. Para obtener más información, consulte Crear un trabajo de agente SQL Server para archivar mensajes y registros de eventos de Database Mail en la documentación de Microsoft.

Para eliminar todos los mensajes de correo electrónico

- Utilice la siguiente instrucción SQL.

```
DECLARE @GETDATE datetime
SET @GETDATE = GETDATE();
EXECUTE msdb.dbo.rds_sysmail_delete_mailitems_sp @sent_before = @GETDATE;
GO
```

Para eliminar todos los mensajes de correo electrónico con un estado determinado

- Utilice la siguiente instrucción SQL para eliminar todos los mensajes fallidos.

```
DECLARE @GETDATE datetime
SET @GETDATE = GETDATE();
EXECUTE msdb.dbo.rds_sysmail_delete_mailitems_sp @sent_status = 'failed';
GO
```

Inicio y detención de la cola de correo

Siga las instrucciones que se indican a continuación para iniciar y detener la cola de correo de la base de datos:

Temas

- Inicio de la cola de correo
- Detención de la cola de correo

Inicio de la cola de correo

Utilice el procedimiento almacenado `rds_sysmail_control` para iniciar el proceso de Database Mail.

> **Note**
>
> Al habilitar Database Mail, se inicia automáticamente la cola de correo.

Para iniciar la cola de correo

- Utilice la siguiente instrucción SQL.

```
EXECUTE msdb.dbo.rds_sysmail_control start;
GO
```

Detención de la cola de correo

Utilice el procedimiento almacenado `rds_sysmail_control` para detener el proceso de Database Mail.

Para detener la cola de correo

- Utilice la siguiente instrucción SQL.

```
EXECUTE msdb.dbo.rds_sysmail_control stop;
GO
```

Trabajar con archivos adjuntos

Las siguientes extensiones de archivos adjuntos no son compatibles con los mensajes de Database Mail de RDS en SQL

Server: .ade, .adp, .apk, .appx, .appxbundle, .bat, .bak, .cab, .chm, .cmd, .com, .cpl, .dll, .dmg, .exe, .hta, .inf y .wsh.

Database Mail utiliza el contexto de seguridad de Microsoft Windows del usuario actual para controlar el acceso a los archivos. Los usuarios que inician sesión con la autenticación de SQL Server no pueden adjuntar archivos mediante el parámetro `@file_attachments` con el procedimiento almacenado `sp_send_dbmail`. Windows no permite que SQL Server proporcione credenciales de un equipo remoto a otro equipo remoto. Por lo tanto, Database Mail no puede adjuntar archivos desde un recurso compartido de red cuando el comando se ejecuta desde un equipo distinto del equipo que ejecuta SQL Server.

Sin embargo, usted puede utilizar trabajos del agente SQL Server para adjuntar archivos. Para obtener más información sobre el Agente SQL Server, consulte Uso del Agente SQL Server para Amazon RDS y Agente SQL Server en la documentación de Microsoft.

Consideraciones para implementaciones Multi-AZ

Al configurar Database Mail en una instancia de base de datos Multi-AZ, la configuración no se propaga automáticamente a la secundaria. Se recomienda convertir la instancia Multi-AZ en una instancia Single-AZ, configurar Database Mail y, a continuación, convertir la instancia de base de datos de nuevo a Multi-AZ. Entonces, tanto el nodo primario como el secundario tienen la configuración de Database Mail.

Si crea una réplica de lectura desde su instancia Multi-AZ que tiene Database Mail configurado, la réplica hereda la configuración, pero sin la contraseña del servidor de protocolo simple de transferencia de correo (SMTP). Actualice la cuenta de Database Mail con la contraseña.

Eliminar la restricción SMTP (puerto 25)

De forma predeterminada, AWS bloquea el tráfico saliente en SMTP (puerto 25) para las instancias de base de datos de RDS para SQL Server. Esto se hace para evitar el spam según las políticas del propietario de la interfaz de red elástica. Puede eliminar esta restricción si es necesario. Para obtener más información, consulte ¿Cómo puedo eliminar la restricción en el puerto 25 de mi instancia de Amazon EC2 o de la función de Lambda?.

Soporte del almacén de instancias para la base de datos tempdb en Amazon RDS for SQL Server

El almacén de instancias ofrece un almacenamiento de nivel de bloques temporal para la instancia de base de datos. Este almacenamiento se encuentra en discos que están conectados físicamente al equipo host. Estos discos tienen almacenamiento de instancias de memoria rápida no volátil (NVMe) basado en unidades de estado sólido (SSD). Este almacenamiento está optimizado para una latencia baja, un rendimiento de E/S aleatorio muy alto y un alto rendimiento de lectura secuencial.

Al colocar archivos de datos `tempdb` y archivos de registro `tempdb` en el almacén de instancias, se pueden lograr latencias de lectura y escritura inferiores en comparación con el almacenamiento estándar basado en Amazon EBS.

> **Note**
>
> Los archivos de base de datos de SQL Server y los archivos de registro de base de datos no se colocan en el almacén de instancias.

Habilitación del almacén de instancias

Cuando RDS aprovisiona instancias de base de datos con una de las siguientes clases de instancia, la base de datos `tempdb` se coloca automáticamente en el almacén de instancias:

- db.m5d
- db.r5d
- db.x2iedn

Para habilitar el almacén de instancias, realice una de las acciones siguientes:

- Cree una instancia de base de datos de SQL Server con uno de estos tipos de instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de SQL Server existente para utilizar una de ellas. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

El almacén de instancias está disponible en todas las regiones de AWS donde se admite uno o más de estos tipos de instancia. Para obtener más información sobre las clases de instancia db.m5d y db.r5d, consulte Clases de instancia de base de datos de . Para obtener más información sobre las clases de instancia admitidas por Amazon RDS for SQL Server, consulte Compatibilidad con clases de instancia de base de datos para Microsoft SQL Server.

Consideraciones sobre la ubicación y el tamaño de los archivos

En instancias sin un almacén de instancias, RDS almacena los datos tempdb y archivos de registros en el directorio D:\rdsdbdata\DATA. Ambos archivos comienzan en 8 MB de forma predeterminada.

En instancias con un almacén de instancias, RDS almacena los datos tempdb y archivos de registros en el directorio T:\rdsdbdata\DATA.

Cuando tempdb tiene solo un archivo de datos (tempdb.mdf) y un archivo de registro (templog.ldf), templog.ldf comienza en 8 MB de forma predeterminada y tempdb.mdf comienza al 80 % o más de la capacidad de almacenamiento de la instancia. El veinte por ciento de la capacidad de almacenamiento o 200 GB, lo que sea menor, se mantiene libre para comenzar. Múltiples archivos de datos tempdb dividen el 80 % de espacio en disco de manera uniforme, mientras que los archivos de registro siempre poseen un tamaño inicial de 8 MB.

Por ejemplo, si se modifica la clase de instancia de base de datos de db.m5.2xlarge a db.m5d.2xlarge, el tamaño de los archivos de datos tempdb aumentan de 8 MB cada uno a un total de 234 GB.

> **Note**
>
> Además de los datos y archivos de registro tempdb en el almacén de instancias (T:\rdsdbdata\DATA), aún se pueden crear datos y archivos de registro tempdb adicionales en el volumen de datos (D:\rdsdbdata\DATA). Esos archivos siempre tienen un tamaño inicial de 8 MB.

Consideraciones sobre copias de seguridad

Es posible que deba retener las copias de seguridad durante largos periodos, lo que hará que incurra en costos a lo largo del tiempo. Los bloques de registros y datos tempdb pueden cambiar muy a

menudo en función de la carga de trabajo. Esto puede aumentar considerablemente el tamaño de la instantánea de base de datos.

Cuando `tempdb` se encuentra en el almacén de instancias, las instantáneas no incluyen archivos temporales. Esto significa que los tamaños de instantáneas son más pequeños y consumen menos de la asignación de copia de seguridad gratuita en comparación con el almacenamiento solo para EBS.

Errores de disco lleno

Si utiliza todo el espacio disponible en el almacén de instancias, es posible que reciba errores como el siguiente:

- The transaction log for database 'tempdb' is full due to 'ACTIVE_TRANSACTION' (El registro de transacciones para la base de datos 'tempdb' está lleno debido a 'ACTIVE_TRANSACTION').
- No se pudo asignar espacio para el objeto "dbo.SORT temporary run storage: 140738941419520" en la base de datos "tempdb" porque el grupo de archivos "PRIMARY" está lleno. Cree espacio en el disco al eliminar archivos innecesarios, borrar objetos en el grupo de archivos, agregar archivos adicionales al grupo de archivos o configurar el crecimiento automático para los archivos existentes en el grupo de archivos.

Puede realizar una o varias de las siguientes acciones cuando el almacén de instancias está lleno:

- Ajuste la carga de trabajo o la forma en que utiliza `tempdb`.
- Escale verticalmente para usar una clase de instancia de base de datos con más almacenamiento NVMe.
- Deje de usar el almacén de instancias y utilice una clase de instancia con almacenamiento solo para EBS.
- Utilice un modo combinado al agregar datos secundarios o archivos de registro para `tempdb` en el volumen de EBS.

Eliminación del almacén de instancias

Para quitar el almacén de instancias, modifique la instancia de base de datos de SQL Server para utilizar un tipo de instancia que no admita el almacén de instancias, como as db.m5, db.r5 o db.x1e.

> **Note**
>
> Al quitar el almacén de instancias, los archivos temporales se mueven al directorio `D:\rdsdbdata\DATA` y reducen su tamaño a 8 MB.

Uso de eventos extendidos con Amazon RDS for Microsoft SQL Server

Puede utilizar eventos extendidos en Microsoft SQL Server para capturar información de depuración y solución de problemas para Amazon RDS for SQL Server. Los eventos extendidos reemplazan SQL Trace y Server Profiler, los cuales Microsoft ha dado de baja. Los eventos extendidos son similares a los trazados del generador de perfiles, pero con un control más granular sobre los eventos que se rastrean. Los eventos extendidos son compatibles con las versiones de SQL Server 2016 y posteriores en Amazon RDS. Para obtener más información, consulte Información general de eventos extendidos en la documentación de Microsoft.

Los eventos extendidos se activan automáticamente para los usuarios con privilegios de usuario maestro en Amazon RDS for SQL Server.

Temas

- Limitaciones y recomendaciones
- Configuración de eventos extendidos en RDS for SQL Server
- Consideraciones para implementaciones Multi-AZ
- Consultar archivos de eventos extendidos

Limitaciones y recomendaciones

Al utilizar eventos extendidos en RDS for SQL Server, se aplican las siguientes limitaciones:

- Los eventos extendidos solo se admiten para las ediciones Enterprise y Standard.
- No puede modificar las sesiones de eventos extendidos predeterminadas.
- Asegúrese de establecer el modo de partición de memoria de sesión en `NONE`.
- El modo de retención de eventos de sesión puede ser `ALLOW_SINGLE_EVENT_LOSS` o `ALLOW_MULTIPLE_EVENT_LOSS`.
- No se admiten los destinos de seguimiento de eventos para Windows (ETW).
- Asegúrese de que los destinos de los archivos estén en el directorio `D:\rdsdbdata\log`.
- Para destinos coincidentes de pares, establezca la propiedad `respond_to_memory_pressure` en `1`.
- La memoria de destino del búfer de anillo no puede ser superior a 4 MB.
- No se admiten las siguientes acciones:
  - `debug_break`

- `create_dump_all_threads`
- `create_dump_single_threads`

- El evento `rpc_completed` se admite en las siguientes versiones y versiones posteriores: 15.0.4083.2, 14.0.3370.1, 13.0.5865.1, 12.0.6433.1, 11.0.7507.2.

Configuración de eventos extendidos en RDS for SQL Server

En RDS for SQL Server, puede configurar los valores de ciertos parámetros de sesiones de eventos extendidos. En la siguiente tabla, se describen los parámetros configurables.

Nombre del parámetro	Descripción
`xe_session_max_memory`	Especifica la cantidad máxima de memoria que se asigna eventos. Este valor corresponde a la configuración `max_`
`xe_session_max_event_size`	Especifica el tamaño máximo de memoria permitido para configuración `max_event_size` de la sesión de evento
`xe_session_max_dispatch_latency`	Especifica la cantidad de tiempo que los eventos se alma distribuyan a destinos de sesión de eventos extendidos. E `tch_latency` de la sesión de evento.
`xe_file_target_size`	Especifica el tamaño máximo del destino del archivo. Est `size` del destino del archivo.
`xe_file_retention`	Especifica el tiempo de retención en días para los archivo sesiones de eventos.

> **Note**
>
> Si `xe_file_retention` se establece en cero, los archivos.xel se quitarán automáticamente después de que SQL Server libere el bloqueo de estos archivos. El bloqueo se libera cada vez que un archivo.xel alcanza el límite de tamaño establecido en `xe_file_target_size`.

Puede utilizar el procedimiento `rdsadmin.dbo.rds_show_configuration` almacenado para mostrar los valores actuales de estos parámetros. Por ejemplo, utilice la siguiente instrucción SQL para ver la configuración actual de `xe_session_max_memory`.

```
exec rdsadmin.dbo.rds_show_configuration 'xe_session_max_memory'
```

Puede utilizar el procedimiento `rdsadmin.dbo.rds_set_configuration` almacenado para modificarlos. Por ejemplo, utilice la siguiente instrucción SQL para establecer `xe_session_max_memory` en 4 MB.

```
exec rdsadmin.dbo.rds_set_configuration 'xe_session_max_memory', 4
```

Consideraciones para implementaciones Multi-AZ

Cuando crea una sesión de evento extendida en una instancia de base de datos principal, no se propaga a la réplica en espera. Puede conmutar por error y crear la sesión de evento extendida en la nueva instancia de base de datos principal. También puede quitar y volver a agregar la configuración Multi-AZ para propagar la sesión de eventos extendida a la réplica en espera. RDS detiene todas las sesiones de eventos extendidos no predeterminadas en la réplica en espera, de modo que estas sesiones no consumen recursos en el modo de espera. Debido a esto, después de que una réplica en espera se convierta en la instancia de base de datos principal, asegúrese de iniciar manualmente las sesiones de evento extendidas en la nueva instancia primaria.

> **Note**
>
> Este enfoque se aplica tanto a los grupos de disponibilidad siempre activa como a la creación de reflejo de bases de datos.

También puede utilizar un trabajo de SQL Server Agent para realizar un seguimiento de la réplica en espera e iniciar las sesiones si el modo en espera se convierte en el principal. Por ejemplo, utilice la siguiente consulta en el paso de trabajo del Agente SQL Server para reiniciar sesiones de eventos en una instancia de base de datos principal.

```
BEGIN
    IF (DATABASEPROPERTYEX('rdsadmin','Updateability')='READ_WRITE'
    AND DATABASEPROPERTYEX('rdsadmin','status')='ONLINE'
    AND (DATABASEPROPERTYEX('rdsadmin','Collation') IS NOT NULL OR
 DATABASEPROPERTYEX('rdsadmin','IsAutoClose')=1)
```

```
    )
    BEGIN
        IF NOT EXISTS (SELECT 1 FROM sys.dm_xe_sessions WHERE name='xe1')
            ALTER EVENT SESSION xe1 ON SERVER STATE=START
        IF NOT EXISTS (SELECT 1 FROM sys.dm_xe_sessions WHERE name='xe2')
            ALTER EVENT SESSION xe2 ON SERVER STATE=START
    END
END
```

Esta consulta reinicia las sesiones de eventos `xe1` y `xe2` en una instancia de base de datos principal si estas sesiones están en un estado detenido. También puede agregar una programación con un intervalo conveniente a esta consulta.

Consultar archivos de eventos extendidos

Puede utilizar SQL Server Management Studio o la función `sys.fn_xe_file_target_read_file` para ver datos de eventos extendidos que utilizan destinos de archivo. Para obtener más información sobre esta función, consulte sys.fn_xe_file_target_read_file (Transact-SQL) en la documentación de Microsoft.

Los destinos de archivos de eventos extendidos solo pueden escribir archivos en el directorio `D:\rdsdbdata\log` en RDS for SQL Server.

Como ejemplo, utilice la siguiente consulta SQL para enumerar el contenido de todos los archivos de sesiones de eventos extendidos cuyos nombres comiencen por `xe`.

```
SELECT * FROM sys.fn_xe_file_target_read_file('d:\rdsdbdata\log\xe*', null,null,null);
```

Acceso a las copias de seguridad del registro de transacciones con RDS para SQL Server

Al tener acceso a las copias de seguridad del registro de transacciones para RDS para SQL Server, puede enumerar los archivos de copia de seguridad del registro de transacciones para una base de datos y copiarlos en un bucket de Amazon S3 de destino. Al copiar las copias de seguridad del registro de transacciones en un bucket de Amazon S3, puede utilizarlas en combinación con copias de seguridad de bases de datos completas y diferenciadas para realizar restauraciones puntuales de bases de datos. Utiliza los procedimientos almacenados de RDS para configurar el acceso a las copias de seguridad del registro de transacciones, enumera las copias de seguridad del registro de transacciones disponibles y las copia en su bucket de Amazon S3.

El acceso a las copias de seguridad del registro de transacciones ofrece las siguientes capacidades y beneficios:

- Puede enumerar y ver los metadatos de las copias de seguridad del registro de transacciones disponibles para una base de datos en una instancia de base de datos de RDS para SQL Server.
- Puede copiar las copias de seguridad del registro de transacciones disponibles de RDS para SQL Server en un bucket de Amazon S3 de destino.
- Puede realizar restauraciones puntuales de bases de datos sin necesidad de restaurar una instancia de base de datos completa. Para obtener más información acerca la restauración de una instancia de base de datos a un momento determinado, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Disponibilidad y soporte

Se puede acceder a las copias de seguridad del registro de transacciones dese todas las regiones de AWS. El acceso a las copias de seguridad del registro de transacciones está disponible para todas las ediciones y versiones de Microsoft SQL Server compatibles con Amazon RDS.

Requisitos

Se deben cumplir los siguientes requisitos antes de permitir el acceso a las copias de seguridad del registro de transacciones:

- Las copias de seguridad automatizadas deben estar habilitadas en la instancia de base de datos y la retención de las copias de seguridad debe establecerse en un valor de uno o más días. Para

obtener más información sobre cómo habilitar las copias de seguridad automatizadas y configurar una política de retención, consulte Habilitar las copias de seguridad automatizadas.

- Debe existir un bucket de Amazon S3 en la misma cuenta y región que la instancia de base de datos de origen. Antes de habilitar el acceso a las copias de seguridad del registro de transacciones, elija un bucket de Amazon S3 existente o cree uno nuevo para usarlo en los archivos de copia de seguridad del registro de transacciones.
- Se debe configurar una política de permisos de bucket de Amazon S3 de la siguiente manera para permitir que Amazon RDS copie los archivos de registro de transacciones en ella:
  1. Establezca la propiedad de la titularidad de la cuenta del objeto en el bucket Bucket Owner Preferred (Propietario del bucket preferido).
  2. Añada la política siguiente. No habrá ninguna política de forma predeterminada, así que utilice las listas de control de acceso (ACL) del bucket para editar la política de bucket y agregarla.

  En el siguiente ejemplo se utiliza un ARN para especificar un recurso. Le recomendamos que utilice las claves de contexto de condición globales de `SourceArn` y `SourceAccount` en las relaciones de confianza basadas en recursos para limitar los permisos del servicio a un recurso específico. Para obtener más información sobre cómo trabajar con ARN, consulte Nombres de recursos de Amazon (ARN) y Nombres de recursos de Amazon (ARN) en Amazon RDS.

  Example de una política de permisos de Amazon S3 para acceder a las copias de seguridad del registro de transacciones

  JSON

```
   {
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": "Only allow writes to my bucket with bucket owner full
control",
           "Effect": "Allow",
           "Principal": {
               "Service": "backups.rds.amazonaws.com"
           },
           "Action": "s3:PutObject",
           "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/{customer_path}/*",
           "Condition": {
```

```
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:sourceAccount": "{customer_account}",
                    "aws:sourceArn": "{db_instance_arn}"
                }
            }
        }
    ]
}
```

- Un rol de (IAM) AWS Identity and Access Management para acceder al bucket de Amazon S3. Si ya tiene un rol de IAM, puede utilizarlo. También puede elegir que un nuevo rol de IAM se cree en su nombre cuando se agregue la opción `SQLSERVER_BACKUP_RESTORE` mediante la AWS Management Console. Si lo desea, puede crear uno nuevo manualmente. Para obtener más información sobre cómo crear y configurar un rol de IAM con `SQLSERVER_BACKUP_RESTORE`, consulte Creación manual de un rol de IAM para la copia de seguridad y la restauración nativas.
- La opción `SQLSERVER_BACKUP_RESTORE` debe añadirse a un grupo de opciones en la instancia de base de datos. Para obtener más información sobre cómo añadir la opción `SQLSERVER_BACKUP_RESTORE`, consulte Compatibilidad con copia de seguridad y restauración nativas en SQL Server.

> **Note**
>
> Si la instancia de base de datos tiene habilitado el cifrado de almacenamiento, la clave y las acciones (KMS) de AWS KMS deben proporcionarse en el rol de IAM indicado en el grupo de opciones de copia de seguridad y restauración nativo.

Si lo desea, si va a utilizar el procedimiento almacenado `rds_restore_log` para realizar restauraciones puntuales de bases de datos, le recomendamos que utilice la misma ruta de Amazon S3 para el grupo de opciones de copia de seguridad y restauración nativas y para acceder a las copias de seguridad del registro de transacciones. Este método garantiza que, cuando Amazon RDS asuma la función del grupo de opciones para realizar las funciones de registro de restauración, tenga acceso para recuperar las copias de seguridad del registro de transacciones desde la misma ruta de Amazon S3.

- Si la instancia de base de datos está cifrada, independientemente del tipo de cifrado (clave administrada por AWS o clave administrada por el cliente), debe proporcionar una clave

de KMS administrada por el cliente en el rol de IAM y en el procedimiento almacenado `rds_tlog_backup_copy_to_S3`.

Limitaciones y recomendaciones

El acceso a las copias de seguridad del registro de transacciones tiene las siguientes limitaciones y recomendaciones:

- Puede enumerar y copiar las copias de seguridad del registro de transacciones de los últimos siete días de cualquier instancia de base de datos que tenga configurada la retención de copias de seguridad entre uno y 35 días.
- Debe existir el bucket de Amazon S3 que se usa para acceder a las copias de seguridad del registro de transacciones en la misma cuenta y región que la instancia de base de datos de origen. No se admite la copia entre cuentas ni entre regiones.
- Solo se puede configurar un bucket de Amazon S3 como destino para copiar las copias de seguridad del registro de transacciones. Puede elegir un nuevo bucket de Amazon S3 de destino con el procedimiento `rds_tlog_copy_setup` almacenado. Para obtener más información sobre cómo elegir un nuevo bucket de Amazon S3 de destino, consulte Configuración del acceso a las copias de seguridad del registro de transacciones.
- No puede especificar la clave KMS cuando utilice el procedimiento `rds_tlog_backup_copy_to_S3` almacenado si la instancia de RDS no está habilitada para el cifrado de almacenamiento.
- No se admite la copia de varias cuentas. El rol de IAM utilizado para copiar solo permitirá el acceso de escritura a los buckets de Amazon S3 dentro de la cuenta del propietario de la instancia de base de datos.
- Solo se pueden ejecutar dos tareas simultáneas de cualquier tipo en una instancia de base de datos de RDS para SQL Server.
- Solo se puede ejecutar una tarea de copia para una única base de datos en un momento dado. Si desea copiar las copias de seguridad del registro de transacciones de varias bases de datos de la instancia de base de datos, utilice una tarea de copia independiente para cada base de datos.
- Si copia una copia de seguridad del registro de transacciones que ya existe con el mismo nombre en el bucket de Amazon S3, se sobrescribirá la copia de seguridad del registro de transacciones existente.
- Solo puede ejecutar los procedimientos almacenados que se proporcionan con acceso a las copias de seguridad del registro de transacciones en la instancia de base de datos principal. No

puede ejecutar estos procedimientos almacenados en una réplica de lectura de RDS para SQL Server ni en una instancia secundaria de un clúster de base de datos Multi-AZ.

- Si la instancia de base de datos de RDS para SQL Server se reinicia mientras se ejecuta el procedimiento`rds_tlog_backup_copy_to_S3` almacenado, la tarea se reiniciará automáticamente desde el principio cuando la instancia de base de datos vuelva a estar en línea. Se sobrescribirán todas las copias de seguridad del registro de transacciones que se hayan copiado al bucket de Amazon S3 mientras se ejecutaba la tarea antes del reinicio.
- Las bases de datos del sistema Microsoft SQL Server y la base de datos `RDSAdmin` no se pueden configurar para acceder a las copias de seguridad del registro de transacciones.
- No se admite la copia a buckets cifrados por SSE-KMS.

Configuración del acceso a las copias de seguridad del registro de transacciones

Para configurar el acceso a las copias de seguridad del registro de transacciones, complete la lista de requisitos de la sección Requisitos y, a continuación, ejecute el procedimiento `rds_tlog_copy_setup` almacenado. El procedimiento habilitará el acceso a la función de copias de seguridad del registro de transacciones en el nivel de instancia de base de datos. No tiene que ejecutarlo para cada base de datos individual de la instancia de base de datos.

> **Important**
>
> Se debe conceder al usuario de la base de datos el rol `db_owner` dentro de SQL Server en cada base de datos para configurar y utilizar la función de acceso a las copias de seguridad del registro de transacciones.

Example de uso:

```
exec msdb.dbo.rds_tlog_copy_setup
@target_s3_arn='arn:aws:s3:::amzn-s3-demo-bucket/myfolder';
```

El siguiente parámetro es obligatorio:

- `@target_s3_arn`: ARN del bucket de Amazon S3 de destino en el que se copian los archivos de copias de seguridad del registro de transacciones.

Example de configuración de un bucket de destino de Amazon S3:

```
exec msdb.dbo.rds_tlog_copy_setup @target_s3_arn='arn:aws:s3:::amzn-s3-demo-logging-bucket/mytestdb1';
```

Para validar la configuración, ejecute el procedimiento`rds_show_configuration` almacenado.

Example de validación de la configuración:

```
exec rdsadmin.dbo.rds_show_configuration @name='target_s3_arn_for_tlog_copy';
```

Para modificar el acceso a las copias de seguridad del registro de transacciones para que apunten a un bucket de Amazon S3 diferente, puede ver el valor actual del bucket de Amazon S3 y volver a ejecutar el procedimiento `rds_tlog_copy_setup` almacenado con un nuevo valor para `@target_s3_arn`.

Example de visualización del bucket de Amazon S3 existente configurado para acceder a las copias de seguridad del registro de transacciones

```
exec rdsadmin.dbo.rds_show_configuration @name='target_s3_arn_for_tlog_copy';
```

Example de actualización de un nuevo bucket de Amazon S3 de destino

```
exec msdb.dbo.rds_tlog_copy_setup @target_s3_arn='arn:aws:s3:::amzn-s3-demo-logging-bucket1/mynewfolder';
```

Publicación de las copias de seguridad del registro de transacciones disponibles

Con RDS para SQL Server, las bases de datos configuradas para utilizar el modelo de recuperación completo y una retención de copias de seguridad de instancias de base de datos establecida en uno o más días tienen habilitadas automáticamente las copias de seguridad del registro de transacciones. Al habilitar el acceso a las copias de seguridad del registro de transacciones, tendrá a su disposición durante siete días esas copias de seguridad del registro de transacciones para que pueda copiarlas en su bucket de Amazon S3.

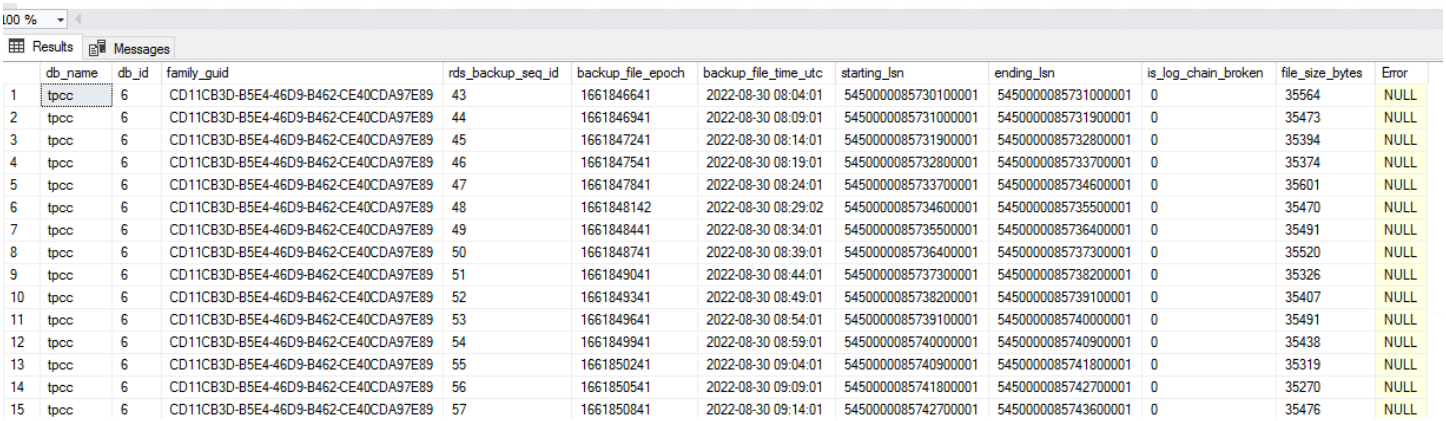
Una vez que haya habilitado el acceso a las copias de seguridad del registro de transacciones, puede empezar a utilizarlas para enumerar y copiar los archivos de copia de seguridad del registro de transacciones disponibles.

Enumerar las copias de seguridad del registro de transacciones

Para mostrar todas las copias de seguridad del registro de transacciones disponibles para una base de datos individual, llame a la función `rds_fn_list_tlog_backup_metadata`. Puede utilizar una cláusula `ORDER BY` o `WHERE` para llamar a la función.

Example de listado y filtrado de los archivos de copia de seguridad del registro de transacciones disponibles

```
SELECT * from msdb.dbo.rds_fn_list_tlog_backup_metadata('mydatabasename');
SELECT * from msdb.dbo.rds_fn_list_tlog_backup_metadata('mydatabasename') WHERE
 rds_backup_seq_id = 3507;
SELECT * from msdb.dbo.rds_fn_list_tlog_backup_metadata('mydatabasename') WHERE
 backup_file_time_utc > '2022-09-15 20:44:01' ORDER BY backup_file_time_utc DESC;
```



Results Messages

	db_name	db_id	family_guid	rds_backup_seq_id	backup_file_epoch	backup_file_time_utc	starting_lsn	ending_lsn	is_log_chain_broken	file_size_bytes	Error
1	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	43	1661846641	2022-08-30 08:04:01	5450000085730100001	5450000085731000001	0	35564	NULL
2	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	44	1661846941	2022-08-30 08:09:01	5450000085731000001	5450000085731900001	0	35473	NULL
3	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	45	1661847241	2022-08-30 08:14:01	5450000085731900001	5450000085732800001	0	35394	NULL
4	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	46	1661847541	2022-08-30 08:19:01	5450000085732800001	5450000085733700001	0	35374	NULL
5	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	47	1661847841	2022-08-30 08:24:01	5450000085733700001	5450000085734600001	0	35601	NULL
6	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	48	1661848142	2022-08-30 08:29:02	5450000085734600001	5450000085735500001	0	35470	NULL
7	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	49	1661848441	2022-08-30 08:34:01	5450000085735500001	5450000085736400001	0	35491	NULL
8	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	50	1661848741	2022-08-30 08:39:01	5450000085736400001	5450000085737300001	0	35520	NULL
9	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	51	1661849041	2022-08-30 08:44:01	5450000085737300001	5450000085738200001	0	35326	NULL
10	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	52	1661849341	2022-08-30 08:49:01	5450000085738200001	5450000085739100001	0	35407	NULL
11	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	53	1661849641	2022-08-30 08:54:01	5450000085739100001	5450000085740000001	0	35491	NULL
12	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	54	1661849941	2022-08-30 08:59:01	5450000085740000001	5450000085740900001	0	35438	NULL
13	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	55	1661850241	2022-08-30 09:04:01	5450000085740900001	5450000085741800001	0	35319	NULL
14	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	56	1661850541	2022-08-30 09:09:01	5450000085741800001	5450000085742700001	0	35270	NULL
15	tpcc	6	CD11CB3D-B5E4-46D9-B462-CE40CDA97E89	57	1661850841	2022-08-30 09:14:01	5450000085742700001	5450000085743600001	0	35476	NULL

La función `rds_fn_list_tlog_backup_metadata` devuelve lo siguiente:

Nombre de la columna	Tipo de datos	Descripción
db_name	sysname	Nombre de la base de datos proporcionado para enumerar las copias de seguridad del registro de transacciones.

Nombre de la columna	Tipo de datos	Descripción
db_id	int	Identificador interno de la base de datos para el parámetro de entrada db_name.
family_guid	uniqueidentifier	Identificador único de la base de datos original en el momento de la creación. Este valor no cambia cuando se restaura la base de datos, incluso con un nombre de base de datos diferente.
rds_backup_seq_id	int	Identificador que RDS utiliza internamente para mantener un número de secuencia para cada archivo de copia de seguridad del registro de transacciones.
backup_file_epoch	bigint	Época en que se generó un archivo de copia de seguridad de transacciones.
backup_file_time_utc	datetime	Valor convertido en hora UTC para el valor backup_file_epoch .
starting_lsn	numeric(25,0)	Número de secuencia de registro del primer registro o del más antiguo de un archivo de copia de seguridad del registro de transacciones.
ending_lsn	numeric(25,0)	Número de secuencia de registro del último registro o del siguiente de un archivo de copia de seguridad del registro de transacciones.
is_log_chain_broken	bit	Valor booleano que indica si la cadena de registro está interrumpida entre el archivo de copia de seguridad del registro de transacciones actual y el archivo de copia de seguridad del registro de transacciones anterior.
file_size_bytes	bigint	Tamaño del conjunto de copias de seguridad transaccional en bytes.

Nombre de la columna	Tipo de datos	Descripción
`Error`	varchar(4000)	Mensaje de error si la función `rds_fn_list_tlog_backup_metadata` lanza una excepción. NULL si no hay excepciones.

Copia de las copias de seguridad del registro de transacciones

Para copiar un conjunto de copias de seguridad del registro de transacciones disponibles para una base de datos individual en su bucket de Amazon S3, ejecute el procedimiento `rds_tlog_backup_copy_to_S3` almacenado. El procedimiento `rds_tlog_backup_copy_to_S3` almacenado iniciará una nueva tarea para copiar las copias de seguridad del registro de transacciones.

> **Note**
>
> El procedimiento `rds_tlog_backup_copy_to_S3` almacenado copiará las copias de seguridad del registro de transacciones sin validarlas con el atributo `is_log_chain_broken`. Por este motivo, debe confirmar manualmente una cadena de registros ininterrumpida antes de ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3`. Para obtener más información, consulte Validación de la cadena de registros de copias de seguridad del registro de transacciones.

Example de uso del procedimiento **`rds_tlog_backup_copy_to_S3`** almacenado

```
exec msdb.dbo.rds_tlog_backup_copy_to_S3
 @db_name='mydatabasename',
 [@kms_key_arn='arn:aws:kms:region:account-id:key/key-id'],
 [@backup_file_start_time='2022-09-01 01:00:15'],
 [@backup_file_end_time='2022-09-01 21:30:45'],
 [@starting_lsn=149000000112100001],
 [@ending_lsn=149000000120400001],
 [@rds_backup_starting_seq_id=5],
 [@rds_backup_ending_seq_id=10];
```

Están disponibles los siguientes parámetros de entrada:

Parámetro	Descripción
`@db_name`	Nombre de la base de datos proporcionado para copiar las copias de seguridad del registro de transacciones.
`@kms_key_arn`	Una clave de KMS administrada por el cliente. Si cifra su instancia de base de datos con una clave de KMS administrada de AWS, debe crear una clave administrada por el cliente. Si cifra la instancia de base de datos con una clave administrada por el cliente, puede utilizar el mismo ARN de clave de KMS.
`@backup_file_start_time`	La marca de tiempo UTC proporcionada en la columna `[backup_file_time_utc]` de la función `rds_fn_list_tlog_backup_metadata` .
`@backup_file_end_time`	La marca de tiempo UTC proporcionada en la columna `[backup_file_time_utc]` de la función `rds_fn_list_tlog_backup_metadata` .
`@starting_lsn`	Número de secuencia de registro (LSN) proporcionado en la columna `[starting_lsn]` de la función `rds_fn_list_tlog_backup_metadata` .
`@ending_lsn`	Número de secuencia de registro (LSN) proporcionado en la columna `[ending_lsn]` de la función `rds_fn_list_tlog_backup_metadata` .
`@rds_backup_starting_seq_id`	ID de secuencia proporcionado en la columna `[rds_backup_seq_id]` de la función `rds_fn_list_tlog_backup_metadata` .
`@rds_backup_ending_seq_id`	ID de secuencia proporcionado en la columna `[rds_backup_seq_id]` de la función `rds_fn_list_tlog_backup_metadata` .

Puede especificar un conjunto de parámetros de tiempo, LSN o ID de secuencia. Solo se requiere un conjunto de parámetros.

También puede especificar un único parámetro en cualquiera de los conjuntos. Por ejemplo, al proporcionar un valor únicamente para el parámetro `backup_file_end_time`, todos los archivos de copia de seguridad del registro de transacciones disponibles antes de esa fecha dentro del límite de siete días se copiarán a su bucket de Amazon S3.

A continuación se muestran las combinaciones de parámetros de entrada válidas para el procedimiento `rds_tlog_backup_copy_to_S3` almacenado.

Parámetros proporcionados	Resultado esperado	
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name = 'testdb1', @backup_file_start_time='2022-08-23 00:00:00', @backup_file_end_time='2022-08-30 00:00:00';`	Copia las copias de seguridad del registro de transacciones de los últimos siete días y se encuentra en el rango proporcionado entre `backup_file_start_time` y `backup_file_end_time` . En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones que se generaron entre «2021-08-23 00:00:00»	

Parámetros proporcionados	Resultado esperado
	y «2021-08-30 00:00:00».
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name = 'testdb1', @backup_file_start_time='2022-08-23 00:00:00';`	Copia las copias de seguridad del registro de transacciones de los últimos siete días empezando por la `backup_file_start_time` proporcionada. En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones desde «2021-08-23 00:00:00» hasta la última copia de seguridad del registro de transacciones.

Parámetros proporcionados	Resultado esperado
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name = 'testdb1', @backup_file_end_time='2022-08-30 00:00:00';`	Copia las copias de seguridad del registro de transacciones de los últimos siete días hasta la `backup_file_end_time` proporcionada. En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones entre «2021-08-23 00:00:00» y «2021-08-30 00:00:00».

Parámetros proporcionados	Resultado esperado
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @starting_lsn =14900000 00040007, @ending_lsn = 149000000 0050009;`	Copia las copias de seguridad del registro de transacciones disponibles en los últimos siete días y que se encuentran en el rango proporcionado entre `starting_lsn` y `ending_lsn` . En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones de los últimos siete días con un intervalo de LSN comprendido entre 1490000000040007 y 149000000 0050009.

Parámetros proporcionados	Resultado esperado
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @starting_lsn =1490000000040007;`	Copia las copias de seguridad del registro de transacciones disponibles en los últimos siete días empezando por la `starting_lsn` . En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones desde el LSN 1490000000040007 hasta la última copia de seguridad del registro de transacciones.

Parámetros proporcionados	Resultado esperado	
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @ending_lsn=14900000 00050009;`	Copia las copias de seguridad del registro de transacciones disponibles en los últimos siete días hasta la `ending_lsn` proporcionada. En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones empezando por los últimos siete días hasta el LSN 149000000 0050009.	

Parámetros proporcionados	Resultado esperado	
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_starting_seq_id= 2000, @rds_backup_ending_seq_id= 5000;`	Copia las copias de seguridad del registro de transacciones disponibles en los últimos siete días y que se encuentran en el rango proporcionado entre `rds_backup_starting_seq_id` y `rds_backup_ending_seq_id` . En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones de los últimos siete días y dentro del rango de ID de secuencia de copia de seguridad de RDS proporcionado, empezando por seq_id 2000 y hasta seq_id 5000.	

Parámetros proporcionados	Resultado esperado
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_starting_seq_id= 2000;`	Copia las copias de seguridad del registro de transacciones disponibles en los últimos siete días empezando por la `rds_backup_starting_seq_id` . En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones desde el seq_id 2000 hasta la última copia de seguridad del registro de transacciones.

Parámetros proporcionados	Resultado esperado
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_ending_seq_id= 5000;`	Copia las copias de seguridad del registro de transacciones disponibles en los últimos siete días hasta la `rds_backup_ending_seq_id` proporcionada. En este ejemplo, el procedimiento almacenado copiará las copias de seguridad del registro de transacciones empezando por los últimos siete días hasta el seq_id 5000.

Parámetros proporcionados	Resultado esperado	
`exec msdb.dbo.rds_tlog_backup_copy_to_S3 @db_name='testdb1', @rds_backup_starting_seq_id= 2000; @rds_backup_ending_seq_id= 2000;`	Copia una única copia de seguridad del registro de transacciones con el `rds_backup_starting_seq_id` proporcionado, si está disponible en los últimos siete días. En este ejemplo, el procedimiento almacenado copiará una única copia de seguridad del registro de transacciones que tenga un seq_id de 2000, si existe en los últimos siete días.	

Validación de la cadena de registros de copias de seguridad del registro de transacciones

Las bases de datos configuradas para acceder a las copias de seguridad del registro de transacciones deben tener habilitada la retención automática de copias de seguridad. La retención automática de copias de seguridad establece las bases de datos de la instancia de base de datos en el modelo de recuperación FULL. Para permitir la restauración puntual de una base de datos, evite cambiar el modelo de recuperación de la base de datos, ya que puede provocar la interrupción de la cadena de registros. Se recomienda mantener la base de datos configurada en el modelo de recuperación FULL.

Para validar manualmente la cadena de registros antes de copiar las copias de seguridad del registro de transacciones, llame a la función `rds_fn_list_tlog_backup_metadata` y revise

los valores de la columna `is_log_chain_broken`. Un valor de 1 indica que la cadena de registro se interrumpió entre la copia de seguridad del registro actual y la copia de seguridad del registro anterior.

El siguiente ejemplo muestra una cadena de registros rota en la salida del procedimiento almacenado `rds_fn_list_tlog_backup_metadata`.

rds_sequence_id	first_lsn	last_lsn	is_log_chain_broken
43	90023	90457	0
44	90457	90985	0
45	90987	92034	1

En una cadena de registros normal, el valor del número de secuencia de registro (LSN) de first_lsn para un un rds_sequence_id determinado debe coincidir con el valor de last_lsn del rds_sequence_id anterior. En la imagen, el rds_sequence_id de 45 tiene un valor first_lsn de 90987, que no coincide con el valor last_lsn de 90985 del rds_sequence_id anterior de 44.

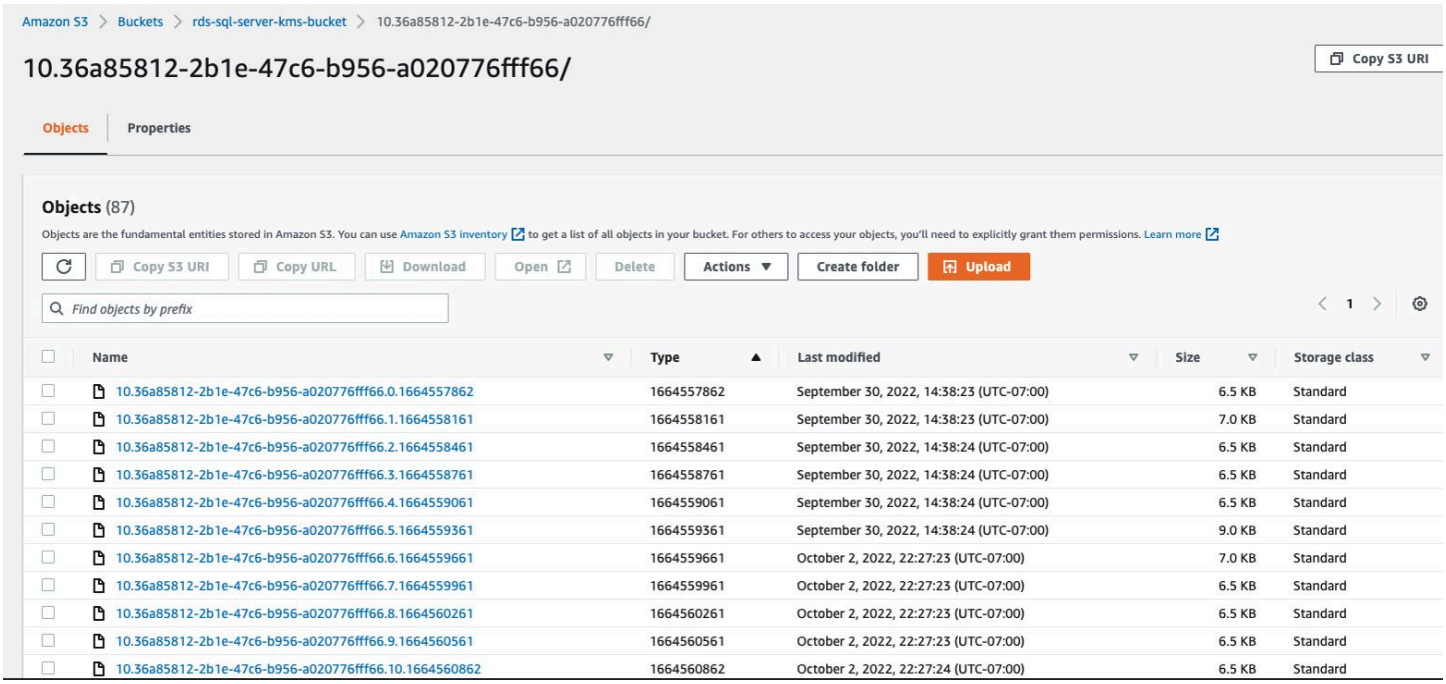
Para obtener más información sobre la arquitectura del registro de transacciones de SQL Server y los números de secuencia de registro, consulte la Arquitectura lógica del registro de transacciones en la documentación de Microsoft SQL Server.

Estructura de archivos y carpetas del bucket de Amazon S3

Las copias de seguridad del registro de transacciones tienen la siguiente estructura y convención de nomenclatura estándar dentro de un bucket de Amazon S3:

- Se crea una nueva carpeta en la ruta `target_s3_arn` de cada base de datos con la estructura de nomenclatura como `{db_id}.{family_guid}`.
- Dentro de la carpeta, las copias de seguridad del registro de transacciones tienen una estructura de nombre de archivo del tipo `{db_id}.{family_guid}.{rds_backup_seq_id}.{backup_file_epoch}`.
- Puede ver los detalles de `family_guid,db_id,rds_backup_seq_id and backup_file_epoch` con la función `rds_fn_list_tlog_backup_metadata`.

En el siguiente ejemplo, se muestra la estructura de archivos y carpetas de un conjunto de copias de seguridad del registro de transacciones en un bucket de Amazon S3.



Seguimiento del estado de las tareas

Para realizar un seguimiento del estado de las tareas de copia, llame al procedimiento almacenado `rds_task_status`. Si no proporciona ningún parámetro, el procedimiento almacenado devuelve el estado de todas las tareas.

Example de uso:

```
exec msdb.dbo.rds_task_status
  @db_name='database_name',
  @task_id=ID_number;
```

Los siguientes parámetros son opcionales:

- `@db_name`: nombre de la base de datos para la que se desea mostrar el estado de una tarea.
- `@task_id`: ID de la tarea cuyo estado se desea mostrar.

Example de enumeración del estado de un ID de tarea específica:

```
exec msdb.dbo.rds_task_status @task_id=5;
```

Example de enumeración del estado de una tarea y una base de datos específicas:

```
exec msdb.dbo.rds_task_status@db_name='my_database',@task_id=5;
```

Example de enumeración de todas las tareas y sus estados en una base de datos específica:

```
exec msdb.dbo.rds_task_status @db_name='my_database';
```

Example de enumeración de todas las tareas y sus estados en la instancia de base de datos actual:

```
exec msdb.dbo.rds_task_status;
```

Cancelación de una tarea

Para cancelar una tarea de ejecución, llame al procedimiento almacenado `rds_cancel_task`.

Example de uso:

```
exec msdb.dbo.rds_cancel_task @task_id=ID_number;
```

El siguiente parámetro es obligatorio:

- `@task_id`: ID de la tarea que se va a cancelar. Puede ver el ID de la tarea llamando al procedimiento almacenado `rds_task_status`.

Para obtener más información acerca de cómo ver y cancelar las tareas en ejecución, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Solución de problemas del acceso a las copias de seguridad del registro de transacciones

A continuación se indican los problemas que se puede encontrar al utilizar los procedimientos almacenados para acceder a las copias de seguridad del registro de transacciones.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_copy_setup	Las copias de seguridad están deshabilitadas en esta instancia de base de datos. Habilite las copias de seguridad de instancias de base de datos con una retención de al menos 1 e inténtelo de nuevo.	Las copias de seguridad automatizadas no están habilitadas para la instancia de base de datos.	La retención de copias de seguridad de instancias de base de datos debe estar habilitada con una retención de al menos un día. Para obtener más información sobre cómo habilitar las copias de seguridad automatizadas y configurar una retención de copias de seguridad, consulte Backup retention period (Periodo de retención de copia de seguridad).
rds_tlog_copy_setup	Error al ejecutar el procedimiento almacenado rds_tlog_copy_setup. Vuelva a conectarse al punto	Se ha producido un error interno.	Vuelva a conectarse al punto de conexión de RDS y vuelva a ejecutar el procedimiento almacenado `rds_tlog_copy_setup` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
	de conexión de RDS e inténtelo de nuevo.		
rds_tlog_copy_setup	No se admite la ejecución del procedimiento almacenado rds_tlog_backup_copy_setup dentro de una transacción. Compruebe que la sesión no tenga transacciones abiertas e inténtelo de nuevo.	El procedimiento almacenado se ha intentado dentro de una transacción utilizando `BEGIN` y `END`.	Evite utilizar`BEGIN` y `END` cuando ejecute el procedimiento almacenado `rds_tlog_copy_setup` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_copy_setup	El nombre del bucket de S3 para el parámetro de entrada `@target_s3_arn` debe contener al menos un carácter que no sea un espacio.	Se ha proporcionado un valor incorrecto para el parámetro de entrada `@target_s3_arn` .	Asegúrese de que el parámetro de entrada `@target_s3_arn` especifique el ARN completo del bucket de Amazon S3.
rds_tlog_copy_setup	La opción `SQLSERVER_BACKUP_RESTORE` no está habilitada o está en proceso de habilitarse. Habilite la opción o vuelva a intentarlo más tarde.	La opción `SQLSERVER_BACKUP_RESTORE` no está habilitada en la instancia de base de datos o simplemente estaba habilitada y pendiente de activación interna.	Habilite la opción `SQLSERVER_BACKUP_RESTORE` tal y como se especifica en la sección Requisitos. Espere unos minutos y vuelva a ejecutar el procedimiento almacenado `rds_tlog_copy_setup` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_copy_setup	El ARN S3 de destino para el parámetro de entrada `@target_s3_arn` no puede estar vacío ni ser nulo.	Se ha proporcionado un valor `NULL` para el parámetro de entrada `@target_s3_arn` o no se ha proporcionado el valor.	Asegúrese de que el parámetro de entrada `@target_s3_arn` especifique el ARN completo del bucket de Amazon S3.
rds_tlog_copy_setup	El ARN de S3 de destino para el parámetro de entrada `@target_s3_arn` debe empezar por arn:aws.	El parámetro de entrada `@target_s3_arn` se ha proporcionado sin `arn:aws` en la parte delantera.	Asegúrese de que el parámetro de entrada `@target_s3_arn` especifique el ARN completo del bucket de Amazon S3.
rds_tlog_copy_setup	El ARN S3 de destino ya está configurado en el valor proporcionado.	El procedimiento almacenado `rds_tlog_copy_setup` se ha ejecutado anteriormente y se ha configurado con un ARN de bucket de Amazon S3.	Para modificar el valor del bucket de Amazon S3 para acceder a las copias de seguridad del registro de transacciones, proporcione otro `target S3 ARN`.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_copy_setup	No se pueden generar las credenciales para habilitar el acceso a las copias de seguridad del registro de transacciones. Confirme el ARN de la ruta de S3 proporcionada con `rds_tlog_copy_setup` e inténtelo de nuevo más tarde.	Se ha producido un error no especificado al generar las credenciales para permitir el acceso a las copias de seguridad del registro de transacciones.	Revise la configuración e inténtelo de nuevo.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_copy_setup	No puede ejecutar el procedimiento almacenado o rds_tlog_copy_setup mientras haya tareas pendientes. Espere a que se completen las tareas pendientes e inténtelo de nuevo.	Solo se pueden ejecutar dos tareas a la vez. Hay tareas pendientes de finalización.	Visualice las tareas pendientes y espere a que se completen. Para obtener más información sobre monitorear el estado de las tareas, consulte Seguimiento del estado de las tareas.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Ya se ha emitido una tarea de copia del archivo de copia de seguridad de T-log para la base de datos: %s con el ID de tarea: %d, inténtelo de nuevo más tarde.	Solo se puede ejecutar una tarea de copia para una base de datos determinada en un momento dado. Hay tareas de copia pendientes que todavía no han finalizado.	Visualice las tareas pendientes y espere a que se completen. Para obtener más información sobre monitorear el estado de las tareas, consulte Seguimiento del estado de las tareas.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Debe proporcionarse al menos uno de estos tres conjuntos de parámetros. SET-1:(@backup_file_start_time, @backup_file_end_time) | SET-2:(@starting_lsn, @ending_lsn) | SET-3:(@rds_backup_starting_seq_id, @rds_backup_ending_seq_id)	No se ha propocionado ninguno de los tres conjuntos de parámetros o a uno de ellos le falta un parámetro obligatorio.	Puede especificar el parámetro de tiempo, el LSN o el ID de secuencia. Se requiere un conjunto de estos tres conjuntos de parámetros. Para obtener más información acerca de los parámetros requeridos, consulte Copia de las copias de seguridad del registro de transacciones.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Las copias de seguridad están deshabilitadas en su instancia. Habilite las copias de seguridad e inténtelo de nuevo más adelante.	Las copias de seguridad automatizadas no están habilitadas para la instancia de base de datos.	Para obtener más información sobre cómo habilitar las copias de seguridad automatizadas y configurar una retención de copias de seguridad, consulte Backup retention period (Periodo de retención de copia de seguridad).
rds_tlog_backup_copy_to_S3	No se encuentra la base de datos %s dada.	El valor proporcionado para el parámetro de entrada `@db_name` no coincide con el nombre de la base de datos de la instancia de base de datos.	Utilice el nombre de la base de datos correcto. Para enumerar todas las bases de datos por nombre, ejecute `SELECT * from sys.databases` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	No se puede ejecutar el procedimiento almacenado o rds_tlog_backup_copy_to_S3 para las bases de datos del sistema SQL Server o la base de datos rdsadmin.	El valor proporcionado para el parámetro de entrada `@db_name` coincide con el nombre de la base de datos del sistema SQL Server o con la base de datos RDSAdmin.	No se permite el uso de las siguientes bases de datos para acceder a las copias de seguridad del registro de transacciones: `master, model, msdb, tempdb, RDSAdmin.`
rds_tlog_backup_copy_to_S3	El nombre de la base de datos del parámetro de entrada @db_name no puede estar vacío ni ser nulo.	El valor proporcionado para el parámetro de entrada `@db_name` estaba vacío o `NULL`.	Utilice el nombre de la base de datos correcto. Para enumerar todas las bases de datos por nombre, ejecute `SELECT * from sys.databases` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	El período de retención de la copia de seguridad de la instancia de base de datos se debe establecer en al menos 1 para ejecutar el procedimiento almacenado rds_tlog_backup_copy_setup.	Las copias de seguridad automatizadas no están habilitadas para la instancia de base de datos.	Para obtener más información sobre cómo habilitar las copias de seguridad automatizadas y configurar una retención de copias de seguridad, consulte Backup retention period (Periodo de retención de copia de seguridad).

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Error al ejecutar el procedimiento almacenado rds_tlog_backup_copy_to_S3. Vuelva a conectarse al punto de conexión de RDS e inténtelo de nuevo.	Se ha producido un error interno.	Vuelva a conectarse al punto de conexión de RDS y vuelva a ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Solo se puede proporcionar uno de estos tres conjuntos de parámetros. SET-1:(@backup_file_start_time, @backup_file_end_time) | SET-2:(@starting_lsn, @ending_lsn) | SET-3:(@rds_backup_starting_seq_id, @rds_backup_ending_seq_id)	Se han proporcionado varios conjuntos de parámetros.	Puede especificar el parámetro de tiempo, el LSN o el ID de secuencia. Se requiere un conjunto de estos tres conjuntos de parámetros. Para obtener más información acerca de los parámetros requeridos, consulte Copia de las copias de seguridad del registro de transacciones.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	No se admite la ejecución del procedimiento almacenado rds_tlog_backup_copy_to_S3 dentro de una transacción. Compruebe que la sesión no tenga transacciones abiertas e inténtelo de nuevo.	El procedimiento almacenado se ha intentado dentro de una transacción utilizando `BEGIN` y `END`.	Evite utilizar`BEGIN` y `END` cuando ejecute el procedimiento almacenado `rds_tlog_backup_copy_to_S3` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Los parámetros proporcionados están fuera del período de retención del registro de copia de seguridad de transacciones. Para ver una lista de los archivos de copia de seguridad del registro de transacciones disponibles, ejecute la función rds_fn_list_tlog_backup_metadata.	No hay copias de seguridad del registro de transacciones disponibles para los parámetros de entrada proporcionados que se ajusten a la ventana de retención de copias.	Vuelva a intentarlo con un conjunto de parámetros válido. Para obtener más información acerca de los parámetros requeridos, consulte Copia de las copias de seguridad del registro de transacciones.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Se ha producido un error de permisos al procesar la solicitud. Asegúrese de que el bucket esté en la misma cuenta y región que la instancia de base de datos y confirme los permisos de la política del bucket de S3 con la plantilla de la documentación pública.	Se ha detectado un problema con el bucket de S3 proporcionado o con sus permisos de política.	Confirme que la configuración de acceso a las copias de seguridad del registro de transacciones es correcta. Para obtener más información sobre los requisitos de configuración de su bucket de S3, consulte Requisitos.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	No está permitido ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3` en una instancia de réplica de lectura de RDS.	Se ha intentado realizar el procedimiento almacenado en una instancia de réplica de lectura de RDS.	Conecte con la instancia de base de datos principal de RDS para ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3` .
rds_tlog_backup_copy_to_S3	El LSN para el parámetro de entrada `@starting_lsn` debe ser inferior a `@ending_lsn` .	El valor proporcionado para el parámetro de entrada `@starting_lsn` era mayor que el valor proporcionado para el parámetro de entrada `@ending_lsn` .	Asegúrese de que el valor proporcionado para el parámetro de entrada `@starting_lsn` sea inferior al valor proporcionado para el parámetro de entrada `@ending_lsn` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	El procedimiento almacenado `rds_tlog_backup_copy_to_S3` solo lo pueden realizar los miembros del rol `db_owner` en la base de datos de origen.	No se ha otorgado el rol `db_owner` a la cuenta que intenta ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3` en el `db_name` proporcionado.	Asegúrese de que la cuenta que ejecuta el procedimiento almacenado esté autorizada con el rol `db_owner` para el `db_name` proporcionado.
rds_tlog_backup_copy_to_S3	El ID de secuencia para el parámetro de entrada`@rds_backup_starting_seq_id` debe ser menor o igual que `@rds_backup_ending_seq_id` .	El valor proporcionado para el parámetro de entrada `@rds_backup_starting_seq_id` era mayor que el valor proporcionado para el parámetro de entrada `@rds_backup_ending_seq_id` .	Asegúrese de que el valor proporcionado para el parámetro de entrada `@rds_backup_starting_seq_id` sea inferior al valor proporcionado para el parámetro de entrada `@rds_backup_ending_seq_id` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	La opción SQLSERVER_BACKUP_RESTORE no está habilitada o está en proceso de habilitarse. Habilite la opción o vuelva a intentarlo más tarde.	La opción `SQLSERVER_BACKUP_RESTORE` no está habilitada en la instancia de base de datos o simplemente estaba habilitada y pendiente de activación interna.	Habilite la opción `SQLSERVER_BACKUP_RESTORE` tal y como se especifica en la sección Requisitos. Espere unos minutos y vuelva a ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3` .
rds_tlog_backup_copy_to_S3	La hora de inicio del parámetro de entrada `@backup_file_start_time` debe ser inferior a `@backup_file_end_time` .	El valor proporcionado para el parámetro de entrada `@backup_file_start_time` era mayor que el valor proporcionado para el parámetro de entrada `@backup_file_end_time` .	Asegúrese de que el valor proporcionado para el parámetro de entrada `@backup_file_start_time` sea inferior al valor proporcionado para el parámetro de entrada `@backup_file_end_time` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	No hemos podido procesar la solicitud por falta de acceso. Compruebe la configuración y los permisos de la función.	Puede que haya un problema con los permisos del bucket de Amazon S3 o que el bucket de Amazon S3 proporcionado o esté en otra cuenta o región.	Asegúrese de que los permisos de la política de bucket de Amazon S3 estén concedidos para poder acceder a RDS. Compruebe que el bucket de Amazon S3 esté en la misma cuenta y región que la instancia de base de datos.
rds_tlog_backup_copy_to_S3	No puede proporcionar un ARN de clave KMS como parámetro de entrada para el procedimiento almacenado para las instancias que no estén cifradas para almacenamiento.	Si el cifrado de almacenamiento no está habilitado en la instancia de base de datos, no se deberá proporcionar el parámetro de entrada `@kms_key_arn` .	No proporcione ningún parámetro de entrada para `@kms_key_arn` .

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Debe proporcionar un ARN de clave KMS como parámetro de entrada para el procedimiento almacenado para almacenar instancias cifradas.	Si el cifrado de almacenamiento está habilitado en la instancia de base de datos, se deberá proporcionar el parámetro de entrada `@kms_key_arn` .	Proporcione un parámetro de entrada para `@kms_key_arn` con un valor que coincida con el ARN del bucket de Amazon S3 para usarlo en las copias de seguridad del registro de transacciones.

Procedimiento almacenado	Mensaje de error	Problema	Sugerencias para la solución de problemas
rds_tlog_backup_copy_to_S3	Debe ejecutar el procedimiento almacenado `rds_tlog_copy_setup` y configurar `@target_s3_arn`, antes de ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3`.	El acceso al procedimiento de configuración de las copias de seguridad del registro de transacciones no se ha completado antes de intentar ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3`.	Debe ejecutar el procedimiento almacenado `rds_tlog_copy_setup` antes de ejecutar el procedimiento almacenado `rds_tlog_backup_copy_to_S3`. Para obtener más información sobre cómo ejecutar el procedimiento de configuración para acceder a las copias de seguridad del registro de transacciones, consulte Configuración del acceso a las copias de seguridad del registro de transacciones.

Opciones para el motor de base de datos de Microsoft SQL Server

En esta sección encontrará descripciones de las opciones que están disponibles para las instancias de Amazon RDS que ejecutan el motor de base de datos de Microsoft SQL Server. Para habilitar estas opciones, puede añadirlas a un grupo de opciones y, a continuación, asociar el grupo de opciones a la instancia de base de datos. Para obtener más información, consulte Trabajo con grupos de opciones.

Si busca características opcionales que no se hayan agregado a través de los grupos de opciones de RDS, (como SSL, la autenticación de Microsoft Windows y la integración de Amazon S3), consulte Características adicionales para Microsoft SQL Server en Amazon RDS.

Amazon RDS admite las siguientes opciones para las instancias de base de datos de Microsoft SQL Server.

Opción	ID de la opción	Ediciones del motor
Servidores enlazados con Oracle OLEDB	`OLEDB_ORACLE`	SQL Server Enterprise Edition SQL Server Standard Edition
Copia de seguridad y restauración nativas	`SQLSERVER_BACKUP_RESTORE`	SQL Server Enterprise Edition SQL Server Standard Edition SQL Server Web Edition SQL Server Express Edition
Cifrado de datos transparente	`TRANSPARENT_DATA_ENCRYPTION` (consola de RDS)	SQL Server 2016–2022 Enterprise Edition

Opción	ID de la opción	Ediciones del motor
	`TDE` (AWS CLI y API de RDS)	SQL Server 2022 Standard Edition
SQL Server Audit	`SQLSERVER_AUDIT`	En RDS, a partir de SQL Server 2016, todas las ediciones de SQL Server admiten auditorías de nivel de servidor, y la edición Enterprise también admite auditorías de nivel de base de datos. A partir del SQL Server SQL Server 2016 (13.x) SP1, todas las ediciones admiten tanto auditorías de nivel de servidor como de nivel de base de datos. Para obtener más información, consulte SQL Server Audit (motor de base de datos) en la documentación de SQL Server.

Opción	ID de la opción	Ediciones del motor
SQL Server Analysis Services	SSAS	SQL Server Enterprise Edition SQL Server Standard Edition
SQL Server Integration Services	SSIS	SQL Server Enterprise Edition SQL Server Standard Edition
SQL Server Reporting Services	SSRS	SQL Server Enterprise Edition SQL Server Standard Edition
Coordinador de transacciones distribuidas de Microsoft	MSDTC	En RDS, a partir de SQL Server 2016, todas las ediciones de SQL Server admiten transacciones distribuidas.

Descripción de las opciones disponibles para las versiones y ediciones de SQL Server

Puede usar el comando `describe-option-group-options` AWS CLI a fin de enumerar las opciones disponibles para las versiones y ediciones de SQL Server, así como la configuración de esas opciones.

En el siguiente ejemplo se muestran las opciones y la configuración de opciones para SQL Server 2019 Enterprise Edition. La opción `--engine-name` es obligatoria.

```
aws rds describe-option-group-options --engine-name sqlserver-ee --major-engine-version
 15.00
```

La salida se parece a la siguiente:

```
{
    "OptionGroupOptions": [
        {
            "Name": "MSDTC",
            "Description": "Microsoft Distributed Transaction Coordinator",
            "EngineName": "sqlserver-ee",
            "MajorEngineVersion": "15.00",
            "MinimumRequiredMinorEngineVersion": "4043.16.v1",
            "PortRequired": true,
            "DefaultPort": 5000,
            "OptionsDependedOn": [],
            "OptionsConflictsWith": [],
            "Persistent": false,
            "Permanent": false,
            "RequiresAutoMinorEngineVersionUpgrade": false,
            "VpcOnly": false,
            "OptionGroupOptionSettings": [
                {
                    "SettingName": "ENABLE_SNA_LU",
                    "SettingDescription": "Enable support for SNA LU protocol",
                    "DefaultValue": "true",
                    "ApplyType": "DYNAMIC",
                    "AllowedValues": "true,false",
                    "IsModifiable": true,
                    "IsRequired": false,
                    "MinimumEngineVersionPerAllowedValue": []
                },
        ...

        {
            "Name": "TDE",
            "Description": "SQL Server - Transparent Data Encryption",
            "EngineName": "sqlserver-ee",
            "MajorEngineVersion": "15.00",
            "MinimumRequiredMinorEngineVersion": "4043.16.v1",
            "PortRequired": false,
            "OptionsDependedOn": [],
            "OptionsConflictsWith": [],
```

```
            "Persistent": true,
            "Permanent": false,
            "RequiresAutoMinorEngineVersionUpgrade": false,
            "VpcOnly": false,
            "OptionGroupOptionSettings": []
        }
    ]
}
```

Compatibilidad con servidores enlazados con Oracle OLEDB en Amazon RDS para SQL Server

Los servidores enlazados con Oracle Provider for OLEDB en RDS para SQL Server le permiten acceder a orígenes de datos externos en una base de datos de Oracle. Puede leer datos de orígenes de datos remotos de Oracle y ejecutar comandos en servidores de bases de datos de Oracle remotos fuera de su instancia de base de datos de RDS para SQL Server. Al usar servidores enlazados con Oracle OLEDB puede:

- Acceder directamente a orígenes de datos distintas de SQL Server
- Realizar consultas en diversos orígenes de datos de Oracle con la misma consulta sin mover los datos
- Emitir consultas, actualizaciones, comandos y transacciones distribuidas en orígenes de datos en un ecosistema empresarial
- Integrar las conexiones a una base de datos de Oracle desde la suite de Microsoft Business Intelligence (SSIS, SSRS, SSAS)
- Migrar desde una base de datos de Oracle a RDS para SQL Server

Puede activar uno o más servidores enlazados para Oracle en una instancia de base de datos de RDS para SQL Server existente o nueva. A continuación, puede integrar orígenes de datos de Oracle externas con su instancia de base de datos.

Contenido

- Versiones y regiones compatibles
- Limitaciones y recomendaciones
- Activación de servidores enlazados con Oracle
  - Creación del grupo de opciones para OLEDB_ORACLE
  - Agregar la opción OLEDB_ORACLE al grupo de opciones
  - Modificación de la opción de la versión de OLEDB_ORACLE a otra versión
  - Asociación del grupo de opciones a su instancia de base de datos
- Modificación de las propiedades del proveedor de OLEDB
- Modificación de las propiedades del controlador OLEDB
- Activación de servidores enlazados con Oracle

Versiones y regiones compatibles

RDS para SQL Server admite servidores vinculados con Oracle OLEDB en todas las regiones para las ediciones Standard y Enterprise de SQL Server en las siguientes versiones:

- SQL Server 2022, todas las versiones
- SQL Server 2019, todas las versiones
- SQL Server 2017, todas las versiones

Los servidores vinculados con Oracle OLEDB son compatibles con las siguientes versiones de Oracle Database:

- Oracle Database 21c, todas las versiones
- Oracle Database 19c, todas las versiones
- Oracle Database 18c, todas las versiones

Los servidores vinculados con Oracle OLEDB son compatibles con las siguientes versiones de controlador de OLEDB Oracle:

- 21.7
- 21.16

Limitaciones y recomendaciones

Tenga en cuenta las siguientes limitaciones y recomendaciones que se aplican a los servidores enlazados con Oracle OLEDB:

- Permita el tráfico de red añadiendo el puerto TCP correspondiente en el grupo de seguridad para cada instancia de base de datos de RDS para SQL Server. Por ejemplo, si está configurando un servidor vinculado entre una instancia de base de datos de Oracle de EC2 y una instancia de base de datos de RDS para SQL Server, debe permitir el tráfico desde la dirección IP de la instancia de base de datos de Oracle de EC2. También debe permitir el tráfico en el puerto que utiliza SQL Server para escuchar la comunicación de la base de datos. Para obtener más información acerca de los grupos de seguridad, consulte Control de acceso con grupos de seguridad.
- Reinicie la instancia de base de datos de RDS para SQL Server después de activar, desactivar o modificar la opción `OLEDB_ORACLE` del grupo de opciones. El estado del grupo de opciones

muestra `pending_reboot` para estos eventos y es obligatorio. Para las instancias Multi-AZ de RDS para SQL Server con las opciones AlwaysOn o Mirroring habilitadas, se espera una conmutación por error cuando la instancia se reinicie tras la creación o restauración de la instancia nueva.

- Solo se admite la autenticación simple con un nombre de usuario y una contraseña para el origen de datos de Oracle.
- No se admiten los controladores de Open Database Connectivity (ODBC). Solo se admiten las versiones de controladores OLEDB indicadas anteriormente.
- Se admiten transacciones distribuidas (XA). Para activar las transacciones distribuidas, active la opción `MSDTC` del grupo de opciones de su instancia de base de datos y asegúrese de que las transacciones XA estén activadas. Para obtener más información, consulte Compatibilidad con el Coordinador de transacciones distribuidas de Microsoft en RDS for SQL Server.
- No se admite la creación de nombres de orígenes de datos (DSN, por sus siglas en inglés) para usarlos como atajos para una cadena de conexión.
- No se admite el rastreo del controlador OLEDB. Puede utilizar eventos extendidos de SQL Server para rastrear eventos de OLEDB. Para obtener más información, consulte Set up Extended Events in RDS for SQL Server (Configuración de eventos extendidos en RDS para SQL Server).
- SQL Server Management Studio (SSMS) no admite el acceso a la carpeta de catálogos para un servidor vinculado a Oracle.

Activación de servidores enlazados con Oracle

Active los servidores enlazados con Oracle al agregar la opción `OLEDB_ORACLE` a la instancia de instancia de base de RDS para SQL Server. Utilice el siguiente proceso:

1. Cree un nuevo grupo de opciones o elija un grupo de opciones ya existente.
2. Añada la opción `OLEDB_ORACLE` al grupo de opciones.
3. Elija una versión del controlador OLEDB que desee utilizar.
4. Asocie el grupo de opciones a la instancia de base de datos.
5. Reinicie la instancia de base de datos.

Creación del grupo de opciones para OLEDB_ORACLE

Para trabajar con servidores enlazados con Oracle, cree un grupo de opciones o modifique un grupo de opciones que corresponda a la edición y versión de SQL Server de la instancia de base de datos

que planea utilizar. Para completar este procedimiento, utilice la AWS Management Console o la AWS CLI.

Consola

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2019.

Para crear el grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En la ventana Create option group (Crear grupo de opciones), haga lo siguiente:
   a. En Nombre, escriba un nombre para el grupo de opciones que sea exclusivo dentro de su cuenta de AWS, como **`oracle-oledb-se-2019`**. El nombre solo puede contener letras, dígitos y guiones.
   b. En Descripción, escriba una breve descripción del grupo de opciones, como **`OLEDB_ORACLE option group for SQL Server SE 2019`**. La descripción se utiliza para fines de visualización.
   c. Para Engine (Motor), elija sqlserver-se.
   d. En Major engine version (Versión principal del motor), elija 15.00.
5. Seleccione Crear.

CLI

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2019.

Para crear el grupo de opciones

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds create-option-group \
```

```
    --option-group-name oracle-oledb-se-2019 \
    --engine-name sqlserver-se \
    --major-engine-version 15.00 \
    --option-group-description "OLEDB_ORACLE option group for SQL Server SE 2019"
```

Para Windows:

```
aws rds create-option-group ^
    --option-group-name oracle-oledb-se-2019 ^
    --engine-name sqlserver-se ^
    --major-engine-version 15.00 ^
    --option-group-description "OLEDB_ORACLE option group for SQL Server SE 2019"
```

Agregar la opción **OLEDB_ORACLE** al grupo de opciones

A continuación, utilice la AWS Management Console o la AWS CLI para agregar la opción `OLEDB_ORACLE` al grupo de opciones.

Consola

Para añadir la opción OLEDB_ORACLE

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que acaba de crear, oracle-oledb-se-2019 en este ejemplo.
4. Elija Agregar opción.
5. En Option details (Detalles de la opción), elija OLEDB_ORACLE para Option name (Nombre de la opción).
6. En Versión, elija la versión del controlador OLEDB Oracle que desee instalar.
7. En Scheduling (Programación), elija si desea agregar la opción inmediatamente o en el siguiente período de mantenimiento.
8. Elija Add option (Agregar opción).

CLI

Para añadir la opción OLEDB_ORACLE

- Agregue la opción `OLEDB_ORACLE` al grupo de opciones.

  Example

  Para Linux, macOS o Unix:

```
aws rds add-option-to-option-group \
    --option-group-name oracle-oledb-se-2019 \
    --options OptionName=OLEDB_ORACLE, OptionVersion=21.16 \
    --apply-immediately
```

  Para Windows:

```
aws rds add-option-to-option-group ^
    --option-group-name oracle-oledb-se-2019 ^
    --options OptionName=OLEDB_ORACLE, OptionVersion=21.16 ^
    --apply-immediately
```

Modificación de la opción de la versión de **`OLEDB_ORACLE`** a otra versión

Para modificar la versión de la opción `OLEDB_ORACLE` a otra versión, utilice la AWS Management Console o la AWS CLI.

Consola

Modificación de la opción OLEDB_ORACLE

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `OLEDB_ORACLE` (oracle-oledb-se-2019 en los ejemplos anteriores).
4. Elija Modify option (Modificar opción).
5. En Option details (Detalles de la opción), elija OLEDB_ORACLE para Option name (Nombre de la opción).

6. En Versión, elija la versión del controlador OLEDB Oracle que desee utilizar.
7. En Programación, elija si desea modificar la opción inmediatamente o en el siguiente periodo de mantenimiento.
8. Elija Modify option (Modificar opción).

CLI

Para modificar la versión de la opción `OLEDB_ORACLE`, use el comando `rds add-option-to-option-group`AWS CLI con el grupo de opciones y la versión de la opción que desea usar.

Modificación de la opción OLEDB_ORACLE

- Example

  Para Linux, macOS o Unix:

```
aws rds add-option-to-option-group \
    --option-group-name oracle-oledb-se-2019 \
    --options OptionName=OLEDB_ORACLE, OptionVersion=21.7 \
    --apply-immediately
```

  Para Windows:

```
aws rds add-option-to-option-group ^
    --option-group-name oracle-oledb-se-2019 ^
    --options OptionName=OLEDB_ORACLE, OptionVersion=21.7 ^
    --apply-immediately
```

Asociación del grupo de opciones a su instancia de base de datos

Para asociar el grupo de opciones `OLEDB_ORACLE` y el grupo de parámetros con su instancia de base de datos, utilice la AWS Management Console o la AWS CLI

Consola

Para terminar de activar los servidores enlazados para Oracle, asocie su grupo de opciones `OLEDB_ORACLE` a una instancia de base de datos nueva o existente:

- Para una nueva instancia de base de datos, asóciela cuando inicie la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, asóciela modificando la instancia. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

CLI

Puede asociar el grupo de opciones `OLEDB_ORACLE` y el grupo de parámetros con una instancia de base de datos nueva o existente.

Para crear una instancia con el grupo de opciones **`OLEDB_ORACLE`** y el grupo de parámetros

- Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de opciones.

  Example

  Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mytestsqlserveroracleoledbinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 15.0.4236.7.v1 \
    --allocated-storage 100 \
    --manage-master-user-password \
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name oracle-oledb-se-2019 \
    --db-parameter-group-name my-parameter-group-name
```

  Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mytestsqlserveroracleoledbinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 15.0.4236.7.v1 ^
```

```
    --allocated-storage 100 ^
    --manage-master-user-password ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
    --domain my-domain-id ^
    --option-group-name oracle-oledb-se-2019 ^
    --db-parameter-group-name my-parameter-group-name
```

Para modificar una instancia y asociar el grupo de opciones **OLEDB_ORACLE**

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mytestsqlserveroracleoledbinstance \
    --option-group-name oracle-oledb-se-2019 \
    --db-parameter-group-name my-parameter-group-name \
    --apply-immediately
```

  Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mytestsqlserveroracleoledbinstance ^
    --option-group-name oracle-oledb-se-2019 ^
    --db-parameter-group-name my-parameter-group-name ^
    --apply-immediately
```

Modificación de las propiedades del proveedor de OLEDB

Puede ver y cambiar las propiedades del proveedor de OLEDB. Solo el usuario `master` puede realizar esta tarea. Todos los servidores enlazados de Oracle que se crean en la instancia de base de datos utilizan las mismas propiedades de ese proveedor de OLEDB. Ejecute el procedimiento almacenado `sp_MSset_oledb_prop` para cambiar las propiedades del proveedor de OLEDB.

Para cambiar las propiedades del proveedor de OLEDB

```
USE [master]
GO
EXEC sp_MSset_oledb_prop N'OraOLEDB.Oracle', N'AllowInProcess', 1
EXEC sp_MSset_oledb_prop N'OraOLEDB.Oracle', N'DynamicParameters', 0
GO
```

Se pueden modificar las siguientes propiedades:

Nombre de la propiedad	Valor recomendado (1 = activado, 0 = desactivado)	Descripción
`Dynamic parameter`	1	Permite los marcadores de posición de SQL (representados por “?”) en consultas parametri zadas.
`Nested queries`	1	Permite sentencias `SELECT` anidadas en la cláusula `FROM`, como las subconsultas.
`Level zero only`	0	Solo las interfaces OLEDB de nivel base se invocan contra el proveedor.
`Allow inprocess`	1	Si está activado, Microsoft SQL Server permite crear instancias del proveedor como un servidor en proceso. Defina esta propiedad en 1 para usar servidores enlazados de Oracle.
`Non transacted updates`	0	Si no es cero, SQL Server permite las actualiza ciones.
`Index as access path`	False	Si no es cero, SQL Server intenta usar los índices del proveedor para obtener datos.
`Disallow adhoc access`	False	Si está configurado, SQL Server no permite ejecutar consultas de transferencia con el proveedor de OLEDB. Si bien se puede marcar esta opción, a veces es adecuado ejecutar consultas de transferencia.

Nombre de la propiedad	Valor recomendado (1 = activado, 0 = desactivado)	Descripción
`Supports LIKE operator`	1	Indica que el proveedor admite consultas con la palabra clave LIKE.

Modificación de las propiedades del controlador OLEDB

Puede ver y cambiar las propiedades del controlador OLEDB al crear un servidor vinculado para Oracle. Solo el usuario `master` puede realizar esta tarea. Las propiedades del controlador definen la forma en que el controlador OLEDB gestiona los datos cuando trabaja con un origen de datos remoto de Oracle. Las propiedades del controlador son específicas de cada servidor vinculado de Oracle creado en la instancia de base de datos. Ejecute el procedimiento almacenado `master.dbo.sp_addlinkedserver` para cambiar las propiedades del controlador OLEDB.

Ejemplo: Para crear un servidor vinculado y cambiar la propiedad `FetchSize` del controlador OLEDB

```
EXEC master.dbo.sp_addlinkedserver
@server = N'Oracle_link2',
@srvproduct=N'Oracle',
@provider=N'OraOLEDB.Oracle',
@datasrc=N'my-oracle-test.cnetsipka.us-west-2.rds.amazonaws.com:1521/ORCL',
@provstr='FetchSize=200'
GO
```

```
EXEC master.dbo.sp_addlinkedsrvlogin
@rmtsrvname=N'Oracle_link2',
@useself=N'False',
@locallogin=NULL,
@rmtuser=N'master',
@rmtpassword='Test#1234'
GO
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Activación de servidores enlazados con Oracle

Para desactivar los servidores enlazados con Oracle, quite la opción `OLEDB_ORACLE` de su grupo de opciones.

> **Important**
>
> La eliminación de la opción no elimina las configuraciones de servidor enlazado a la instancia de la base de datos. Debe eliminarlos manualmente para eliminarlos de la instancia de base de datos.
> Puede volver a activar la opción `OLEDB_ORACLE` después de eliminarla para volver a utilizar las configuraciones del servidor enlazado que se configuraron previamente en la instancia de base de datos.

Consola

El procedimiento siguiente quita la opción `OLEDB_ORACLE`.

Para quitar la opción OLEDB_ORACLE de su grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `OLEDB_ORACLE` (`oracle-oledb-se-2019` en los ejemplos anteriores).
4. Elija Delete option (Eliminar opción).
5. En Deletion options (Eliminar opciones), elija OLEDB_ORACLE para Options to delete (Opciones para eliminar).
6. En Apply immediately (Aplicar inmediatamente), seleccione Yes (Sí) para eliminar la opción inmediatamente o No para eliminarla en el siguiente período de mantenimiento.

7. Elija Delete (Eliminar).

CLI

El procedimiento siguiente quita la opción `OLEDB_ORACLE`.

Para quitar la opción OLEDB_ORACLE de su grupo de opciones

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds remove-option-from-option-group \
    --option-group-name oracle-oledb-se-2019 \
    --options OLEDB_ORACLE \
    --apply-immediately
```

  Para Windows:

```
aws rds remove-option-from-option-group ^
    --option-group-name oracle-oledb-se-2019 ^
    --options OLEDB_ORACLE ^
    --apply-immediately
```

Servidores enlazados con ODBC de Teradata en RDS para SQL Server

La compatibilidad para servidores enlazados con el controlador ODBC de Teradata en RDS para SQL Server le permite acceder a orígenes de datos externos en una base de datos de Teradata. Puede leer datos y ejecutar comandos desde servidores de bases de datos de Teradata remotos fuera de la instancia de RDS para SQL Server. Utilice servidores enlazados con ODBC de Teradata para habilitar las siguientes capacidades:

- Acceda directamente a orígenes de datos distintos de SQL Server.
- Realice consultas en diversos orígenes de datos de Teradata con la misma consulta sin mover los datos.
- Emita consultas, actualizaciones, comandos y transacciones distribuidas en orígenes de datos en un ecosistema empresarial.
- Integre las conexiones a una base de datos de Teradata desde el conjunto de inteligencia empresarial de Microsoft (SSIS, SSRS, SSAS).
- Migre desde una base de datos de Teradata a RDS para SQL Server.

Tiene la opción de elegir activar uno o más servidores enlazados para Teradata en una instancia de base de datos de RDS para SQL Server existente o nueva. A continuación, puede integrar orígenes de datos de Teradata externos con la instancia de base de datos.

Temas

- Versiones y regiones compatibles
- Limitaciones y recomendaciones
- Consideraciones para implementaciones multi-AZ
- Activación de servidores enlazados con Teradata
- Creación de servidores enlazados con Teradata
- Desactivación de los servidores vinculados a Teradata

Versiones y regiones compatibles

RDS para SQL Server admite servidores vinculados con ODBC de Teradata en todas las Regiones de AWS para las ediciones Standard y Enterprise de SQL Server para las siguientes versiones:

- SQL Server 2022, todas las versiones

- SQL Server 2019, todas las versiones
- SQL Server 2017, todas las versiones

Las siguientes versiones de bases de datos de Teradata admiten la vinculación con RDS para SQL Server

- Teradata 17.20, todas las versiones

Limitaciones y recomendaciones

Las siguientes limitaciones se aplican a los servidores enlazados con ODBC de Teradata:

- RDS para SQL Server admite solo la autenticación simple con un nombre de usuario y una contraseña para el origen de Teradata.
- RDS para SQL Server solo admite la versión 17.20.0.33 del controlador ODBC de Teradata.
- RDS para SQL Server no admite la creación de nombres de orígenes de datos (DSN) para usarlos como atajos para una cadena de conexión.
- RDS para SQL Server no admite el seguimiento de controladores ODBC. Utilice eventos extendidos de SQL Server para realizar un seguimiento de los eventos de ODBC. Para obtener más información, consulte Set up Extended Events in RDS for SQL Server (Configuración de eventos extendidos en RDS para SQL Server).
- RDS para SQL Server no admite el acceso a la carpeta de catálogos para un servidor vinculado a Teradata cuando se usa SQL Server Management Studio (SSMS).

Tenga en cuenta las siguientes recomendaciones cuando utilice servidores vinculados con ODBC de Teradata:

- Permita el tráfico de red añadiendo el puerto TCP correspondiente en el grupo de seguridad para cada instancia de base de datos de RDS para SQL Server. Si configura un servidor vinculado entre una instancia de base de datos de Teradata de EC2 y una instancia de base de datos de RDS para SQL Server, debe permitir el tráfico desde la dirección IP de la instancia de base de datos de Teradata de EC2. También debe permitir el tráfico en el puerto que utiliza la instancia de base de datos de RDS para SQL Server para escuchar la comunicación de la base de datos. Para obtener más información acerca de los grupos de seguridad, consulte Control de acceso con grupos de seguridad.

- Se admiten transacciones distribuidas (XA). Para activar las transacciones distribuidas, active la opción `MSDTC` del grupo de opciones de la instancia de base de datos y asegúrese de que las transacciones XA estén activadas. Para obtener más información, consulte Compatibilidad con el Coordinador de transacciones distribuidas de Microsoft en RDS for SQL Server.
- ODBC vinculados de Teradata admiten SSL/TLS siempre que estén configurados en el servidor de Teradata. Para obtener más información, consulte Habilitar la conectividad TLS en Teradata Vantage.

Consideraciones para implementaciones multi-AZ

Actualmente, RDS para SQL Server no replica los servidores vinculados en el servidor de base de datos reflejado (o en el servidor secundario del grupo de disponibilidad Always On) en una implementación multi-AZ. Si los servidores vinculados se agregan antes de cambiar la configuración para agregar replicación o Always On, entonces los servidores vinculados se copian para los servidores vinculados existentes.

Otra opción, puede crear los servidores vinculados en la instancia principal, realizar la conmutación por error a la instancia del servidor de alta disponibilidad y, a continuación, volver a crear los servidores vinculados para que estén en ambas instancias de RDS para SQL Server.

Activación de servidores enlazados con Teradata

Active los servidores enlazados con Teradata al agregar la opción `ODBC_TERADATA` a la instancia de base de datos de RDS para SQL Server. Utilice el siguiente proceso:

Temas

- Creación del grupo de opciones para ODBC_TERADATA
- Agregar la opción ODBC_TERADATA al grupo de opciones
- Asociación de la opción ODBC_TERADATA a la instancia de base de datos

Creación del grupo de opciones para **`ODBC_TERADATA`**

Para trabajar con servidores enlazados con Teradata, cree un grupo de opciones o modifique un grupo de opciones que corresponda a la edición y versión de SQL Server de la instancia de base de datos que planea utilizar. Para completar este procedimiento, utilice la AWS Management Console o la AWS CLI.

Consola

Use el siguiente procedimiento para crear un grupo de opciones para SQL Server Standard Edition 2019.

Para crear el grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En la ventana Create option group (Crear grupo de opciones), haga lo siguiente:
    a. En Name (Nombre), escriba un nombre para el grupo de opciones que sea exclusivo dentro de su Cuenta de AWS, como `teradata-odbc-se-2019`. El nombre solo puede contener letras, dígitos y guiones.
    b. Para Descripción, ingrese una breve descripción del grupo de opciones.
    c. Para Engine (Motor), elija sqlserver-se.
    d. En Major engine version (Versión principal del motor), elija 15.00.
5. Seleccione Crear.

AWS CLI

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2019.

Example

Para Linux, macOS o Unix:

```
aws rds create-option-group \
    --option-group-name teradata-odbc-se-2019 \
    --engine-name sqlserver-se \
    --major-engine-version 15.00 \
    --option-group-description "ODBC_TERADATA option group for SQL Server SE 2019"
```

Example

Para Windows:

```
aws rds create-option-group ^
    --option-group-name teradata-odbc-se-2019 ^
    --engine-name sqlserver-se ^
    --major-engine-version 15.00 ^
    --option-group-description "ODBC_TERADATA option group for SQL Server SE 2019"
```

Agregar la opción **ODBC_TERADATA** al grupo de opciones

A continuación, utilice la AWS Management Console o la AWS CLI para agregar la opción `ODBC_Teradata` al grupo de opciones.

Consola

El uso del siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2019.

Agregación de la opción de **ODBC_TERADATA**

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el nuevo grupo de opciones.
4. Elija Agregar opción.
5. En Detalles de la opción:
    a. Elija ODBC_TERADATA para Nombre de la opción.
    b. Para `17.20.33.00` para Versión de la opción.
6. En la programación, elija si desea agregar la opción inmediatamente o en el siguiente periodo de mantenimiento.
7. Elija Add option (Agregar opción).

AWS CLI

El siguiente procedimiento agrega la opción `ODBC_TERADATA` al grupo de opciones.

Example

Para Linux, macOS o Unix:

```
aws rds add-option-to-option-group \
    --option-group-name teradata-odbc-se-2019 \
    --options "OptionName=ODBC_TERADATA,OptionVersion=17.20.33.00" \
    --apply-immediately
```

Example

Para Windows:

```
aws rds add-option-to-option-group ^
    --option-group-name teradata-odbc-se-2019 ^
    --options "OptionName=ODBC_TERADATA,OptionVersion=17.20.33.00" ^
    --apply-immediately
```

Asociación de la opción **ODBC_TERADATA** a la instancia de base de datos

Para asociar el grupo de opciones de ODBC_TERADATA a la instancia de base de datos, use la AWS Management Console o la AWS CLI.

Consola

Para terminar de activar los servidores enlazados para Teradata, asocie el grupo de opciones a una instancia de base de datos nueva o existente:

- Para una nueva instancia de base de datos, asóciela cuando lance la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, asóciela modificando la instancia. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de opciones.

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mytestsqlserverteradataodbcinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 15.00 \
```

```
    --license-model license-included \
    --allocated-storage 100 \
    --master-username admin \
    --master-user-password password \
    --storage-type gp2 \
    --option-group-name teradata-odbc-se-2019
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mytestsqlserverteradataodbcinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 15.00 ^
    --license-model license-included ^
    --allocated-storage 100 ^
    --master-username admin ^
    --master-user-password password ^
    --storage-type gp2 ^
    --option-group-name teradata-odbc-se-2019
```

Para modificar una instancia y asociar el grupo de opciones nuevo:

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mytestsqlserverteradataodbcinstance \
    --option-group-name teradata-odbc-se-2019 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mytestsqlserverteradataodbcinstance ^
    --option-group-name teradata-odbc-se-2019 ^
    --apply-immediately
```

Creación de servidores enlazados con Teradata

Para crear un servidor vinculado con Teradata, ejecute los siguientes comandos:

```
EXECUTE master.dbo.sp_addlinkedserver
```

```
    @server = N'LinkedServer_NAME',
    @srvproduct=N'',
    @provider=N'MSDASQL',
    @provstr=N'"PROVIDER=MSDASQL;DRIVER={Teradata Database ODBC Driver 17.20};
                DBCName=Server;UID=user_name;PWD=user_password;
                UseDataEncryption=YES/NO;SSLMODE=PREFER/ALLOW/DISABLE>;"',
    @catalog='database'
```

```
EXECUTE master.dbo.sp_addlinkedsrvlogin
    @rmtsrvname = N'LinkedServer_NAME',
    @locallogin = NULL ,
    @useself = N'False',
    @rmtuser = N'user_name',
    @rmtpassword = N'user_password'
```

A continuación, se muestra un ejemplo de los comandos anteriores:

```
EXECUTE master.dbo.sp_addlinkedserver
    @server = N'LinkedServerToTeradata',
    @srvproduct=N'',
    @provider=N'MSDASQL',
    @provstr=N'"PROVIDER=MSDASQL;DRIVER={Teradata Database ODBC Driver 17.20};
                DBCName=my-teradata-test.cnetsipka.us-west-2.rds.amazonaws.com;
                UID=master;
                PWD=Test#1234;
                UseDataEncryption=YES;
                SSLMODE=PREFER;"',
    @catalog='MyTestTeradataDB'

EXECUTE master.dbo.sp_addlinkedsrvlogin
    @rmtsrvname = N'LinkedServerToTeradata',
    @locallogin = NULL ,
    @useself = N'False',
    @rmtuser = N'master',
    @rmtpassword = N'Test#1234'
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Desactivación de los servidores vinculados a Teradata

Para desactivar los servidores enlazados con Teradata, quite la opción `ODBC_TERADATA` de su grupo de opciones.

> **Important**
>
> La eliminación de la opción no elimina las configuraciones de servidor enlazado a la instancia de la base de datos. Debe eliminarlos manualmente para eliminarlos de la instancia de base de datos.
> Puede volver a activar `ODBC_TERADATA` después de eliminarlo para volver a utilizar las configuraciones del servidor enlazado que se configuraron previamente en la instancia de base de datos.

Consola

Eliminación de la opción `ODBC_TERADATA` del grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `ODBC_TERADATA`.
4. Elija Eliminar.
5. En Opciones de eliminación, elija `ODBC_TERADATA` en Opciones para eliminar.
6. En Apply immediately (Aplicar inmediatamente), seleccione Yes (Sí) para eliminar la opción inmediatamente o No para eliminarla en el siguiente período de mantenimiento.
7. Elija Eliminar.

AWS CLI

Los comandos siguientes eliminan la opción `ODBC_TERADATA`.

Para Linux, macOS o Unix:

```
aws rds remove-option-from-option-group \
    --option-group-name teradata-odbc-se-2019 \
```

```
    --options ODBC_TERADATA \
    --apply-immediately
```

Para Windows:

```
aws rds remove-option-from-option-group ^
    --option-group-name teradata-odbc-se-2019 ^
    --options ODBC_TERADATA ^
    --apply-immediately
```

Compatibilidad con copia de seguridad y restauración nativas en SQL Server

Al utilizar las características de copia de seguridad y restauración nativas para bases de datos de SQL Server, puede crear una copia de seguridad diferencial o completa en la base de datos que tiene en las instalaciones y almacenar los archivos de copia de seguridad en Amazon S3. A continuación, puede restaurar a una instancia de base de datos de Amazon RDS existente que ejecute SQL Server. También puede realizar una copia de seguridad de una base de datos de SQL Server de RDS, almacenarla en Amazon S3 y restaurarla en otras ubicaciones. Además, puede restaurar la copia de seguridad a un servidor local, o bien a otra instancia de base de datos de Amazon RDS que ejecute SQL Server. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.

Amazon RDS da soporte a la copia de seguridad y la restauración nativas de bases de datos de Microsoft SQL Server mediante los archivos de copia de seguridad diferenciales y completos (archivos .bak).

Adición de opciones de copia de seguridad y restauración nativas

El proceso general para añadir la opción de copia de seguridad y restauración nativas a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción `SQLSERVER_BACKUP_RESTORE` al grupo de opciones.
3. Asocie un rol de AWS Identity and Access Management (IAM) con la opción. El rol de IAM debe tener acceso a un bucket de S3 para almacenar las copias de seguridad de base de datos.

   Es decir, la opción debe tener como ajuste de opción un nombre de recurso de Amazon (ARN) válido en el formato `arn:aws:iam::`*`account-id`*`:role/`*`role-name`*. Para obtener más información, consulte Nombres de recurso de Amazon (ARN) en la Referencia general de AWS.

   El rol de IAM también debe tener una relación de confianza y una política de permisos adjunta. La relación de confianza permite a RDS asumir el rol y la política de permisos define las acciones que puede realizar el rol. Para obtener más información, consulte Creación manual de un rol de IAM para la copia de seguridad y la restauración nativas.
4. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir la opción de copia de seguridad y restauración nativas, no es necesario reiniciar la instancia de base de datos. En cuanto el grupo de opciones esté activo, podrá empezar a crear copias de seguridad y restauraciones.

Consola

Para añadir la opción de copia de seguridad y restauración nativas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Cree un nuevo grupo de opciones o utilice un grupo de opciones existente. Para obtener más información sobre cómo crear un grupo de opciones de base de datos personalizado, consulte Creación de un grupo de opciones.

   Para utilizar un grupo de opciones existente, vaya al siguiente paso.
4. Añada la opción SQLSERVER_BACKUP_RESTORE al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
5. Aplique alguna de las siguientes acciones:

   - Para utilizar un rol de IAM existente y configuración de Amazon S3, elija un rol de IAM existente para IAM Role (Rol de IAM). Si utiliza un rol de IAM existente, RDS utiliza los ajustes de Amazon S3 configurados para este rol.
   - Para crear un nuevo rol y establecer las configuraciones de Amazon S3, haga lo siguiente:
     1. En IAM Role (Rol de IAM), elija Create a New Role (Crear un nuevo rol).
     2. Para S3 bucket (bucket de S3), elija un bucket de S3 de la lista.
     3. En S3 prefix (optional) (Prefijo de S3 [opcional]), especifique un prefijo para usarlo con los archivos almacenados en el bucket de Amazon S3.

        Este prefijo puede incluir una ruta de archivo, pero no es obligatorio. Si proporciona un prefijo, RDS asocia dicho prefijo a todos los archivos de copia de seguridad. RDS utiliza a continuación el prefijo durante una restauración para identificar archivos relacionados y omitir archivos irrelevantes. Por ejemplo, podría usar el bucket de S3 para otros fines además de mantener archivos de copia de seguridad. En este caso, puede utilizar el prefijo para que RDS realice la copia de seguridad y restauración nativas solo en una carpeta específica y sus subcarpetas.

Si deja el prefijo en blanco, RDS no utiliza un prefijo para identificar archivos de copia de seguridad o archivos que restaurar. En consecuencia, durante una restauración de varios archivos, RDS trata de restaurar todos los archivos de todas las carpetas del bucket de S3.

4. Elija la casilla Enable Encryption (habilitar cifrado) para cifrar el archivo de copia de seguridad. No seleccione la casilla de verificación (predeterminada) para que el archivo de copia de seguridad no esté cifrado.

   Si eligió Enable encryption (habilitar cifrado), seleccione una clave de cifrado para AWS KMS key. Para obtener más información acerca de las claves de cifrado, consulte la introducción en la guía para desarrolladores de AWS Key Management Service.

6. Elija Add option (Agregar opción).
7. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

CLI

En este procedimiento se parte de las siguientes suposiciones:

- Usted está agregando la opción SQLSERVER_BACKUP_RESTORE a un grupo de opciones que ya existe. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
- Está asociando la opción a un rol de IAM que ya existe y tiene acceso a un bucket de S3 para almacenar las copias de seguridad.
- Está aplicando el grupo de opciones a una instancia de base de datos que ya existe. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Para agregar la opción de copia de seguridad y restauración nativas

1. Añada la opción `SQLSERVER_BACKUP_RESTORE` al grupo de opciones.

Example

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
 --apply-immediately \
 --option-group-name mybackupgroup \
 --options "OptionName=SQLSERVER_BACKUP_RESTORE, \
   OptionSettings=[{Name=IAM_ROLE_ARN,Value=arn:aws:iam::account-id:role/role-
name}]"
```

En:Windows

```
aws rds add-option-to-option-group ^
 --option-group-name mybackupgroup ^
 --options "[{\"OptionName\": \"SQLSERVER_BACKUP_RESTORE\", ^
 \"OptionSettings\": [{\"Name\": \"IAM_ROLE_ARN\", ^
 \"Value\": \"arn:aws:iam::account-id:role/role-name"}]}]" ^
 --apply-immediately
```

> **Note**
>
> Al utilizar el símbolo del sistema de Windows, debe aplicar escape con comillas dobles (") en código JSON al ponerlas como prefijo con una barra invertida (\).

2. Aplique el grupo de opciones a la instancia de base de datos.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
 --db-instance-identifier mydbinstance \
 --option-group-name mybackupgroup \
 --apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
 --db-instance-identifier mydbinstance ^
```

```
    --option-group-name mybackupgroup ^
    --apply-immediately
```

Modificación de opciones de copia de seguridad y restauración nativas

Después de habilitar la opción de copia de seguridad y restauración nativas, puede modificar su configuración. Para obtener más información acerca de cómo modificar la configuración de las opciones, consulte Modificación de una configuración de opciones.

Quitar la opción de copia de seguridad y restauración nativas

Puede desactivar la característica de copia de seguridad y restauración nativas eliminando la opción de su instancia de base de datos. Después de eliminar la opción de copia de seguridad y restauración nativas, no es necesario reiniciar la instancia de base de datos.

Para eliminar la opción de copia de seguridad y restauración nativas de una instancia de base de datos, lleve a cabo el siguiente procedimiento:

- Quite la opción del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
- Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción de copia de seguridad y restauración nativas. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Compatibilidad con el Cifrado de datos transparente en SQL Server

Amazon RDS admite el Cifrado de datos transparente (TDE) para cifrar los datos almacenados en las instancias de base de datos en las que se ejecuta Microsoft SQL Server. La característica TDE cifra automáticamente los datos antes de que se escriban en el sistema de almacenamiento y los descifra también automáticamente cuando se leen.

Amazon RDS admite TDE para las siguientes versiones y ediciones de SQL Server:

- SQL Server 2022: Standard y Enterprise Editions
- SQL Server 2019: Standard y Enterprise Editions
- SQL Server 2017 Enterprise Edition
- SQL Server 2016 Enterprise Edition

Con el cifrado de datos transparente para SQL Server se ofrece administración de claves de cifrado mediante el uso de una arquitectura de claves de dos niveles. Para proteger las claves de cifrado de datos se usa un certificado generado desde la clave maestra de la base de datos. La clave de cifrado de base de datos efectúa el cifrado y descifrado real de los datos en la base de datos del usuario. Amazon RDS crea copias de seguridad y administra la clave maestra de la base de datos y el certificado de TDE

El cifrado de datos transparente se usa en situaciones en las que es necesario cifrar información confidencial. Por ejemplo, es posible que desee proporcionar archivos de datos y copias de seguridad a un tercero, o bien solucionar problemas de cumplimiento normativo relacionados con la seguridad. No puede cifrar las bases de datos del sistema para SQL Server, por ejemplo las bases de datos `model` o `master`.

Ofrece una descripción detallada del cifrado de datos transparente va más allá del alcance de esta guía, pero asegúrese de conocer los puntos fuertes y débiles de cada algoritmo y cada clave de cifrado. Para obtener información sobre el cifrado transparente de datos para SQL Server, consulte Transparent Data Encryption (TDE) (Cifrado transparente de datos) en la documentación de Microsoft.

Temas

- Activación de TDE en RDS para SQL Server
- Cifrado de datos en RDS para SQL Server
- Copia de seguridad y restauración de certificados TDE en RDS para SQL Server

- Copia de seguridad y restauración de certificados TDE para bases de datos en las instalaciones
- Desactivación de TDE en RDS para SQL Server

Activación de TDE en RDS para SQL Server

A fin de activar el cifrado de datos transparente para una instancia de base de datos de SQL Server de RDS, especifique la opción de TDE en un grupo de opciones de RDS que esté asociado con esa instancia de base de datos:

1. Determine si la instancia de base de datos ya está asociada con un grupo de opciones que tiene la opción TDE. Para ver el grupo de opciones al que está asociada una instancia de base de datos, utilice la consola de RDS, el comando describe-db-instance de la AWS CLI o la operación DescribeDBInstances de la API.
2. Si la instancia de base de datos no está asociada a un grupo de opciones con TDE activado, dispone de dos alternativas: Puede crear un grupo de opciones o añadir la opción TDE, o bien modificar el grupo de opciones asociado para añadirla.

   > **Note**
   >
   > En la consola de RDS, la opción se denomina `TRANSPARENT_DATA_ENCRYPTION`. En la AWS CLI y la API de RDS, se denomina `TDE`.

   Para obtener información acerca de cómo crear o modificar un grupo de opciones, consulte Trabajo con grupos de opciones. Para obtener información acerca de cómo añadir una opción a un grupo de opciones, consulte Agregar una opción a un grupo de opciones.
3. Asocie la instancia de base de datos al grupo de opciones que tiene la opción TDE. Para obtener información acerca de cómo asociar una instancia de base de datos a un grupo de opciones, consulte Modificación de una instancia de base de datos de Amazon RDS.

Consideraciones relativas al grupo de opciones

La opción TDE es persistente. No se puede eliminar de un grupo de opciones a menos que todas las instancias de base de datos y las copias de seguridad dejen de estar asociadas al grupo de opciones. Una vez que la opción TDE se agrega a un grupo de opciones, este solo se puede asociar a instancias de base de datos que usan TDE. Para obtener más información acerca de las opciones persistentes de un grupo de opciones, use Información general sobre grupos de opciones.

Como TDE es una opción persistente, puede producirse un conflicto entre el grupo de opciones y una instancia de base de datos asociada. Puede tener un conflicto en las siguientes situaciones:

- El grupo de opciones actual tiene la opción TDE y lo reemplaza por un grupo de opciones que no la tiene.
- Restaura desde una instantánea de base de datos a una nueva instancia de base de datos que no tiene un grupo de opciones que contenga la opción TDE. Para obtener más información acerca de esta situación, consulte Aspectos a tener en cuenta sobre los grupos de opciones.

Consideraciones sobre el rendimiento de SQL Server

El uso del cifrado de datos transparente puede afectar al rendimiento de una instancia de base de datos de SQL Server.

El desempeño de las bases de datos sin cifrar puede reducirse también si están en una instancia de base de datos que tenga al menos una base de datos cifrada. Como resultado, es recomendable mantener las bases de datos cifradas y sin cifrar en instancias de base de datos diferentes.

Cifrado de datos en RDS para SQL Server

Cuando la opción TDE se agrega a un grupo de opciones, Amazon RDS genera un certificado que se usa en el proceso de cifrado. A continuación puede usar el certificado para ejecutar instrucciones SQL que cifren los datos de una base de datos de la instancia de base de datos.

En el siguiente ejemplo se usa un certificado creado por RDS llamado `RDSTDECertificateName` para cifrar una base de datos denominada `myDatabase`.

```
---------- Turning on TDE -------------

-- Find an RDS TDE certificate to use
USE [master]
GO
SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'
GO

USE [myDatabase]
GO
-- Create a database encryption key (DEK) using one of the certificates from the
 previous step
CREATE DATABASE ENCRYPTION KEY WITH ALGORITHM = AES_256
```

```
ENCRYPTION BY SERVER CERTIFICATE [RDSTDECertificateName]
GO

-- Turn on encryption for the database
ALTER DATABASE [myDatabase] SET ENCRYPTION ON
GO

-- Verify that the database is encrypted
USE [master]
GO
SELECT name FROM sys.databases WHERE is_encrypted = 1
GO
SELECT db_name(database_id) as DatabaseName, * FROM sys.dm_database_encryption_keys
GO
```

El tiempo que tarda en cifrarse una base de datos de SQL Server con TDE depende de varios factores. Estos incluyen el tamaño de la instancia de base de datos, si la instancia usa el almacenamiento de IOPS aprovisionadas, la cantidad de datos y otros factores.

Copia de seguridad y restauración de certificados TDE en RDS para SQL Server

RDS para SQL Server proporciona procedimientos almacenados para realizar copias de seguridad de los certificados TDE, restaurarlos y eliminarlos. RDS para SQL Server también proporciona una función para ver los certificados TDE de usuario restaurados.

Los certificados TDE de usuario se utilizan para restaurar las bases de datos en RDS para SQL Server que están en las instalaciones y tienen TDE activado. Estos certificados tienen el prefijo `UserTDECertificate_`. Después de restaurar las bases de datos, y antes de hacer que estén disponibles para usarlas, RDS modifica las bases de datos que tienen TDE activado a fin de utilizar los certificados TDE generados por RDS. Estos certificados tienen el prefijo `RDSTDECertificate`.

Los certificados TDE de usuario permanecen en la instancia de base de datos de RDS para SQL Server, a menos que los elimine mediante el procedimiento almacenado `rds_drop_tde_certificate`. Para obtener más información, consulte Eliminación de certificados TDE restaurados.

Puede utilizar un certificado TDE de usuario para restaurar otras bases de datos desde la instancia de base de datos de origen. Las bases de datos que se van a restaurar deben utilizar el mismo certificado TDE y tener TDE activado. No tiene que volver a importar (restaurar) el mismo certificado.

Temas

- Requisitos previos
- Limitaciones
- Copia de seguridad de un certificado TDE
- Restauración de un certificado TDE
- Visualización de certificados TDE
- Eliminación de certificados TDE restaurados

Requisitos previos

Para poder hacer una copia de seguridad de los certificados TDE o restaurarlos en RDS para SQL Server, asegúrese de realizar las siguientes tareas. Las tres primeras se describen en Configuración de la copia de seguridad y la restauración nativas.

1. Cree buckets de Amazon S3 a fin de almacenar archivos para copia de seguridad y restauración.

   Le recomendamos que utilice buckets distintos para las copias de seguridad de la base de datos y para las copias de seguridad de los certificados TDE.
2. Cree un rol de IAM para hacer copias de seguridad de los archivos y restaurarlos.

   El rol de IAM debe ser tanto un usuario como un administrador para la AWS KMS key.

   Además de los permisos necesarios para la copia de seguridad y restauración nativas de SQL Server, el rol de IAM también requiere los siguientes permisos:
   - `s3:GetBucketAcl`, `s3:GetBucketLocation` y `s3:ListBucket` en el recurso de bucket de S3
   - `s3:ListAllMyBuckets` en el recurso `*`
3. Agregue la opción `SQLSERVER_BACKUP_RESTORE` a un grupo de opciones en su instancia de base de datos.

   Esto se agrega a la opción `TRANSPARENT_DATA_ENCRYPTION` (`TDE`).
4. Asegúrese de que tiene una clave de KMS de cifrado simétrica. Dispone de las opciones siguientes:
   - Si ya dispone de una clave de KMS en la cuenta, puede utilizarla. No hay que hacer nada más.
   - Si no tiene una clave de cifrado KMS simétrica existente en su cuenta, cree una clave KMS mediante las instrucciones de Creating keys (Crear claves) en la AWS Key Management ServiceDeveloper Guide (Guía para desarrolladores).

5. Habilite la integración de Amazon S3 para transferir archivos entre la instancia de base de datos y Amazon S3.

   Para obtener información sobre la habilitación de la integración de Amazon S3, consulte Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3.

Limitaciones

El uso de procedimientos almacenados para hacer copias de seguridad de certificados TDE y restaurarlos tiene las siguientes limitaciones:

- Las opciones `SQLSERVER_BACKUP_RESTORE` y `TRANSPARENT_DATA_ENCRYPTION` (`TDE`) deben agregarse al grupo de opciones que haya asociado a su instancia de base de datos.
- Las copias de seguridad y la restauración de los certificados TDE no son compatibles con las instancias de base de datos Multi-AZ.
- No se admite la cancelación de tareas de copia de seguridad y restauración de certificados TDE.
- No puede utilizar un certificado TDE de usuario para el cifrado TDE de otra base de datos en su instancia de base de datos RDS para SQL Server. Puede utilizarlo para restaurar solo otras bases de datos de la instancia de base de datos de origen que tengan TDE activado y que utilicen el mismo certificado TDE.
- Solo puede eliminar certificados TDE de usuario.
- El número máximo de certificados TDE de usuario admitidos en RDS es 10. Si el número es superior a diez, elimine los certificados TDE no utilizados y vuelva a intentarlo.
- El nombre del certificado no puede estar vacío ni ser nulo.
- Al restaurar un certificado, su nombre no puede incluir la palabra clave `RDSTDECERTIFICATE` y debe comenzar por el prefijo `UserTDECertificate_`.
- El parámetro `@certificate_name` solo puede incluir los siguientes caracteres: a-z, 0-9, @, $, # y guion bajo (_).
- La extensión del archivo para `@certificate_file_s3_arn` debe ser .cer (no se distingue entre mayúsculas y minúsculas).
- La extensión del archivo para `@private_key_file_s3_arn` debe ser .pvk (no se distingue entre mayúsculas y minúsculas).
- Los metadatos S3 del archivo de clave privada deben incluir la etiqueta `x-amz-meta-rds-tde-pwd`. Para obtener más información, consulte Copia de seguridad y restauración de certificados TDE para bases de datos en las instalaciones.

Copia de seguridad de un certificado TDE

Para hacer copias de seguridad de los certificados TDE, utilice el procedimiento almacenado `rds_backup_tde_certificate`. Tiene la siguiente sintaxis.

```
EXECUTE msdb.dbo.rds_backup_tde_certificate
    @certificate_name='UserTDECertificate_certificate_name |
 RDSTDECertificatetimestamp',
    @certificate_file_s3_arn='arn:aws:s3:::bucket_name/certificate_file_name.cer',
    @private_key_file_s3_arn='arn:aws:s3:::bucket_name/key_file_name.pvk',
    @kms_password_key_arn='arn:aws:kms:region:account-id:key/key-id',
    [@overwrite_s3_files=0|1];
```

Se requieren los siguientes parámetros:

- `@certificate_name`: nombre del certificado TDE del que se hará una copia de seguridad.
- `@certificate_file_s3_arn`: nombre de recurso de Amazon (ARN) de destino para el archivo de copia de seguridad de certificados en Amazon S3.
- `@private_key_file_s3_arn`: ARN de S3 de destino del archivo de clave privada que protege el certificado TDE.
- `@kms_password_key_arn`: ARN de la clave de KMS simétrica utilizada para cifrar la contraseña de clave privada.

El siguiente parámetro es opcional:

- `@overwrite_s3_files`: indica si se deben sobrescribir los archivos de certificado y de clave privada existentes en S3:
  - `0`: no se sobrescriben los archivos existentes. Este valor es el valor predeterminado.

    Al establecer `@overwrite_s3_files` en 0, se devuelve un error si ya existe un archivo.
  - `1`: se sobrescribe un archivo existente que tenga el nombre especificado, aunque no sea un archivo de copia de seguridad.

Example de copia de seguridad de un certificado TDE

```
EXECUTE msdb.dbo.rds_backup_tde_certificate
    @certificate_name='RDSTDECertificate20211115T185333',
    @certificate_file_s3_arn='arn:aws:s3:::TDE_certs/mycertfile.cer',
```

```
    @private_key_file_s3_arn='arn:aws:s3:::TDE_certs/mykeyfile.pvk',
    @kms_password_key_arn='arn:aws:kms:us-
west-2:123456789012:key/AKIAIOSFODNN7EXAMPLE',
    @overwrite_s3_files=1;
```

Restauración de un certificado TDE

Use el procedimiento almacenado `rds_restore_tde_certificate` para restaurar (importar) certificados TDE de usuario. Tiene la siguiente sintaxis.

```
EXECUTE msdb.dbo.rds_restore_tde_certificate
    @certificate_name='UserTDECertificate_certificate_name',
    @certificate_file_s3_arn='arn:aws:s3:::bucket_name/certificate_file_name.cer',
    @private_key_file_s3_arn='arn:aws:s3:::bucket_name/key_file_name.pvk',
    @kms_password_key_arn='arn:aws:kms:region:account-id:key/key-id';
```

Se requieren los siguientes parámetros:

- `@certificate_name`: nombre del certificado TDE que se va a restaurar. El nombre debe comenzar por el prefijo `UserTDECertificate_`.
- `@certificate_file_s3_arn`: ARN de S3 del archivo de copia de seguridad que se usa para restaurar el certificado TDE.
- `@private_key_file_s3_arn`: ARN de S3 del archivo de copia de seguridad de clave privada del certificado TDE que se va a restaurar.
- `@kms_password_key_arn`: ARN de la clave de KMS simétrica utilizada para cifrar la contraseña de clave privada.

Example de restauración de un certificado TDE

```
EXECUTE msdb.dbo.rds_restore_tde_certificate
    @certificate_name='UserTDECertificate_myTDEcertificate',
    @certificate_file_s3_arn='arn:aws:s3:::TDE_certs/mycertfile.cer',
    @private_key_file_s3_arn='arn:aws:s3:::TDE_certs/mykeyfile.pvk',
    @kms_password_key_arn='arn:aws:kms:us-
west-2:123456789012:key/AKIAIOSFODNN7EXAMPLE';
```

Visualización de certificados TDE

Use la función `rds_fn_list_user_tde_certificates` para ver los certificados TDE de usuario restaurados (importados). Tiene la siguiente sintaxis.

```
SELECT * FROM msdb.dbo.rds_fn_list_user_tde_certificates();
```

La salida se parece a la siguiente. Aquí no se muestran todas las columnas.

name	certif te_id	princi _id	pvt_ke ncrypt _type_ c	issuer me	cert_s al_num	thumbp t	subjec	start_ e	expiry te	pvt_key_l ast_backu p_date
UserTD rtific _tde_c	343	1	ENCRYP _BY_MA R_KEY	AnyCom y Shippi	79 3e 57 a3 69 fd 1d 9e 47 2c 32 67 1d 9c ca af	0x6BB2 341103 80B FE1BA2 C69509 5B5	AnyCom y Shippi	2022-0 5 19:49: 000000	2023-0 5 19:49: 000000	NULL

Eliminación de certificados TDE restaurados

Para eliminar los certificados TDE de usuario restaurados (importados) que no esté utilizando, utilice el procedimiento almacenado `rds_drop_tde_certificate`. Tiene la siguiente sintaxis.

```
EXECUTE msdb.dbo.rds_drop_tde_certificate
 @certificate_name='UserTDECertificate_certificate_name';
```

El siguiente parámetro es obligatorio:

- `@certificate_name`: el nombre del certificado TDE que se va a eliminar.

Solo puede eliminar los certificados TDE restaurados (importados). No se pueden eliminar los certificados creados por RDS.

Example de eliminación de un certificado TDE

```
EXECUTE msdb.dbo.rds_drop_tde_certificate
 @certificate_name='UserTDECertificate_myTDEcertificate';
```

Copia de seguridad y restauración de certificados TDE para bases de datos en las instalaciones

Puede realizar una copia de seguridad de los certificados TDE para las bases de datos en las instalaciones y, posteriormente, restaurarlos en RDS para SQL Server. También puede restaurar un certificado TDE de RDS para SQL Server en una instancia de base de datos en las instalaciones.

El siguiente procedimiento hace una copia de seguridad de un certificado TDE y una clave privada. La clave privada se cifra mediante una clave de datos generada a partir de su clave de KMS de cifrado simétrico.

Para hacer una copia de seguridad de un certificado TDE en las instalaciones

1. Genere la clave de datos mediante el comando generate-data-key de AWS CLI.

   ```
   aws kms generate-data-key \
       --key-id my_KMS_key_ID \
       --key-spec AES_256
   ```

   La salida se parece a la siguiente.

   ```
   {
   "CiphertextBlob": "AQIDAHimL2NEoAlOY6Bn7LJfnxi/OZe9kTQo/
   XQXduug1rmerwGiL7g5ux4av9GfZLxYTDATAAAAfjB8BgkqhkiG9w0B
   ```

```
BwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMyCxLMi7GRZgKqD65AgEQgDtjvZLJo2cQ31Vetng
2RezQy3sAS6ZHrCjfnfn0c65bFdhsXxjSMnudIY7AKw==",
"Plaintext": "U/fpGtmzGCYBi8A2+0/9qcRQRK2zmG/aOn939ZnKi/0=",
"KeyId": "arn:aws:kms:us-west-2:123456789012:key/1234abcd-00ee-99ff-88dd-
aa11bb22cc33"
}
```

La salida de texto sin formato se utiliza en el siguiente paso como contraseña de la clave privada.

2. Haga una copia de seguridad de su certificado TDE como se muestra en el siguiente ejemplo.

```
BACKUP CERTIFICATE myOnPremTDEcertificate TO FILE = 'D:\tde-cert-backup.cer'
WITH PRIVATE KEY (
FILE = 'C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\cert-
backup-key.pvk',
ENCRYPTION BY PASSWORD = 'U/fpGtmzGCYBi8A2+0/9qcRQRK2zmG/aOn939ZnKi/0=');
```

3. Guarde el archivo de copia de seguridad de certificados en el bucket de certificados de Amazon S3.
4. Guarde el archivo de copia de seguridad de clave privada en su bucket de certificados de S3, con la siguiente etiqueta en los metadatos del archivo:

   - Clave: `x-amz-meta-rds-tde-pwd`
   - Valor: el valor de `CiphertextBlob` de la generación de la clave de datos, como en el siguiente ejemplo.

     ```
     AQIDAHimL2NEoAlOY6Bn7LJfnxi/OZe9kTQo/
     XQXduug1rmerwGiL7g5ux4av9GfZLxYTDATAAAAfjB8BgkqhkiG9w0B
     BwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMyCxLMi7GRZgKqD65AgEQgDtjvZLJo2cQ31Vet
     2RezQy3sAS6ZHrCjfnfn0c65bFdhsXxjSMnudIY7AKw==
     ```

El siguiente procedimiento restaura un certificado TDE de RDS para SQL Server en una instancia de base de datos en las instalaciones. Copie y restaure el certificado TDE en su instancia de base de datos de destino mediante la copia de seguridad del certificado, el archivo de clave privada correspondiente y la clave de datos. El certificado restaurado está cifrado con la clave maestra de base de datos del nuevo servidor.

Para restaurar un certificado TDE

1. Copie el archivo de copia de seguridad del certificado TDE y el archivo de clave privada de Amazon S3 en la instancia de destino. Para obtener más información sobre la copia de archivos desde Amazon S3, consulte Transferencia de archivos entre RDS for SQL Server y Amazon S3.
2. Utilice la clave de KMS para descifrar el texto de cifrado de salida y recuperar el texto sin formato de la clave de datos. El texto de cifrado se encuentra en los metadatos de S3 del archivo de copia de seguridad de la clave privada.

   ```
   aws kms decrypt \
       --key-id my_KMS_key_ID \
       --ciphertext-blob fileb://exampleCiphertextFile | base64 -d \
       --output text \
       --query Plaintext
   ```

   La salida de texto sin formato se utiliza en el siguiente paso como contraseña de la clave privada.
3. Utilice el siguiente comando SQL para restaurar su certificado TDE.

   ```
   CREATE CERTIFICATE myOnPremTDEcertificate FROM FILE='D:\tde-cert-backup.cer'
   WITH PRIVATE KEY (FILE = N'D:\tde-cert-key.pvk',
   DECRYPTION BY PASSWORD = 'plain_text_output');
   ```

Para obtener más información sobre el descifrado de KMS, consulte decrypt en la sección KMS de la referencia de comandos de AWS CLI.

Una vez restaurado el certificado TDE en la instancia de base de datos de destino, podrá restaurar las bases de datos cifradas con ese certificado.

> **Note**
>
> Puede utilizar el mismo certificado TDE para cifrar varias bases de datos de SQL Server en la instancia de base de datos de origen. Para migrar varias bases de datos a una instancia de destino, copie el certificado TDE asociado a ellas en la instancia de destino solo una vez.

Desactivación de TDE en RDS para SQL Server

Para desactivar TDE en una instancia de base de datos de RDS para SQL Server, asegúrese primero de que no quedan objetos cifrados en la instancia de base de datos. Para ello, descifre los objetos o elimínelos. Si existe algún objeto cifrado en la instancia de base de datos, no podrá desactivar TDE para la instancia de base de datos. Al usar la consola para eliminar la opción TDE de un grupo de opciones, la consola indica que se está procesando. Además, se creará un evento de error si el grupo de opciones se asocia a una instantánea de base de datos o una instancia de base de datos cifrada.

En el siguiente ejemplo se elimina el cifrado de TDE de una base de datos llamada `customerDatabase`.

```
------------- Removing TDE ----------------

USE [customerDatabase]
GO

-- Turn off encryption of the database
ALTER DATABASE [customerDatabase]
SET ENCRYPTION OFF
GO

-- Wait until the encryption state of the database becomes 1. The state is 5
 (Decryption in progress) for a while
SELECT db_name(database_id) as DatabaseName, * FROM sys.dm_database_encryption_keys
GO

-- Drop the DEK used for encryption
DROP DATABASE ENCRYPTION KEY
GO

-- Alter to SIMPLE Recovery mode so that your encrypted log gets truncated
USE [master]
GO
ALTER DATABASE [customerDatabase] SET RECOVERY SIMPLE
GO
```

Cuando todos los objetos estén descifrados, tendrá a su disposición dos opciones:

1. Puede modificar la instancia de base de datos para asociarla a un grupo de opciones sin la opción TDE.

2. Puede quitar la opción TDE del grupo de opciones.

SQL Server Audit

En Amazon RDS, puede auditar las bases de datos de Microsoft SQL Server mediante el mecanismo de auditoría de SQL Server integrado. Puede crear auditorías y especificaciones de auditoría del mismo modo que las crea para los servidores de base de datos locales.

RDS carga los registros de auditoría completados en su bucket de S3 mediante el rol de IAM que proporciona. Si habilita la retención, RDS conservará sus registros de auditoría en su instancia de base de datos durante el periodo de tiempo configurado.

Para obtener más información, consulte la sección sobre SQL Server Audit (motor de base de datos) en la documentación de Microsoft SQL Server.

Auditoría de SQL Server con flujos de actividad de bases de datos

Puede utilizar los flujos de actividad de bases de datos para RDS para integrar los eventos de SQL Server Audit con las herramientas de supervisión de la actividad de las bases de datos de Imperva, McAfee e IBM. Para obtener más información acerca de cómo auditar con flujos de actividad de bases de datos para RDS SQL Server, consulte Auditoría en Microsoft SQL Server

Temas

- Compatibilidad con SQL Server Audit
- Incorporación de SQL Server Audit a las opciones de instancia de base de datos
- Uso de SQL Server Audit
- Visualización de registros de auditoría
- Uso de SQL Server Audit con instancias Multi-AZ
- Configuración de un bucket de S3
- Creación manual de un rol de IAM para SQL Server Audit

Compatibilidad con SQL Server Audit

En Amazon RDS, a partir de SQL Server 2016, todas las ediciones de SQL Server admiten auditorías de nivel de servidor y la edición Enterprise también admite auditorías de nivel de base de datos. A partir de SQL Server 2016 (13.x) SP1, todas las ediciones admiten tanto auditorías de nivel de servidor como de nivel de base de datos. Para obtener más información, consulte SQL Server Audit (motor de base de datos) en la documentación de SQL Server.

RDS admite ajustar la siguiente configuración de opciones para SQL Server Audit.

Ajuste de la opción	Valores válidos	Descripción
`IAM_ROLE_ARN`	Nombre de recurso de Amazon (ARN) válido en el formato `arn:aws:iam::` *`account-id`* `:role/`*`role-name`* .	ARN del rol de IAM que concede acceso al bucket de S3 donde desea almacenar sus registros de auditoría. Para obtener más información, consulte Nombres de recurso de Amazon (ARN) en la Referencia general de AWS.
`S3_BUCKET_ARN`	ARN válido en el formato `arn:aws:s3:::` *`amzn-s3-demo-bucket`* o `arn:aws:s3:::` *`amzn-s3-demo-bucket`* `/key-prefix`	ARN para el bucket de S3 donde desea almacenar sus registros de auditoría.
`ENABLE_COMPRESSION`	`true` o `false`	Controla la compresión de registros de auditoría. De forma predeterminada, la compresión está habilitada (establecida en `true`).
`RETENTION_TIME`	`0` De a `840`	El tiempo de retención (en horas) durante el que se conservan los registros de auditoría de SQL Server en su instancia RDS. De forma predeterminada, la retención está deshabilitada.

Incorporación de SQL Server Audit a las opciones de instancia de base de datos

Habilitar SQL Server Audit requiere dos pasos: habilitar la opción en la instancia de base de datos y habilitar la característica dentro de SQL Server. El proceso de incorporación de la opción SQL Server Audit a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada y configure todas las opciones necesarias.
3. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir la opción SQL Server Audit, no es necesario reiniciar la instancia de base de datos. En cuanto el grupo de opciones esté activo, podrá crear auditorías y almacenar registros de auditoría en su bucket de S3.

Para añadir y configurar SQL Server Audit en el grupo de opciones de una instancia de base de datos

1. Elija una de las siguientes opciones:
   - Use un grupo de opciones existente.
   - Cree un grupo de opciones de base de datos personalizado y úselo. Para obtener más información, consulte Creación de un grupo de opciones.
2. Agregue la opción SQLSERVER_AUDIT al grupo de opciones y establezca la configuración de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
   - En Rol de IAM, si ya tiene un rol de IAM con las políticas necesarias, puede elegir ese rol. Para crear un nuevo rol de IAM, elija Crear un nuevo rol. Para obtener información acerca de las políticas necesarias, consulte Creación manual de un rol de IAM para SQL Server Audit.
   - En la opción para Select S3 destination (Seleccionar el destino de S3), si ya dispone de un bucket de S3 que desee usar, elíjalo. Para crear un bucket de S3, elija Create a New S3 Bucket (Crear un nuevo bucket de S3).
   - En Enable Compression (Habilitar compresión), deje esta opción elegida para comprimir archivos de auditoría. La compresión está habilitada de forma predeterminada. Para deshabilitar la compresión, borre Enable Compression (Habilitar compresión).

- En Audit log retention (Retención de registros de auditoría), para conservar los registros de auditoría en la instancia de base de datos, elija esta opción. Especifique un tiempo de retención en horas. El tiempo de retención máximo son 35 días.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente. Elija una de las siguientes opciones:

   - Si está creando una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia.
   - En una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Modificación de la opción SQL Server Audit

Después de habilitar la opción SQL Server Audit, puede modificar la configuración. Para obtener más información acerca de cómo modificar la configuración de opciones, consulte Modificación de una configuración de opciones.

Eliminación de SQL Server Audit de las opciones de instancia de base de datos

Puede desactivar la característica SQL Server Audit deshabilitando las auditorías y, a continuación, eliminando la opción.

Para eliminar auditorías

1. Deshabilite toda la configuración de auditorías dentro de SQL Server. Para obtener información acerca de dónde se ejecutan las auditorías, consulte las vistas de catálogo de seguridad de SQL Server. Para obtener más información, consulte la sección sobre Vistas de catálogo de seguridad en la documentación de Microsoft SQL Server.
2. Elimine la opción SQL Server Audit de la instancia de base de datos. Elija una de las siguientes opciones:

   - Elimine la opción SQL Server Audit del grupo de opciones que la instancia de base de datos usa. Este cambio afecta a todas las instancias de base de datos que utilizan el mismo grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
   - Modifique la instancia de base de datos y, a continuación, elija un grupo de opciones sin la opción SQL Server Audit. Este cambio solo afecta a la instancia de base de datos que

modifique. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

3. Una vez que elimine la opción SQL Server Audit de la instancia de base de datos, no será necesario reiniciar la instancia. Elimine los archivos de auditoría innecesarios de su bucket de S3.

Uso de SQL Server Audit

Puede controlar auditorías de servidor y especificaciones de auditoría tanto de servidor como de base de datos del mismo modo que las controla para servidores de base de datos locales.

Creación de auditorías

Crea auditorías de servidor del mismo modo que las crea para los servidores de base de datos locales. Para obtener información acerca de cómo crear auditorías de servidor, consulte CREATE SERVER AUDIT en la documentación de Microsoft SQL Server.

Para evitar errores, cumpla las siguientes limitaciones:

- No sobrepase el número máximo de auditorías de servidor admitidas por instancia de 50.
- Pida a SQL Server que escriba datos en un archivo binario.
- No use `RDS_` como prefijo en el nombre de auditoría de servidor.
- En `FILEPATH`, especifique `D:\rdsdbdata\SQLAudit`.
- En `MAXSIZE`, especifique un tamaño entre 2 y 50 MB.
- No configure `MAX_ROLLOVER_FILES` ni `MAX_FILES`.
- No configure SQL Server para cerrar la instancia de base de datos si no escribe el registro de auditoría.

Creación de especificaciones de auditoría

Puede crear especificaciones de auditoría tanto de servidor como de base de datos del mismo modo que las crea para servidores de base de datos locales. Para obtener información acerca de cómo crear especificaciones de auditoría, consulte CREATE SERVER AUDIT SPECIFICATION y CREATE DATABASE AUDIT SPECIFICATION en la documentación de Microsoft SQL Server.

Para evitar errores, no use `RDS_` como prefijo en el nombre de la especificación de auditoría de base de datos o de servidor.

Visualización de registros de auditoría

Sus registros de auditoría se almacenan en `D:\rdsdbdata\SQLAudit`.

Una vez que SQL Server termina de escribir en un archivo de registro de auditoría (cuando el archivo alcanza su límite de tamaño), Amazon RDS lo carga en su bucket de S3. Si se habilita la retención, Amazon RDS mueve el archivo a la carpeta de retención: `D:\rdsdbdata\SQLAudit\transmitted`.

Para obtener información acerca de cómo configurar la retención, consulte Incorporación de SQL Server Audit a las opciones de instancia de base de datos.

Los registros de auditoría se conservan en la instancia de base de datos hasta que se carga el archivo de registro de auditoría. Puede ver los registros de auditoría ejecutando el siguiente comando.

```
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
             ('D:\rdsdbdata\SQLAudit\*.sqlaudit'
             , default
             , default )
```

Puede usar el mismo comando para ver los registros de auditoría en su carpeta de retención cambiando el filtro a `D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit`.

```
SELECT   *
 FROM     msdb.dbo.rds_fn_get_audit_file
             ('D:\rdsdbdata\SQLAudit\transmitted\*.sqlaudit'
             , default
             , default )
```

Uso de SQL Server Audit con instancias Multi-AZ

En el caso de las instancias Multi-AZ, el proceso de envío de archivos de registro de auditoría a Amazon S3 es similar al de las instancias Single-AZ. No obstante, hay algunas diferencias importantes:

- Los objetos de especificación de auditoría de base de datos se replican en todos los nodos.

- Las auditorías de servidor y las especificaciones de auditoría de servidor no se replican en nodos secundarios. En su lugar, debe crearlas o modificarlas manualmente.

Para capturar auditorías de servidor o una especificación de auditoría de servidor desde ambos nodos:

1. Cree una auditoría de servidor o una especificación de auditoría de servidor en el nodo principal.
2. Realice una conmutación por error al nodo secundario y cree una auditoría de servidor o una especificación de auditoría de servidor con los mismos nombre y GUID en el nodo secundario. Use el parámetro `AUDIT_GUID` para especificar el GUID.

Configuración de un bucket de S3

Los archivos de registro de auditoría se cargan automáticamente desde la instancia de base de datos en su bucket de S3. Se aplican las siguientes restricciones al bucket de S3 que usa como destino para los archivos de auditoría:

- Debe estar en la misma AWS región que la instancia de base de datos.
- No debe estar abierto al público.
- El propietario del bucket también debe ser el propietario del rol de IAM.
- Su rol de IAM debe tener permisos para la clave KMS administrada por el cliente asociada al cifrado del servidor del bucket de S3.

La clave de destino que se usa para almacenar los datos sigue este esquema de nomenclatura: *`amzn-s3-demo-bucket`*`/key-prefix/instance-name/audit-name/node_file-name.ext`

> **Note**
>
> Establece los valores del nombre del bucket y del prefijo de clave con la configuración de opciones `S3_BUCKET_ARN`.

El esquema se compone de los siguientes elementos:

- ***`amzn-s3-demo-bucket`***: el nombre del bucket de S3.
- **`key-prefix`** – prefijo de clave personalizado que desea usar para los registros de auditoría.

- **`instance-name`** – nombre de su instancia Amazon RDS.
- **`audit-name`** – nombre de la auditoría.
- **`node`**: identificador del nodo que es el origen de los registros de auditoría (`node1` o `node2`). Hay un nodo para una instancia Single-AZ y dos nodos de replicación para una instancia Multi-AZ. Estos no son nodos principales ni secundarios, ya que los roles de principal y secundario cambian con el tiempo. En su lugar, el identificador de nodo es una simple etiqueta.
  - **`node1`** – primer nodo de replicación (Single-AZ tiene solo un nodo).
  - **`node2`** – segundo nodo de replicación (Multi-AZ tiene dos nodos).
- **`file-name`** – nombre del archivo de destino. El nombre del archivo se toma tal y como es de SQL Server.
- **`ext`**: extensión del archivo (`zip` o `sqlaudit`):
  - **`zip`** – si la compresión está habilitada (valor predeterminado).
  - **`sqlaudit`** – si la compresión está deshabilitada.

Creación manual de un rol de IAM para SQL Server Audit

Normalmente, al crear una nueva opción, la AWS Management Console crea el rol de IAM y la política de confianza de IAM en su nombre. No obstante, puede crear manualmente un nuevo rol de IAM para usarlo con instancias de SQL Server Audit de modo que pueda personalizarlo con los requisitos adicionales que pueda tener. Para ello, debe crear un rol de IAM y delegar permisos de modo que el servicio Amazon RDS pueda usar su bucket de Amazon S3. Cuando cree este rol de IAM, debe asociar políticas de confianza y de permisos. La política de confianza permite a Amazon RDS asumir este rol. La política de permisos define las acciones que puede realizar este rol. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de AWS Identity and Access Management.

Puede usar los ejemplos de esta sección para crear las relaciones de confianza y las políticas de permisos que necesite.

El siguiente ejemplo muestra una relación de confianza para SQL Server Audit. Usa el principal de servicio `rds.amazonaws.com` para permitir que RDS escriba en el bucket de S3 Un principal de servicio es un identificador que se utiliza para conceder permisos a un servicio. Cada vez que conceda acceso a `rds.amazonaws.com` de esta forma, permitirá a RDS realizar una acción en su nombre. Para obtener más información acerca de las entidades principales de servicio, consulte la sección sobre elementos de las políticas de JSON de:AWS entidad principal.

Example relación de confianza para SQL Server Audit

JSON

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Principal": {
                 "Service": "rds.amazonaws.com"
             },
             "Action": "sts:AssumeRole"
         }
     ]
 }
```

Se recomienda usar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las relaciones de confianza basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

Puede utilizar claves de contexto de condición globales y hacer que el valor de `aws:SourceArn` contenga el ID de cuenta. En estos casos, el valor de `aws:SourceAccount` y la cuenta del valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilizan en la misma instrucción.

- Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
- Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En la relación de confianza, asegúrese de usar la clave de contexto de la condición global `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo de los recursos que acceden al rol. En el caso de SQL Server Audit, asegúrese de incluir tanto el grupo de opciones de base de datos y las instancias de base de datos, como se muestra en el siguiente ejemplo.

Example relación de confianza con clave de contexto de condición global para SQL Server Audit

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:rds:Region:my_account_ID:db:db_instance_identifier",
                        "arn:aws:rds:Region:my_account_ID:og:option_group_name"
                    ]
                }
            }
        }
    ]
}
```

En el siguiente ejemplo de política de permisos para SQL Server Audit, especificamos un ARN para el bucket de Simple Storage Service (Amazon S3). Puede usar ARN para identificar una cuenta, un usuario o un rol específicos a los que desea conceder acceso. Para obtener más información acerca de cómo usar los ARN, consulte Nombres de recurso de Amazon (ARN).

Example política de permisos para SQL Server Audit

JSON

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
```

```
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketACL",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:ListMultipartUploadParts",
                "s3:AbortMultipartUpload"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/key_prefix/*"
        }
    ]
}
```

> **Note**
>
> La `s3:ListAllMyBuckets` acción es necesaria para verificar que la misma AWS cuenta posee tanto el bucket S3 como la instancia de base de datos de SQL Server. La acción enumera los nombres de los buckets de la cuenta.
> Los espacios de nombres del bucket de S3 son globales. Si elimina accidentalmente el bucket, otro usuario puede crear un bucket con el mismo nombre en una cuenta distinta. A continuación, los datos de auditoría de SQL Server se escriben en el nuevo bucket.

Compatibilidad con SQL Server Analysis Services en Amazon RDS for SQL Server

Microsoft SQL Server Analysis Services (SSAS) forma parte del conjunto Microsoft Business Intelligence (MSBI). SSAS es una herramienta de procesamiento analítico en línea (OLAP) y minería de datos instalada en SQL Server. Utilice SSAS para analizar datos como ayuda para tomar decisiones empresariales. SSAS es diferente de la base de datos relacional de SQL Server porque SSAS está optimizado para consultas y cálculos comunes en un entorno de inteligencia empresarial.

Puede habilitar SSAS para instancias de base de datos existentes o nuevas. Está instalado en la misma instancia de base de datos que su motor de base de datos. Para obtener más información sobre SSAS, consulte la documentación de Microsoft Analysis Services.

Amazon RDS admite SSAS para las ediciones Standard y Enterprise de SQL Server en las siguientes versiones:

- Modo tabular:
  - SQL Server 2019, versión 15.00.4043.16.v1 y posteriores
  - SQL Server 2017, versión 14.00.3223.3.v1 y posteriores
  - SQL Server 2016, versión 13.00.5426.0.v1 y posteriores
- Modo multidimensional:
  - SQL Server 2019, versión 15.00.4153.1.v1 y posteriores
  - SQL Server 2017, versión 14.00.3381.3.v1 y posteriores
  - SQL Server 2016, versión 13.00.5882.1.v1 y posteriores

Contenido

- Limitaciones
- Activación de SSAS
  - Crear un grupo de opciones para SSAS
  - Agregar la opción de SSAS al grupo de opciones
  - Asociación del grupo de opciones a su instancia de base de datos
  - Permitir el acceso de entrada a su grupo de seguridad de VPC
  - Habilitación de la integración de Simple Storage Service (Amazon S3)
- Implementación de proyectos SSAS en Amazon RDS

- Monitoreo del estado de una tarea de implementación
- Uso de SSAS en Amazon RDS
  - Configuración de un usuario autenticado por Windows para SSAS
  - Agregar un usuario de dominio como administrador de bases de datos
  - Creación de un proxy de SSAS
  - Programación del procesamiento de bases de datos SSAS mediante SQL Server Agent
  - Revocación de acceso de SSAS desde el proxy
- Copia de seguridad de una base de datos SSAS
- Restauración de una base de datos SSAS
  - Restauración de una instancia de base de datos a un momento especificado
- Cambiar el modo de SSAS
- Desactivación de SSAS
- Solución de problemas de SSAS

Limitaciones

Las siguientes limitaciones se aplican al uso de SSAS en RDS for SQL Server:

- RDS for SQL Server admite la ejecución de SSAS en modo tabular o multidimensional. Para obtener más información, consulte Comparación de soluciones tabulares y multidimensionales en la documentación de Microsoft.
- Solo puede utilizar un modo de SSAS a la vez. Antes de cambiar de modo, asegúrese de eliminar todas las bases de datos SSAS.

  Para obtener más información, consulte Cambiar el modo de SSAS.
- No se da soporte a las instancias Multi-AZ.
- Las instancias deben utilizar Active Directory autoadministrado o AWS Directory Service for Microsoft Active Directory para la autenticación SSAS. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.
- Los usuarios no tienen acceso de administrador del servidor SSAS, pero se les puede conceder acceso de administrador en el nivel de base de datos.
- El único puerto con soporte para obtener acceso a SSAS es 2383.

- No se pueden implementar proyectos directamente. Para implementarlos, proporcionamos un procedimiento almacenado de RDS. Para obtener más información, consulte Implementación de proyectos SSAS en Amazon RDS.
- No se da soporte a los procesamientos durante la implementación.
- No se da soporte al uso de archivos .xmla para la implementación.
- Los archivos de entrada del proyecto SSAS y los archivos de salida de copia de seguridad de la base de datos solo pueden estar en la carpeta `D:\S3` de la instancia de base de datos.

Activación de SSAS

Utilice el siguiente proceso para activar SSAS para su instancia de base de datos:

1. Cree un nuevo grupo de opciones o elija un grupo de opciones ya existente.
2. Añada la opción `SSAS` al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.
4. Permitir el acceso entrante al grupo de seguridad de la nube virtual privada (VPC) para el puerto de escucha de SSAS.
5. Activar la integración de Simple Storage Service (Amazon S3).

Crear un grupo de opciones para SSAS

Utilice la AWS Management Console o la AWS CLI para crear un grupo de opciones que corresponda al motor de SQL Server y la versión de la instancia de base de datos que planee utilizar.

> **Note**
>
> También puede utilizar un grupo de opciones ya existente si es para el motor y la versión correctos de SQL Server.

Consola

El siguiente procedimiento de consola crea un grupo de opciones para SQL Server Standard Edition 2017.

Para crear el grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En el panel Create option group (Crear grupo de opciones), haga lo siguiente:
   a. En Nombre, escriba un nombre para el grupo de opciones que sea exclusivo dentro de su cuenta de AWS, como **`ssas-se-2017`**. El nombre solo puede contener letras, dígitos y guiones.
   b. En Descripción, escriba una breve descripción del grupo de opciones, como **`SSAS option group for SQL Server SE 2017`**. La descripción se utiliza para fines de visualización.
   c. Para Engine (Motor), elija sqlserver-se.
   d. En Major engine version (Versión principal dle motor), elija 14.00.
5. Elija Create (Crear).

CLI

En el siguiente ejemplo de CLI se crea un grupo de opciones para SQL Server Standard Edition 2017.

Para crear el grupo de opciones

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-option-group \
    --option-group-name ssas-se-2017 \
    --engine-name sqlserver-se \
    --major-engine-version 14.00 \
    --option-group-description "SSAS option group for SQL Server SE 2017"
```

  En:Windows

```
aws rds create-option-group ^
    --option-group-name ssas-se-2017 ^
    --engine-name sqlserver-se ^
    --major-engine-version 14.00 ^
    --option-group-description "SSAS option group for SQL Server SE 2017"
```

Agregar la opción de SSAS al grupo de opciones

A continuación, utilice la AWS Management Console o la AWS CLI para agregar la opción SSAS al grupo de opciones.

Consola

Para agregar la opción de SSAS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que acaba de crear.
4. Seleccione Add option (Añadir opción).
5. En Option details (Detalles de la opción), elija SSAS para Option name (Nombre de la opción).
6. En Option settings (Configuración de opciones), haga lo siguiente:

    a. Para Max memory (Memoria máxima), ingrese un valor en el rango 10-80.

    En Max memory (Memoria máxima) se especifica el umbral superior por encima del cual SSAS comienza a liberar memoria con mayor rapidez para dejar espacio a las solicitudes que se están ejecutando, así como a las nuevas solicitudes de alta prioridad. El número es un porcentaje de la memoria total de la instancia de base de datos. Se permiten los valores entre 10 y 80, y el valor predeterminado es 45.

    b. Para Mode (Modo), elija el modo de servidor SSAS, Tabular o Multidimensional.

    Si no ve la opción Mode (Modo), significa que el modo Multidimensional no es compatible con su región de AWS. Para obtener más información, consulte Limitaciones.

    Tabular es el modo predeterminado.

c. En Security groups (Grupos de seguridad), elija el grupo de seguridad de VPC que desea asociar a la opción.

> **Note**
>
> El puerto para obtener acceso a SSAS, 2383, se rellena previamente.

7. En Scheduling (Programación), elija si desea agregar la opción inmediatamente o en el siguiente período de mantenimiento.
8. Elija Add option (Agregar opción).

CLI

Para agregar la opción de SSAS

1. Cree un archivo JSON, por ejemplo `ssas-option.json`, con los siguientes parámetros:

   - `OptionGroupName`: el nombre del grupo de opciones que ha creado o elegido anteriormente (`ssas-se-2017` en el ejemplo siguiente).
   - `Port`: el puerto que se utiliza para obtener acceso a SSAS. Solo se da soporte al puerto 2383.
   - `VpcSecurityGroupMemberships`: membresías para los grupos de seguridad de la VPC para la instancia de base de datos RDS.
   - `MAX_MEMORY`: el umbral superior por encima del cual SSAS debería comenzar a liberar más memoria para dejar espacio a las solicitudes que se estén ejecutando y para nuevas solicitudes de alta prioridad. El número es un porcentaje de la memoria total de la instancia de base de datos. Se permiten los valores entre 10 y 80, y el valor predeterminado es 45.
   - `MODE`: el modo de servidor de SSAS, ya sea `Tabular` o `Multidimensional`. `Tabular` es el predeterminado.

     Si recibe un error que indica que la configuración de la opción `MODE` no es válida, significa que el modo multidimensional no es compatible con su región AWS. Para obtener más información, consulte Limitaciones.

   El siguiente es un ejemplo de un archivo JSON con la configuración de las opciones de SSAS.

```
{
```

```
"OptionGroupName": "ssas-se-2017",
"OptionsToInclude": [
 {
 "OptionName": "SSAS",
 "Port": 2383,
 "VpcSecurityGroupMemberships": ["sg-0abcdef123"],
 "OptionSettings": [{"Name":"MAX_MEMORY","Value":"60"},
{"Name":"MODE","Value":"Multidimensional"}]
 }],
"ApplyImmediately": true
}
```

2. Agregue la opción SSAS al grupo de opciones.

   Example

   Para Linux, macOS o:Unix

   ```
   aws rds add-option-to-option-group \
       --cli-input-json file://ssas-option.json \
       --apply-immediately
   ```

   En:Windows

   ```
   aws rds add-option-to-option-group ^
       --cli-input-json file://ssas-option.json ^
       --apply-immediately
   ```

Asociación del grupo de opciones a su instancia de base de datos

Puede utilizar la consola o la CLI para asociar el grupo de opciones con la instancia de base de datos.

Consola

Asocie su grupo de opciones a una instancia de base de datos nueva o ya existente:

- Si se trata de una instancia de base de datos nueva, asocie el grupo de opciones a la instancia de base de datos al iniciar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

- Si se trata de una instancia de base de datos ya existente, modifique la instancia y asóciele el nuevo grupo de opciones. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Note**
>
> Si usa una instancia que ya existe, esta debe tener ya asociados un dominio de Active Directory y un rol de AWS Identity and Access Management (IAM). Si crea una instancia nueva, especifique un rol de IAM y un dominio de Active Directory ya existentes. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.

CLI

Puede asociar su grupo de opciones a una instancia de base de datos nueva o ya existente.

> **Note**
>
> Si usa una instancia que ya existe, esta debe tener ya asociados un dominio de Active Directory y un rol de IAM. Si crea una instancia nueva, especifique un rol de IAM y un dominio de Active Directory ya existentes. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.

Para crear una instancia de base de datos que utilice el grupo de opciones

- Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de opciones.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --db-instance-identifier myssasinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 14.00.3223.3.v1 \
    --allocated-storage 100 \
    --manage-master-user-password \
```

```
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name ssas-se-2017
```

En:Windows

```
aws rds create-db-instance ^
    --db-instance-identifier myssasinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 14.00.3223.3.v1 ^
    --allocated-storage 100 ^
    --manage-master-user-password ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
    --domain my-domain-id ^
    --option-group-name ssas-se-2017
```

Para modificar una instancia de base de datos para asociar el grupo de opciones

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier myssasinstance \
    --option-group-name ssas-se-2017 \
    --apply-immediately
```

  En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier myssasinstance ^
    --option-group-name ssas-se-2017 ^
```

```
    --apply-immediately
```

Permitir el acceso de entrada a su grupo de seguridad de VPC

Cree una regla de entrada para el puerto del agente de escucha de SSAS especificado en el grupo de seguridad de VPC asociado a su instancia de base de datos. Para obtener más información acerca de la configuración de grupos de seguridad, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

Habilitación de la integración de Simple Storage Service (Amazon S3)

Para descargar los archivos de configuración del modelo en su host para su implementación, utilice la integración de Simple Storage Service (Amazon S3). Para obtener más información, consulte Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3.

Implementación de proyectos SSAS en Amazon RDS

En RDS, no puede implementar directamente proyectos SSAS mediante SQL Server Management Studio (SSMS). Para implementar proyectos, utilice un procedimiento almacenado de RDS.

> **Note**
>
> No se da soporte al uso de archivos .xmla para la implementación.

Antes de implementar proyectos, asegúrese de lo siguiente:

- La integración de Simple Storage Service (Amazon S3) está activada. Para obtener más información, consulte Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3.
- El valor de configuración de `Processing Option` tiene que estar establecido en `Do Not Process`. Esta configuración significa que no se ejecutará ningún procesamiento después de la implementación.
- Tiene los archivos *`myssasproject`*`.asdatabase` y *`myssasproject`*`.deploymentoptions`. Se generan automáticamente cuando se crea el proyecto SSAS.

Para implementar un proyecto SSAS en RDS

1. Descargue el archivo `.asdatabase` (modelo SSAS) desde su bucket S3 a su instancia de base de datos, tal y como se muestra en el siguiente ejemplo. Para obtener más información sobre los parámetros de descarga, consulte Descarga de archivos desde un bucket de Amazon S3 a una instancia de base de datos de SQL Server.

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/myssasproject.asdatabase',
[@rds_file_path='D:\S3\myssasproject.asdatabase'],
[@overwrite_file=1];
```

2. Descargue el archivo `.deploymentoptions` desde su bucket S3 hasta la instancia de base de datos.

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/myssasproject.deploymentoptions',
[@rds_file_path='D:\S3\myssasproject.deploymentoptions'],
[@overwrite_file=1];
```

3. Implemente el proyecto.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_DEPLOY_PROJECT',
@file_path='D:\S3\myssasproject.asdatabase';
```

Monitoreo del estado de una tarea de implementación

Para realizar un seguimiento del estado de la tarea de implementación (o descarga), llame a la función `rds_fn_task_status`. Tiene dos parámetros. El primer parámetro tiene que ser siempre `NULL` porque no se aplica a SSAS. El segundo parámetro acepta un ID de tarea.

Para obtener una lista de todas las tareas, establezca el primer parámetro en `NULL` y el segundo en `0`, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Para obtener una tarea específica, establezca el primer parámetro en `NULL` y el segundo en el ID de la tarea, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La función `rds_fn_task_status` devuelve la siguiente información.

Parámetro de salida	Descripción
`task_id`	El ID de la tarea.
`task_type`	Para SSAS, las tareas pueden tener los siguientes tipos de tareas: • `SSAS_DEPLOY_PROJECT` • `SSAS_ADD_DB_ADMIN_MEMBER` • `SSAS_BACKUP_DB` • `SSAS_RESTORE_DB`
`database_name`	No aplicable a tareas de SSAS.
`% complete`	El porcentaje de progreso de la tarea.
`duration (mins)`	El tiempo empleado en la tarea, en minutos.
`lifecycle`	El estado de la tarea. Los posibles estados son los siguientes: • `CREATED` – después de llamar a uno de los procedimientos almacenados de SSAS, se crea una tarea y el estado se establece en `CREATED`. • `IN_PROGRESS` – cuando una tarea comienza, el estado se establece en `IN_PROGRESS` . Pueden pasar hasta cinco minutos hasta que el estado cambie de `CREATED` a `IN_PROGRESS` . •

Parámetro de salida	Descripción
	SUCCESS – cuando una tarea se completa, el estado se establece en SUCCESS. • ERROR – si se produce un error con una tarea, el estado se establece en ERROR. Para obtener más información acerca del error, consulte la columna task_info . • CANCEL_REQUESTED : después de llamar a rds_cancel_task , el estado de la tarea se establece en CANCEL_REQUESTED . • CANCELLED – después de que se cancela una tarea correctamente, se establece su estado en CANCELLED .
task_info	Información adicional acerca de la tarea. Si se produce un error durante el procesamiento, esta columna contiene información acerca del error. Para obtener más información, consulte Solución de problemas de SSAS.
last_updated	La fecha y hora en que se actualizó por última vez el estado de la tarea.
created_at	La fecha y hora en que se creó la tarea.
S3_object_arn	No aplicable a tareas de SSAS.
overwrite_S3_backup_file	No aplicable a tareas de SSAS.
KMS_master_key_arn	No aplicable a tareas de SSAS.

Parámetro de salida	Descripción
`filepath`	No aplicable a tareas de SSAS.
`overwrite_file`	No aplicable a tareas de SSAS.
`task_metadata`	Metadatos asociados a la tarea de SSAS.

Uso de SSAS en Amazon RDS

Después de implementar el proyecto SSAS, puede procesar directamente la base de datos OLAP en SSMS.

Para utilizar SSAS en RDS

1. En SSMS, conéctese a SSAS mediante el nombre de usuario y la contraseña del dominio de Active Directory.
2. Expanda Databases (Bases de datos). Aparece la base de datos SSAS recién implementada.
3. Localice la cadena de conexión y actualice el nombre de usuario y la contraseña para dar acceso a la base de datos SQL de origen. Esta operación es necesaria para procesar los objetos de SSAS.
    a. Para el modo tabular, haga lo siguiente:
        1. Despliegue la pestaña Connections (Conexiones).
        2. Abra el menú contextual (con el botón derecho del ratón) del objeto de conexión y elija Properties (Propiedades).
        3. Actualice el nombre de usuario y la contraseña en la cadena de conexión.
    b. Para el modo multidimensional, haga lo siguiente:
        1. Despliegue la pestaña Data Sources (Orígenes de datos).
        2. Abra el menú contextual (con el botón derecho del ratón) del objeto origen de datos y, a continuación, elija Properties (Propiedades).
        3. Actualice el nombre de usuario y la contraseña en la cadena de conexión.

4. Abra el menú contextual (haga clic con el botón derecho) de la base de datos SSAS que ha creado y elija Process Database (Procesar base de datos).

   Según el tamaño de los datos de entrada, la operación de procesamiento puede tardar varios minutos en completarse.

Temas

- Configuración de un usuario autenticado por Windows para SSAS
- Agregar un usuario de dominio como administrador de bases de datos
- Creación de un proxy de SSAS
- Programación del procesamiento de bases de datos SSAS mediante SQL Server Agent
- Revocación de acceso de SSAS desde el proxy

Configuración de un usuario autenticado por Windows para SSAS

El usuario administrador principal (a veces llamado usuario maestro) puede utilizar el siguiente ejemplo de código para configurar un inicio de sesión autenticado por Windows y conceder los permisos de procedimiento necesarios. Al hacer esto se conceden permisos al usuario de dominio para ejecutar tareas de cliente de SSAS, utilizar procedimientos de transferencia de archivos S3, crear credenciales y trabajar con el proxy de SQL Server Agent. Para obtener más información, consulte Credenciales (Motor de base de datos) y Crear un proxy de SQL Server Agent en la documentación de Microsoft.

Puede conceder algunos o todos los permisos siguientes, según sea necesario, a los usuarios autenticados de Windows.

Example

```
-- Create a server-level domain user login, if it doesn't already exist
USE [master]
GO
CREATE LOGIN [mydomain\user_name] FROM WINDOWS
GO

-- Create domain user, if it doesn't already exist
USE [msdb]
GO
CREATE USER [mydomain\user_name] FOR LOGIN [mydomain\user_name]
```

```
GO

-- Grant necessary privileges to the domain user
USE [master]
GO
GRANT ALTER ANY CREDENTIAL TO [mydomain\user_name]
GO

USE [msdb]
GO
GRANT EXEC ON msdb.dbo.rds_msbi_task TO [mydomain\user_name] with grant option
GRANT SELECT ON msdb.dbo.rds_fn_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_cancel_task TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_download_from_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_upload_to_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_delete_from_filesystem TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.rds_gather_file_details TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_add_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_update_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_grant_login_to_proxy TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_revoke_login_from_proxy TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_delete_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_enum_login_for_proxy to [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_enum_proxy_for_subsystem TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.rds_sqlagent_proxy TO [mydomain\user_name] with grant option
ALTER ROLE [SQLAgentUserRole] ADD MEMBER [mydomain\user_name]
GO
```

Agregar un usuario de dominio como administrador de bases de datos

Puede agregar un usuario de dominio como administrador de base de datos SSAS de las siguientes maneras:

- Un administrador de base de datos puede usar SSMS para crear un rol con privilegios de `admin` y, a continuación, agregar usuarios a dicho rol.
- Puede utilizar el siguiente procedimiento almacenado.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_ADD_DB_ADMIN_MEMBER',
@database_name='myssasdb',
@ssas_role_name='exampleRole',
@ssas_role_member='domain_name\domain_user_name';
```

Se requieren los siguientes parámetros:

- `@task_type` – el tipo de la tarea MSBI; en este caso `SSAS_ADD_DB_ADMIN_MEMBER`.
- `@database_name`: el nombre de la base de datos SSAS a la que concede privilegios de administrador.
- `@ssas_role_name`: el nombre del rol de administrador de base de datos SSAS. Si el rol no existe, se crea.
- `@ssas_role_member`: el usuario de la base de datos SSAS que va a agregar al rol de administrador.

Creación de un proxy de SSAS

Para poder programar el procesamiento de la base de datos de SSAS mediante SQL Server Agent, cree una credencial de SSAS y un proxy de SSAS. Ejecute estos procedimientos como usuario autenticado por Windows.

Para crear la credencial de SSAS

- Cree la credencial para el proxy. Para ello, puede utilizar SSMS o la siguiente instrucción SQL.

```
USE [master]
GO
CREATE CREDENTIAL [SSAS_Credential] WITH IDENTITY = N'mydomain\user_name', SECRET =
 N'mysecret'
GO
```

> **Note**
>
> `IDENTITY` debe ser un inicio de sesión autenticado por dominio. Reemplace *`mysecret`* por la contraseña para el inicio de sesión autenticado por el dominio.

Para crear el proxy de SSAS

1. Utilice la siguiente instrucción SQL para crear el proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_add_proxy
 @proxy_name=N'SSAS_Proxy',@credential_name=N'SSAS_Credential',@description=N''
GO
```

2. Utilice la siguiente instrucción SQL para conceder acceso al proxy a otros usuarios.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_grant_login_to_proxy
 @proxy_name=N'SSAS_Proxy',@login_name=N'mydomain\user_name'
GO
```

3. Utilice la siguiente instrucción SQL para conceder acceso al subsistema de SSAS al proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
 @task_type='GRANT_SUBSYSTEM_ACCESS',@proxy_name='SSAS_Proxy',@proxy_subsystem='SSAS'
GO
```

Para consultar el proxy y las concesiones en el proxy

1. Utilice la siguiente instrucción SQL para consultar los beneficiarios del proxy.

```
USE [msdb]
GO
EXEC sp_help_proxy
GO
```

2. Utilice la siguiente instrucción SQL para consultar las concesiones del subsistema.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_enum_proxy_for_subsystem
GO
```

Programación del procesamiento de bases de datos SSAS mediante SQL Server Agent

Después de crear la credencial y el proxy y conceder acceso a SSAS al proxy, puede crear un trabajo de SQL Server Agent para programar el procesamiento de la base de datos de SSAS.

Para programar el procesamiento de base de datos de SSAS

- Use SSMS o T-SQL para crear el trabajo de SQL Server Agent. En el siguiente ejemplo se utiliza T-SQL. Además, puede configurar la programación de trabajo a través de SSMS o T-SQL.
  - El parámetro `@command` indica el comando XML for Analysis (XMLA) que debe ejecutar el trabajo de SQL Server Agent Este ejemplo configura el procesamiento de la base de datos multidimensional de SSAS.
  - El parámetro `@server` indica el nombre del servidor SSAS de destino del trabajo de SQL Server Agent.

    Para llamar al servicio de SSAS dentro de la misma instancia de base de datos RDS donde reside el trabajo de SQL Server Agent, utilice `localhost:2383`.

    Para llamar al servicio de SSAS desde fuera de la instancia de base de datos RDS, utilice el punto de conexión RDS. También puede utilizar el punto de conexión de Kerberos Active Directory (AD) (*`your-DB-instance-name`*`.`*`your-AD-domain-name`*) si las instancias de la base de datos RDS están unidas por el mismo dominio. En el caso de las instancias de base de datos externas, asegúrese de configurar correctamente el grupo de seguridad de la VPC asociado a la instancia de base de datos RDS para obtener una conexión segura.

  Puede editar aún más la consulta para admitir varias operaciones XMLA. Realice las ediciones modificando directamente la consulta T-SQL o mediante la UI de SSMS tras la creación del trabajo de SQL Server Agent.

```
USE [msdb]
GO
DECLARE @jobId BINARY(16)
EXEC msdb.dbo.sp_add_job @job_name=N'SSAS_Job',
    @enabled=1,
    @notify_level_eventlog=0,
    @notify_level_email=0,
    @notify_level_netsend=0,
    @notify_level_page=0,
    @delete_level=0,
```

```
    @category_name=N'[Uncategorized (Local)]',
    @job_id = @jobId OUTPUT
GO
EXEC msdb.dbo.sp_add_jobserver
    @job_name=N'SSAS_Job',
    @server_name = N'(local)'
GO
EXEC msdb.dbo.sp_add_jobstep @job_name=N'SSAS_Job',
 @step_name=N'Process_SSAS_Object',
    @step_id=1,
    @cmdexec_success_code=0,
    @on_success_action=1,
    @on_success_step_id=0,
    @on_fail_action=2,
    @on_fail_step_id=0,
    @retry_attempts=0,
    @retry_interval=0,
    @os_run_priority=0, @subsystem=N'ANALYSISCOMMAND',
    @command=N'<Batch xmlns="http://schemas.microsoft.com/analysisservices/2003/
engine">
        <Parallel>
            <Process xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xmlns:ddl2="http://schemas.microsoft.com/analysisservices/2003/
engine/2" xmlns:ddl2_2="http://schemas.microsoft.com/analysisservices/2003/
engine/2/2"
                xmlns:ddl100_100="http://schemas.microsoft.com/
analysisservices/2008/engine/100/100" xmlns:ddl200="http://schemas.microsoft.com/
analysisservices/2010/engine/200"
                xmlns:ddl200_200="http://schemas.microsoft.com/
analysisservices/2010/engine/200/200" xmlns:ddl300="http://schemas.microsoft.com/
analysisservices/2011/engine/300"
                xmlns:ddl300_300="http://schemas.microsoft.com/
analysisservices/2011/engine/300/300" xmlns:ddl400="http://schemas.microsoft.com/
analysisservices/2012/engine/400"
                xmlns:ddl400_400="http://schemas.microsoft.com/
analysisservices/2012/engine/400/400" xmlns:ddl500="http://schemas.microsoft.com/
analysisservices/2013/engine/500"
                xmlns:ddl500_500="http://schemas.microsoft.com/
analysisservices/2013/engine/500/500">
                <Object>
                    <DatabaseID>Your_SSAS_Database_ID</DatabaseID>
                </Object>
                <Type>ProcessFull</Type>
```

```
                <WriteBackTableCreation>UseExisting</WriteBackTableCreation>
            </Process>
        </Parallel>
    </Batch>',
    @server=N'localhost:2383',
    @database_name=N'master',
    @flags=0,
    @proxy_name=N'SSAS_Proxy'
GO
```

Revocación de acceso de SSAS desde el proxy

Puede revocar el acceso al subsistema de SSAS y eliminar el proxy de SSAS mediante los siguientes procedimientos almacenados.

Para revocar el acceso y eliminar el proxy

1. Revoque el acceso al subsistema.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
 @task_type='REVOKE_SUBSYSTEM_ACCESS',@proxy_name='SSAS_Proxy',@proxy_subsystem='SSAS'
GO
```

2. Revoque las concesiones en el proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_revoke_login_from_proxy
 @proxy_name=N'SSAS_Proxy',@name=N'mydomain\user_name'
GO
```

3. Elimine el proxy.

```
USE [msdb]
GO
EXEC dbo.sp_delete_proxy @proxy_name = N'SSAS_Proxy'
GO
```

Copia de seguridad de una base de datos SSAS

Puede crear archivos de copia de seguridad de base de datos SSAS solo en la carpeta `D:\S3` de la instancia de base de datos. Para mover los archivos de copia de seguridad al bucket de S3, utilice Amazon S3.

Puede realizar una copia de seguridad de una base de datos SSAS de la siguiente manera:

- Un usuario de dominio con el rol `admin` de una base de datos determinada puede utilizar SSMS para realizar una copia de seguridad de la base de datos en la carpeta `D:\S3`.

  Para obtener más información, consulte Agregar un usuario de dominio como administrador de bases de datos.
- Puede utilizar el siguiente procedimiento almacenado. Este procedimiento almacenado no admite la codificación.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_BACKUP_DB',
@database_name='myssasdb',
@file_path='D:\S3\ssas_db_backup.abf',
[@ssas_apply_compression=1],
[@ssas_overwrite_file=1];
```

  Se requieren los siguientes parámetros:

  - `@task_type` – el tipo de la tarea MSBI; en este caso `SSAS_BACKUP_DB`.
  - `@database_name`: el nombre de la base de datos SSAS cuya copia de seguridad está realizando.
  - `@file_path`: la ruta de acceso del archivo de copia de seguridad de SSAS. La extensión `.abf` es necesaria.

  Los siguientes parámetros son opcionales:

  - `@ssas_apply_compression`: indica si se aplicará la compresión de copia de seguridad de SSAS. Los valores válidos son 1 (Sí) y 0 (No).
  - `@ssas_overwrite_file`: indica si se sobrescribe el archivo de copia de seguridad de SSAS. Los valores válidos son 1 (Sí) y 0 (No).

Restauración de una base de datos SSAS

Utilice el siguiente procedimiento almacenado para restaurar una base de datos SSAS a partir de una copia de seguridad.

No puede restaurar una base de datos si ya existe una base de datos SSAS con el mismo nombre. El procedimiento almacenado para restaurar no da soporte a archivos de copia de seguridad cifrados.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSAS_RESTORE_DB',
@database_name='mynewssasdb',
@file_path='D:\S3\ssas_db_backup.abf';
```

Se requieren los siguientes parámetros:

- `@task_type` – el tipo de la tarea MSBI; en este caso `SSAS_RESTORE_DB`.
- `@database_name`: el nombre de la nueva base de datos SSAS en la que está realizando la restauración.
- `@file_path`: la ruta de acceso al archivo de copia de seguridad de SSAS.

Restauración de una instancia de base de datos a un momento especificado

La recuperación a un momento dado (PITR) no se aplica a las bases de datos SSAS. Si ejecuta una PITR, solo los datos SSAS de la última instantánea antes de la hora solicitada estarán disponibles en la instancia restaurada.

Para tener bases de datos SSAS actualizadas en una instancia de base de datos restaurada

1. Haga una copia de seguridad de las bases de datos SSAS en la carpeta `D:\S3` de la instancia de origen.
2. Transfiera los archivos de copia de seguridad al bucket S3.
3. Transfiera los archivos de copia de seguridad del bucket S3 a la carpeta `D:\S3` de la instancia restaurada.
4. Ejecute el procedimiento almacenado para restaurar las bases de datos SSAS en la instancia restaurada.

   También puede volver a procesar el proyecto SSAS para restaurar las bases de datos.

Cambiar el modo de SSAS

Puede cambiar el modo en el que se ejecuta SSAS, ya sea Tabular o Multidimensional. Para cambiar el modo, utilice la AWS Management Console o la AWS CLI para modificar la configuración de las opciones en la opción de SSAS.

> **Important**
>
> Solo puede utilizar un modo de SSAS a la vez. Asegúrese de eliminar todas las bases de datos de SSAS antes de cambiar el modo o aparecerá un error.

Consola

El siguiente procedimiento de la consola de Amazon RDS cambia el modo de SSAS a Tabular y establece el parámetro `MAX_MEMORY` al 70 por ciento.

Para modificar la opción de SSAS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `SSAS` que desea modificar (`ssas-se-2017` en los ejemplos anteriores).
4. Elija Modify option (Modificar opción).
5. Cambie la configuración de las opciones:
    a. Para Max memory (Memoria máxima), ingrese **`70`**.
    b. Para el Mode (Modo), elija Tabular
6. Elija Modify option (Modificar opción).

AWS CLI

El siguiente ejemplo de la AWS CLI cambia el modo de SSAS a Tabular y establece el parámetro `MAX_MEMORY` al 70 por ciento.

Para que el comando de la CLI funcione, asegúrese de incluir todos los parámetros requeridos, incluso si no los está modificando.

Para modificar la opción de SSAS

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name ssas-se-2017 \
    --options
 "OptionName=SSAS,VpcSecurityGroupMemberships=sg-12345e67,OptionSettings=[{Name=MAX_MEMORY,
{Name=MODE,Value=Tabular}]" \
    --apply-immediately
```

  En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name ssas-se-2017 ^
    --options
 OptionName=SSAS,VpcSecurityGroupMemberships=sg-12345e67,OptionSettings=[{Name=MAX_MEMORY,V
{Name=MODE,Value=Tabular}] ^
    --apply-immediately
```

Desactivación de SSAS

Para descativar SSAS, quite la opción SSAS de su grupo de opciones.

> **Important**
>
> Antes de quitar la opción SSAS, elimine las bases de datos SSAS.
> Es muy recomendable que realice una copia de seguridad de las bases de datos SSAS antes de eliminarlas y quitar la opción SSAS.

Consola

Para quitar la opción SSAS de su grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `SSAS` que desea quitar (`ssas-se-2017` en los ejemplos anteriores).
4. Elija Delete option (Eliminar opción).
5. En Deletion options (Opciones de eliminación), elija SSAS para Options to delete (Opciones para eliminar).
6. En Apply immediately (Aplicar inmediatamente), seleccione Yes (Sí) para eliminar la opción inmediatamente o No para eliminarla en el siguiente período de mantenimiento.
7. Elija Eliminar.

AWS CLI

Para quitar la opción de SSAS de su grupo de opciones

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds remove-option-from-option-group \
    --option-group-name ssas-se-2017 \
    --options SSAS \
    --apply-immediately
```

  En:Windows

```
aws rds remove-option-from-option-group ^
    --option-group-name ssas-se-2017 ^
    --options SSAS ^
    --apply-immediately
```

Solución de problemas de SSAS

Es posible que se encuentre con los siguientes problemas al utilizar SSAS.

Problema	Tipo	Sugerencias para la solución de problemas
No se puede configurar la opción de SSAS. El modo de SSAS solicitado es *new_mode*, pero la instancia de base de datos actual tiene un *número* de bases de datos *current_mode* . Elimine las bases de datos existentes antes de cambiar al modo *new_mode*. Para recuperar el acceso al modo *current_mode* a fin de eliminar las bases de datos, actualice el grupo de opciones de la base de datos actual o adjunte un nuevo grupo de opciones con %s como valor de configuración de la opción MODE para la opción de SSAS.	Evento de RDS	No se puede cambiar el modo de SSAS si todavía tiene bases de datos de SSAS que utilizan el modo actual. Elimine las bases de datos de SSAS y vuelva a intentarlo.
No se puede eliminar la opción de SSAS porque hay un *número* de bases de datos de *modo* existente. La opción de SSAS no se puede eliminar hasta que se eliminen todas las bases de datos de SSAS. Agregue la opción de SSAS de nuevo, elimine todas las bases de datos de SSAS e inténtelo de nuevo.	Evento de RDS	No se puede desactivar SSAS si todavía tiene bases de datos de SSAS. Elimine las bases de datos de SSAS y vuelva a intentarlo.
La opción de SSAS no está habilitada o está en proceso de habilitarse. Inténtelo de nuevo más tarde.	Procedimiento almacenado de RDS	No se puede ejecutar procedimientos almacenados de SSAS cuando la opción está desactivada ni cuando se encuentra activada.

Problema	Tipo	Sugerencias para la solución de problemas
La opción de SSAS está configura da incorrectamente Asegúrese de que el estado de pertenencia al grupo de opciones sea “in-sync” y revise los registros de eventos de RDS en busca de mensajes de error de configuración de SSAS relevantes Tras estas investigaciones, inténtelo de nuevo. Si los errores continúan, contacte con AWS Support.	Procedimi ento almacenad o de RDS	No se puede ejecutar procedimientos almacenados de SSAS cuando la membresía de su grupo de opciones no tiene el estado `in-sync`. Esto pone a la opción de SSAS en un estado de configura ción incorrecto. Si el estado de membresía de su grupo de opciones cambia a `failed` debido a la modificación de la opción de SSAS, hay dos posibles razones: 1. La opción de SSAS se eliminó sin que las bases de datos de SSAS se hayan borrado. 2. El modo de SSAS se actualizó de Tabular a Multidimensional, o de Multidimensional a Tabular, sin que las bases de datos de SSAS existentes se hayan borrado. Reconfigure la opción de SSAS, porque RDS solo permite un modo de SSAS a la vez y no admite la eliminación de la opción de SSAS con bases de datos de SSAS presentes. Compruebe los registros de eventos de RDS en busca de errores de configuración para la instancia de SSAS y resuelva los problemas en consecuencia.

Problema	Tipo	Sugerencias para la solución de problemas
Error de implementación El cambio solo puede implementarse en un servidor que se ejecute en el modo *deployment_file_mode* . El modo de servidor actual es *current_mode* .	Procedimiento almacenado de RDS	No se puede implementar una base de datos tabular en un servidor multidimensional ni una base de datos multidimensional en un servidor tabular. Asegúrese de utilizar archivos con el modo correcto y verifique que la configuración de la opción `MODE` esté establecida en el valor apropiado.
Error en la restauración. El archivo de copia de seguridad solo se puede restaurar en un servidor que se ejecute en el modo *restore_file_mode* . El modo de servidor actual es *current_mode* .	Procedimiento almacenado de RDS	No se puede restaurar una base de datos tabular a un servidor multidimensional ni una base de datos multidimensional a un servidor tabular. Asegúrese de utilizar archivos con el modo correcto y verifique que la configuración de la opción `MODE` esté establecida en el valor apropiado.
Error en la restauración. Las versiones del archivo de copia de seguridad y de instancia de la base de datos RDS son incompatibles.	Procedimiento almacenado de RDS	No se puede restaurar una base de datos de SSAS con una versión incompatible con la versión de la instancia de SQL Server. Para obtener más información, consulte Niveles de compatibilidad para modelos tabulares y Nivel de compatibilidad de una base de datos multidimensional en la documentación de Microsoft.

Problema	Tipo	Sugerencias para la solución de problemas
Error en la restauración. El archivo de copia de seguridad especificado en la operación de restauración está dañado o no es un archivo de copia de seguridad de SSAS. Asegúrese de que @rds_file_path se encuentre correctamente formateado.	Procedimiento almacenado de RDS	No se puede restaurar una base de datos de SSAS con un archivo dañado. Asegúrese de que el archivo no esté dañado o corrupto. Este error también puede aparecer cuando `@rds_file_path` no está correctamente formateado (por ejemplo, tiene doble barra invertida como en `D:\S3\\incorrect_format.abf`).
Error en la restauración. El nombre de la base de datos restaurada no puede contener palabras reservadas o caracteres no válidos: . , ; ' ` : / \ * | ? ¡\" & % $! + = ( ) [ ] { } < >, o tener más de 100 caracteres.	Procedimiento almacenado de RDS	El nombre de la base de datos restaurada no puede contener palabras reservadas o caracteres que no sean válidos ni tener más de 100 caracteres. Para conocer las convenciones de denominación de objetos de SSAS, consulte Normas de nomenclatura de objetos en la documentación de Microsoft.
Se proporcionó un nombre de rol no válido. El nombre del rol no puede contener ninguna cadena reservada.	Procedimiento almacenado de RDS	El nombre del rol no puede contener ninguna cadena reservada. Para conocer las convenciones de denominación de objetos de SSAS, consulte Normas de nomenclatura de objetos en la documentación de Microsoft.
Se proporcionó un nombre de rol no válido. El nombre del rol no puede contener ninguno de los siguientes caracteres reservados: . , ; ' ` : / \\ * | ? ¡\" & % $! + = ( ) [ ] { } < >	Procedimiento almacenado de RDS	El nombre del rol no puede contener ningún carácter reservado. Para conocer las convenciones de denominación de objetos de SSAS, consulte Normas de nomenclatura de objetos en la documentación de Microsoft.

Compatibilidad de SQL Server Integration Services en Amazon RDS for SQL Server

Microsoft SQL Server Integration Services (SSIS) es un componente que puede utilizar para realizar un intervalo amplio de tareas de migración de datos. SSIS es una plataforma para aplicaciones de integración de datos y flujo de trabajo. Cuenta con una herramienta de almacenamiento de datos utilizada para la extracción, transformación y carga de datos (ETL). También puede utilizar esta herramienta para automatizar el mantenimiento de bases de datos de SQL Server y las actualizaciones de datos de cubo multidimensionales.

Los proyectos SSIS se organizan en paquetes guardados como archivos .dtsx basados en XML. Los paquetes pueden contener flujos de control y flujos de datos. Los flujos de datos se utilizan para representar operaciones ETL. Después de la implementación, los paquetes se almacenan en SQL Server en la base de datos SSISDB. SSISDB es una base de datos de procesamiento de transacciones en línea (OLTP) en el modo de recuperación completa.

Amazon RDS for SQL Server admite la ejecución de SSIS directamente en una instancia de base de datos RDS. Puede habilitar SSIS en una instancia de base de datos existente o nueva. SSIS se instala en la misma instancia de base de datos que su motor de base de datos.

RDS admite SSIS para las ediciones Standard y Enterprise de SQL Server en las siguientes versiones:

- SQL Server 2022, todas las versiones
- SQL Server 2019, versión 15.00.4043.16.v1 y posteriores
- SQL Server 2017, versión 14.00.3223.3.v1 y posteriores
- SQL Server 2016, versión 13.00.5426.0.v1 y posteriores

Contenido

- Limitaciones y recomendaciones
- Habilitación de SSIS
  - Creación del grupo de opciones para SSIS
  - Agregar la opción SSIS al grupo de opciones
  - Creación del grupo de parámetros para SSIS
  - Modificación del parámetro para SSIS
  - Asociación del grupo de opciones y el grupo de parámetros con su instancia de base de datos

- Habilitación de la integración de S3
- Permisos administrativos en SSISDB
  - Configuración de un usuario autenticado por Windows para SSIS
- Implementación de un proyecto SSIS
- Monitoreo del estado de una tarea de implementación
- Uso de SSIS
  - Configuración de administradores de conexión de base de datos para proyectos SSIS
  - Creación de un proxy de SSIS
  - Programación de un paquete SSIS mediante SQL Server Agent
  - Revocación de acceso SSIS desde el proxy
- Deshabilitación y eliminación de la base de datos de SSIS
  - Deshabilitación de SSIS
  - Borrado de la base de datos SSISDB

Limitaciones y recomendaciones

Las siguientes limitaciones y recomendaciones se aplican a la ejecución de SSIS en RDS para SQL Server:

- La instancia de base de datos debe tener un grupo de parámetros asociado con el parámetro `clr enabled` establecido en 1. Para obtener más información, consulte Modificación del parámetro para SSIS.

  > **Note**
  >
  > Si habilita el parámetro `clr enabled` en SQL Server 2017 o 2019, no podrá utilizar el tiempo de ejecución del lenguaje común (CLR) en su instancia de base de datos. Para obtener más información, consulte Características no compatibles y características con compatibilidad limitada.

- Se admiten las siguientes tareas de flujo de control:
  - Tarea DDL Execute de Analysis Services
  - Tarea de procesamiento de Analysis Services
  - Tarea de inserción masiva

  - Tarea comprobar integridad de la base de datos
  - Tarea de flujo de datos
  - Tarea de consulta de minería de datos
  - Tarea de creación de perfiles de datos
  - Tarea ejecutar paquete
  - Tarea ejecutar trabajo de SQL Server Agent
  - Tarea ejecutar SQL
  - Tarea ejecutar instrucción T-SQL
  - Tarea notificar operador
  - Tarea de reconstruir índice
  - Tarea de reorganizar índice
  - Tarea de reducir base de datos
  - Tarea de transferencia de base de datos
  - Tarea de transferencia de trabajos
  - Tarea de transferencia de inicios de sesión
  - Tarea de transferencia de objetos de SQL Server
  - Tarea de actualizar estadísticas
- Solo se admite la implementación del proyecto.
- Se admite la ejecución de paquetes SSIS mediante SQL Server Agent.
- Los registros de SSIS solo se pueden insertar en bases de datos creadas por el usuario.
- Utilice solo la carpeta `D:\S3` para trabajar con archivos. Los archivos colocados en cualquier otro directorio se eliminan. Tenga en cuenta algunos otros detalles de ubicación de archivos:
  - Coloque los archivos de entrada y salida del proyecto SSIS en la carpeta `D:\S3`.
  - Para la tarea de flujo de datos, cambie la ubicación de `BLOBTempStoragePath` y `BufferTempStoragePath` a un archivo dentro de la carpeta `D:\S3`. La ruta del archivo debe comenzar con `D:\S3\`.
  - Asegúrese de que todos los parámetros, variables y expresiones utilizados para las conexiones de archivos apuntan a la carpeta `D:\S3`.
  - En las instancias multi-AZ, los archivos creados por SSIS en la carpeta `D:\S3` se eliminan después de una conmutación por error. Para obtener más información, consulte Limitaciones multi-AZ para la integración S3.

  - Cargue los archivos creados por SSIS en la carpeta `D:\S3` en su bucket de Amazon S3 para que sean permanentes.
- No se admiten las transformaciones "importar columna" y "exportar columna" ni el componente script de la tarea de flujo de datos.
- No puede habilitar el volcado en paquetes SSIS en ejecución y no puede agregar pulsaciones de datos en paquetes SSIS.
- No se admite la característica SSIS Scale Out.
- No se pueden implementar proyectos directamente. Proporcionamos procedimientos almacenados de RDS para ello. Para obtener más información, consulte Implementación de un proyecto SSIS.
- Cree archivos de proyecto SSIS (.ispac) con el modo de protección `DoNotSavePasswords` para la implementación en RDS.
- SSIS no se admite en instancias Always On con réplicas de lectura.
- No puede realizar una copia de seguridad de la base de datos SSISDB asociada con la opción `SSIS`.
- No se admite la importación y restauración de la base de datos SSISDB desde otras instancias SSIS.
- Puede conectarse a otras instancias de base de datos de SQL Server o a un origen de datos de Oracle. La conexión a otros motores de bases de datos, como MySQL o PostgreSQL, no es compatible con SSIS en RDS para SQL Server. Para obtener más información acerca de la conexión a un origen de datos de Oracle, consulte Servidores enlazados con Oracle OLEDB.
- SSIS no admite una instancia unida a un dominio con una confianza saliente a un dominio en las instalaciones. Cuando utilice una confianza saliente, ejecute el trabajo de SSIS desde una cuenta del dominio de AWS local.

Habilitación de SSIS

Para habilitar SSIS, agregue la opción SSIS a su instancia de base de datos. Utilice el siguiente proceso:

1. Cree un nuevo grupo de opciones o elija un grupo de opciones ya existente.
2. Añada la opción `SSIS` al grupo de opciones.
3. Cree un nuevo grupo de parámetros o elija un grupo de parámetros existente.
4. Modifique el grupo de parámetros para establecer el parámetro `clr enabled` en 1.
5. Asocie el grupo de opciones y el grupo de parámetros a la instancia de base de datos.

6. Habilite la integración de Amazon S3.

> **Note**
>
> Si ya existe una base de datos con el nombre SSISDB o un inicio de sesión SSIS reservado en la instancia de base de datos, no puede habilitar SSIS en la instancia.

Creación del grupo de opciones para SSIS

Para trabajar con SSIS, cree un grupo de opciones o modifique un grupo de opciones que corresponda a la edición y versión de SQL Server de la instancia de base de datos que planea utilizar. Para ello, utilice la opción AWS Management Console o la AWS CLI.

Consola

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2016.

Para crear el grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En la ventana Create option group (Crear grupo de opciones), haga lo siguiente:
    a. En Nombre, escriba un nombre para el grupo de opciones que sea exclusivo dentro de su cuenta de AWS, como **`ssis-se-2016`**. El nombre solo puede contener letras, dígitos y guiones.
    b. En Descripción, escriba una breve descripción del grupo de opciones, como **`SSIS option group for SQL Server SE 2016`**. La descripción se utiliza para fines de visualización.
    c. Para Engine (Motor), elija sqlserver-se.
    d. En Versión principal del motor, elija 13.00.
5. Seleccione Crear.

CLI

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2016.

Para crear el grupo de opciones

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds create-option-group \
    --option-group-name ssis-se-2016 \
    --engine-name sqlserver-se \
    --major-engine-version 13.00 \
    --option-group-description "SSIS option group for SQL Server SE 2016"
```

  Para Windows:

```
aws rds create-option-group ^
    --option-group-name ssis-se-2016 ^
    --engine-name sqlserver-se ^
    --major-engine-version 13.00 ^
    --option-group-description "SSIS option group for SQL Server SE 2016"
```

Agregar la opción SSIS al grupo de opciones

A continuación, utilice la AWS Management Console o la AWS CLI para agregar la opción `SSIS` al grupo de opciones.

Consola

Para agregar la opción SSIS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que acaba de crear, ssis-se-2016 en este ejemplo.
4. Seleccione Add option (Añadir opción).

5. En Detalles de la opción, elija SSIS para Nombre de la opción.
6. En Scheduling (Programación), elija si desea agregar la opción inmediatamente o en el siguiente período de mantenimiento.
7. Elija Add option (Agregar opción).

CLI

Para agregar la opción SSIS

- Añada la opción `SSIS` al grupo de opciones.

  Example

  Para Linux, macOS o Unix:

  ```
  aws rds add-option-to-option-group \
      --option-group-name ssis-se-2016 \
      --options OptionName=SSIS \
      --apply-immediately
  ```

  Para Windows:

  ```
  aws rds add-option-to-option-group ^
      --option-group-name ssis-se-2016 ^
      --options OptionName=SSIS ^
      --apply-immediately
  ```

Creación del grupo de parámetros para SSIS

Cree o modifique un grupo de parámetros para el parámetro `clr enabled` que corresponde a la edición y versión de SQL Server de la instancia de base de datos que piensa utilizar para SSIS.

Consola

El procedimiento siguiente crea un grupo de parámetros para SQL Server Standard Edition 2016.

Para crear el grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija Create parameter group.
4. En el panel Create parameter group (Crear grupo de parámetros), haga lo siguiente:
   a. En Familia de grupos de parámetros, elija sqlserver-se-13.0.
   b. En Nombre de grupo, escriba un identificador para el grupo de parámetros, como **`ssis-sqlserver-se-13`**.
   c. En Descripción, escriba **`clr enabled parameter group`**.
5. Seleccione Crear.

CLI

El procedimiento siguiente crea un grupo de parámetros para SQL Server Standard Edition 2016.

Para crear el grupo de parámetros

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds create-db-parameter-group \
    --db-parameter-group-name ssis-sqlserver-se-13 \
    --db-parameter-group-family "sqlserver-se-13.0" \
    --description "clr enabled parameter group"
```

  Para Windows:

```
aws rds create-db-parameter-group ^
    --db-parameter-group-name ssis-sqlserver-se-13 ^
    --db-parameter-group-family "sqlserver-se-13.0" ^
    --description "clr enabled parameter group"
```

Modificación del parámetro para SSIS

Modifique el parámetro `clr enabled` en el grupo de parámetros que corresponde a la edición y la versión de SQL Server de su instancia de base de datos. Para SSIS, establezca el parámetro `clr enabled` en 1.

Consola

El procedimiento siguiente modifica el grupo de parámetros que ha creado para SQL Server Standard Edition 2016.

Para modificar el grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija el grupo de parámetros, como ssis-sqlserver-se-13.
4. En Parámetros, filtre la lista de parámetros para **`clr`**.
5. Elija clr habilitado.
6. Elija Edit parameters (Editar parámetros).
7. En Valores, elija 1.
8. Seleccione Save changes (Guardar cambios).

CLI

El procedimiento siguiente modifica el grupo de parámetros que ha creado para SQL Server Standard Edition 2016.

Para modificar el grupo de parámetros

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name ssis-sqlserver-se-13 \
```

```
    --parameters "ParameterName='clr
 enabled',ParameterValue=1,ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
    --db-parameter-group-name ssis-sqlserver-se-13 ^
    --parameters "ParameterName='clr
 enabled',ParameterValue=1,ApplyMethod=immediate"
```

Asociación del grupo de opciones y el grupo de parámetros con su instancia de base de datos

Para asociar el grupo de opciones de SSIS y el grupo de parámetros con su instancia de base de datos, utilice la AWS Management Console o la AWS CLI

> **Note**
>
> Si usa una instancia que ya existe, esta debe tener ya asociados un dominio de Active Directory y un rol de AWS Identity and Access Management (IAM). Si crea una instancia nueva, especifique un rol de IAM y un dominio de Active Directory ya existentes. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.

Consola

Para terminar de habilitar SSIS, asocie su grupo de opciones de SSIS y el grupo de parámetros con una instancia de base de datos nueva o existente:

- Para una nueva instancia de base de datos, asóciela cuando inicie la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, asóciela modificando la instancia. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

CLI

Puede asociar el grupo de opciones de SSIS y el grupo de parámetros con una instancia de base de datos nueva o existente.

Para crear una instancia con el grupo de opciones de SSIS y el grupo de parámetros

- Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de opciones.

  Example

  Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier myssisinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 13.00.5426.0.v1 \
    --allocated-storage 100 \
    --manage-master-user-password \
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name ssis-se-2016 \
    --db-parameter-group-name ssis-sqlserver-se-13
```

  Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier myssisinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 13.00.5426.0.v1 ^
    --allocated-storage 100 ^
    --manage-master-user-password ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
    --domain my-domain-id ^
    --option-group-name ssis-se-2016 ^
    --db-parameter-group-name ssis-sqlserver-se-13
```

Para modificar una instancia y asociar el grupo de opciones y el grupo de parámetros de SSIS

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier myssisinstance \
    --option-group-name ssis-se-2016 \
    --db-parameter-group-name ssis-sqlserver-se-13 \
    --apply-immediately
```

  Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier myssisinstance ^
    --option-group-name ssis-se-2016 ^
    --db-parameter-group-name ssis-sqlserver-se-13 ^
    --apply-immediately
```

Habilitación de la integración de S3

Para descargar archivos de proyecto SSIS (.ispac) en su host para su implementación, utilice la integración de archivos S3. Para obtener más información, consulte Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3.

Permisos administrativos en SSISDB

Cuando la instancia se crea o modifica con la opción SSIS, el resultado es una base de datos SSISDB con los roles ssis_admin y ssis_logreader concedidos al usuario maestro. El usuario maestro tiene los siguientes privilegios en SSISDB:

- alter on ssis_admin role
- alter on ssis_logreader role
- alter any user

Dado que el usuario maestro es un usuario autenticado por SQL, no se puede utilizar el usuario maestro para ejecutar paquetes SSIS. El usuario maestro puede utilizar estos privilegios para crear nuevos usuarios de SSISDB y agregarlos a los roles ssis_admin y ssis_logreader. Hacer esto es útil para conceder acceso a los usuarios de su dominio para usar SSIS.

Configuración de un usuario autenticado por Windows para SSIS

El usuario maestro puede utilizar el ejemplo de código siguiente para configurar un inicio de sesión autenticado por Windows en SSISDB y conceder los permisos de procedimiento necesarios. Al hacerlo, se conceden permisos al usuario del dominio para implementar y ejecutar paquetes SSIS, utilizar procedimientos de transferencia de archivos S3, crear credenciales y trabajar con el proxy de SQL Server Agent. Para obtener más información, consulte Credenciales (Motor de base de datos) y Crear un proxy de SQL Server Agent en la documentación de Microsoft.

> **Note**
>
> Puede conceder algunos o todos los permisos siguientes, según sea necesario, a los usuarios autenticados de Windows.

Example

```
-- Create a server-level SQL login for the domain user, if it doesn't already exist
USE [master]
GO
CREATE LOGIN [mydomain\user_name] FROM WINDOWS
GO

-- Create a database-level account for the domain user, if it doesn't already exist

USE [SSISDB]
GO
CREATE USER [mydomain\user_name] FOR LOGIN [mydomain\user_name]

-- Add SSIS role membership to the domain user
ALTER ROLE [ssis_admin] ADD MEMBER [mydomain\user_name]
ALTER ROLE [ssis_logreader] ADD MEMBER [mydomain\user_name]
GO

-- Add MSDB role membership to the domain user
USE [msdb]
```

```
GO
CREATE USER [mydomain\user_name] FOR LOGIN [mydomain\user_name]

-- Grant MSDB stored procedure privileges to the domain user
GRANT EXEC ON msdb.dbo.rds_msbi_task TO [mydomain\user_name] with grant option
GRANT SELECT ON msdb.dbo.rds_fn_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_task_status TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_cancel_task TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_download_from_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_upload_to_s3 TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.rds_delete_from_filesystem TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.rds_gather_file_details TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_add_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_update_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_grant_login_to_proxy TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_revoke_login_from_proxy TO [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_delete_proxy TO [mydomain\user_name] with grant option
GRANT EXEC ON msdb.dbo.sp_enum_login_for_proxy to [mydomain\user_name] with grant
 option
GRANT EXEC ON msdb.dbo.sp_enum_proxy_for_subsystem TO [mydomain\user_name]  with grant
 option
GRANT EXEC ON msdb.dbo.rds_sqlagent_proxy TO [mydomain\user_name] WITH GRANT OPTION


-- Add the SQLAgentUserRole privilege to the domain user
USE [msdb]
GO
ALTER ROLE [SQLAgentUserRole] ADD MEMBER [mydomain\user_name]
GO

-- Grant the ALTER ANY CREDENTIAL privilege to the domain user
USE [master]
GO
GRANT ALTER ANY CREDENTIAL TO [mydomain\user_name]
GO
```

Implementación de un proyecto SSIS

En RDS, no puede implementar directamente proyectos SSIS mediante procedimientos de SQL Server Management Studio (SSMS) o SSIS. Para descargar archivos de proyecto de Amazon S3 y, a continuación, implementarlos, utilice procedimientos almacenados de RDS.

Para ejecutar los procedimientos almacenados, inicie sesión como cualquier usuario al que haya concedido permisos para ejecutar los procedimientos almacenados. Para obtener más información, consulte Configuración de un usuario autenticado por Windows para SSIS.

Para implementar el proyecto SSIS

1. Descargue el archivo del proyecto (.ispac).

```
exec msdb.dbo.rds_download_from_s3
@s3_arn_of_file='arn:aws:s3:::bucket_name/ssisproject.ispac',
@rds_file_path='D:\S3\ssisproject.ispac',
@overwrite_file=1;
```

2. Envíe la tarea de implementación, asegurándose de lo siguiente:

   - La carpeta está presente en el catálogo de SSIS.
   - El nombre del proyecto coincide con el nombre del proyecto que utilizó al desarrollar el proyecto SSIS.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSIS_DEPLOY_PROJECT',
@folder_name='DEMO',
@project_name='ssisproject',
@file_path='D:\S3\ssisproject.ispac';
```

Monitoreo del estado de una tarea de implementación

Para realizar un seguimiento del estado de la tarea de implementación, llame a la función `rds_fn_task_status`. Tiene dos parámetros. El primer parámetro tiene que ser siempre `NULL` porque no se aplica a SSIS. El segundo parámetro acepta un ID de tarea.

Para obtener una lista de todas las tareas, establezca el primer parámetro en `NULL` y el segundo en `0`, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Para obtener una tarea específica, establezca el primer parámetro en NULL y el segundo en el ID de la tarea, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La función `rds_fn_task_status` devuelve la siguiente información.

Parámetro de salida	Descripción
`task_id`	El ID de la tarea.
`task_type`	`SSIS_DEPLOY_PROJECT`
`database_name`	No aplicable a tareas SSIS.
`% complete`	El porcentaje de progreso de la tarea.
`duration (mins)`	El tiempo empleado en la tarea, en minutos.
`lifecycle`	El estado de la tarea. Los posibles estados son los siguientes: • `CREATED`: después de llamar al procedimiento almacenado `msdb.dbo.rds_msbi_task`, se crea una tarea y el estado se establece en `CREATED`. • `IN_PROGRESS` – cuando una tarea comienza, el estado se establece en `IN_PROGRESS`. Pueden pasar hasta cinco minutos hasta que el estado cambie de `CREATED` a `IN_PROGRESS`. • `SUCCESS` – cuando una tarea se completa, el estado se establece en `SUCCESS`.

Parámetro de salida	Descripción
	• ERROR – si se produce un error con una tarea, el estado se establece en ERROR. Para obtener más información acerca del error, consulte la columna task_info . • CANCEL_REQUESTED : después de llamar a rds_cancel_task , el estado de la tarea se establece en CANCEL_REQUESTED . • CANCELLED – después de que se cancela una tarea correctamente, se establece su estado en CANCELLED .
task_info	Información adicional acerca de la tarea. Si se produce un error durante el procesamiento, esta columna contiene información acerca del error.
last_updated	La fecha y hora en que se actualizó por última vez el estado de la tarea.
created_at	La fecha y hora en que se creó la tarea.
S3_object_arn	No aplicable a tareas SSIS.
overwrite_S3_backup_file	No aplicable a tareas SSIS.
KMS_master_key_arn	No aplicable a tareas SSIS.
filepath	No aplicable a tareas SSIS.
overwrite_file	No aplicable a tareas SSIS.
task_metadata	Metadatos asociados con la tarea SSIS.

Uso de SSIS

Después de implementar el proyecto SSIS en el catálogo de SSIS, puede ejecutar paquetes directamente desde SSMS o programarlos mediante SQL Server Agent. Debe usar un inicio de sesión autenticado por Windows para ejecutar paquetes SSIS. Para obtener más información, consulte Configuración de un usuario autenticado por Windows para SSIS.

Temas

- Configuración de administradores de conexión de base de datos para proyectos SSIS
- Creación de un proxy de SSIS
- Programación de un paquete SSIS mediante SQL Server Agent
- Revocación de acceso SSIS desde el proxy

Configuración de administradores de conexión de base de datos para proyectos SSIS

Cuando utiliza un administrador de conexiones, puede utilizar estos tipos de autenticación:

- Para conexiones de base de datos locales con AWS Managed Active Directory, puede utilizar la autenticación de SQL o la autenticación de Windows. Para la autenticación de Windows, utilice *DB_instance_name*.*fully_qualified_domain_name* como nombre de servidor de la cadena de conexión.

  Un ejemplo es `myssisinstance.corp-ad.example.com`, donde `myssisinstance` es el nombre de instancia de base de datos y `corp-ad.example.com` es el nombre de dominio completo.
- Para conexiones remotas, utilice siempre la autenticación de SQL.
- Para conexiones de base de datos locales con Active Directory autoadministrado, puede utilizar la autenticación de SQL o la autenticación de Windows. Para la autenticación de Windows, utilice `.` o *`LocalHost`* como nombre de servidor de la cadena de conexión.

Creación de un proxy de SSIS

Para poder programar paquetes SSIS utilizando SQL Server Agent, cree credenciales de SSIS y un proxy de SSIS. Ejecute estos procedimientos como usuario autenticado por Windows.

Para crear la credencial de SSIS

- Cree la credencial para el proxy. Para ello, puede utilizar SSMS o la siguiente instrucción SQL.

```
USE [master]
GO
CREATE CREDENTIAL [SSIS_Credential] WITH IDENTITY = N'mydomain\user_name', SECRET =
 N'mysecret'
GO
```

> **Note**
>
> IDENTITY debe ser un inicio de sesión autenticado por dominio. Reemplace *mysecret* por la contraseña para el inicio de sesión autenticado por el dominio.
> Siempre que se cambie el host principal de SSISDB, modifique las credenciales del proxy de SSIS para permitir que el nuevo host tenga acceso a ellas.

Para crear el proxy de SSIS

1. Utilice la siguiente instrucción SQL para crear el proxy.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_add_proxy
 @proxy_name=N'SSIS_Proxy',@credential_name=N'SSIS_Credential',@description=N''
GO
```

2. Utilice la siguiente instrucción SQL para conceder acceso al proxy a otros usuarios.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_grant_login_to_proxy
 @proxy_name=N'SSIS_Proxy',@login_name=N'mydomain\user_name'
GO
```

3. Utilice la siguiente instrucción SQL para conceder acceso al subsistema de SSIS al proxy.

```
USE [msdb]
GO
```

```
EXEC msdb.dbo.rds_sqlagent_proxy
 @task_type='GRANT_SUBSYSTEM_ACCESS',@proxy_name='SSIS_Proxy',@proxy_subsystem='SSIS'
GO
```

Para consultar el proxy y las concesiones en el proxy

1. Utilice la siguiente instrucción SQL para consultar los beneficiarios del proxy.

```
USE [msdb]
GO
EXEC sp_help_proxy
GO
```

2. Utilice la siguiente instrucción SQL para consultar las concesiones del subsistema.

```
USE [msdb]
GO
EXEC msdb.dbo.sp_enum_proxy_for_subsystem
GO
```

Programación de un paquete SSIS mediante SQL Server Agent

Después de crear la credencial y el proxy y conceder acceso SSIS al proxy, puede crear un trabajo de SQL Server Agent para programar el paquete SSIS.

Para programar el paquete SSIS

- Puede utilizar SSMS o T-SQL para crear el trabajo de SQL Server Agent. En el siguiente ejemplo se utiliza T-SQL.

```
USE [msdb]
GO
DECLARE @jobId BINARY(16)
EXEC msdb.dbo.sp_add_job @job_name=N'MYSSISJob',
@enabled=1,
@notify_level_eventlog=0,
@notify_level_email=2,
@notify_level_page=2,
@delete_level=0,
@category_name=N'[Uncategorized (Local)]',
```

```
@job_id = @jobId OUTPUT
GO
EXEC msdb.dbo.sp_add_jobserver @job_name=N'MYSSISJob',@server_name=N'(local)'
GO
EXEC msdb.dbo.sp_add_jobstep
 @job_name=N'MYSSISJob',@step_name=N'ExecuteSSISPackage',
@step_id=1,
@cmdexec_success_code=0,
@on_success_action=1,
@on_fail_action=2,
@retry_attempts=0,
@retry_interval=0,
@os_run_priority=0,
@subsystem=N'SSIS',
@command=N'/ISSERVER "\"\SSISDB\MySSISFolder\MySSISProject\MySSISPackage.dtsx\"" /
SERVER "\"my-rds-ssis-instance.corp-ad.company.com/\""
/Par "\"$ServerOption::LOGGING_LEVEL(Int16)\"";1 /Par
 "\"$ServerOption::SYNCHRONIZED(Boolean)\"";True /CALLERINFO SQLAGENT /REPORTING
 E',
@database_name=N'master',
@flags=0,
@proxy_name=N'SSIS_Proxy'
GO
```

Revocación de acceso SSIS desde el proxy

Puede revocar el acceso al subsistema de SSIS y eliminar el proxy de SSIS mediante los siguientes procedimientos almacenados.

Para revocar el acceso y eliminar el proxy

1. Revoque el acceso al subsistema.

```
USE [msdb]
GO
EXEC msdb.dbo.rds_sqlagent_proxy
 @task_type='REVOKE_SUBSYSTEM_ACCESS',@proxy_name='SSIS_Proxy',@proxy_subsystem='SSIS'
GO
```

2. Revoque las concesiones en el proxy.

```
USE [msdb]
```

```
GO
EXEC msdb.dbo.sp_revoke_login_from_proxy
 @proxy_name=N'SSIS_Proxy',@name=N'mydomain\user_name'
GO
```

3. Elimine el proxy.

```
USE [msdb]
GO
EXEC dbo.sp_delete_proxy @proxy_name = N'SSIS_Proxy'
GO
```

Deshabilitación y eliminación de la base de datos de SSIS

Siga los pasos que se indican a continuación para deshabilitar o eliminar las bases de datos de SSIS:

Temas

- Deshabilitación de SSIS
- Borrado de la base de datos SSISDB

Deshabilitación de SSIS

Para deshabilitar SSIS, quite la opción `SSIS` del grupo de opciones.

> **Important**
>
> Quitar la opción no elimina la base de datos SSISDB, por lo que puede eliminar la opción de forma segura sin perder los proyectos SSIS.
> Puede volver a habilitar la opción `SSIS` después de la eliminación para volver a utilizar los proyectos SSIS que se implementaron anteriormente en el catálogo de SSIS.

Consola

El procedimiento siguiente quita la opción `SSIS`.

Para quitar la opción SSIS de su grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `SSIS` (`ssis-se-2016` en los ejemplos anteriores).
4. Elija Delete option (Eliminar opción).
5. En Opciones de eliminación, elija SSIS para Opciones que se van a eliminar.
6. En Apply immediately (Aplicar inmediatamente), seleccione Yes (Sí) para eliminar la opción inmediatamente o No para eliminarla en el siguiente período de mantenimiento.
7. Elija Eliminar.

CLI

El procedimiento siguiente quita la opción `SSIS`.

Para quitar la opción SSIS de su grupo de opciones

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds remove-option-from-option-group \
    --option-group-name ssis-se-2016 \
    --options SSIS \
    --apply-immediately
```

  En:Windows

```
aws rds remove-option-from-option-group ^
    --option-group-name ssis-se-2016 ^
    --options SSIS ^
    --apply-immediately
```

Borrado de la base de datos SSISDB

Después de quitar la opción SSIS, la base de datos SSISDB no se elimina. Para eliminar la base de datos SSISDB, utilice el procedimiento almacenado `rds_drop_ssis_database` después de quitar la opción SSIS.

Para eliminar la base de datos SSIS

- Utilice el siguiente procedimiento almacenado.

```
USE [msdb]
GO
EXEC dbo.rds_drop_ssis_database
GO
```

Después de eliminar la base de datos SSISDB, si vuelve a habilitar la opción SSIS obtendrá un nuevo catálogo de SSISDB.

Compatibilidad con SQL Server Reporting Services en Amazon RDS for SQL Server

Microsoft SQL Server Reporting Services (SSRS) es una aplicación basada en servidor que se utiliza para la generación y la distribución de informes. Forma parte de un conjunto de servicios de SQL Server que también incluye SQL Server Analysis Services (SSAS) y SQL Server Integration Services (SSIS). SSRS es un servicio construido sobre SQL Server. Puede usarlo para recopilar datos de diversos orígenes de datos y presentarlos de una manera que sea fácilmente comprensible y lista para el análisis.

Amazon RDS for SQL Server admite la ejecución de SSRS directamente en instancias de base de datos RDS. Puede usar SSRS con instancias de base de datos ya existentes o nuevas.

RDS admite SSRS para las ediciones Standard y Enterprise de SQL Server en las siguientes versiones:

- SQL Server 2022, todas las versiones
- SQL Server 2019, versión 15.00.4043.16.v1 y posteriores
- SQL Server 2017, versión 14.00.3223.3.v1 y posteriores
- SQL Server 2016, versión 13.00.5820.21.v1 y posteriores

Contenido

- Limitaciones y recomendaciones
- Activación de SSRS
  - Creación de un grupo de opciones para SSRS
  - Agregar la opción SSRS a su grupo de opciones
  - Asociación de un grupo de opciones a su instancia de base de datos
  - Permitir el acceso de entrada a su grupo de seguridad de VPC
- Bases de datos del servidor de informes
- Archivos de registro de SSRS
- Acceso al portal web de SSRS
  - Uso de SSL en RDS
  - Concesión de acceso a usuarios de dominio
  - Acceso al portal web

- Implementación de informes y configuración de orígenes de datos de informes
  - Implementación de informes en SSRS
  - Configuración del origen de datos del informe
- Uso del correo electrónico de SSRS para enviar informes
- Revocación de permisos de nivel de sistema
- Monitoreo del estado de una tarea
- Deshabilitación y eliminación de bases de datos de SSRS
  - Desactivación de SSRS
  - Eliminación de las bases de datos SSRS

Limitaciones y recomendaciones

Las siguientes limitaciones y recomendaciones se aplican a la ejecución de SSRS en RDS para SQL Server:

- No puede usar SSRS en instancias de base de datos que tienen réplicas de lectura.
- Las instancias deben utilizar Active Directory autoadministrado o AWS Directory Service for Microsoft Active Directory para la autenticación del portal web y del servidor web SSRS. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.
- No puede realizar una copia de seguridad de las bases de datos del servidor de informes creadas con la opción SSRS.
- No se admite la importación y restauración de bases de datos del servidor de informes desde otras instancias de SSRS. Para obtener más información, consulte Bases de datos del servidor de informes.
- No puede configurar SSRS para que escuche en el puerto SSL predeterminado (443). Los valores permitidos son 1150–49.511, excepto 1234, 1434, 3260, 3343, 3389 y 47.001.
- Las suscripciones a través de un recurso compartido de archivos de Microsoft Windows no son compatibles.
- No se admite el uso de Reporting Services Configuration Manager.
- No se admite la creación y modificación de roles.
- No se admite la modificación de propiedades del servidor de informes.
- No se conceden los roles administrador del sistema y usuario del sistema.
- No puede editar asignaciones de roles a nivel de sistema a través del portal web.

Activación de SSRS

Utilice el siguiente proceso para activar SSRS para su instancia de base de datos:

1. Cree un nuevo grupo de opciones o elija un grupo de opciones ya existente.
2. Añada la opción SSRS al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.
4. Permitir el acceso entrante al grupo de seguridad de la nube virtual privada (VPC) para el puerto de agente de escucha de SSRS.

Creación de un grupo de opciones para SSRS

Para trabajar con SSRS, cree un grupo de opciones que corresponda al motor de SQL Server y la versión de la instancia de base de datos que planee utilizar. Para ello, utilice la opción AWS Management Console o la AWS CLI.

> **Note**
>
> También puede utilizar un grupo de opciones ya existente si es para el motor y la versión correctos de SQL Server.

Consola

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2017.

Para crear el grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En el panel Create option group (Crear grupo de opciones), haga lo siguiente:
   a. En Name (Nombre), escriba un nombre para el grupo de opciones que sea exclusivo dentro de su Cuenta de AWS, como **`ssrs-se-2017`**. El nombre solo puede contener letras, dígitos y guiones.

b. En Descripción, escriba una breve descripción del grupo de opciones, como **`SSRS option group for SQL Server SE 2017`**. La descripción se utiliza para fines de visualización.

c. Para Engine (Motor), elija sqlserver-se.

d. En Major engine version (Versión principal dle motor), elija 14.00.

5. Elija Create (Crear).

CLI

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2017.

Para crear el grupo de opciones

- Ejecute uno de los siguientes comandos.

Example

Para Linux, macOS o:Unix

```
aws rds create-option-group \
    --option-group-name ssrs-se-2017 \
    --engine-name sqlserver-se \
    --major-engine-version 14.00 \
    --option-group-description "SSRS option group for SQL Server SE 2017"
```

En:Windows

```
aws rds create-option-group ^
    --option-group-name ssrs-se-2017 ^
    --engine-name sqlserver-se ^
    --major-engine-version 14.00 ^
    --option-group-description "SSRS option group for SQL Server SE 2017"
```

Agregar la opción SSRS a su grupo de opciones

A continuación, utilice la AWS Management Console o la AWS CLI para agregar la opción SSRS al grupo de opciones.

Consola

Para agregar la opción SSRS

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que acaba de crear y, a continuación, elija Add option (Añadir opción).
4. En Detalles de la opción, elija SSRS para Nombre de la opción.
5. En Configuración de opciones, haga lo siguiente:

   a. Introduzca el puerto que debe escuchar el servicio SSRS. El valor predeterminado es 8443. Para obtener una lista de valores permitidos, consulte Limitaciones y recomendaciones.

   b. Escriba un valor en Memoria máxima.

      Memoria máxima especifica el umbral superior por encima del cual no se conceden nuevas solicitudes de asignación de memoria para las aplicaciones de servidor de informes. El número es un porcentaje de la memoria total de la instancia de base de datos. Los valores permitidos son 10–80.

   c. En Security groups (Grupos de seguridad), elija el grupo de seguridad de VPC que desea asociar a la opción. Utilice el mismo grupo de seguridad asociado a su instancia de base de datos.

6. Para usar el correo electrónico de SSRS para enviar informes, seleccione la casilla de verificación Configure email delivery options (Configurar las opciones de entrega de correo electrónico) enEmail delivery in reporting services (Entrega de correo electrónico en servicios de informes) y, a continuación, haga lo siguiente:

   a. En Email address (Dirección de correo electrónico), escriba la dirección de correo electrónico que desea usar en el campo From (De) de los mensajes enviados por correo electrónico de SSRS.

      Especifique una cuenta de usuario que tenga permiso para enviar correo desde el servidor SMTP.

   b. En SMTP server (Servidor SMTP), especifique el servidor SMTP o la puerta de enlace que se va a utilizar.

Puede ser una dirección IP, el nombre NetBIOS de un equipo de la intranet corporativa o un nombre de dominio completo.

c. En SMTP port (Puerto SMTP), introduzca el puerto que se utilizará para conectarse al servidor de correo. El valor predeterminado es 25.

d. Para usar la autenticación:

i. Seleccione la casilla de verificación Use authentication (Usar autenticación).

ii. En Secret Amazon Resource Name (ARN) (Nombre de recurso de Amazon [ARN]), escriba el ARN de AWS Secrets Manager para las credenciales de usuario.

Use el siguiente formato:

`arn:aws:secretsmanager:`*`Region`*`:`*`AccountId`*`:secret:`*`SecretName`*`-6RandomChara`

Por ejemplo:

`arn:aws:secretsmanager:`*`us-west-2`*`:`*`123456789012`*`:secret:`*`MySecret-a1b2c3`

Para obtener más información sobre la creación del secreto, consulte Uso del correo electrónico de SSRS para enviar informes.

e. Seleccione la casilla de verificación Use Secure Sockets Layer (SSL) (Utilizar capa de sockets seguros) para cifrar los mensajes de correo electrónico mediante SSL.

7. En Scheduling (Programación), elija si desea agregar la opción inmediatamente o en el siguiente período de mantenimiento.

8. Elija Add option (Agregar opción).

CLI

Para agregar la opción SSRS

1. Cree un archivo JSON, por ejemplo `ssrs-option.json`.

a. Defina los siguientes parámetros obligatorios:

- `OptionGroupName`: el nombre del grupo de opciones que ha creado o elegido anteriormente (`ssrs-se-2017` en el ejemplo siguiente).

- `Port`: el puerto donde debe escuchar el servicio SSRS. El valor predeterminado es 8443. Para obtener una lista de valores permitidos, consulte Limitaciones y recomendaciones.
- `VpcSecurityGroupMemberships`: las suscripciones del grupo de seguridad de VPC para su instancia de base de datos de RDS.
- `MAX_MEMORY` : el umbral superior por encima del cual no se conceden nuevas solicitudes de asignación de memoria para las aplicaciones de servidor de informes. El número es un porcentaje de la memoria total de la instancia de base de datos. Los valores permitidos son 10–80.

b. (Opcional) Defina los siguientes parámetros para usar el correo electrónico de SSRS:

- `SMTP_ENABLE_EMAIL`: defínalo en `true` para usar el correo electrónico de SSRS. El valor predeterminado es `false`.
- `SMTP_SENDER_EMAIL_ADDRESS`: la dirección de correo electrónico que se va a utilizar en el campo From (De) de los mensajes enviados por correo electrónico de SSRS. Especifique una cuenta de usuario que tenga permiso para enviar correo desde el servidor SMTP.
- `SMTP_SERVER`: el servidor SMTP o la puerta de enlace que se va a utilizar. Puede ser una dirección IP, el nombre NetBIOS de un equipo de la intranet corporativa o un nombre de dominio completo.
- `SMTP_PORT`: el puerto que se va a usar para conectarse al servidor de correo. El valor predeterminado es 25.
- `SMTP_USE_SSL`: defínalo en`true` para cifrar los mensajes de correo electrónico mediante SSL. El valor predeterminado es `true`.
- `SMTP_EMAIL_CREDENTIALS_SECRET_ARN`: el ARN de Secrets Manager que contiene las credenciales de usuario. Use el siguiente formato:

  arn:aws:secretsmanager:*Region*:*AccountId*:secret:*SecretName*-*6RandomCharact*

  Para obtener más información sobre la creación del secreto, consulte Uso del correo electrónico de SSRS para enviar informes.
- `SMTP_USE_ANONYMOUS_AUTHENTICATION`: defínalo en `true` y no incluya `SMTP_EMAIL_CREDENTIALS_SECRET_ARN` si no quiere usar la autenticación.

  El valor predeterminado es `false` cuando `SMTP_ENABLE_EMAIL` es `true`.

El siguiente ejemplo incluye los parámetros de correo electrónico de SSRS, que utilizan el ARN secreto.

```
{
"OptionGroupName": "ssrs-se-2017",
"OptionsToInclude": [
 {
 "OptionName": "SSRS",
 "Port": 8443,
 "VpcSecurityGroupMemberships": ["sg-0abcdef123"],
 "OptionSettings": [
            {"Name": "MAX_MEMORY","Value": "60"},
            {"Name": "SMTP_ENABLE_EMAIL","Value": "true"}
            {"Name": "SMTP_SENDER_EMAIL_ADDRESS","Value": "nobody@example.com"},
            {"Name": "SMTP_SERVER","Value": "email-smtp.us-west-2.amazonaws.com"},
            {"Name": "SMTP_PORT","Value": "25"},
            {"Name": "SMTP_USE_SSL","Value": "true"},
            {"Name": "SMTP_EMAIL_CREDENTIALS_SECRET_ARN","Value":
 "arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3"}
            ]
 }],
"ApplyImmediately": true
}
```

2. Agregue la opción SSRS al grupo de opciones.

   Example

   Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --cli-input-json file://ssrs-option.json \
    --apply-immediately
```

   En:Windows

```
aws rds add-option-to-option-group ^
    --cli-input-json file://ssrs-option.json ^
    --apply-immediately
```

Asociación de un grupo de opciones a su instancia de base de datos

Puede utilizar la AWS Management Console o la AWS CLI para asociar el grupo de opciones a la instancia de base de datos.

Si usa una instancia de base de datos existente, debe tener ya asociados un dominio de Active Directory y un rol de AWS Identity and Access Management (IAM). Si crea una instancia nueva, especifique un rol de IAM y un dominio de Active Directory ya existentes. Para obtener más información, consulte Uso de Active Directory con RDS para SQL Server.

Consola

Puede asociar su grupo de opciones a una instancia de base de datos nueva o ya existente:

- Para una nueva instancia de base de datos, asocie el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, modifique la instancia y asóciele el nuevo grupo de opciones. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

CLI

Puede asociar su grupo de opciones a una instancia de base de datos nueva o ya existente.

Para crear una instancia de base de datos que utilice el grupo de opciones

- Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de opciones.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --db-instance-identifier myssrsinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 14.00.3223.3.v1 \
    --allocated-storage 100 \
    --manage-master-user-password  \
```

```
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name ssrs-se-2017
```

En:Windows

```
aws rds create-db-instance ^
    --db-instance-identifier myssrsinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 14.00.3223.3.v1 ^
    --allocated-storage 100 ^
    --manage-master-user-password ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
    --domain my-domain-id ^
    --option-group-name ssrs-se-2017
```

Para modificar una instancia de base de datos para utilizar su grupo de opciones

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier myssrsinstance \
    --option-group-name ssrs-se-2017 \
    --apply-immediately
```

  En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier myssrsinstance ^
    --option-group-name ssrs-se-2017 ^
```

```
    --apply-immediately
```

Permitir el acceso de entrada a su grupo de seguridad de VPC

Para permitir el acceso entrante al grupo de seguridad de la VPC asociado a su instancia de base de datos, cree una regla de entrada para el puerto de agente de escucha de SSRS especificado. Para obtener más información acerca de la configuración de grupos de seguridad, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

Bases de datos del servidor de informes

Cuando la instancia de base de datos está asociada a la opción SSRS, se crean dos nuevas bases de datos en la instancia de base de datos:

- `rdsadmin_ReportServer`
- `rdsadmin_ReportServerTempDB`

Estas bases de datos actúan como bases de datos ReportServer y ReportServerTempDB. SSRS almacena sus datos en la base de datos ReportServer y almacena en caché sus datos en la base de datos ReportServerTempDB. Para obtener más información, consulte Report Server Database (Base de datos de servidores de inforems) en la documentación de Microsoft.

RDS posee y administra estas bases de datos, por lo que no se permiten operaciones de base de datos en ellas, como ALTER y DROP. No se permite el acceso a la base de datos `rdsadmin_ReportServerTempDB`. Sin embargo, puede realizar operaciones de lectura en la base de datos `rdsadmin_ReportServer`.

Archivos de registro de SSRS

Puede enumerar, ver y descargar archivos de registro de SSRS. Los archivos de registro de SSRS siguen la convención de nomenclatura ReportServerService_*marca de tiempo*.log. Estos registros del servidor de informes se encuentran en el directorio `D:\rdsdbdata\Log\SSRS`. (El directorio `D:\rdsdbdata\Log` es también el directorio principal de los registros de errores y los registros del agente de SQL Server). Para obtener más información, consulte Visualización y descripción de archivos de registro de base de datos.

Para las instancias SSRS existentes, es posible que sea necesario reiniciar el servicio SSRS para acceder a los registros del servidor de informes. Puede reiniciar el servicio actualizando la opción `SSRS`.

Para obtener más información, consulte Uso de registros de Amazon RDS para Microsoft SQL Server.

Acceso al portal web de SSRS

Utilice el siguiente proceso para acceder al portal web de SSRS:

1. Active la capa de conexión segura (SSL)
2. Conceder acceso a los usuarios del dominio.
3. Acceda al portal web mediante un explorador y las credenciales de usuario del dominio.

Uso de SSL en RDS

SSRS utiliza el protocolo SSL de HTTPS para sus conexiones. Para trabajar con este protocolo, importe un certificado SSL en el sistema operativo Microsoft Windows del equipo cliente.

Para obtener más información sobre los certificados SSL, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener más información acerca de cómo usar SSL con SQL Server, consulte ???.

Concesión de acceso a usuarios de dominio

En una nueva activación de SSRS, no hay asignaciones de roles en SSRS. Para dar acceso al portal web a un usuario de dominio o grupo de usuarios, RDS proporciona un procedimiento almacenado.

Para conceder acceso a un usuario de dominio en el portal web

- Utilice el siguiente procedimiento almacenado.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSRS_GRANT_PORTAL_PERMISSION',
@ssrs_group_or_username=N'AD_domain\user';
```

Al usuario o grupo de usuarios del dominio se le concede el rol del sistema `RDS_SSRS_ROLE`. Este rol tiene asignadas las siguientes tareas en el nivel de sistema:

- Ejecutar informes
- Administrar trabajos
- Administrar programaciones compartidas

- Ver programaciones compartidas

También se concede el rol de nivel de elemento de `Content Manager` en la carpeta raíz.

Acceso al portal web

Una vez finalizada la tarea `SSRS_GRANT_PORTAL_PERMISSION` correctamente, tendrá acceso al portal mediante un explorador web. La URL del portal web tiene el siguiente formato.

```
https://rds_endpoint:port/Reports
```

En este formato, se aplica lo siguiente:

- *`rds_endpoint`* – el punto de enlace de la instancia de base de datos de RDS que está utilizando con SSRS.

  Puede encontrar el punto de enlace en la pestaña Conectividad y seguridad de su instancia de base de datos. Para obtener más información, consulte Conexión a la instancia de base de datos de Microsoft SQL Server.
- *`port`*: el puerto del agente de escucha para SSRS que se establece en la opción `SSRS`.

Para acceder al portal web

1. Introduzca la URL del portal web en su navegador.

   ```
   https://myssrsinstance.cg034itsfake.us-east-1.rds.amazonaws.com:8443/Reports
   ```
2. Inicie sesión con las credenciales de un usuario de dominio al que haya otorgado acceso con la tarea `SSRS_GRANT_PORTAL_PERMISSION`.

Implementación de informes y configuración de orígenes de datos de informes

Utilice los siguientes procedimientos para implementar los informes en SSRS y configurar los orígenes de datos de los informes:

Temas

- Implementación de informes en SSRS
- Configuración del origen de datos del informe

Implementación de informes en SSRS

Después de tener acceso al portal web, puede implementar informes en él. Puede utilizar la herramienta Cargar en el portal web para cargar informes o implementarlos directamente desde SQL Server Data Tools (SSDT). Al implementarlos desde SSDT, asegúrese de lo siguiente:

- El usuario que inició SSDT tiene acceso al portal web de SSRS.
- El valor `TargetServerURL` de las propiedades del proyecto de SSRS se establece en el punto de enlace de HTTPS de la instancia de base de datos de RDS con el sufijo `ReportServer`, por ejemplo:

```
https://myssrsinstance.cg034itsfake.us-east-1.rds.amazonaws.com:8443/ReportServer
```

Configuración del origen de datos del informe

Después de implementar un informe en SSRS, debe configurar el origen de datos del informe. Al configurar el origen de datos del informe, asegúrese de lo siguiente:

- Para instancias de base de datos de RDS para SQL Server unidas a AWS Directory Service for Microsoft Active Directory, utilice el nombre de dominio completo (FQDN) como nombre del origen de datos de la cadena de conexión. Un ejemplo es *`myssrsinstance.corp-ad.example.com`*, donde *`myssrsinstance`* es el nombre de instancia de base de datos y *`corp-ad.example.com`* es el nombre de dominio completo.
- Para las instancias de base de datos de RDS para SQL Server unidas a Active Directory autogestionado, utilice `.` o *`LocalHost`* como nombre del origen de datos de la cadena de conexión.

Uso del correo electrónico de SSRS para enviar informes

SSRS incluye la extensión de correo electrónico de SSRS, que puede usar para enviar informes a los usuarios.

Para configurar el correo electrónico de SSRS, utilice la opción de configuración `SSRS`. Para obtener más información, consulte Agregar la opción SSRS a su grupo de opciones.

Después de configurar el correo electrónico de SSRS, puede suscribirse a los informes en el servidor de informes. Para obtener más información, consulte Email delivery in Reporting Services (Entrega de correo electrónico en servicios de informes) en la documentación de Microsoft.

La integración con AWS Secrets Manager es necesaria para que el correo electrónico de SSRS funcione en RDS. Para integrarse con Secrets Manager, debe crear un secreto.

> **Note**
>
> Si cambia el secreto más adelante, también tendrá que actualizar la opción SSRS del grupo de opciones.

Para crear un secreto para el correo electrónico de SSRS

1. Siga los pasos de Creación de un secreto en la Guía del usuario de AWS Secrets Manager.

   a. En Select secret type (Seleccionar tipo de secreto), elija Other type of secrets (Otro tipo de secretos).

   b. En Key/value pairs (Pares clave/valor), escriba lo siguiente:

      - **SMTP_USERNAME**: introduzca un usuario con permiso para enviar correo desde el servidor SMTP.
      - **SMTP_PASSWORD**: introduzca una contraseña para el usuario SMTP.

   c. En Encryption key (Clave de cifrado), no utilice el valor predeterminado AWS KMS key. Utilice su propia clave existente o cree una nueva.

      La política de claves de KMS debe permitir la acción `kms:Decrypt`, por ejemplo:

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "rds.amazonaws.com"
        ]
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

2. Siga los pasos de Adjuntar una política de permisos a un secretoen la Guía del usuario de AWS Secrets Manager. La política de permisos otorga la acción `secretsmanager:GetSecretValue` principal del servicio `rds.amazonaws.com`.

   Le recomendamos que utilice la `aws:sourceAccount` y las condiciones `aws:sourceArn` de la política para evitar el problema del suplente confuso. Utilice su Cuenta de AWS para `aws:sourceAccount` y el ARN del grupo de opciones para `aws:sourceArn`. Para obtener más información, consulte Prevención de los problemas del suplente confuso entre servicios.

   El ejemplo siguiente muestra una política de permisos.

   JSON

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : "rds.amazonaws.com"
    },
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "aws:sourceAccount" : "123456789012"
      },
      "ArnLike" : {
        "aws:sourceArn" : "arn:aws:rds:us-west-2:123456789012:og:ssrs-
se-2017"
      }
    }
  } ]
}
```

   Para ver más ejemplos, consulte Ejemplos de políticas de permisos para AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Revocación de permisos de nivel de sistema

El rol del sistema `RDS_SSRS_ROLE` no tiene permisos suficientes para eliminar asignaciones de roles de nivel del sistema. Para quitar un usuario o un grupo de usuarios de `RDS_SSRS_ROLE`, utilice el mismo procedimiento almacenado que utilizó para otorgar el rol pero utilice el tipo de tarea `SSRS_REVOKE_PORTAL_PERMISSION`.

Para revocar el acceso de un usuario de dominio para el portal web

- Utilice el siguiente procedimiento almacenado.

```
exec msdb.dbo.rds_msbi_task
@task_type='SSRS_REVOKE_PORTAL_PERMISSION',
@ssrs_group_or_username=N'AD_domain\user';
```

Al hacerlo, se elimina al usuario del rol del sistema `RDS_SSRS_ROLE`. También elimina al usuario del rol de nivel de elemento `Content Manager` si el usuario lo tiene.

Monitoreo del estado de una tarea

Para realizar un seguimiento del estado de la tarea de concesión o revocación, llame a la función `rds_fn_task_status`. Tiene dos parámetros. El primer parámetro tiene que ser siempre `NULL` porque no se aplica a SSRS. El segundo parámetro acepta un ID de tarea.

Para obtener una lista de todas las tareas, establezca el primer parámetro en `NULL` y el segundo en `0`, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,0);
```

Para obtener una tarea específica, establezca el primer parámetro en `NULL` y el segundo en el ID de la tarea, como se muestra en el siguiente ejemplo.

```
SELECT * FROM msdb.dbo.rds_fn_task_status(NULL,42);
```

La función `rds_fn_task_status` devuelve la siguiente información.

Parámetro de salida	Descripción
`task_id`	El ID de la tarea.

Parámetro de salida	Descripción
`task_type`	Para SSRS, las tareas pueden tener los siguientes tipos de tareas: • `SSRS_GRANT_PORTAL_PERMISSION` • `SSRS_REVOKE_PORTAL_PERMISSION`
`database_name`	No aplicable a tareas de SSRS.
`% complete`	El porcentaje de progreso de la tarea.
`duration (mins)`	El tiempo empleado en la tarea, en minutos.

Parámetro de salida	Descripción
`lifecycle`	El estado de la tarea. Los posibles estados son los siguientes: • `CREATED` – después de llamar a uno de los procedimientos almacenados de SSRS, se crea una tarea y el estado se establece en `CREATED`. • `IN_PROGRESS` – cuando una tarea comienza, el estado se establece en `IN_PROGRESS` . Pueden pasar hasta cinco minutos hasta que el estado cambie de `CREATED` a `IN_PROGRESS` . • `SUCCESS` – cuando una tarea se completa, el estado se establece en `SUCCESS`. • `ERROR` – si se produce un error con una tarea, el estado se establece en `ERROR`. Para obtener más información acerca del error, consulte la columna `task_info` . • `CANCEL_REQUESTED` : después de llamar al procedimiento almacenado `rds_cancel_task` , el estado de la tarea se establece en `CANCEL_REQUESTED` . • `CANCELLED` – después de que se cancela una tarea correctamente, se establece su estado en `CANCELLED` .
`task_info`	Información adicional acerca de la tarea. Si se produce un error durante el procesamiento, esta columna contiene información acerca del error.

Parámetro de salida	Descripción
`last_updated`	La fecha y hora en que se actualizó por última vez el estado de la tarea.
`created_at`	La fecha y hora en que se creó la tarea.
`S3_object_arn`	No aplicable a tareas de SSRS.
`overwrite_S3_backup_file`	No aplicable a tareas de SSRS.
`KMS_master_key_arn`	No aplicable a tareas de SSRS.
`filepath`	No aplicable a tareas de SSRS.
`overwrite_file`	No aplicable a tareas de SSRS.
`task_metadata`	Metadatos asociados a la tarea de SSRS.

Deshabilitación y eliminación de bases de datos de SSRS

Utilice los siguientes procedimientos para deshabilitar SSRS y eliminar las bases de datos de SSRS:

Temas

- Desactivación de SSRS
- Eliminación de las bases de datos SSRS

Desactivación de SSRS

Para desactivar SSRS, quite la opción `SSRS` de su grupo de opciones. La eliminación de la opción no elimina las bases de datos SSRS. Para obtener más información, consulte Eliminación de las bases de datos SSRS.

Puede volver a activar SSRS si vuelve a añadir la opción `SSRS`. Si también ha eliminado las bases de datos de SSRS, al volver a añadir la opción en la misma instancia de base de datos, se crean nuevas bases de datos del servidor de informes.

Consola

Para quitar la opción SSRS de su grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `SSRS` (`ssrs-se-2017` en los ejemplos anteriores).
4. Elija Delete option (Eliminar opción).
5. En Opciones de eliminación, elija SSRS para Opciones para eliminar.
6. En Apply immediately (Aplicar inmediatamente), seleccione Yes (Sí) para eliminar la opción inmediatamente o No para eliminarla en el siguiente período de mantenimiento.
7. Elija Eliminar.

CLI

Para quitar la opción SSRS de su grupo de opciones

- Ejecute uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds remove-option-from-option-group \
    --option-group-name ssrs-se-2017 \
    --options SSRS \
    --apply-immediately
```

  En:Windows

```
aws rds remove-option-from-option-group ^
    --option-group-name ssrs-se-2017 ^
    --options SSRS ^
    --apply-immediately
```

Eliminación de las bases de datos SSRS

Al quitar la opción SSRS, no se eliminan las bases de datos del servidor de informes. Para eliminarlas, utilice el siguiente procedimiento almacenado.

Para eliminar las bases de datos del servidor de informes, asegúrese de quitar primero la opción SSRS.

Para eliminar las bases de datos SSRS

- Utilice el siguiente procedimiento almacenado.

```
exec msdb.dbo.rds_drop_ssrs_databases
```

Compatibilidad con el Coordinador de transacciones distribuidas de Microsoft en RDS for SQL Server

Una transacción distribuida es una transacción de base de datos en la que participan dos o más anfitriones de red. RDS for SQL Server admite transacciones distribuidas entre anfitriones, donde un solo anfitrión puede ser uno de los siguientes:

- Instancia de base de datos de RDS para SQL Server
- Host local de SQL Server
- Host de Amazon EC2 con SQL Server instalado
- Cualquier otro host de EC2 o instancia de base de datos de RDS con un motor de base de datos que admita transacciones distribuidas

En RDS, a partir de SQL Server 2012 (versión 11.00.5058.0.v1 y posterior), todas las ediciones de RDS for SQL Server admiten transacciones distribuidas. La compatibilidad se proporciona con el Coordinador de transacciones distribuidas de Microsoft (MSDTC). Para obtener información detallada acerca de MSDTC, consulte Distributed Transaction Coordinator en la documentación de Microsoft.

Contenido

- Limitaciones
- Habilitación de MSDTC
  - Creación del grupo de opciones para MSDTC
  - Agregar la opción de MSDTC al grupo de opciones
  - Creación del grupo de parámetros para MSDTC
  - Modificación del parámetro para MSDTC
  - Asociación del grupo de opciones y el grupo de parámetros con la instancia de base de datos
  - Modificación de la opción MSDTC
- Utilización de transacciones
  - Uso de transacciones distribuidas
  - Utilización de transacciones XA
  - Uso del seguimiento de transacciones
- Deshabilitación de MSDTC
- Solución de problemas de MSDTC para SQL Server de RDS

Limitaciones

Las siguientes limitaciones se aplican al uso de MSDTC en RDS para SQL Server:

- MSDTC no se admite en instancias que utilizan la creación de reflejo de base de datos de SQL Server. Para obtener más información, consulte Transacciones - Grupos de disponibilidad y creación de reflejo de la base de datos.
- El parámetro `in-doubt xact resolution` debe estar establecido en 1 o 2. Para obtener más información, consulte Modificación del parámetro para MSDTC.
- MSDTC requiere que todos los nombres de host que participan en transacciones distribuidas se puedan resolver mediante sus nombres de host. RDS mantiene automáticamente esta funcionalidad para instancias unidas a dominios. Sin embargo, para instancias independientes, asegúrese de configurar manualmente el servidor DNS.
- Las transacciones XA de Java Database Connectivity (JDBC) son compatibles con SQL Server 2017 versión 14.00.3223.3 y posteriores, así como con SQL Server 2019.
- No se admiten transacciones distribuidas que dependan de bibliotecas de vínculos dinámicos (DLL) del cliente en instancias de RDS.
- No se admite el uso de bibliotecas de vínculos dinámicos XA personalizadas.

Habilitación de MSDTC

Ejecute el siguiente proceso para habilitar MSDTC para su instancia de base de datos:

1. Cree un nuevo grupo de opciones o elija un grupo de opciones ya existente.
2. Añada la opción `MSDTC` al grupo de opciones.
3. Cree un nuevo grupo de parámetros o elija un grupo de parámetros existente.
4. Modifique el grupo de parámetros para establecer el parámetro `in-doubt xact resolution` en 1 o 2.
5. Asocie el grupo de opciones y el grupo de parámetros a la instancia de base de datos.

Creación del grupo de opciones para MSDTC

Utilice la AWS Management Console o la AWS CLI para crear un grupo de opciones que corresponda al motor de SQL Server y la versión de su instancia de base de datos.

> **Note**
>
> También puede utilizar un grupo de opciones ya existente si es para el motor y la versión correctos de SQL Server.

Consola

El siguiente procedimiento crea un grupo de opciones para SQL Server Standard Edition 2016.

Para crear el grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija Create group.
4. En el panel Create option group (Crear grupo de opciones), haga lo siguiente:
   a. En Nombre, escriba un nombre para el grupo de opciones que sea exclusivo dentro de su cuenta de AWS, como **`msdtc-se-2016`**. El nombre solo puede contener letras, dígitos y guiones.
   b. En Descripción, escriba una breve descripción del grupo de opciones, como **`MSDTC option group for SQL Server SE 2016`**. La descripción se utiliza para fines de visualización.
   c. Para Engine (Motor), elija sqlserver-se.
   d. En Versión principal del motor, elija 13.00.
5. Elija Create (Crear).

CLI

En el siguiente ejemplo se crea un grupo de opciones para SQL Server Standard Edition 2016.

Para crear el grupo de opciones

- Utilice uno de los siguientes comandos.

Example

Para Linux, macOS o:Unix

```
aws rds create-option-group \
    --option-group-name msdtc-se-2016 \
    --engine-name sqlserver-se \
    --major-engine-version 13.00 \
    --option-group-description "MSDTC option group for SQL Server SE 2016"
```

En:Windows

```
aws rds create-option-group ^
    --option-group-name msdtc-se-2016 ^
    --engine-name sqlserver-se ^
    --major-engine-version 13.00 ^
    --option-group-description "MSDTC option group for SQL Server SE 2016"
```

Agregar la opción de MSDTC al grupo de opciones

A continuación, utilice la AWS Management Console o la AWS CLI para agregar la opción `MSDTC` al grupo de opciones.

Se requieren los siguientes ajustes de opciones:

- Puerto: el puerto que utilice para acceder a MSDTC. Los valores permitidos son 1150–49.151 excepto 1234, 1434, 3260, 3343, 3389 y 47.001. El valor predeterminado es 5000.

  Asegúrese de que el puerto que desea utilizar está habilitado en las reglas de firewall. Además, asegúrese de que este puerto esté habilitado, según sea necesario, en las reglas de entrada y salida del grupo de seguridad asociado a su instancia de base de datos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.
- Grupos de seguridad: la pertenencia a grupos de seguridad de VPC para la instancia de base de datos de RDS.
- Tipo de autenticación: el modo de autenticación entre alojamientos. Se admiten los siguientes tipos de autenticación:

  - Mutua: las instancias RDS se autentican mutuamente mediante la autenticación integrada. Si se selecciona esta opción, todas las instancias asociadas a este grupo de opciones deben estar unidas al dominio.
  - Ninguna: no se realiza ninguna autenticación entre alojamientos. No recomendamos utilizar este modo en entornos de producción.
- Tamaño del registro de transacciones: el tamaño del registro de transacciones de MSDTC. Los valores permitidos son 4–1024. El tamaño predeterminado es 4 MB.

Los siguientes ajustes de opciones son opcionales:

- Habilitar conexiones entrantes: indica si se permiten conexiones MSDTC entrantes a instancias asociadas a este grupo de opciones.
- Habilitar conexiones salientes: indica si desea permitir conexiones MSDTC salientes desde instancias asociadas a este grupo de opciones.
- Habilitar XA: si desea permitir transacciones XA. Para obtener más información sobre el protocolo XA, consulte Especificación XA.
- Habilitar LU de SNA: indica si se va a permitir que el protocolo LU de SNA se utilice para transacciones distribuidas. Para obtener más información sobre la compatibilidad con el protocolo LU de SNA, consulte Managing IBM CICS LU 6.2 Transactions en la documentación de Microsoft.

Consola

Para agregar la opción MSDTC

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones que acaba de crear.
4. Seleccione Add option (Añadir opción).
5. En Detalles de la opción, elija MSDTC en Nombre de la opción.
6. En Configuración de opciones:
   a. En Puerto, escriba el número de puerto para acceder a MSDTC. El valor predeterminado es 5000.

b. En Security groups (Grupos de seguridad), elija el grupo de seguridad de VPC que desea asociar a la opción.

c. En Tipo de autenticación, elija Mutua o Ninguna.

d. En Tamaño del registro de transacciones, escriba un valor entre 4 y 1024. El valor predeterminado es 4.

7. En Configuración adicional, haga lo siguiente:

a. En Conexiones, elija Habilitar conexiones entrantes y Habilitar conexiones salientes según sea necesario.

b. En Protocolos permitidos, elija Habilitar XA y Habilitar LU de SNA.

8. En Scheduling (Programación), elija si desea agregar la opción inmediatamente o en el siguiente período de mantenimiento.

9. Seleccione Add option (Añadir opción).

Para agregar esta opción, no es necesario reiniciar.

CLI

Para agregar la opción MSDTC

1. Cree un archivo JSON, por ejemplo `msdtc-option.json`, con los siguientes parámetros obligatorios:

```
{
"OptionGroupName":"msdtc-se-2016",
"OptionsToInclude": [
 {
 "OptionName":"MSDTC",
 "Port":5000,
 "VpcSecurityGroupMemberships":["sg-0abcdef123"],
 "OptionSettings":[{"Name":"AUTHENTICATION","Value":"MUTUAL"},
{"Name":"TRANSACTION_LOG_SIZE","Value":"4"}]
 }],
"ApplyImmediately": true
}
```

2. Añada la opción `MSDTC` al grupo de opciones.

Example

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --cli-input-json file://msdtc-option.json \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --cli-input-json file://msdtc-option.json ^
    --apply-immediately
```

No es necesario reiniciar el equipo.

Creación del grupo de parámetros para MSDTC

Cree o modifique un grupo de parámetros para el parámetro `in-doubt xact resolution` que corresponde a la edición y versión de SQL Server de la instancia de base de datos.

Consola

En el ejemplo siguiente se crea un grupo de parámetros para SQL Server Standard Edition 2016.

Para crear el grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija Create parameter group.
4. En el panel Create parameter group (Crear grupo de parámetros), haga lo siguiente:
   a. En Familia de grupos de parámetros, elija sqlserver-se-13.0.
   b. En Nombre de grupo, escriba un identificador para el grupo de parámetros, como **`msdtc-sqlserver-se-13`**.
   c. En Descripción, escriba **`in-doubt xact resolution`**.
5. Elija Create (Crear).

CLI

En el ejemplo siguiente se crea un grupo de parámetros para SQL Server Standard Edition 2016.

Para crear el grupo de parámetros

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-db-parameter-group \
    --db-parameter-group-name msdtc-sqlserver-se-13 \
    --db-parameter-group-family "sqlserver-se-13.0" \
    --description "in-doubt xact resolution"
```

  En:Windows

```
aws rds create-db-parameter-group ^
    --db-parameter-group-name msdtc-sqlserver-se-13 ^
    --db-parameter-group-family "sqlserver-se-13.0" ^
    --description "in-doubt xact resolution"
```

Modificación del parámetro para MSDTC

Modifique el parámetro `in-doubt xact resolution` en el grupo de parámetros que corresponde a la edición y la versión de SQL Server de su instancia de base de datos.

Para MSDTC, establezca el parámetro `in-doubt xact resolution` en uno de los siguientes:

- 1 – `Presume commit`: se supone que todas las transacciones de MSDTC en duda se han confirmado.
- 2 – `Presume abort`: se supone que todas las transacciones de MSDTC en duda se han detenido.

Para obtener más información, consulte in-doubt xact resolution (opción de configuración del servidor) en la documentación de Microsoft.

Consola

En el ejemplo siguiente se modifica el grupo de parámetros que ha creado para SQL Server Standard Edition 2016.

Para modificar el grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Parameter groups (Grupos de parámetros).
3. Elija el grupo de parámetros, como msdtc-sqlserver-se-13.
4. En Parámetros, filtre la lista de parámetros para **xact**.
5. Elija in-doubt xact resolution.
6. Elija Edit parameters (Editar parámetros).
7. Escriba **1** o **2**.
8. Elija Guardar cambios.

CLI

En el ejemplo siguiente se modifica el grupo de parámetros que ha creado para SQL Server Standard Edition 2016.

Para modificar el grupo de parámetros

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name msdtc-sqlserver-se-13 \
    --parameters "ParameterName='in-doubt xact
 resolution',ParameterValue=1,ApplyMethod=immediate"
```

  En:Windows

```
aws rds modify-db-parameter-group ^
```

```
    --db-parameter-group-name msdtc-sqlserver-se-13 ^
    --parameters "ParameterName='in-doubt xact
resolution',ParameterValue=1,ApplyMethod=immediate"
```

Asociación del grupo de opciones y el grupo de parámetros con la instancia de base de datos

Puede utilizar la AWS Management Console o la AWS CLI para asociar el grupo de opciones MSDTC y el grupo de parámetros con la instancia de base de datos.

Consola

Puede asociar el grupo de opciones de MSDTC y el grupo de parámetros con una instancia de base de datos nueva o existente.

- Para una nueva instancia de base de datos, asóciela cuando inicie la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, asóciela modificando la instancia. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Note**
>
> Si utiliza una instancia de base de datos que existe, esta ya debe tener asociado un dominio de Active Directory y un rol de AWS Identity and Access Management (IAM). Si crea una instancia unida a dominio nueva, especifique un rol de IAM y un dominio de Active Directory ya existentes. Para obtener más información, consulte Uso de AWS Managed Active Directory con RDS para SQL Server.

CLI

Puede asociar el grupo de opciones de MSDTC y el grupo de parámetros con una instancia de base de datos nueva o existente.

> **Note**
>
> Si usa una instancia de base de datos unidad a dominio que ya existe, esta debe tener ya asociada un dominio de Active Directory y un rol de IAM. Si crea una instancia unida a dominio nueva, especifique un rol de IAM y un dominio de Active Directory ya existentes.

Para obtener más información, consulte Uso de AWS Managed Active Directory con RDS para SQL Server.

Para crear una instancia de base de datos con el grupo de opciones y el grupo de parámetros de MSDTC

- Especifique el mismo tipo de motor de base de datos y la misma versión principal que ha utilizado al crear el grupo de opciones.

  Example

  Para Linux, macOS o:Unix

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --db-instance-class db.m5.2xlarge \
    --engine sqlserver-se \
    --engine-version 13.00.5426.0.v1 \
    --allocated-storage 100 \
    --manage-master-user-password \
    --master-username admin \
    --storage-type gp2 \
    --license-model li \
    --domain-iam-role-name my-directory-iam-role \
    --domain my-domain-id \
    --option-group-name msdtc-se-2016 \
    --db-parameter-group-name msdtc-sqlserver-se-13
```

  En:Windows

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-instance-class db.m5.2xlarge ^
    --engine sqlserver-se ^
    --engine-version 13.00.5426.0.v1 ^
    --allocated-storage 100 ^
    --manage-master-user-password ^
    --master-username admin ^
    --storage-type gp2 ^
    --license-model li ^
    --domain-iam-role-name my-directory-iam-role ^
```

```
    --domain my-domain-id ^
    --option-group-name msdtc-se-2016 ^
    --db-parameter-group-name msdtc-sqlserver-se-13
```

Para modificar una instancia de base de datos y asociar el grupo de opciones y el grupo de parámetros de MSDTC

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --option-group-name msdtc-se-2016 \
    --db-parameter-group-name msdtc-sqlserver-se-13 \
    --apply-immediately
```

  En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --option-group-name msdtc-se-2016 ^
    --db-parameter-group-name msdtc-sqlserver-se-13 ^
    --apply-immediately
```

Modificación de la opción MSDTC

Después de habilitar la opción `MSDTC`, puede modificar su configuración. Para obtener más información acerca de cómo modificar la configuración de opciones, consulte Modificación de una configuración de opciones.

> **Note**
>
> Algunos cambios en la configuración de la opción MSDTC requieren que se reinicie el servicio MSDTC. Este requisito puede afectar a las transacciones distribuidas en ejecución.

Utilización de transacciones

Uso de transacciones distribuidas

En Amazon RDS for SQL Server, ejecute transacciones distribuidas de la misma manera que las transacciones distribuidas que se ejecutan en las instalaciones:

- Usando transacciones promocionables `System.Transactions` de .NET Framework , que optimizan las transacciones distribuidas aplazando su creación hasta que sean necesarias.

  En este caso, la promoción es automática y no requiere ninguna intervención. Si solo hay un administrador de recursos dentro de la transacción, no se realiza ninguna promoción. Para obtener más información acerca de los ámbitos de transacción implícitos, consulte Implementación de una transacción implícita usando el ámbito de transacción en la documentación de Microsoft.

  Las transacciones promocionables son compatibles con estas implementaciones .NET:

  - A partir de ADO.NET 2.0, `System.Data.SqlClient` admite transacciones promocionables con SQL Server. Para obtener más información, consulte Integración de System.Transactions con SQL Server en la documentación de Microsoft.
  - ODP.NET admite `System.Transactions`. Se crea una transacción local para la primera conexión abierta en el ámbito `TransactionsScope` a Oracle Database 11g versión 1 (versión 11.1) y posteriores. Cuando se abre una segunda conexión, esta transacción se promueve automáticamente a una transacción distribuida. Para obtener más información acerca de la compatibilidad con transacciones distribuidas en ODP.NET, consulte Integración con Coordinador de transacciones distribuidas de Microsoft en la documentación de Microsoft.
- Uso de la instrucción `BEGIN DISTRIBUTED TRANSACTION`. Para obtener más información, consulte BEGIN DISTRIBUTION TRANSACT-SQL (Transact-SQL) en la documentación de Microsoft.

Utilización de transacciones XA

A partir de RDS for SQL Server 2017 versión 14.00.3223.3, puede controlar las transacciones distribuidas mediante JDBC. Cuando establece la opción `Enable XA` en `true` en la opción `MSDTC`, RDS habilita automáticamente las transacciones de JDBC y otorga el rol `SqlJDBCXAUser` al usuario `guest`. Esto permite ejecutar transacciones distribuidas mediante JDBC. Para obtener más información, incluido un ejemplo de código, consulte Descripción de las transacciones XA en la documentación de Microsoft.

Uso del seguimiento de transacciones

RDS admite controlar los seguimientos de transacciones de MSDTC y descargarlos desde la instancia de base de datos de RDS para solucionar problemas. Puede controlar las sesiones de seguimiento de transacciones ejecutando el siguiente procedimiento almacenado de RDS.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'trace_action',
[@traceall='0|1'],
[@traceaborted='0|1'],
[@tracelong='0|1'];
```

El siguiente parámetro es obligatorio:

- `trace_action`: la acción de rastreo. Puede ser `START`, `STOP`, o `STATUS`.

Los siguientes parámetros son opcionales:

- `@traceall`: establezca en 1 para realizar un seguimiento de todas las transacciones distribuidas. El valor predeterminado es 0.
- `@traceaborted`: establezca en 1 para realizar un seguimiento de las transacciones distribuidas canceladas. El valor predeterminado es 0.
- `@tracelong`: establezca en 1 para realizar un seguimiento de transacciones distribuidas de larga duración. El valor predeterminado es 0.

Example de acción de seguimiento START

Para iniciar una nueva sesión de seguimiento de transacciones, ejecute la instrucción de ejemplo siguiente.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'START',
@traceall='0',
@traceaborted='1',
@tracelong='1';
```

> **Note**
>
> Solo puede estar activa una sesión de seguimiento de transacciones a la vez. Si se emite un nuevo comando START de sesión de seguimiento mientras una sesión de seguimiento está activa, se devuelve un error y la sesión de seguimiento activa se mantiene sin cambios.

Example de acción de seguimiento STOP

Para detener una sesión de seguimiento de transacciones, ejecute la siguiente instrucción.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'STOP'
```

Esta instrucción detiene la sesión de seguimiento de transacciones activa y guarda los datos de seguimiento de la transacción en el directorio de registro de la instancia de base de datos de RDS. La primera fila de la salida contiene el resultado general y las siguientes líneas indican los detalles de la operación.

A continuación se muestra un ejemplo de una detención satisfactoria de sesión de seguimiento.

```
OK: Trace session has been successfully stopped.
Setting log file to: D:\rdsdbdata\MSDTC\Trace\dtctrace.log
Examining D:\rdsdbdata\MSDTC\Trace\msdtctr.mof for message formats,  8 found.
Searching for TMF files on path: (null)
Logfile D:\rdsdbdata\MSDTC\Trace\dtctrace.log:
 OS version    10.0.14393  (Currently running on 6.2.9200)
 Start Time    <timestamp>
 End Time      <timestamp>
 Timezone is   @tzres.dll,-932 (Bias is 0mins)
 BufferSize            16384 B
 Maximum File Size     10 MB
 Buffers  Written      Not set (Logger may not have been stopped).
 Logger Mode Settings (11000002) ( circular paged
 ProcessorCount         1
Processing completed   Buffers: 1, Events: 3, EventsLost: 0 :: Format Errors: 0,
 Unknowns: 3
Event traces dumped to d:\rdsdbdata\Log\msdtc_<timestamp>.log
```

Puede utilizar la información detallada para consultar el nombre del archivo de registro generado. Para obtener más información acerca de la descarga de archivos de registro de la instancia de base de datos de RDS, consulte Supervisión de archivos de registro de Amazon RDS.

Los registros de sesión de seguimiento permanecen en la instancia durante 35 días. Los registros de sesión de seguimiento anteriores se eliminan automáticamente.

Example de acción de seguimiento de STATUS

Para rastrear el estado de una sesión de seguimiento de transacciones, ejecute la siguiente instrucción.

```
exec msdb.dbo.rds_msdtc_transaction_tracing 'STATUS'
```

Esta instrucción genera lo siguiente como filas separadas del conjunto de resultados.

```
OK
SessionStatus: <Started|Stopped>
TraceAll: <True|False>
TraceAborted: <True|False>
TraceLongLived: <True|False>
```

La primera línea indica el resultado general de la operación: `OK` o `ERROR` con detalles, si procede. Las líneas siguientes indican detalles sobre el estado de la sesión de seguimiento:

- `SessionStatus` puede ser uno de los siguientes:
  - `Started` si se está ejecutando una sesión de seguimiento.
  - `Stopped` si no se está ejecutando ninguna sesión de seguimiento.
- Los indicadores de sesión de seguimiento pueden ser `True` o `False` en función de cómo se establecieron en el `START` comando.

Deshabilitación de MSDTC

Para deshabilitar MSDTC, quite la opción `MSDTC` de su grupo de opciones.

Consola

Para quitar la opción MSDTC de su grupo de opciones

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Elija el grupo de opciones con la opción `MSDTC` (`msdtc-se-2016` en los ejemplos anteriores).

4. Elija Delete option (Eliminar opción).
5. En Opciones de eliminación, elija MSDTC para Opciones para eliminar.
6. En Apply immediately (Aplicar inmediatamente), seleccione Yes (Sí) para eliminar la opción inmediatamente o No para eliminarla en el siguiente período de mantenimiento.
7. Elija Eliminar.

CLI

Para quitar la opción MSDTC de su grupo de opciones

- Utilice uno de los siguientes comandos.

  Example

  Para Linux, macOS o:Unix

```
aws rds remove-option-from-option-group \
    --option-group-name msdtc-se-2016 \
    --options MSDTC \
    --apply-immediately
```

  En:Windows

```
aws rds remove-option-from-option-group ^
    --option-group-name msdtc-se-2016 ^
    --options MSDTC ^
    --apply-immediately
```

Solución de problemas de MSDTC para SQL Server de RDS

En algunos casos, puede tener problemas para establecer una conexión entre MSDTC que se ejecuta en un equipo cliente y el servicio de MSDTC que se ejecuta en una instancia de base de datos de SQL Server de RDS. Si es así, asegúrese de lo siguiente:

- Las reglas de entrada para el grupo de seguridad asociado a la instancia de base de datos están configuradas correctamente. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.
- El equipo cliente está configurado correctamente.

- Las reglas de firewall de MSDTC en el equipo del cliente están habilitadas.

Para configurar el equipo cliente

1. Abra Servicios de componentes.

   O bien, en Administrador del servidor, elija Herramientas, y, a continuación, elija Servicios de componentes.
2. Expanda Servicios de componentes, expanda Equipos, expanda Mi PC, y, a continuación, expanda Coordinador de transacciones distribuidas.
3. Abra el menú contextual (clic derecho) de DTC local y elija Propiedades.
4. Elija la pestaña Seguridad.
5. Elija todas las opciones siguientes:
   - Acceso DTC de red
   - Permitir entrada
   - Permitir salida
6. Asegúrese de que se haya elegido el modo de autenticación correcto:
   - Autenticación mutua requerida: el equipo cliente se une al mismo dominio que otros nodos que participan en transacciones distribuidas o existe una relación de confianza configurada entre dominios.
   - No se requiere autenticación: todos los demás casos.
7. Elija Aceptar para guardar los cambios.
8. Si se le pide que reinicie el servicio, elija Sí.

Para habilitar las reglas de firewall de MSDTC

1. Abra el Firewall de Windows y, a continuación, elija Configuración avanzada.

   O, en Administrador del servidor, elija Herramientas y, a continuación, elija Firewall de Windows con seguridad avanzada.

> **Note**
>
> En función del sistema operativo,el Firewall de Windows puede llamarse Firewall de Windows Defender.

2. Elija Reglas de entrada en el panel izquierdo.
3. Habilite las siguientes reglas de firewall, si aún no están habilitadas:
   - Coordinador de transacciones distribuidas (RPC)
   - Coordinador de transacciones distribuidas (RPC) -EPMAP
   - Coordinador de Transacciones Distribuidas (TCP-In)
4. Cierre el firewall de Windows.

Tareas comunes de administrador de bases de datos de Amazon RDS para Microsoft SQL Server

En esta sección se describen las implementaciones específicas de Amazon RDS de algunas tareas frecuentes de administración de bases de datos para las instancias de base de datos que ejecutan el motor de base de datos de Microsoft SQL Server. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso de shell a las instancias de base de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

> **Note**
>
> Cuando se trabaja con una instancia de base de datos de SQL Server, se pueden ejecutar scripts para modificar una base de datos que se acaba de crear, pero no se puede modificar la base de datos [model], que se usa como modelo para las nuevas bases de datos.

Temas

- Acceso a la base de datos tempdb de las instancias de bases de datos de Microsoft SQL Server en Amazon RDS
- Análisis de la carga de trabajo de una base de datos de una instancia de base de datos de Amazon RDS for SQL Server con el Asistente para la optimización del motor de base de datos
- Cambio del db_owner a la cuenta de rdsa de la base de datos de Amazon RDS para SQL Server
- Administración de intercalaciones y conjuntos de caracteres de Amazon RDS para Microsoft SQL Server
- Creación de un usuario de base de datos de Amazon RDS para SQL Server
- Determinación de un modelo de recuperación para una base de datos de Amazon RDS para SQL Server
- Determinación de la hora de la última conmutación por error de Amazon RDS para SQL Server
- Solución de problemas de recuperación en un momento dado debido a una brecha en el número de secuencia de registros
- Denegación o permiso para ver los nombres de las bases de datos de Amazon RDS para SQL Server
- Desactivación de inserciones rápidas durante la carga masiva de Amazon RDS para SQL Server

- Eliminación de una base de datos en una instancia de base de datos de Amazon RDS para Microsoft SQL Server
- Cambio del nombre de una base de datos de Amazon RDS para Microsoft SQL Server en una implementación multi-AZ
- Restablecimiento de la pertenencia al rol db_owner para el usuario maestro de Amazon RDS para SQL Server
- Restauración de instancias de base de datos con licencia caducada de Amazon RDS para SQL Server
- Transición de una base de datos de Amazon RDS para SQL Server de OFFLINE a ONLINE
- Uso de la captura de datos de cambios de Amazon RDS para SQL Server
- Uso del Agente SQL Server para Amazon RDS
- Uso de registros de Amazon RDS para Microsoft SQL Server
- Uso de archivos de seguimiento y volcado de Amazon RDS para SQL Server

Acceso a la base de datos tempdb de las instancias de bases de datos de Microsoft SQL Server en Amazon RDS

Es posible acceder a la base de datos `tempdb` de las instancias de bases de datos de Microsoft SQL Server en Amazon RDS. También es posible ejecutar código en `tempdb` mediante Transact-SQL a través de Microsoft SQL Server Management Studio (SSMS) o cualquier otra aplicación cliente estándar de SQL. Para obtener más información acerca de cómo conectarse a la instancia de base de datos, consulte Conexión a la instancia de base de datos de Microsoft SQL Server.

Al usuario principal de la instancia de base de datos se le concede el acceso `CONTROL` a `tempdb` para que pueda modificar las opciones de la base de datos `tempdb`. El usuario principal no es el propietario de la base de datos `tempdb`. Si es necesario, el usuario principal puede conceder el acceso `CONTROL` a otros usuarios para que también puedan modificar las opciones de la base de datos `tempdb`.

> **Note**
>
> No es posible ejecutar comandos de consola de base de datos (DBCC) en la base de datos `tempdb`.

Modificación de las opciones de la base de datos tempdb

Es posible modificar las opciones de la base de datos `tempdb` de las instancias de bases de datos de Amazon RDS. Para obtener más información acerca de las opciones que se pueden modificar, consulte Base de datos tempdb en la documentación de Microsoft.

Las opciones de base de datos como las opciones de tamaño máximo de archivo son persistentes después de reiniciar la instancia de base de datos. Es posible modificar las opciones de base de datos para optimizar el desempeño al importar datos y para evitar que se quede sin almacenamiento.

Optimización del rendimiento al importar datos

Para optimizar el desempeño al importar grandes cantidades de datos en la instancia de base de datos, asigne valores grandes a las propiedades `SIZE` y `FILEGROWTH` de la base de datos tempdb. Para obtener más información acerca de cómo optimizar `tempdb`, consulte Optimizar el rendimiento de tempdb en la documentación de Microsoft.

En el siguiente ejemplo se muestra cómo configurar un tamaño de 100 GB y un crecimiento de archivo del 10 por ciento.

```
alter database[tempdb] modify file (NAME = N'templog', SIZE=100GB, FILEGROWTH = 10%)
```

Cómo evitar problemas de almacenamiento

Para evitar que la base de datos `tempdb` utilice todo el espacio en disco disponible, establezca la propiedad `MAXSIZE`. En el siguiente ejemplo se muestra cómo establecer la propiedad en 2048 MB.

```
alter database [tempdb] modify file (NAME = N'templog', MAXSIZE = 2048MB)
```

Reducción del tamaño de la base de datos tempdb

Hay dos maneras de reducir el tamaño de la base de datos `tempdb` de una instancia de base de datos de Amazon RDS. Es posible utilizar el procedimiento `rds_shrink_tempdbfile` o bien establecer la propiedad `SIZE`.

Uso del procedimiento rds_shrink_tempdbfile

Puede utilizar el procedimiento `msdb.dbo.rds_shrink_tempdbfile` de Amazon RDS para reducir el tamaño de la base de datos `tempdb`. Solo se puede llamar a `rds_shrink_tempdbfile` si se tiene el acceso `CONTROL` a `tempdb`. Cuando se llama a `rds_shrink_tempdbfile`, no se produce tiempo de inactividad en la instancia de base de datos.

El procedimiento `rds_shrink_tempdbfile` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`@temp_filename`	SYSNAME	—	obligatorio	El nombre lógico del archivo cuyo tamaño se va a reducir.
`@target_size`	int	nulo	opcional	El tamaño nuevo del archivo, en megabytes.

En el siguiente ejemplo se obtienen los nombres de los archivos de la base de datos `tempdb`.

```
use tempdb;
GO

select name, * from sys.sysfiles;
GO
```

En el siguiente ejemplo se reduce el tamaño de un archivo de base de datos `tempdb` denominado `test_file` y se solicita un tamaño nuevo de megabytes `10`:

```
exec msdb.dbo.rds_shrink_tempdbfile @temp_filename = N'test_file', @target_size = 10;
```

Configuración de la propiedad SIZE

También es posible reducir el tamaño de la base de datos `tempdb` estableciendo la propiedad `SIZE` y reiniciando la instancia de base de datos. Para obtener más información acerca de cómo reiniciar una instancia de base de datos, consulte Reinicio de una instancia de base de datos.

En el siguiente ejemplo se muestra cómo establecer la propiedad `SIZE` en 1024 MB.

```
alter database [tempdb] modify file (NAME = N'templog', SIZE = 1024MB)
```

Configuración de TempDB para implementaciones multi-AZ

Si la instancia de base de datos de RDS para SQL Server está en una implementación multi-AZ mediante creación de reflejos de base de datos (DBM) o grupos de disponibilidad AlwaysOn (AG), tenga en cuenta lo siguiente al utilizar la base de datos `tempdb`.

No puede replicar datos de `tempdb` de la instancia de base de datos principal a la instancia de base de datos secundaria. Si realiza una conmutación por error a una instancia de base de datos secundaria, `tempdb` en esa instancia de base de datos secundaria estará vacía.

Puede sincronizar la configuración de las opciones de la base de datos `tempdb`, incluidos el tamaño de los archivos y la configuración de crecimiento automático, desde la instancia de base de datos principal a la instancia de base de datos secundaria. Todas las versiones de RDS para SQL Server admiten la sincronización de la configuración de `tempDB`. Puede activar la sincronización automática de la configuración de `tempdb` mediante el siguiente procedimiento almacenado:

```
EXECUTE msdb.dbo.rds_set_system_database_sync_objects @object_types = 'TempDbFile';
```

> **Important**
>
> Antes de utilizar el procedimiento almacenado `rds_set_system_database_sync_objects`, asegúrese de haber establecido la configuración preferida de `tempdb` en la instancia de base de datos principal, en lugar de en la instancia de base de datos secundaria. Si realizó el cambio de configuración en su instancia de base de datos secundaria, su configuración preferida de `tempdb` podría eliminarse al activar la sincronización automática.

Puede utilizar la siguiente función para confirmar si la sincronización automática de la configuración de `tempdb` está activada:

```
SELECT * from msdb.dbo.rds_fn_get_system_database_sync_objects();
```

Cuando se active la sincronización automática de la configuración de `tempdb`, se devolverá un valor para el campo `object_class`. Cuando está desactivada, no se devuelve ningún valor.

Puede utilizar la siguiente función para saber cuál fue la última vez que se sincronizaron los objetos, en hora UTC:

```
SELECT * from msdb.dbo.rds_fn_server_object_last_sync_time();
```

Por ejemplo, si modificó la configuración de `tempdb` a la 1:00 y, a continuación, ejecutó la función `rds_fn_server_object_last_sync_time`, el valor devuelto para `last_sync_time` debería ser posterior a la 1:00, lo que indica que se ha producido una sincronización automática.

Si también utiliza la replicación de trabajos del agente de SQL Server, puede habilitar la replicación tanto para los trabajos del agente de SQL como para la configuración de `tempdb`. Para ello, proporciónelos en el parámetro `@object_type`:

```
EXECUTE msdb.dbo.rds_set_system_database_sync_objects @object_types =
 'SQLAgentJob,TempDbFile';
```

Para obtener más información acerca de la replicación de trabajos del agente de SQL Server, consulte Activación de la replicación de trabajos del agente de SQL Server.

Como alternativa a utilizar el procedimiento almacenado `rds_set_system_database_sync_objects` para garantizar que los cambios de configuración de `tempdb` se sincronicen automáticamente, puede utilizar uno de los siguientes métodos manuales:

> **Note**
>
> Recomendamos activar la sincronización automática de la configuración de `tempdb` mediante el procedimiento almacenado `rds_set_system_database_sync_objects`. El uso de la sincronización automática evita la necesidad de realizar estas tareas manuales cada vez que se cambia la configuración de `tempdb`.

- En primer lugar, modifique la instancia de base de datos y desactive el despliegue Multi-AZ, a continuación, modifique tempdb y, por último, vuelva a activar el despliegue Multi-AZ. Este método no provoca ningún tiempo de inactividad.

  Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
- En primer lugar, modifique `tempdb` en la instancia principal original, a continuación, realice una conmutación por error manualmente y, por último, modifique `tempdb` en la nueva instancia principal. Este método provoca un tiempo de inactividad.

  Para obtener más información, consulte Reinicio de una instancia de base de datos.

Análisis de la carga de trabajo de una base de datos de una instancia de base de datos de Amazon RDS for SQL Server con el Asistente para la optimización del motor de base de datos

El Asistente para la optimización del motor de base de datos es una aplicación cliente proporcionada por Microsoft que analiza la carga de trabajo de la base de datos y recomienda un conjunto de índices óptimo para las bases de datos de Microsoft SQL Server en función de los tipos de consultas que se ejecutan. Al igual que SQL Server Management Studio, el Asistente para la optimización se ejecuta desde un equipo conectado a la instancia de base de datos de Amazon RDS que ejecuta SQL Server. El equipo cliente puede ser un equipo local que ejecuta localmente en su propia red o una instancia de Amazon EC2 Windows que se ejecuta en la misma región que la instancia de base de datos de Amazon RDS.

Esta sección muestra cómo capturar una carga de trabajo para que la analice el Asistente para la optimización. Este es el proceso preferido para capturar una carga de trabajo, ya que Amazon RDS restringe el acceso de host a la instancia de SQL Server. Para obtener más información, consulte el Asesor de ajuste del motor de base de datos en la documentación de Microsoft.

Para usar el Asistente para la optimización, debe proporcionar al asistente lo que se denomina una carga de trabajo. Una carga de trabajo es un conjunto de instrucciones Transact-SQL que se ejecutan en una o varias bases de datos que se desea optimizar. El Asistente para la optimización del motor de base de datos usa archivos de seguimiento, tablas de seguimiento, scripts de Transact-SQL o archivos XML como entradas de carga de trabajo al ajustar las bases de datos. Cuando se trabaja con Amazon RDS, una carga de trabajo puede ser un archivo en un equipo cliente o una tabla una base de datos Amazon RDS for SQL Server a la que su equipo cliente pueda obtener acceso. El archivo o la tabla deben contener consultas para las bases de datos que se desea ajustar en un formato adecuado para la repetición.

Para que el Asistente para la optimización sea más eficaz, una carga de trabajo debe ser lo más realista posible. Puede generar un archivo o una tabla de carga de trabajo realizando un seguimiento en su instancia de base de datos. Mientras se ejecuta un seguimiento, puede simular una carga en su instancia de base de datos o ejecutar sus aplicaciones con una carga normal.

Hay dos tipos de seguimientos: del lado del cliente y del lado del servidor. Un seguimiento del lado del cliente es más fácil de configurar y permite ver los eventos de seguimiento mientras se capturan en tiempo real en SQL Server Profiler. Un seguimiento del lado del servidor es más difícil de configurar y requiere scripting de Transact-SQL. Además, como el seguimiento se escribe en un archivo en la instancia de base de datos de Amazon RDS, consume espacio de almacenamiento. Es importante realizar un seguimiento del espacio de almacenamiento que usa un seguimiento del lado del servidor en ejecución, ya que la instancia de base de datos podría llegar a un estado de almacenamiento lleno y dejar de estar disponible si se queda sin espacio de almacenamiento.

Para un seguimiento del lado del cliente, cuando se ha capturado la cantidad necesaria de datos de seguimiento en SQL Server Profiler, puede generar el archivo de carga de trabajo guardando el seguimiento en un archivo del equipo local o en una tabla de base de datos de una instancia de base de datos que esté disponible en el equipo cliente. La principal desventaja de usar un seguimiento del lado del cliente es que el seguimiento podría no capturar todas las consultas si la carga es elevada. Esto podría reducir la eficacia del análisis realizado por el Asistente para la optimización del motor de base de datos. Si necesita ejecutar un seguimiento con una carga elevada y quiere asegurarse de que captura todas las consultas que se producen durante una sesión de seguimiento, debe usar un seguimiento del lado del servidor.

Para un seguimiento del lado del servidor, debe convertir los archivos de seguimiento de la instancia de base de datos en un archivo de carga de trabajo adecuado o puede guardar el seguimiento en una tabla de la instancia de base de datos una vez que se complete el seguimiento. Puede usar SQL Server Profiler para guardar el seguimiento en un archivo de su equipo local o hacer que el Asistente para la optimización lea de la tabla de seguimiento de la instancia de base de datos.

Ejecución de un seguimiento del lado del cliente en una instancia de base de datos de SQL Server

Para ejecutar un seguimiento del lado del cliente en una instancia de base de SQL Server

1. Inicie SQL Server Profiler. Está instalado en la carpeta Performance Tools de la carpeta de la instancia de SQL Server. Debe cargar o definir una plantilla de definición de seguimiento para iniciar un seguimiento del lado del cliente.
2. En el menú Archivo de SQL Server Profiler, elija New Trace (Nuevo seguimiento). En el cuadro de diálogo Conectar con el servidor, escriba el punto de enlace de la instancia de base de datos, el puerto, el nombre del usuario maestro y la contraseña de la base de datos en la que desea ejecutar un seguimiento.
3. En el cuadro de diálogo Propiedades de seguimiento, escriba un nombre de seguimiento y elija una plantilla de definición de seguimiento. Con la aplicación se suministra una plantilla predeterminada, TSQL_Replay. Puede editar esta plantilla para definir el seguimiento. Edite los eventos y la información de eventos en la pestaña Selección de eventos del cuadro de diálogo Propiedades de seguimiento.

   Para obtener más información acerca de las plantillas de definición de seguimiento y acerca del uso de SQL Server Profiler para especificar un seguimiento del lado del cliente, consulte Asesor de ajuste del motor de baseen la documentación de Microsoft.
4. Inicie el seguimiento del lado del cliente y vea las consultas de SQL en tiempo real mientras se ejecutan en la instancia de base de datos.
5. Seleccione Stop Trace (Detener seguimiento) en el menú File (Archivo) cuando haya completado el seguimiento. Guarde los resultados como un archivo o como una tabla de seguimiento en su instancia de base de datos.

Ejecución de un seguimiento del lado del servidor en una instancia de base de datos de SQL Server

Escribir scripts para crear un seguimiento del lado del servidor puede ser complicado y está fuera del alcance de este documento. Esta sección contiene scripts de muestra que se pueden usar como ejemplos. Al igual que en el seguimiento del lado del cliente, el objetivo es crear un archivo de carga de trabajo o una tabla de seguimiento que se puede abrir con el Asistente para la optimización del motor de base de datos.

A continuación se muestra un script de ejemplo abreviado que inicia un seguimiento del lado del servidor y captura detalles en un archivo de carga de trabajo. El seguimiento se guarda inicialmente en el archivo RDSTrace.trc del directorio D:\RDSDBDATA\Log y cambia cada 100 MB, de modo que los archivos de seguimiento posteriores se llaman RDSTrace_1.trc, RDSTrace_2.trc, etc.

```
DECLARE @file_name NVARCHAR(245) = 'D:\RDSDBDATA\Log\RDSTrace';
DECLARE @max_file_size BIGINT = 100;
DECLARE @on BIT = 1
DECLARE @rc INT
DECLARE @traceid INT

EXEC @rc = sp_trace_create @traceid OUTPUT, 2, @file_name, @max_file_size
IF (@rc = 0) BEGIN
   EXEC sp_trace_setevent @traceid, 10, 1, @on
   EXEC sp_trace_setevent @traceid, 10, 2, @on
   EXEC sp_trace_setevent @traceid, 10, 3, @on
 . . .
   EXEC sp_trace_setfilter @traceid, 10, 0, 7, N'SQL Profiler'
   EXEC sp_trace_setstatus @traceid, 1
   END
```

En el siguiente ejemplo se muestra un script que detiene un seguimiento. Un seguimiento creado por el script anterior sigue en ejecución hasta que el seguimiento se detiene expresamente o el proceso se queda sin espacio en el disco.

```
DECLARE @traceid INT
SELECT @traceid = traceid FROM ::fn_trace_getinfo(default)
WHERE property = 5 AND value = 1 AND traceid <> 1

IF @traceid IS NOT NULL BEGIN
   EXEC sp_trace_setstatus @traceid, 0
   EXEC sp_trace_setstatus @traceid, 2
```

```
END
```

Puede guardar los resultados del seguimiento del lado del servidor en una tabla de base de datos y usar dicha tabla como carga de trabajo en el Asistente para la optimización por medio de la función fn_trace_gettable. Los siguientes comandos cargan los resultados de todos los archivos con el nombre RDSTrace.trc en el directorio D:\rdsdbdata\Log, incluidos todos los archivos de sustitución incremental, como RDSTrace_1.trc, en una tabla llamada RDSTrace en la base de datos actual.

```
SELECT * INTO RDSTrace
FROM fn_trace_gettable('D:\rdsdbdata\Log\RDSTrace.trc', default);
```

Para guardar un archivo de sustitución incremental en una tabla, por ejemplo el archivo RDSTrace_1.trc, especifique el nombre del archivo de sustitución incremental y cambie por 1 el valor predeterminado del último parámetro de fn_trace_gettable.

```
SELECT * INTO RDSTrace_1
FROM fn_trace_gettable('D:\rdsdbdata\Log\RDSTrace_1.trc', 1);
```

Ejecución del Asistente para la optimización con un seguimiento

Una vez que se crea un seguimiento, como archivo local o como tabla de base de datos, se puede ejecutar el Asistente para la optimización en una instancia de base de datos. Usar el Asistente para la optimización con Amazon RDS es el mismo proceso que trabajar con una instancia de SQL Server independiente y remota. Puede usar la interfaz de usuario del Asistente para la optimización de su equipo cliente o usar la utilidad dta.exe desde la línea de comando. En ambos casos, debe conectar con la instancia de base de datos de Amazon RDS a través del punto de enlace de la instancia de base de datos y proporcionar su nombre de usuario maestro y su contraseña de usuario maestra cuando utilice el Asistente para la optimización.

El siguiente ejemplo de código demuestra el uso de la utilidad de línea de comando dta.exe con una instancia de base de datos de Amazon RDS con un punto de enlace de **`dta.cnazcmklsdei.us-east-1.rds.amazonaws.com`**. El ejemplo incluye el nombre de usuario maestro **`admin`** y la contraseña **`test`**de usuario maestro; la base de datos de ejemplo que se va a ajustar se denomina máquina denominada **`C:\RDSTrace.trc`**. El código de ejemplo de la línea de comando especifica también una sesión de seguimiento llamada **`RDSTrace1`** y archivos de salida en el equipo local con los nombres **`RDSTrace.sql`** para el script de salida de SQL, **`RDSTrace.txt`** para un archivo de resultado y **`RDSTrace.xml`** para un archivo XML del análisis. También se especifica en la base de datos RDSDTA una tabla de errores denominada **`RDSTraceErrors`**.

```
dta -S dta.cnazcmklsdei.us-east-1.rds.amazonaws.com -U admin -P test -D RDSDTA -
if C:\RDSTrace.trc -s RDSTrace1 -of C:\ RDSTrace.sql -or C:\ RDSTrace.txt -ox C:\
 RDSTrace.xml -e RDSDTA.dbo.RDSTraceErrors
```

A continuación se muestra el mismo código de línea de comando de ejemplo, salvo en que la carga de trabajo de entrada es una tabla en la instancia de Amazon RDS remota llamada **`RDSTrace`** que está en la base de datos **`RDSDTA`**.

```
dta -S dta.cnazcmklsdei.us-east-1.rds.amazonaws.com -U admin -P test -D RDSDTA -it
 RDSDTA.dbo.RDSTrace -s RDSTrace1 -of C:\ RDSTrace.sql -or C:\ RDSTrace.txt -ox C:\
 RDSTrace.xml -e RDSDTA.dbo.RDSTraceErrors
```

Para obtener una lista completa de los parámetros de línea de comandos de la utilidad dta, consulte Utilidad dta en la documentación de Microsoft.

Cambio del **`db_owner`** a la cuenta de **`rdsa`** de la base de datos de Amazon RDS para SQL Server

Al crear o restaurar una base de datos en una instancia de base de datos de RDS para SQL Server, Amazon RDS establece el propietario de la base de datos en `rdsa`. Si tiene una implementación multi-AZ mediante SQL Server Database Mirroring (DBM) o los grupos de disponibilidad (AG), Amazon RDS establece el propietario de la base de datos en la instancia de base de datos secundaria en `NT AUTHORITY\SYSTEM`. El propietario de la base de datos secundaria no se puede cambiar hasta que la instancia de base de datos secundaria pase al rol principal. En la mayoría de los casos, establecer el propietario de la base de datos en `NT AUTHORITY\SYSTEM` no supone ningún problema al ejecutar consultas; sin embargo, puede provocar errores al ejecutar procedimientos almacenados del sistema, como `sys.sp_updatestats`, que requiere permisos elevados para ejecutarse.

Puede utilizar la siguiente consulta para identificar al propietario de las bases de datos de`NT AUTHORITY\SYSTEM`:

```
SELECT name FROM sys.databases WHERE SUSER_SNAME(owner_sid) = 'NT AUTHORITY\SYSTEM';
```

Puede utilizar el procedimiento almacenado de Amazon RDS `rds_changedbowner_to_rdsa` para cambiar el propietario de la base de datos a `rdsa`. No se permite el uso de las siguientes bases de datos con `rds_changedbowner_to_rdsa`: `master, model, msdb, rdsadmin, rdsadmin_ReportServer, rdsadmin_ReportServerTempDB, SSISDB`.

Para cambiar el propietario de la base de datos a `rdsa`, llame al procedimiento almacenado `rds_changedbowner_to_rdsa` y proporcione el nombre de la base de datos.

Example de uso:

```
exec msdb.dbo.rds_changedbowner_to_rdsa 'TestDB1';
```

El siguiente parámetro es obligatorio:

- `@db_name`: el nombre de la base de datos a la que se va a cambiar el propietario de la base de datos por `rdsa`.

> **Important**
>
> No se puede utilizar `rds_changedbowner_to_rdsa` para cambiar la propiedad de una base de datos a un inicio de sesión que no sea `rdsa`. Por ejemplo, no puede cambiar la propiedad del inicio de sesión con el que creó la base de datos. Para restablecer la pertenencia perdida en el rol `db_owner` para el usuario maestro cuando no se pueda utilizar ningún otro usuario de la base de datos para concederla, restablezca la contraseña del usuario maestro para obtener la pertenencia en el rol `db_owner`. Para obtener más información, consulte Restablecimiento de la pertenencia al rol db_owner para el usuario maestro de Amazon RDS para SQL Server.

Administración de intercalaciones y conjuntos de caracteres de Amazon RDS para Microsoft SQL Server

En este tema se proporciona orientación sobre cómo administrar intercalaciones y conjuntos de caracteres para Microsoft SQL Server en Amazon RDS. En él se explica cómo configurar las intercalaciones durante la creación de una base de datos y cómo modificarlas posteriormente, lo que garantiza una gestión adecuada de los datos de texto en función de los requisitos de idioma y configuración regional. Además, describe las prácticas recomendadas para mantener la compatibilidad y el rendimiento en los entornos de SQL Server en Amazon RDS.

SQL Server admite intercalaciones en varios niveles. Tiene que establecer la intercalación de servidor predeterminada al crear una instancia de base de datos. Puede anular la intercalación en el nivel de columna, tabla o base de datos.

Temas

- Intercalación de nivel de servidor para Microsoft SQL Server
- Intercalación de nivel de base de datos para Microsoft SQL Server

Intercalación de nivel de servidor para Microsoft SQL Server

Al crear una instancia de base de datos de Microsoft SQL Server, puede establecer la intercalación de servidor que desee utilizar. Si no selecciona una intercalación diferente, la intercalación de nivel de servidor predeterminada es SQL_Latin1_General_CP1_CI_AS. La intercalación de servidor se aplica por defecto a todas las bases de datos y los objetos de base de datos.

> **Note**
>
> No puede cambiar la intercalación al restaurar desde una instantánea de base de datos.

Actualmente, Amazon RDS admite las siguientes intercalaciones de servidor:

Collation (Intercalación)	Descripción
Arabic_CI_AS	Árabe, no distingue entre mayúsculas y minúsculas, no distingue acentos, tipos de kana ni anchura
Chinese_PRC_BIN2	Chinese-PRC, orden de clasificación de puntos de código binario
Chinese_PRC_CI_AS	Chino de RPC, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Chinese_Taiwan_Stroke_CI_AS	Chino de Taiwán (trazos), distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Danish_Norwegian_CI_AS	Danés-noruego, no distingue entre mayúscula s y minúsculas, distingue acentos, no distingue tipos de kana ni anchura

Collation (Intercalación)	Descripción
Danish_Norwegian_CI_AS_KS	Danés-noruego, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura
Danish_Norwegian_CI_AS_KS_WS	Danés-noruego, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura
Danish_Norwegian_CI_AS_WS	Danés-noruego, no distingue entre mayúscula s y minúsculas, distingue acentos, no distingue tipos de kana, distingue anchura
Danish_Norwegian_CS_AI	Danés-noruego, distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Danish_Norwegian_CS_AI_KS	Danés-noruego, distingue entre mayúsculas y minúsculas, no distingue acentos, distingue tipos de kana, no distingue anchura
Finnish_Swedish_100_BIN	Finnish-Swedish-100, orden binario
Finnish_Swedish_100_BIN2	Finnish-Swedish-100, orden por comparación de puntos de código binario
Finnish_Swedish_100_CI_AI	Finnish-Swedish-100, no distingue entre mayúsculas y minúsculas, no distingue acentos, no distingue tipos de kana, no distingue anchura
Finnish_Swedish_100_CI_AS	Finnish-Swedish-100, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura

Collation (Intercalación)	Descripción
Finnish_Swedish_CI_AS	Finlandés, sueco y sueco (Finlandia), no distingue entre mayúsculas y minúsculas, acentos, tipos de kana ni anchura
French_CI_AS	Francés, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Hebrew_BIN	Hebreo, orden binario
Hebrew_CI_AS	Hebreo, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Japanese_BIN	Japonés, clasificación binaria
Japanese_CI_AS	Japonés, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Japanese_CS_AS	Japonés, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Japanese_XJIS_140_CI_AS	Japonés, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caracteres suplementarios, no distingue selectores de variación
Japanese_XJIS_140_CI_AS_KS_VSS	Japonés, no distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, no distingue anchura, caracteres suplementarios, no distingue selectores de variaciones

Collation (Intercalación)	Descripción
Japanese_XJIS_140_CI_AS_VSS	Japonés, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura, caractere s suplementarios, no distingue selectores de variaciones
Japanese_XJIS_140_CS_AS_KS_WS	Japonés, distingue entre mayúsculas y minúsculas, distingue acentos, distingue tipos de kana, distingue anchura, caractere s suplementarios, no distingue selectores de variaciones
Korean_Wansung_CI_AS	Coreano (Wansung), distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_100_BIN	Latin1-General-100, orden binario
Latin1_General_100_BIN2	Latin1-General-100, orden de clasificación de puntos de código binario
Latin1_General_100_BIN2_UTF8	Latin1-General-100, orden de clasificación de puntos de código binario, cifrado UTF-8
Latin1_General_100_CI_AS	Latin1 general 100, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_100_CI_AS_SC_UTF8	Latin1-General-100, distingue acentos y no distingue entre mayúsculas y minúsculas, caracteres adicionales, cifrado UTF-8
Latin1_General_BIN	Latín 1 general, orden binario
Latin1_General_BIN2	Latin1-General-100, orden de clasificación de puntos de código binario

Collation (Intercalación)	Descripción
Latin1_General_CI_AI	Latín 1 general, no distingue entre mayúsculas y minúsculas, acentos, tipos de kana ni anchura
Latin1_General_CI_AS	Latín 1 general, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_CI_AS_KS	Latín1-General, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Latin1_General_CS_AS	Latín 1 general, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana ni anchura
Modern_Spanish_CI_AS	Español moderno, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura
Polish_CI_AS	Polaco, no distingue entre mayúsculas y minúsculas, no distingue acentos, tipos de kana ni anchura
SQL_1xCompat_CP850_CI_AS	Latín1-General, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 49 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_CP1_CI_AI	Latín 1 general, no distingue entre mayúsculas y minúsculas, acentos, tipos de kana ni anchura para datos Unicode; orden de clasificación 54 de SQL Server en la página de códigos 1252 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP1_CI_AS (predeter minado)	Latín 1 general, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 52 de SQL Server en la página de códigos 1252 para datos que no son Unicode
SQL_Latin1_General_CP1_CS_AS	Latín 1 general, distingue acentos y entre mayúsculas y minúsculas y no distingue tipos de kana ni anchura para datos Unicode; orden de clasificación 51 de SQL Server en la página de códigos 1252 para datos que no son Unicode
SQL_Latin1_General_CP437_CI_AI	Latín 1 general, no distingue entre mayúscula s y minúsculas, acentos, tipos de kana ni anchura para datos Unicode; orden de clasifica ción 34 de SQL Server en la página de códigos 437 para datos que no son Unicode
SQL_Latin1_General_CP850_BIN	Latin1-General, orden de clasificación binario para datos Unicode, orden de clasificación de SQL Server 40 en la página de códigos 850 para datos no Unicode
SQL_Latin1_General_CP850_BIN2	Latin1-General, orden de clasificación de puntos de código binario para datos Unicode, orden de clasificación de SQL Server 40 en la página de códigos 850 para datos no Unicode
SQL_Latin1_General_CP850_CI_AI	Latín 1 general, no distingue entre mayúscula s y minúsculas, acentos, tipos de kana ni anchura para datos Unicode; orden de clasifica ción 44 de SQL Server en la página de códigos 850 para datos que no son Unicode

Collation (Intercalación)	Descripción
SQL_Latin1_General_CP850_CI_AS	Latín 1 general, distingue acentos y no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 42 de SQL Server en la página de códigos 850 para datos que no son Unicode
SQL_Latin1_General_CP1256_CI_AS	Latín1-General, distingue acentos; no distingue entre mayúsculas y minúsculas, tipos de kana ni anchura para datos Unicode; orden de clasificación 146 de SQL Server en la página de códigos 1256 para datos que no son Unicode
SQL_Latin1_General_CP1255_CS_AS	Latin1-General, distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana, no distingue anchura para datos Unicode; orden de clasificación 137 de SQL Server en la página de códigos 1255 para datos que no son Unicode
Thai_CI_AS	Tailandés, no distingue entre mayúsculas y minúsculas, no distingue acentos, tipos de kana ni anchura
Turkish_CI_AS	Turco, no distingue entre mayúsculas y minúsculas, no distingue acentos, tipos de kana ni anchura

Para elegir la intercalación:

- Si utiliza la consola de Amazon RDS, al crear una nueva instancia de base de datos elija Additional configuration (Configuración adicional) y, a continuación, introduzca la intercalación en el campo Collation (Intercalación). Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

- Si está utilizando la AWS CLI, utilice la opción `--character-set-name` con el comando `create-db-instance`. Para obtener más información, consulte create-db-instance.
- Si está utilizando la API de Amazon RDS, utilice el parámetro `CharacterSetName` con la operación `CreateDBInstance`. Para obtener más información, consulte CreateDBInstance.

Intercalación de nivel de base de datos para Microsoft SQL Server

Puede cambiar la intercalación predeterminada en el nivel de la base de datos, la tabla o la columna reemplazando la intercalación cuando se crea una nueva base de datos o un objeto de base de datos. Por ejemplo, si la intercalación de servidor predeterminada es SQL_Latin1_General_CP1_CI_AS, puede cambiarla a Mohawk_100_CI_AS para que admita la intercalación de Mohawk. Incluso los argumentos de una consulta se pueden convertir para usar una intercalación diferente si es necesario.

Por ejemplo, la siguiente consulta cambiaría la intercalación predeterminada de la columna AccountName a Mohawk_100_CI_AS

```
CREATE TABLE [dbo].[Account]
 (
     [AccountID] [nvarchar](10) NOT NULL,
     [AccountName] [nvarchar](100) COLLATE Mohawk_100_CI_AS NOT NULL
 ) ON [PRIMARY];
```

El motor de base de datos de Microsoft SQL Server admite Unicode mediante los tipos de datos integrados NCHAR, NVARCHAR y NTEXT. Por ejemplo, si necesita compatibilidad con CJK, use estos tipos de datos de Unicode para el almacenamiento de caracteres y anule la intercalación de servidor predeterminada al crear las bases de datos y tablas. En los siguientes enlaces de Microsoft se tratan la compatibilidad con Unicode y la intercalación para SQL Server:

- Working with Collations
- Collation and International Terminology
- Using SQL Server Collations
- International Considerations for Databases and Database Engine Applications

Creación de un usuario de base de datos de Amazon RDS para SQL Server

Para crear un usuario de base de datos para su instancia de base de datos de Amazon RDS for Microsoft SQL Server, ejecute un script de T-SQL como el ejemplo siguiente. Utilice una aplicación como SQL Server Management Suite (SSMS). Inicie sesión en la instancia de base de datos como el usuario maestro que se creó cuando creó la instancia de base de datos.

```
--Initially set context to master database
USE [master];
GO
--Create a server-level login named theirname with password theirpassword
CREATE LOGIN [theirname] WITH PASSWORD = 'theirpassword';
GO
--Set context to msdb database
USE [msdb];
GO
--Create a database user named theirname and link it to server-level login theirname
CREATE USER [theirname] FOR LOGIN [theirname];
GO
```

Para ver un ejemplo de cómo agregar un usuario de base de datos a un rol, consulte Agregar un usuario al rol SQLAgentUser.

> **Note**
>
> Si obtiene errores de permiso al agregar un usuario, puede restaurar los privilegios modificando la contraseña para el usuario maestro de la instancia de base de datos. Para obtener más información, consulte Restablecimiento de la pertenencia al rol db_owner para el usuario maestro de Amazon RDS para SQL Server.
>
> No se recomienda clonar los permisos de usuario principal en las aplicaciones. Para obtener más información, consulte Cómo clonar los permisos del usuario principal en Amazon RDS para SQL Server.

Determinación de un modelo de recuperación para una base de datos de Amazon RDS para SQL Server

En Amazon RDS, el modelo de recuperación, el periodo de retención y el estado de las bases de datos están vinculados.

Es importante comprender las consecuencias antes de realizar un cambio en uno de estos ajustes. Un ajuste puede afectar a los demás. Por ejemplo:

- Si cambia el modelo de recuperación de la base de datos a SIMPLE o BULK_LOGGED mientras la retención de copia de seguridad está habilitada, Amazon RDS restablece el modelo de recuperación a FULL en cinco minutos. Esto también da como resultado que RDS tome una instantánea de la instancia de base de datos.
- Si establece la retención de copias de seguridad en `0` días, RDS establece el modo de recuperación en SIMPLE.
- Si cambia el modelo de recuperación de la base de datos de SIMPLE a cualquier otra opción mientras la retención de copias de seguridad está establecida en `0` días, RDS restablece el modelo de recuperación en SIMPLE.

> **Important**
>
> No cambie nunca el modelo de recuperación en instancias de Multi-AZ, incluso si parece que puede hacerlo, por ejemplo, mediante ALTER DATABASE. La retención de copias de seguridad y, por lo tanto el modo de recuperación FULL, son necesarios para Multi-AZ. Si modifica el modelo de recuperación, RDS vuelve a cambiar de inmediato a FULL.
> Este restablecimiento automático fuerza a RDS a recompilar el reflejo al completo. Durante esta recompilación, la disponibilidad de la base de datos desciende durante aproximadamente 30-90 minutos hasta que el reflejo está listo para la conmutación por error. La instancia de base de datos también experimenta una degradación del rendimiento de la misma forma que lo hace durante una conversión de Single-AZ a Multi-AZ. El nivel de degradación del rendimiento depende del tamaño de almacenamiento de la base de datos: conforme más grande sea la base de datos almacenada, más prolongada será la degradación.

Para obtener más información sobre los modelos de recuperación de SQL Server, consulte Modelos de recuperación (SQL Server) en la documentación de Microsoft.

Determinación de la hora de la última conmutación por error de Amazon RDS para SQL Server

Para determinar la hora de la última conmutación por error, utilice el siguiente procedimiento almacenado:

```
execute msdb.dbo.rds_failover_time;
```

Este procedimiento devuelve la siguiente información.

Parámetro de salida	Descripción
errorlog_available_from	Muestra la hora a partir de la cual los registros de errores están disponibles en el directorio de registro.
recent_failover_time	Muestra la hora de la última conmutación por error si está disponible en los registros de errores. De lo contrario, muestra `null`.

> **Note**
>
> El procedimiento almacenado busca todos los registros de error de SQL Server disponibles en el directorio de registro para recuperar la hora de la conmutación por error más reciente. Si SQL Server sobrescribió los mensajes de conmutación por error, el procedimiento no recupera la hora de conmutación por error.

Example de No hay conmutación por error reciente

Este ejemplo muestra el resultado cuando no hay conmutación por error reciente en los registros de errores. No se ha producido ninguna conmutación por error desde 2020-04-29 23:59:00 .01.

errorlog_available_from	recent_failover_time

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	null

Example de Conmutación por error reciente

Este ejemplo muestra el resultado cuando hay una conmutación por error en los registros de errores. La conmutación por error más reciente fue en 2020-05-05 18:57:51 .89.

errorlog_available_from	recent_failover_time
2020-04-29 23:59:00.0100000	2020-05-05 18:57:51.8900000

Solución de problemas de recuperación en un momento dado debido a una brecha en el número de secuencia de registros

Al intentar una recuperación en un momento dado (PITR) en RDS para SQL Server, es posible que se produzcan errores debido a brechas en los números de secuencia de registro (LSN). Estas brechas impiden que RDS restaure la base de datos a la hora solicitada y RDS coloca la instancia de restauración en estado `incompatible-restore`.

Las causas más frecuentes para este problema son:

- Cambios manuales en el modelo de recuperación de la base de datos.
- Cambios automáticos del modelo de recuperación por parte de RDS debido a recursos insuficientes para completar las copias de seguridad del registro de transacciones.

Para identificar las brechas de LSN en la base de datos, ejecute esta consulta:

```
SELECT * FROM msdb.dbo.rds_fn_list_tlog_backup_metadata(database_name)
ORDER BY backup_file_time_utc desc;
```

Si detecta una brecha de LSN, puede:

- Elegir un punto de restauración anterior a la brecha de LSN.

- Esperar y restaurar a un punto posterior a la finalización de la siguiente copia de seguridad de la instancia.

Para evitar este problema, le recomendamos que no cambie manualmente el modelo de recuperación de las bases de datos de RDS para SQL Server, ya que interrumpe la durabilidad de la instancia. También le recomendamos que elija un tipo de instancia con recursos suficientes para la carga de trabajo a fin de garantizar copias de seguridad regulares del registro de transacciones.

Para obtener más información sobre la administración de registros de transacciones, consulte la Guía de administración y arquitectura de registros de transacciones de SQL Server en la documentación de Microsoft SQL Server.

Denegación o permiso para ver los nombres de las bases de datos de Amazon RDS para SQL Server

El usuario maestro no puede configurar `DENY VIEW ANY DATABASE TO LOGIN` para que oculte las bases de datos a un usuario.
Para cambiar este permiso, utilice en su lugar el siguiente procedimiento almacenado:

- Cómo denegar el acceso a *LOGIN* para ver la base de datos:

```
EXEC msdb.dbo.rds_manage_view_db_permission @permission='DENY',
 @server_principal='LOGIN'

go
```

- Cómo permitir el acceso a *LOGIN* para ver la base de datos:

```
EXEC msdb.dbo.rds_manage_view_db_permission @permission='GRANT',
 @server_principal='LOGIN'

go
```

Tenga en cuenta lo siguiente al usar este procedimiento almacenado:

- Los nombres de las bases de datos están ocultos en el SSMS y en el DMV interno (vistas de administración dinámica). Sin embargo, los nombres de las bases de datos siguen siendo visibles

en las tablas de auditoría, registros y metadatos. Se trata de permisos de servidor `VIEW ANY DATABASE` protegidos. Para obtener más información, consulte DENY Server Permissions.

- Una vez que el permiso se haya revertido a `GRANT` (permitido), *`LOGIN`* podrá ver todas las bases de datos.
- Si elimina y vuelve a crear *`LOGIN`*, el permiso de visualización relacionado con LOGIN se restablecerá a `ALLOW`.
- Para las instancias multi-AZ, configure el permiso `DENY` o `GRANT` solo para *`LOGIN`* en el host principal. Los cambios se propagan automáticamente al host secundario.
- Este permiso solo cambia si un login puede ver los nombres de las bases de datos. Sin embargo, el acceso a las bases de datos y a los objetos que contiene se administra por separado.

Desactivación de inserciones rápidas durante la carga masiva de Amazon RDS para SQL Server

A partir de SQL Server 2016, las inserciones rápidas están habilitadas de forma predeterminada. Las inserciones rápidas aprovechan el registro mínimo que se produce mientras la base de datos se encuentra en el modelo de recuperación de registro simple o masivo para optimizar el rendimiento de la inserción. Con las inserciones rápidas, cada lote de carga masiva adquiere nuevas extensiones, evitando la búsqueda de asignación para las extensiones existentes con espacio libre disponible para optimizar el rendimiento de la inserción.

Sin embargo, con las inserciones rápidas, las cargas masivas con tamaños de lote pequeños pueden provocar un aumento del espacio no utilizado consumido por los objetos. Si no es posible aumentar el tamaño del lote, habilitar el indicador de rastreo 692 puede ayudar a reducir el espacio reservado no utilizado, pero a expensas del rendimiento. Al habilitar este indicador de rastreo, se desactivan las inserciones rápidas mientras se cargan datos de forma masiva en el montón o en los índices agrupados en clústeres.

Habilite el indicador de rastreo 692 como parámetro de inicio mediante grupos de parámetros de base de datos. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

El indicador de rastreo 692 es compatible con Amazon RDS en SQL Server 2016 y versiones posteriores. Para obtener más información acerca de los indicadores de rastreo, consulte DBCC TRACEON: marcas de seguimiento en la documentación de Microsoft.

Eliminación de una base de datos en una instancia de base de datos de Amazon RDS para Microsoft SQL Server

Puede eliminar con drop una base de datos de una instancia de base de datos de Amazon RDS en la que se ejecuta Microsoft SQL Server en una implementación Single-AZ o Multi-AZ. Para eliminar con drop la base de datos, utilice el siguiente comando:

```
--replace your-database-name with the name of the database you want to drop
EXECUTE msdb.dbo.rds_drop_database  N'your-database-name'
```

> **Note**
>
> Use comillas simples en el comando. Las comillas inteligentes provocarán un error.

Tras emplear este procedimiento para eliminar con drop la base de datos, Amazon RDS borra todas las conexiones existentes con la base de datos y elimina el historial de copias de seguridad de la base de datos.

Para conceder permisos de copia de seguridad y restauración a otros usuarios, siga este procedimiento:

```
USE master
GO
CREATE LOGIN user1 WITH PASSWORD=N'changeThis', DEFAULT_DATABASE=master,
 CHECK_EXPIRATION=OFF, CHECK_POLICY=OFF
GO
USE msdb
GO
CREATE USER user1 FOR LOGIN user1
GO
use msdb
GO
GRANT EXECUTE ON msdb.dbo.rds_backup_database TO user1
GO
GRANT EXECUTE ON msdb.dbo.rds_restore_database TO user1
GO
```

Cambio del nombre de una base de datos de Amazon RDS para Microsoft SQL Server en una implementación multi-AZ

Para cambiar el nombre de instancia de base de datos de Microsoft SQL Server que usa Multi-AZ, utilice este procedimiento:

1. En primer lugar, desactive Multi-AZ para la instancia de base de datos.
2. Cambie el nombre de la base de datos ejecutando `rdsadmin.dbo.rds_modify_db_name`.
3. Después, active la creación de reflejo o grupos de disponibilidad Always On de Multi-AZ para la instancia de base de datos, para devolverla a su estado original.

Para obtener más información, consulte Adición de implementaciones Multi-AZ a una instancia de base de datos de Microsoft SQL Server.

> **Note**
>
> Si la instancia no usa Multi-AZ, no es necesario cambiar ninguna configuración antes ni después de ejecutar `rdsadmin.dbo.rds_modify_db_name`.
> No puede cambiar el nombre de una base de datos en una instancia de origen de réplica de lectura.

Ejemplo: En el ejemplo siguiente, el procedimiento almacenado `rdsadmin.dbo.rds_modify_db_name` cambia el nombre de una base de datos de **`MOO`** a **`ZAR`**. Esto es similar a ejecutar la instrucción `DDL ALTER DATABASE [MOO] MODIFY NAME = [ZAR]`.

```
EXEC rdsadmin.dbo.rds_modify_db_name N'MOO', N'ZAR'
GO
```

Restablecimiento de la pertenencia al rol db_owner para el usuario maestro de Amazon RDS para SQL Server

Si bloquea a su usuario maestro de la pertenencia al rol `db_owner` en su base de datos de RDS para SQL Server y ningún otro usuario de la base de datos puede concederle la pertenencia, puede restaurar la pertenencia perdida modificando la contraseña del usuario maestro de la instancia de base de datos.

Al cambiar la contraseña del usuario maestro de la instancia de base de datos, RDS concede la pertenencia de `db_owner` a las bases de datos en la instancia de base de datos que podrían haberse revocado accidentalmente. La contraseña de la instancia de base de datos se puede cambiar por medio de la consola de Amazon RDS, el comando modify-db-instance de la AWS CLI o la operación de la API ModifyDBInstance. Para obtener más información acerca de la modificación de una instancia de base de datos de , consulte Modificación de una instancia de base de datos de Amazon RDS.

Restauración de instancias de base de datos con licencia caducada de Amazon RDS para SQL Server

Microsoft ha solicitado que algunos clientes de Amazon RDS que no notificaron su información de Microsoft License Mobility terminen su instancia de base de datos. Amazon RDS crea instantáneas de estas instancias de base de datos,y usted puede restaurar a partir de la instantánea a una nueva instancia de base de datos que tiene el modelo de licencia incluida.

Puede restaurar a partir de una instantánea de Standard Edition a Standard Edition o Enterprise Edition.

Puede restaurar a partir de una instantánea de Enterprise Edition a Standard Edition o Enterprise Edition.

Para restaurar desde una instantánea de SQL Server después de que Amazon RDS haya creado una instantánea final de su instancia:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea de la instancia de base de datos de SQL Server. Amazon RDS crea una instantánea final de la instancia de base de datos. El nombre de la instantánea de instancia terminada tiene el formato *`instance_name`*`-final-snapshot`. Por ejemplo, si el nombre de su instancia de base de datos es **`mytest.cdxgahslksma.us-east-1.rds.com`**, la instantánea final tendrá el nombre **`mytest-final-snapshot`** y estará situado en la misma región de AWS que la instancia de base de datos original.
4. En Actions (Acciones), seleccione Restore Snapshot (Restaurar instantánea).

   Aparece la ventana Restore DB Instance.
5. En License Model (Modelo de licencia), seleccione license-included (licencia incluida).

6. Elija el motor de base de datos de SQL Server que desea usar.
7. Escriba el nombre de la instancia de base de datos restaurada en DB Instance Identifier (Identificador de instancias de bases de datos).
8. Elija Restore DB Instance (Restaurar instancia de base de datos).

Para obtener más información acerca de la restauración desde una instantánea, consulte Restauración a una instancia de base de datos.

Transición de una base de datos de Amazon RDS para SQL Server de OFFLINE a ONLINE

Puede cambiar una base de datos de Microsoft SQL Server de una instancia de base de datos de Amazon RDS de `OFFLINE` a `ONLINE`.

Método de SQL Server	Método de Amazon RDS
ALTER DATABASE *db_name* SET ONLINE;	EXEC rdsadmin.dbo.rds_set_database_online *db_name*

Uso de la captura de datos de cambios de Amazon RDS para SQL Server

Amazon RDS admite la captura de datos de cambios (CDC) para las instancias de base de datos que ejecutan Microsoft SQL Server. CDC captura los cambios que se realizando en los datos de las tablas. Almacena metadatos sobre cada cambio, a los que puede obtener acceso posteriormente. Para obtener más información sobre el funcionamiento de CDC, consulte Captura de datos de cambio en la documentación de Microsoft. Antes de usar CDC con sus instancias de base de datos de Amazon RDS, habilítela en la base de datos ejecutando `msdb.dbo.rds_cdc_enable_db`. Después de que se haya habilitado CDC, cualquier usuario que sea `db_owner` de esa base de datos puede habilitar o deshabilitar CDC en las tablas de esa base de datos.

> **Important**
>
> Durante las restauraciones, se deshabilitará CDC. Todos los metadatos relacionados se quitan automáticamente de la base de datos. Esto se aplica a las restauraciones de instantánea, restauraciones de un momento dado y restauraciones nativas de SQL Server

desde S3. Después de llevar a cabo uno de estos tipos de restauraciones, puede volver a habilitar CDC y especificar de nuevo las tablas de las que se realizará un seguimiento.

Para habilitar CDC para una instancia de base de datos, ejecute el procedimiento almacenado `msdb.dbo.rds_cdc_enable_db`.

```
exec msdb.dbo.rds_cdc_enable_db 'database_name'
```

Para desactivar CDC para una instancia de base de datos, ejecute el procedimiento almacenado `msdb.dbo.rds_cdc_disable_db`.

```
exec msdb.dbo.rds_cdc_disable_db 'database_name'
```

Para conceder permisos de CDC a un usuario, utilice el siguiente procedimiento:

```
go
  GRANT EXECUTE ON msdb.dbo.rds_cdc_enable_db TO User1
  GRANT EXECUTE ON msdb.dbo.rds_cdc_disable_db TO User1
```

Temas

- Seguimiento de tablas con la captura de datos de cambios
- Trabajos de captura de datos de cambio
- Captura de datos de cambio para instancias Multi-AZ

Seguimiento de tablas con la captura de datos de cambios

Después de que CDC se habilite en la base de datos, puede comenzar a realizar el seguimiento de tablas específicas. Puede elegir las tablas de las que se efectuará el seguimiento ejecutando sys.sp_cdc_enable_table.

```
--Begin tracking a table
exec sys.sp_cdc_enable_table
   @source_schema           = N'source_schema'
,  @source_name             = N'source_name'
,  @role_name               = N'role_name'

--The following parameters are optional:
```

```
--, @capture_instance       = 'capture_instance'
--, @supports_net_changes   = supports_net_changes
--, @index_name             = 'index_name'
--, @captured_column_list   = 'captured_column_list'
--, @filegroup_name         = 'filegroup_name'
--, @allow_partition_switch = 'allow_partition_switch'
;
```

Para ver la configuración de CDC de sus tablas, ejecute sys.sp_cdc_help_change_data_capture.

```
--View CDC configuration
exec sys.sp_cdc_help_change_data_capture

--The following parameters are optional and must be used together.
--  'schema_name', 'table_name'
;
```

Para obtener más información sobre las tablas, las funciones y los procedimientos almacenados de CDC, consulte lo siguiente en la documentación de SQL Server:

- Procedimientos almacenados de captura de cambio de datos (Transact-SQL)
- Funciones de captura de cambio de datos (Transact-SQL)
- Tablas de captura de cambio de datos (Transact-SQL)

Trabajos de captura de datos de cambio

Al habilitar CDC, SQL Server crea los trabajos de CDC. Los propietarios de base de datos (`db_owner`) pueden ver, crear, modificar y eliminar trabajos de CDC. Sin embargo, la cuenta del sistema de RDS es la propietaria de ellos. Por lo tanto, los trabajos no están visibles en las vistas nativas, en los procedimientos o en SQL Server Management Studio.

Para controlar el comportamiento de CDC en una base de datos, use procedimientos de SQL Server nativos, como sp_cdc_enable_table y sp_cdc_start_job. Para cambiar los parámetros de trabajo de CDC, como `maxtrans` y `maxscans`, puede usar sp_cdc_change_job..

Para obtener más información en relación con los trabajos de CDC, puede consultar las siguientes vistas de administración dinámicas:

- sys.dm_cdc_errors

- sys.dm_cdc_log_scan_sessions
- sysjobs
- sysjobhistory

Captura de datos de cambio para instancias Multi-AZ

Si utiliza CDC en una instancia Multi-AZ, asegúrese de que la configuración de trabajo de CDC del reflejo coincide con el del principal. Los trabajos de CDC se mapean a `database_id`. Si los ID de base de datos en el secundario son distintos del principal, los trabajos no se asociarán con la base de datos correcta. Para intentar evitar errores después de la conmutación por error, RDS borra y vuelve a crear los trabajos en el nuevo principal. Los trabajos que se han vuelto a crear usan los parámetros que el principal registró antes de la conmutación por error.

Aunque este proceso se ejecuta rápidamente, sigue siendo posible que los trabajos de CDC se ejecuten antes de que RDS pueda corregirlos. A continuación se indican tres formas de forzar a que los parámetros sean coherentes entre el principal y las réplicas secundarias:

- Usar los mismos parámetros de trabajo para todas las bases de datos que hayan habilitado CDC.
- Antes de cambiar la configuración de trabajo de CDC, convertir la instancia Multi-AZ a Single-AZ.
- Transferir manualmente los parámetros siempre que se cambien en el principal.

Para ver y definir los parámetros de CDC que se utilizaron para volver a crear los trabajos de CDC después de una conmutación por error, use `rds_show_configuration` y `rds_set_configuration`.

En el siguiente ejemplo, se devuelve el valor establecido para `cdc_capture_maxtrans`. Para cualquier parámetro establecido en `RDS_DEFAULT`, RDS configura automáticamente el valor.

```
-- Show configuration for each parameter on either primary and secondary replicas.
exec rdsadmin.dbo.rds_show_configuration 'cdc_capture_maxtrans';
```

Para establecer la configuración en el secundario, ejecute `rdsadmin.dbo.rds_set_configuration`. Este procedimiento establece los valores de los parámetros de todas las bases de datos en el servidor secundario. Esta configuración solo se usa después de una conmutación por error. En el siguiente ejemplo, se establece `maxtrans` de todos los trabajos de captura de CDC en *`1000`*:

```
--To set values on secondary. These are used after failover.
exec rdsadmin.dbo.rds_set_configuration 'cdc_capture_maxtrans', 1000;
```

Para establecer los parámetros de trabajo de CDC en la entidad principal, use sys.sp_cdc_change_jobs en su lugar.

Uso del Agente SQL Server para Amazon RDS

Con Amazon RDS, puede usar el Agente SQL Server en una instancia de base de datos en la que se ejecuta Microsoft SQL Server Enterprise Edition, Standard Edition o Web Edition. El Agente SQL Server es un servicio de Microsoft Windows que ejecuta tareas administrativas programadas que se denominan trabajos. Puede usar el Agente SQL Server para ejecutar trabajos de T-SQL que reconstruyan índices, ejecuten comprobaciones de daños y agrupen datos en una instancia de base de datos de SQL Server.

Cuando se crea una instancia de base de datos de SQL Server, el usuario maestro tiene asignado el rol `SQLAgentUserRole`.

El Agente SQL Server puede ejecutar un trabajo según un calendario, en respuesta a un evento concreto o bajo demanda. Para obtener más información, consulte SQL Server Agent en la documentación de Microsoft.

> **Note**
>
> Evite programar trabajos para que se ejecuten durante los periodos de mantenimiento y de copia de seguridad de la instancia de base de datos. Los procesos de mantenimiento y copia de seguridad lanzados por AWS podrían interrumpir el trabajo o hacer que se cancele.
> En las implementaciones Multi-AZ, los trabajos de SQL Server Agent se replican desde el host principal al host secundario cuando la función de replicación de trabajos está activada. Para obtener más información, consulte Activación de la replicación de trabajos del agente de SQL Server.
> Las implementaciones multi-AZ tienen un límite de 10 000 trabajos del Agente SQL Server. Si se necesitan límites más altos, solicite un aumento; para ello, contáctese con Soporte. Abra la página del centro de AWS Support, inicie sesión si es preciso y, luego, elija Create Case (Crear caso). Seleccione Service limit increase (Aumento del límite de servicio). Rellene y envíe el formulario.

Para ver el historial de un trabajo individual del Agente de SQL Server en SQL Server Management Studio (SSMS), abra el explorador de objetos, haga clic con el botón derecho en el trabajo y, a continuación, elija View History (Ver historial).

Como el Agente SQL Server se ejecuta en un anfitrión administrado de una instancia de base de datos, algunas opciones no son compatibles:

- No se admite la ejecución de trabajos de reproducción y de scripts de línea de comando por medio de ActiveX, el shell de comandos de Windows o Windows PowerShell.
- No puede iniciar, detener ni reiniciar el Agente de SQL Server de forma manual.
- Las notificaciones de email a través del Agente de SQL Server no están disponibles desde una instancia de base de datos.
- No se admiten las alertas ni los operadores del Agente de SQL Server.
- No se admite el uso del Agente de SQL Server para crear copias de seguridad. Utilice Amazon RDS para realizar una copia de seguridad de la instancia de base de datos.
- Actualmente, RDS para SQL Server no admite el uso de tokens del Agente SQL Server.

Activación de la replicación de trabajos del agente de SQL Server

Puede activar la replicación de trabajos del agente de SQL Server mediante el siguiente procedimiento almacenado:

```
EXECUTE msdb.dbo.rds_set_system_database_sync_objects @object_types = 'SQLAgentJob';
```

Puede ejecutar el procedimiento almacenado en todas las versiones de SQL Server compatibles con Amazon RDS for SQL Server. Los trabajos de las siguientes categorías se replican:

- [Sin categoría (local)]
- [Sin categoría (multiservidor)]
- [Sin categoría]
- Recopilador de datos
- Asesor de ajuste del motor de base de datos
- Mantenimiento de bases de datos
- Texto completo

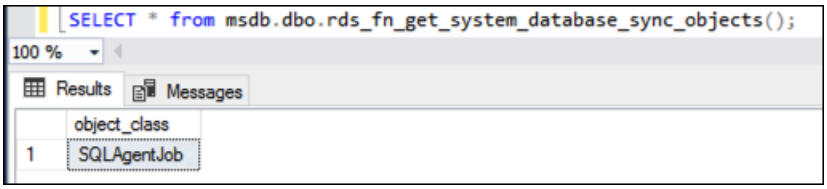
Solo se replican los trabajos que utilizan pasos de trabajo de T-SQL. Los trabajos con tipos de pasos como SQL Server Integration Services (SSIS), SQL Server Reporting Services (SSRS), Replication y PowerShell no se replican. Los trabajos que utilizan Database Mail y objetos de nivel de servidor no se replican.

> **Important**
>
> El host principal es el origen de información para la replicación. Antes de activar la replicación de trabajos, asegúrese de que sus trabajos de SQL Server Agent están en el principal. Si no lo hace, podría eliminar sus trabajos de SQL Server Agent si activa la característica cuando hay trabajos más nuevos en el host secundario.

Puede utilizar la siguiente función para confirmar si la replicación está activada.

```
SELECT * from msdb.dbo.rds_fn_get_system_database_sync_objects();
```

La consulta T-SQL devuelve lo siguiente si los trabajos del agente de SQL Server se están replicando. Si no se están replicando, no devuelve nada para `object_class`.

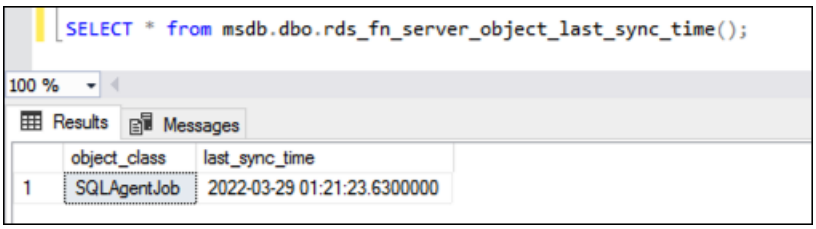


Puede utilizar la siguiente función para saber cuál fue la última vez que se sincronizaron los objetos con la configuración de hora UTC.

```
SELECT * from msdb.dbo.rds_fn_server_object_last_sync_time();
```

Por ejemplo, supongamos que modifica un trabajo de agente de SQL Server a las 01:00. Se espera que la hora de sincronización más reciente sea posterior a las 01:00, lo que indica que se ha producido la sincronización.

Tras la sincronización, se espera que los valores que se devuelven para `date_created` y `date_modified` en el nodo secundario coincidan.



Si también utiliza la replicación con `tempdb`, puede habilitar la replicación tanto para los trabajos del Agente SQL como para la configuración de `tempdb` proporcionándolos en el parámetro `@object_type`:

```
EXECUTE msdb.dbo.rds_set_system_database_sync_objects @object_types =
 'SQLAgentJob,TempDbFile';
```

Para obtener información sobre la replicación con `tempdb`, consulte Configuración de TempDB para implementaciones multi-AZ.

Roles de Agente SQL Server

RDS para SQL Server admite los siguientes roles de Agente SQL Server con diferentes niveles de permisos para administrar los trabajos:

- SQLAgentUserRole

  Permisos

  - Crear y administrar trabajos, programaciones y operadores propios
  - Ver las propiedades de los trabajos y las programaciones propios
  - No puede ver ni administrar trabajos creados por otros usuarios

  Este rol es adecuado para usuarios que necesitan crear y administrar trabajos propios, pero no requieren acceso a los trabajos creados por otros usuarios.
- SQLAgentReaderRole

  Permisos

  - Todos los permisos de SQLAgentUserRole
  - Ver una lista de todos los trabajos y programaciones, incluidos los creados por otros
  - Ver las propiedades de todos los trabajos
  - Consultar el historial de trabajos

Este rol es adecuado para usuarios que necesitan supervisar el estado de todos los trabajos, pero no necesitan administrarlos.

- SQLAgentOperatorRole

  Permisos

  - Todos los permisos de SQLAgentUserRole y SQLAgentReaderRole
  - Ejecutar, detener o iniciar trabajos
  - Administrar el historial de trabajos
  - Habilitar o deshabilitar trabajos y programaciones
  - Ver operadores y proxies

  Este rol proporciona los permisos más completos y es adecuado para usuarios que necesitan tener control total sobre todos los trabajos.

Utilice el siguiente comando para asignar los roles al inicio de sesión de SQL Server:

```
USE msdb;
EXEC sp_addrolemember 'SQLAgentOperatorRole', 'username';
```

Administración de SQLAgentOperatorRole en RDS para SQL Server

Para ver los trabajos actuales, debe agregar SQLAgentOperatorRole al inicio de sesión de SQL Server y eliminarlo antes de desconectarse de la base de datos.

Para visualizar el árbol de Agente SQL Server en SQL Server Management Studio, siga estas instrucciones:

Visualización de Agente SQL Server en SQL Server Management Studio (SSMS)

1. Con las credenciales maestras de RDS, inicie sesión en la instancia de RDS SQL Server y conceda al usuario deseado el rol SQLAgentUserRole.

   ```
   USE msdb
   GO
   IF NOT EXISTS(SELECT name FROM sys.database_principals WHERE name = 'UserName')
   BEGIN
   CREATE USER UserName FROM LOGIN UserName
   END
   ```

```
GO
ALTER ROLE SQLAgentUserRole ADD MEMBER UserName
GO
GRANT ALTER ON ROLE::[SQLAgentOperatorRole] to UserName
GO
```

Estos comandos crean el usuario en la base de datos `msdb`, en caso de que no exista. También agrega al usuario a SQLAgentUserRole, para que se pueda ver el árbol de Agente SQL Server en SSMS. Por último, concede permisos de alteración en SQLAgentOperatorRole al usuario. Esto permite al usuario agregarse o eliminarse de ese rol.

2. Para agregarse al rol mencionado anteriormente, conéctese a la instancia de RDS SQL Server con el usuario que necesita ver los trabajos y ejecute el siguiente script.

```
use msdb
go
ALTER ROLE SQLAgentOperatorRole ADD MEMBER UserName
GO
```

Después de esto, haga clic con el botón derecho en la carpeta Trabajos y elija Actualizar.

3. Al realizar esta acción, la pestaña Trabajos muestra el botón + (más). Haga clic para expandir la lista de trabajos de Agente SQL Server.

4. **Important**

   Antes de desconectarse de la instancia de RDS SQL Server, debe eliminarse de SQLAgentOperatorRole.

   Para eliminar el inicio de sesión de SQLAgentOperatorRole, ejecute la siguiente consulta antes de desconectarse o cerrar Management Studio:

```
USE msdb
GO
ALTER ROLE SQLAgentOperatorRole DROP MEMBER UserName
GO
```

Para obtener más información, consulte Leveraging SQLAgentOperatorRole in RDS SQL Server.

Agregar un usuario al rol SQLAgentUser

Para que otro inicio de sesión o usuario pueda utilizar el agente de SQL Server, debe iniciar sesión como usuario maestro y hacer lo siguiente:

1. Cree otro inicio de sesión de nivel de servidor con el comando `CREATE LOGIN`.
2. Cree un usuario en `msdb` con el comando `CREATE USER` y, a continuación, vincule este usuario al inicio de sesión que creó en el paso anterior.
3. Agregue el usuario a `SQLAgentUserRole` con el procedimiento almacenado en el sistema `sp_addrolemember`.

Por ejemplo, suponga que su nombre de usuario principal es **`admin`** y que desea dar acceso al agente de SQL Server a un usuario llamado **`theirname`** con la contraseña **`theirpassword`**. En ese caso, puede usar el siguiente procedimiento.

Para agregar un usuario al rol SQLAgentUser

1. Inicie sesión como usuario maestro.
2. Ejecute los comandos siguientes:

```
--Initially set context to master database
USE [master];
GO
--Create a server-level login named theirname with password theirpassword
CREATE LOGIN [theirname] WITH PASSWORD = 'theirpassword';
GO
--Set context to msdb database
USE [msdb];
GO
--Create a database user named theirname and link it to server-level login
 theirname
CREATE USER [theirname] FOR LOGIN [theirname];
GO
--Added database user theirname in msdb to SQLAgentUserRole in msdb
EXEC sp_addrolemember [SQLAgentUserRole], [theirname];
```

Eliminación de un trabajo del Agente de SQL Server

Utilice el procedimiento almacenado `sp_delete_job` para eliminar trabajos del Agente de SQL Server en Amazon RDS para Microsoft SQL Server.

No puede utilizar SSMS para eliminar trabajos del Agente de SQL Server. Si intenta hacerlo, obtendrá un mensaje de error similar al siguiente:

```
The EXECUTE permission was denied on the object 'xp_regread', database
 'mssqlsystemresource', schema 'sys'.
```

Como servicio administrado, RDS tiene la restricción de ejecutar procedimientos que obtienen acceso al registro de Windows. Cuando utiliza SSMS, este intenta ejecutar un proceso (`xp_regread`) para el que RDS no está autorizado.

> **Note**
>
> En RDS para SQL Server, solo los miembros del rol de administrador del sistema pueden actualizar o eliminar trabajos que pertenezcan a un inicio de sesión diferente. Para obtener más información, consulte Aprovechamiento de SQLAgentOperatorRole en el servidor de RDS para SQL.

Para eliminar un trabajo del Agente de SQL Server

- Ejecute la siguiente instrucción T-SQL:

```
EXEC msdb..sp_delete_job @job_name = 'job_name';
```

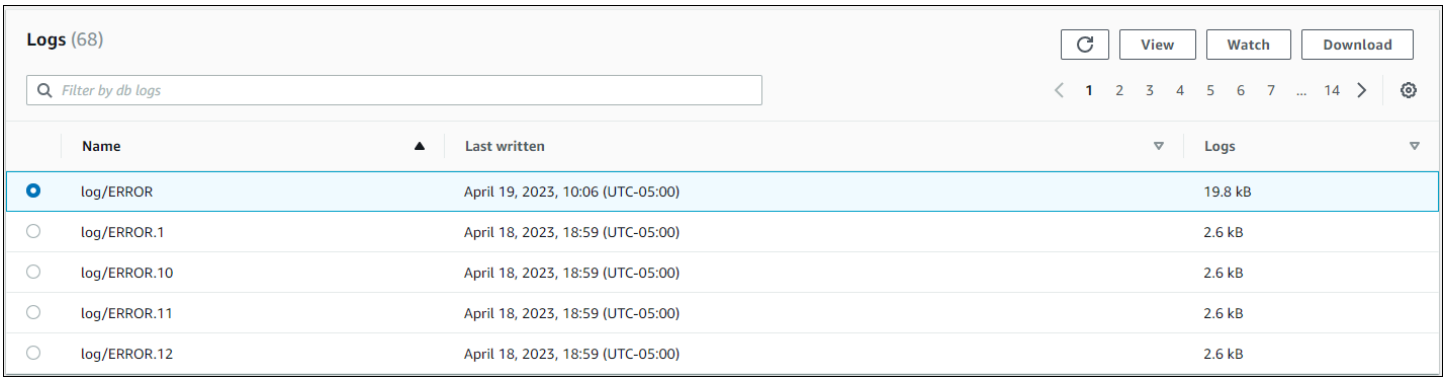
Uso de registros de Amazon RDS para Microsoft SQL Server

Puede usar la consola de Amazon RDS para ver, supervisar y descargar los registros del Agente SQL Server y los registros de errores de Microsoft SQL Server.

Supervisión de archivos de registro

Si ve un registro en la consola de Amazon RDS, puede ver su contenido tal y como está en ese momento. Supervisar un registro en la consola lo abre en un estado dinámico que permite ver las actualizaciones que se producen en él prácticamente en tiempo real.

El registro más reciente es el único activo para la supervisión. Por ejemplo, suponga que tiene los registros que se muestran a continuación:



Solo log/ERROR, el registro más reciente, se actualiza activamente. Puede elegir otros para supervisarlos, pero son estáticos y no se actualizarán.

Archivado de archivos de registro

La consola de Amazon RDS muestra registros de la semana anterior hasta el día en curso. Puede descargar y archivar los registros para usarlos como referencia después de ese tiempo. Una forma de archivar los registros es cargarlos en un bucket de Amazon S3. Para ver instrucciones acerca de cómo configurar un bucket de Amazon S3 y cargar un archivo, consulte Conceptos básicos de Amazon S3 en la Guía de introducción de Amazon Simple Storage Service y haga clic en Get Started (Comenzar).

Visualización de registros de agentes y errores

Para ver los registros del agente y de errores de Microsoft SQL Server, use el procedimiento almacenado de Amazon RDS `rds_read_error_log` con los siguientes parámetros:

- **`@index`** – la versión del registro que se va a recuperar. El valor predeterminado es 0, que recupera el registro de errores actual. Especifique 1 para recuperar el registro anterior, especifique 2 para recuperar el anterior a ese y así sucesivamente.
- **`@type`** – el tipo de registro que se va a recuperar. Especifique 1 para recuperar un registro de errores. Especifique 2 para recuperar un registro del Agente.

Example

En el ejemplo siguiente se solicita el registro de errores actual.

```
EXEC rdsadmin.dbo.rds_read_error_log @index = 0, @type = 1;
```

Para obtener más información acerca de los errores de SQL Server, vea Errores del motor de base de datos en la documentación de Microsoft.

Uso de archivos de seguimiento y volcado de Amazon RDS para SQL Server

En esta sección se describe el trabajo con los archivos de seguimiento y volcado para las instancias de base de datos de Amazon RDS en las que se ejecuta Microsoft SQL Server.

Generación de una consulta de seguimiento de SQL

```
declare @rc int
declare @TraceID int
declare @maxfilesize bigint

set @maxfilesize = 5

exec @rc = sp_trace_create @TraceID output,  0, N'D:\rdsdbdata\log\rdstest',
 @maxfilesize, NULL
```

Visualización de un seguimiento abierto

```
select * from ::fn_trace_getinfo(default)
```

Visualización del contenido del seguimiento

```
select * from ::fn_trace_gettable('D:\rdsdbdata\log\rdstest.trc', default)
```

Definición del periodo de retención para los archivos de seguimiento y volcado

Los archivos de seguimiento y volcado pueden acumular y consumir espacio en el disco. De manera predeterminada, Amazon RDS limpia los archivos de seguimiento y volcado que tienen más de siete días de antigüedad.

Para ver el periodo de retención actual de los archivos de seguimiento y volcado, use el procedimiento `rds_show_configuration`, como se muestra en el siguiente ejemplo.

```
exec rdsadmin..rds_show_configuration;
```

Para modificar el periodo de retención de los archivos de seguimiento, use el procedimiento `rds_set_configuration` y defina `tracefile retention` en minutos. El ejemplo siguiente define el periodo de retención de los archivos de seguimiento en 24 horas.

```
exec rdsadmin..rds_set_configuration 'tracefile retention', 1440;
```

Para modificar el periodo de retención de los archivos de volcado, use el procedimiento `rds_set_configuration` y defina `dumpfile retention` en minutos. El ejemplo siguiente define el periodo de retención de los archivos de volcado en 3 días.

```
exec rdsadmin..rds_set_configuration 'dumpfile retention', 4320;
```

Por motivos de seguridad, no puede eliminar un archivo de seguimiento o de volcado de una instancia de base de datos de SQL Server. Para eliminar todos los archivos de seguimiento o de volcado que no se utilicen, defina el periodo de retención de los archivos en 0.

Amazon RDS para MySQL

Amazon RDS admite distintas versiones de MySQL para instancias de bases de datos. Para obtener toda la información necesaria sobre versiones compatibles, consulte Versiones de MySQL en Amazon RDS.

Para crear una instancia de base de datos de Amazon RDS para MySQL, utilice las herramientas o interfaces de administración de Amazon RDS. A continuación puede hacer lo siguiente:

- cambiar el tamaño de la instancia de base de datos
- autorizar las conexiones a la instancia de base de datos
- crear y restaurar desde copias de seguridad o instantáneas
- crear secundarios de Multi-AZ
- crea réplicas de lectura
- supervisar el rendimiento de su instancia de base de datos

Use las utilidades y aplicaciones estándar de MySQL para almacenar los datos de su instancia de base de datos y acceder a ellos.

Amazon RDS for MySQL cumple con muchos estándares del sector. Por ejemplo, puede utilizar RDS para bases de datos MySQL a fin de crear aplicaciones que cumplan con HIPAA. Puede utilizar las bases de datos de RDS para MySQL con el fin de almacenar información relacionada con la atención sanitaria, incluida la información sanitaria protegida (PHI) en virtud de un acuerdo de asociación empresarial (BAA) con AWS. Amazon RDS para MySQL también cumple los requisitos de seguridad del Programa federal de administración de riesgos y autorizaciones (FedRAMP). Además, Amazon RDS para MySQL ha recibido una autorización provisional para operar (P-ATO) de la Junta de Autorización Conjunta (JAB) de FedRAMP en la referencia FedRAMP HIGH dentro de las regiones de AWS GovCloud (US). Para obtener más información acerca de los estándares de conformidad admitidos, consulte Conformidad en la nube de AWS.

Para obtener más información sobre las características de cada versión de MySQL, consulte The Main Features of MySQL en la documentación de MySQL.

Antes de crear una instancia de base de datos, complete los pasos que se describen en Configuración del entorno para Amazon RDS. Cuando crea una instancia de base de datos, el usuario maestro de RDS obtiene privilegios de DBA, con algunas limitaciones. Utilice esta cuenta para tareas administrativas, como crear cuentas de base de datos adicionales.

Puede crear lo siguiente:

- Instancias de base de datos
- Instantáneas de base de datos
- Restauraciones a un momento dado
- Copias de seguridad automatizadas
- Copias de seguridad manuales

Puede utilizar instancias de base de datos que ejecuten MySQL en una nube privada virtual (VPC) basada en Amazon VPC. También puede agregar características a su instancia de base de datos MySQL mediante la activación de varias opciones. Amazon RDS admite implementaciones multi-AZ para MySQL como una solución de conmutación por error de alta disponibilidad.

> **Important**
>
> Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Puede acceder a la base de datos con clientes estándar de SQL, como mysql. No obstante, no puede acceder al host directamente mediante Telnet o Secure Shell (SSH).

Temas

- Compatibilidad con características de MySQL en Amazon RDS
- Versiones de MySQL en Amazon RDS
- Conexión a la instancia de base de datos de MySQL
- Protección de las conexiones de instancias de base de datos MySQL
- Mejora del rendimiento de las consultas de RDS para MySQL con lecturas optimizadas de Amazon RDS
- Mejora del rendimiento de escritura con escrituras optimizadas para RDS para MySQL
- Actualizaciones del motor de base de datos de RDS para MySQL
- Actualización de una versión del motor de instantáneas de base de datos de MySQL
- Importación de datos en una instancia de base de datos de Amazon RDS para MySQL
- Uso de la replicación de MySQL en Amazon RDS

- Configuración de clústeres activo-activo para RDS para MySQL
- Exportación de datos desde una instancia de base de datos MySQL mediante replicación
- Opciones para las instancias de bases de datos MySQL
- Parámetros de MySQL
- Tareas comunes de administración de bases de datos para las instancias de bases de datos MySQL
- Zona horaria local para las instancias de bases de datos MySQL
- Problemas conocidos y limitaciones para Amazon RDS para MySQL
- Referencia de procedimientos almacenados de RDS para MySQL

Compatibilidad con características de MySQL en Amazon RDS

RDS para MySQL admite la mayoría de las características y capacidades de MySQL. Algunas características pueden disponer de una compatibilidad limitada o de privilegios restringidos.

Puede filtrar nuevas características de Amazon RDS en la página Novedades de Database. En el filtro Products (Productos), elija Amazon RDS. A continuación, busque con palabras clave como **`MySQL 2022`**.

> **Note**
>
> Las listas que siguen no son exhaustivas.

Temas

- Compatibilidad con características de MySQL en las versiones principales de Amazon RDS para MySQL
- Motores de almacenamiento admitidos por RDS for MySQL
- Uso de memcached y otras opciones con MySQL en Amazon RDS
- Calentamiento de caché de InnoDB para MySQL en Amazon RDS
- Cambios de lenguaje inclusivo en RDS para MySQL 8.4
- Características de MySQL que no admite Amazon RDS

Compatibilidad con características de MySQL en las versiones principales de Amazon RDS para MySQL

En las siguientes secciones, encontrará información sobre la compatibilidad de características de MySQL en las versiones principales de Amazon RDS para MySQL:

Temas

- Compatibilidad con MySQL 8.4 en Amazon RDS

Para obtener información acerca de la compatibilidad de las versiones secundarias de Amazon RDS para MySQL, consulte Versiones secundarias de MySQL compatibles en Amazon RDS.

Compatibilidad con MySQL 8.4 en Amazon RDS

Amazon RDS admite las siguientes características nuevas de las instancias de base de datos en las que se ejecuta la versión MySQL 8.4 o una posterior.

- Biblioteca criptográfica: RDS para MySQL ha sustituido a OpenSSL por AWS Libcrypto (AWS-LC), que cuenta con la certificación FIPS 140-3. Para obtener más información, consulte el repositorio de GitHub sobre AWS-LC en https://github.com/aws/aws-lc.
- Cambios de TLS: RDS para MySQL solo admite TLS 1.2 y TLS 1.3. Para obtener más información, consulte the section called “Compatibilidad de SSL/TLS con MySQL”.
- Compatibilidad con memcached: la interfaz memcached ya no está disponible en MySQL 8.4. Para obtener más información, consulte Compatibilidad con memcached para MySQL.
- Complemento de autenticación predeterminado: el complemento de autenticación predeterminado es `caching_sha2_password`. Para obtener más información, consulte the section called “Complemento de autenticación predeterminado de MySQL”.
- Utilidad de cliente **`mysqlpump`**: la utilidad de cliente `mysqlpump` ya no está disponible en MySQL 8.4. Para obtener más información, consulte Modelo de privilegios basado en roles de RDS para MySQL y mysqldump y mysqlpump en Recomendaciones de AWS.
- Procedimientos de replicación administrada almacenados: cuando utilice procedimientos almacenados para administrar la replicación con un usuario de replicación configurado con `caching_sha2_password`, debe configurar TLS especificando `SOURCE_SSL=1`. `caching_sha2_password` es el complemento de autenticación predeterminado de RDS para MySQL 8.4.
- Cambios en el comportamiento de los parámetros: se han modificado los siguientes parámetros para MySQL 8.4.
  - `innodb_dedicated_server`: este parámetro está habilitado de forma predeterminada. Para obtener más información, consulte Configuración del tamaño del grupo de búferes y la capacidad de registros redo en MySQL 8.4.
  - `innodb_buffer_pool`: el motor de base de datos calcula ahora este parámetro, pero puede anular este ajuste. Para obtener más información, consulte Configuración del tamaño del grupo de búferes y la capacidad de registros redo en MySQL 8.4.
  - `innodb_redo_log_capacity`: este parámetro ahora controla el tamaño de los archivos de registro redo. El motor de base de datos calcula ahora este parámetro, pero puede anular este ajuste. Para obtener más información, consulte Configuración del tamaño del grupo de búferes y la capacidad de registros redo en MySQL 8.4.

- Parámetros obsoletos o eliminados: RDS para MySQL ha eliminado los siguientes parámetros de los grupos de parámetros de las instancias de base de datos MySQL 8.4. El parámetro `innodb_redo_log_capacity` ahora controla el tamaño de los archivos de registro redo.
  - `innodb_log_file_size`
  - `innodb_log_files_in_group`
- Valores nuevos predeterminados para los parámetros: los siguientes parámetros tienen valores predeterminados nuevos para las instancias de base de datos de la versión 8.4 de MySQL:
  - Se han modificado varios parámetros de la comunidad MySQL relacionados con el rendimiento. Para obtener más información, consulte What is New in MySQL 8.4 since MySQL 8.0.

    Le recomendamos que pruebe el rendimiento de su aplicación en RDS para MySQL 8.4 antes de migrar una instancia de producción.
  - `innodb_purge_threads`: el valor por defecto se establece en la fórmula `LEAST({DBInstanceVCPU/2},4)` para evitar que la longitud de la lista del historial de InnoDB aumente demasiado.
  - `group_replication_exit_state_action`: el valor predeterminado es `OFFLINE_MODE`, que se alinea con el valor predeterminado de MySQL Community. Para obtener más información, consulte Aspectos a tener en cuenta y prácticas recomendadas de los clústeres activo-activo de RDS para MySQL.
  - `binlog_format`: el valor predeterminado es `ROW`, que se alinea con el valor predeterminado de MySQL Community. Puede modificar el parámetro para las instancias de base de datos Single-AZ o Multi-AZ, pero no para los clústeres de base de datos Multi-AZ. Los clústeres de bases de datos Multi-AZ utilizan la replicación semisincrónica y, cuando `binlog_format` se establece en `MIXED` o en `STATEMENT`, la replicación falla.
- Cambios de lenguaje inclusivos: RDS para MySQL 8.4 incluye cambios de RDS para MySQL 8.0 relacionados con palabras clave y esquemas del sistema para un lenguaje inclusivo. Para obtener más información, consulte Cambios de lenguaje inclusivo en RDS para MySQL 8.4.

Para obtener una lista de todas las características y cambios de MySQL 8.4, consulte What Is New in MySQL 8.4 since MySQL 8.0 en la documentación de MySQL.

Para ver una lista de las características no admitidas, consulte the section called “Características no admitidas”.

Motores de almacenamiento admitidos por RDS for MySQL

Si bien MariaDB admite varios motores de almacenamiento con diversas capacidades, no todos están optimizados para la recuperación y la durabilidad de los datos. Amazon RDS admite por completo el motor de almacenamiento InnoDB para las instancias de base de datos de MySQL. Las características de Amazon RDS de recuperación a un momento dado y la restauración de instantáneas requieren un motor de almacenamiento que pueda recuperarse y solo son compatibles con el motor de almacenamiento de InnoDB. Para obtener más información, consulte Compatibilidad con memcached para MySQL.

Actualmente, Amazon RDS for MySQL no admite el motor de almacenamiento federado.

Para los esquemas creados por el usuario, el motor de almacenamiento MyISAM no admite la recuperación fiable y puede dar lugar a datos perdidos o dañados cuando se reinicia MySQL después de una recuperación, lo que evita que la restauración a un momento dado o la restauración de instantáneas funcionen según lo previsto. Si, a pesar de ello, decide usar MyISAM con Amazon RDS, las instantáneas pueden ser útiles en determinadas condiciones.

> **Note**
>
> Las tablas del sistema del esquema `mysql` pueden residir en el almacenamiento MyISAM.

Si desea convertir las tablas de MyISAM en tablas de InnoDB, puede usar el comando `ALTER TABLE` (por ejemplo, `alter table TABLE_NAME engine=innodb;`). Tenga en cuenta que MyISAM e InnoDB tienen diferentes puntos fuertes y débiles, por lo que debe evaluar completamente el impacto de este cambio en sus aplicaciones antes de realizarlo.

MySQL 5.1 y 5.5 y 5.6 ya no se admiten en Amazon RDS. Sin embargo, puede restaurar instantáneas de MySQL 5.1 y 5.5 y 5.6 existentes. Cuando se restaura una instantánea de MySQL 5.1 o 5.5 o 5.6 la instancia de base de datos se actualiza automáticamente a MySQL 5.7.

Uso de memcached y otras opciones con MySQL en Amazon RDS

La mayoría de los motores de bases de datos de Amazon RDS admiten grupos de opciones que permiten seleccionar características adicionales para una instancia de base de datos. Las instancias de base de datos de RDS para MySQL admiten la opción `memcached`, una caché sencilla, basada en claves. Para obtener más información acerca de `memcached` y otras opciones, consulte Opciones

para las instancias de bases de datos MySQL. Para obtener más información acerca de cómo trabajar con grupos de opciones, consulte Trabajo con grupos de opciones.

Calentamiento de caché de InnoDB para MySQL en Amazon RDS

El calentamiento de caché de InnoDB puede proporcionar ganancias de desempeño para la instancia de base de datos MySQL guardando el estado actual del grupo del búfer cuando se cierra la instancia de base de datos y volviendo a cargar el grupo del búfer a partir de la información guardada, cuando se inicia la instancia de base de datos. Esto omite la necesidad del grupo del búfer de "calentarse" con el uso normal de la base de datos y, en su lugar, precarga el grupo del búfer con las páginas de las consultas comunes conocidas. El archivo que almacena la información guardada del grupo del búfer solo almacena metadatos para las páginas que están en el grupo del búfer y no las páginas propiamente dichas. Por este motivo, el archivo no requiere mucho espacio de almacenamiento. El tamaño del archivo es de aproximadamente un 0,2% del tamaño de la caché. Por ejemplo, para una caché de 64 GiB, el tamaño del archivo de calentamiento de caché es de 128 MiB. Para obtener más información acerca del calentamiento de caché de InnoDB, consulte Saving and Restoring the Buffer Pool State en la documentación de MySQL.

Las instancias de base de datos de RDS para MySQL admiten la activación de caché InnoDB. Para activar el calentamiento de caché de InnoDB, establezca los parámetros `innodb_buffer_pool_dump_at_shutdown` e `innodb_buffer_pool_load_at_startup` en 1 en el grupo de parámetros de la instancia de base de datos. Si se cambian los valores de estos parámetros en un grupo de parámetros, todas las instancias de bases de datos MySQL que utilicen ese grupo de parámetros resultarán afectadas. Para activar el calentamiento de caché de InnoDB para instancias de bases de datos MySQL específicas, es posible que deba crear un nuevo grupo de parámetros para esas instancias. Para obtener información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

El calentamiento de caché de InnoDB proporciona principalmente un beneficio de desempeño para las instancias de bases de datos que utilizan almacenamiento estándar. Si utiliza almacenamiento PIOPS, normalmente no se observa un beneficio de desempeño significativo.

> **Important**
>
> Si la instancia de base de datos MySQL no se cierra de forma normal como, por ejemplo, durante una conmutación por error, el estado del grupo del búfer no se guardará en el disco. En este caso, MySQL carga cualquier archivo de grupo del búfer que esté disponible cuando se reinicia la instancia de base de datos. Esto no es perjudicial, pero el grupo del búfer

restaurado podría no reflejar el estado más reciente del grupo del búfer antes del reinicio. Para asegurarse de que tiene un estado reciente del grupo del búfer disponible para calentar la caché de InnoDB al iniciar, recomendamos que vuelque periódicamente el grupo del búfer "bajo demanda".
Puede crear un evento para volcar el grupo del búfer automáticamente de forma periódica. Por ejemplo, la siguiente instrucción crea un evento denominado `periodic_buffer_pool_dump` que vuelca el grupo del búfer cada hora.

```
CREATE EVENT periodic_buffer_pool_dump
ON SCHEDULE EVERY 1 HOUR
DO CALL mysql.rds_innodb_buffer_pool_dump_now();
```

Para obtener más información acerca de los eventos de MySQL, consulte Event Syntax en la documentación de MySQL.

Volcado y carga del grupo del búfer bajo demanda

Puede guardar y cargar la caché de InnoDB «bajo demanda».

- Para volcar el estado actual del grupo del búfer en el disco, llame al procedimiento almacenado mysql.rds_innodb_buffer_pool_dump_now.
- Para cargar el estado guardado del grupo del búfer desde el disco, llame al procedimiento almacenado mysql.rds_innodb_buffer_pool_load_now.
- Para cancelar una operación de carga en curso, llame al procedimiento almacenado mysql.rds_innodb_buffer_pool_load_abort.

Cambios de lenguaje inclusivo en RDS para MySQL 8.4

RDS para MySQL 8.4 incluye cambios de la edición de la comunidad de MySQL 8.4 relacionados con palabras clave y esquemas del sistema para un lenguaje inclusivo. Por ejemplo, el comando `SHOW REPLICA STATUS` reemplaza a `SHOW SLAVE STATUS`.

Temas

- Cambio del nombre del parámetro de configuración
- Cambios en los nombres de los procedimientos almacenados

Cambio del nombre del parámetro de configuración

Los siguientes parámetros de configuración tienen nombres nuevos en RDS para MySQL 8.4.

Para obtener compatibilidad, puede verificar los nombres de los parámetros en el cliente de `mysql` usando cualquiera de los dos nombres. Solo podrá utilizar los nuevos nombres cuando modifique los valores de un grupo de parámetros de MySQL 8.4 personalizado. Para obtener más información, consulte Grupos de parámetros predeterminados y personalizados.

Nombre que se va a eliminar	Nombre nuevo o preferido
`init_slave`	`init_replica`
`log_slave_updates`	`log_replica_updates`
`log_slow_slave_statements`	`log_slow_replica_statements`
`rpl_stop_slave_timeout`	`rpl_stop_replica_timeout`
`skip_slave_start`	`skip_replica_start`
`slave_checkpoint_group`	`replica_checkpoint_group`
`slave_checkpoint_period`	`replica_checkpoint_period`
`slave_compressed_protocol`	`replica_compressed_protocol`
`slave_exec_mode`	`replica_exec_mode`
`slave_load_tmpdir`	`replica_load_tmpdir`
`slave_max_allowed_packet`	`replica_max_allowed_packet`
`slave_net_timeout`	`replica_net_timeout`

Nombre que se va a eliminar	Nombre nuevo o preferido
slave_parallel_type	replica_parallel_type
slave_parallel_workers	replica_parallel_workers
slave_pending_jobs_size_max	replica_pending_jobs_size_max
slave_preserve_commit_order	replica_preserve_commit_order
slave_skip_errors	replica_skip_errors
slave_sql_verify_checksum	replica_sql_verify_checksum
slave_transaction_retries	replica_transaction_retries
slave_type_conversions	replica_type_conversions
sql_slave_skip_counter	sql_replica_skip_counter

> **Note**
>
> El parámetro `replica_allow_batching` no está disponible porque Amazon RDS no admite clústeres NDB.

Cambios en los nombres de los procedimientos almacenados

Los siguientes procedimientos almacenados tienen nombres nuevos en RDS para MySQL 8.4.

Para obtener compatibilidad, puede utilizar cualquiera de los dos nombres en la versión inicial de RDS para MySQL 8.4. Los nombres de procedimientos antiguos se eliminarán en una próxima versión. Para obtener más información, consulte Configuración, inicio y detención de la replicación del registro binario (binlog).

Nombre que se va a eliminar	Nombre nuevo o preferido
`mysql.rds_next_master_log`	`mysql.rds_next_source_log`
`mysql.rds_reset_external_master`	`mysql.rds_reset_external_source`
`mysql.rds_set_external_master`	`mysql.rds_set_external_source`
`mysql.rds_set_external_master_with_auto_position`	`mysql.rds_set_external_source_with_auto_position`
`mysql.rds_set_external_master_with_delay`	`mysql.rds_set_external_source_with_delay`
`mysql.rds_set_master_auto_position`	`mysql.rds_set_source_auto_position`

Características de MySQL que no admite Amazon RDS

Amazon RDS no admite actualmente las siguientes características de MySQL:

- Complemento de autenticación
- Registro de errores en el registro del sistema
- Cifrado de espacio de tabla de InnoDB
- Clústeres NDB
- Complemento de nivel de seguridad de las contraseñas
- Variables persistentes del sistema

- Complemento de reescritura de consultas de reescritor
- Replicación semisincrónica, excepto en los clústeres de base de datos Multi-AZ
- Espacio de tabla transportable
- Complemento X

Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Amazon RDS permite el acceso a las bases de datos de una instancia de base de datos usando cualquier aplicación cliente de SQL estándar. Amazon RDS no permite el acceso de anfitrión directo a una instancia de base de datos a través de Telnet, Secure Shell (SSH) o conexión a escritorio remoto de Windows. Cuando se crea una instancia de base de datos, se le asigna db_owner para todas las bases de datos de esa instancia y todos los permisos en la base de datos, excepto los utilizados para las copias de seguridad. Amazon RDS administra las copias de seguridad por usted.

Versiones de MySQL en Amazon RDS

En MySQL, los números de la versión se organizan como versión = X.Y.Z. En la terminología de Amazon RDS, X.Y denota la versión principal, y Z es el número de la versión secundaria. Para Amazon RDS implementaciones, un cambio de versión se considera importante si el número de versión principal cambia,—por ejemplo, al pasar de la versión 5.7 a la 8.0. Un cambio de versión se considera secundario si solo cambia el número de la versión secundaria, por ejemplo, al pasar de la versión 8.0.32 a la 8.0.34.

Temas

- Versiones secundarias de MySQL compatibles en Amazon RDS
- Versiones principales de MySQL compatibles en Amazon RDS
- Versiones de soporte extendido de Amazon RDS para RDS para MySQL
- Trabajo con el entorno de vista previa de bases de datos
- MySQL versión 8.4 en el entorno de vista previa de bases de datos
- MySQL versión 8.3 en el entorno de vista previa de bases de datos
- MySQL versión 8.2 en el entorno de vista previa de bases de datos
- MySQL versión 8.1 en el entorno de vista previa de base de datos
- Versiones obsoleta para Amazon RDS for MySQL

Versiones secundarias de MySQL compatibles en Amazon RDS

Amazon RDS admite actualmente las siguientes versiones secundarias de MySQL.

> **Note**
>
> Las fechas con solo un mes y un año son aproximadas y se actualizan con una fecha exacta cuando se conoce.
> El Soporte extendido de Amazon RDS no está disponible para las versiones secundarias.

En la siguiente tabla se muestran las versiones secundarias de MySQL 8.0 compatibles actualmente con Amazon RDS.

Versión del motor MySQL	Fecha de versiones de la comunidad	Fecha de versión de RDS	Fecha de fin de soporte estándar de RDS
8.0.39	23 de julio de 2024	12 de agosto de 2024	Septiembre de 2025
8.0.37	30 de abril de 2024	18 de junio de 2024	Septiembre de 2025
8.0.36	16 de enero de 2024	12 de febrero de 2024	Marzo de 2025
8.0.35	25 de octubre de 2023	9 de noviembre de 2023	Marzo de 2025
8.0.34	18 de julio de 2023	9 de agosto de 2023	Marzo de 2025
8.0.33	18 de abril de 2023	15 de junio de 2023	Marzo de 2025
8.0.32	17 de enero de 2023	7 de febrero de 2023	Marzo de 2025

En la siguiente tabla, se muestran las versiones secundarias de MySQL 5.7 disponibles con el Soporte extendido de Amazon RDS.

Versión del motor MySQL	Fecha de versiones de la comunidad	Fecha de versiones de RDS	Fecha de finalización del soporte extendido de RDS
5.7.44-RDS.20240529*	No aplicable	25 de junio de 2024	Septiembre de 2025
5.7.44-RDS.20240408*	No aplicable	17 de mayo de 2024	Septiembre de 2025
5.7.44	25 de octubre de 2023	2 de noviembre de 2023	Marzo de 2025

* MySQL Community retiró la versión principal 5.7 y no lanzará nuevas versiones secundarias. Se trata de una versión secundaria que Amazon RDS publicó con parches de seguridad críticos y

correcciones de errores para las bases de datos de MySQL 5.7 incluidas en el Soporte extendido de RDS. Para obtener más información sobre estas versiones secundarias, consulte the section called "Versiones de soporte extendido de RDS para RDS para MySQL". Para obtener más información sobre el Soporte extendido de Amazon RDS, consulte Soporte extendido de Amazon RDS con Amazon RDS.

Las versiones secundarias pueden llegar al final del soporte estándar antes que las versiones principales. Por ejemplo, la versión 8.0.28 alcanzó su fecha de fin de soporte estándar el 28 de marzo de 2024, mientras que la versión principal 8.0 llegará al fin del soporte el 31 de julio de 2026. RDS admitirá las versiones secundarias 8.0.* adicionales que la comunidad MySQL publique entre estas fechas.

Puede especificar cualquier versión admitida actualmente de MySQL al crear una nueva instancia de base de datos. Puede especificar la versión principal (como MySQL 5.7) y cualquier versión secundaria admitida para la versión principal especificada. Si no se especifica ninguna versión, Amazon RDS cambia de forma predeterminada a una versión admitida, normalmente la más reciente. Si se especifica una versión principal pero no una versión secundaria, Amazon RDS usa de manera predeterminada una versión reciente de la versión principal especificada. Para ver una lista de las versiones admitidas, así como de las versiones predeterminadas para instancias de bases de datos recién creadas, utilice el comando `describe-db-engine-versions` de la AWS CLI.

Por ejemplo, para enumerar las versiones de motor compatibles con RDS para MySQL, ejecute el siguiente comando de la CLI:

```
aws rds describe-db-engine-versions --engine mysql --query "*[].
{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

La versión predeterminada de MySQL puede variar según la Región de AWS. Para crear una instancia de base de datos con una versión secundaria concreta, especifique la versión secundaria durante la creación de la instancia de base de datos. Puede determinar la versión secundaria predeterminada de una Región de AWS mediante el siguiente comando de la:AWS CLI

```
aws rds describe-db-engine-versions --default-only --engine mysql
 --engine-version major-engine-version --region region --query "*[].
{Engine:Engine,EngineVersion:EngineVersion}" --output text
```

Reemplace *major-engine-version* por la versión principal del motor y reemplace *region* por la Región de AWS. Por ejemplo, el siguiente comando de la AWS CLI devuelve la versión

predeterminada del motor secundario de MySQL para la versión principal 5.7 y la Región de AWS de Oeste de EE. UU. (Oregón) (us-west-2):

```
aws rds describe-db-engine-versions --default-only --engine mysql --engine-version 5.7
 --region us-west-2 --query "*[].{Engine:Engine,EngineVersion:EngineVersion}" --output
 text
```

Con Amazon RDS, puede controlar cuándo se actualiza una instancia de MySQL a una nueva versión principal admitida por Amazon RDS. Puede mantener la compatibilidad con versiones específicas de MySQL, probar nuevas versiones con una aplicación antes de implementarlas en producción y realizar las actualizaciones de versiones principales en el momento que le resulte más conveniente.

Cuando se habilita la actualización automática de versiones secundarias, la instancia de base de datos se actualizará automáticamente a las nuevas versiones secundarias de MySQL a medida que sean compatibles con Amazon RDS. Los parches se instalan durante el periodo de mantenimiento programado. Puede modificar una instancia de base de datos para habilitar o desactivar actualizaciones automáticas de versiones secundarias.

Si desactiva las actualizaciones programadas automáticamente, puede actualizar manualmente a una versión secundaria admitida siguiendo el mismo procedimiento que utilizaría para una actualización de la versión principal. Para obtener información, consulte Actualización de una versión del motor de una instancia de base de datos.

Amazon RDS admite las actualizaciones de la versión principal 5.6 a 5.7 de MySQL y de la versión 5.7 a 8.0 de MySQL. Debido a que las actualizaciones de la versión principal implican cierto riesgo de compatibilidad, no se realizan automáticamente; debe realizar una solicitud para modificar la instancia de base de datos. Debe probar exhaustivamente cualquier actualización antes de actualizar las instancias de producción. Para obtener información acerca de la actualización de una instancia de base de datos MySQL, consulte Actualizaciones del motor de base de datos de RDS para MySQL.

Puede probar una instancia de base de datos con una nueva versión antes de actualizar. Para ello, cree una instantánea de base de datos a partir de su instancia de base de datos, restaure luego desde la instantánea de base de datos para crear una nueva instancia de base de datos e inicie a continuación una actualización de versión para la nueva instancia de base de datos. Puede experimentar con seguridad en el clon actualizado de la instancia de base de datos antes de decidir si debe o no actualizar la instancia de base de datos original.

Versiones secundarias de MySQL en Amazon RDS

Versiones secundarias

- MySQL versión 8.0.39
- MySQL versión 8.0.37

MySQL versión 8.0.39

La versión 8.0.39 de MySQL ya está disponible en Amazon RDS. Esta versión contiene correcciones y mejoras añadidas por la comunidad MySQL y Amazon RDS.

Nuevas características y mejoras

- Se ha corregido un error que impedía que `sql_log_off` funcionara correctamente con el privilegio `SESSION_VARIABLES_ADMIN`.
- Se ha corregido un error que impedía que el usuario maestro pudiera conceder el privilegio `SESSION_VARIABLE_ADMIN` a otros usuarios de la base de datos.
- Se ha corregido un error que provocaba una combinación ilegal de intercalación al ejecutar los procedimientos almacenados proporcionados por RDS.

MySQL versión 8.0.37

La versión 8.0.37 de MySQL ya está disponible en Amazon RDS. Esta versión contiene correcciones y mejoras añadidas por la comunidad MySQL y Amazon RDS.

Nuevas características y mejoras

Se ha corregido un error con la ejecución de una instrucción DDL instantánea seguida de un UPDATE y que provocaba un error de aserción.

Versiones principales de MySQL compatibles en Amazon RDS

Las versiones principales de RDS para MySQL están disponibles bajo soporte estándar al menos hasta el final de la vida útil de la comunidad para la versión de la comunidad correspondiente. Puede seguir ejecutando una versión principal después de la fecha de finalización del soporte estándar de RDS si paga una cuota. Para obtener más información, consulte Soporte extendido de Amazon RDS con Amazon RDS y Precios de Amazon RDS para MySQL.

Puede utilizar las siguientes fechas para planificar sus ciclos de prueba y actualización.

> **Note**
>
> Las fechas con solo un mes y un año son aproximadas y se actualizan con una fecha exacta cuando se conoce.

Versión principal de MySQL	Fecha de versiones de la comunidad	Fecha de versiones de RDS	Fecha de fin de vida útil de la comunidad	Fecha de fin de soporte estándar de RDS	Fecha de inicio del precio del primer año del soporte extendido de RDS	Fecha de inicio del precio del tercer año del soporte extendido de RDS	Fecha de finalización del soporte extendido de RDS
MySQL 8.0	19 de abril de 2018	23 de octubre de 2018	Abril de 2022	31 de julio de 2026	1 de agosto de 2026	1 de agosto de 2028	31 de julio de 2029
MySQL 5.7*	21 de octubre de 2015	22 de febrero de 2016	Octubre de 2023	29 de febrero de 2024	1 de marzo de 2024	1 de marzo de 2026	28 de febrero de 2027

* MySQL 5.7 ahora solo está disponible bajo el Soporte extendido de RDS. Para obtener más información, consulte Soporte extendido de Amazon RDS con Amazon RDS.

Versiones de soporte extendido de Amazon RDS para RDS para MySQL

En la siguiente sección se enumeran todas las versiones del soporte extendido de RDS para RDS para MySQL.

Versiones

- Soporte extendido de RDS para RDS para MySQL versión 5.7.44-RDS.20240529
- Soporte extendido de RDS para RDS para MySQL versión 5.7.44-RDS.20240408

Soporte extendido de RDS para RDS para MySQL versión 5.7.44-RDS.20240529

Se encuentra disponible el soporte extendido de RDS para RDS para MySQL versión 5.7.44-RDS.20240529.

Errores corregidos:

- Se ha corregido un error de aserción de `field.cc` mediante la implementación de `fix_after_pullout`.
- Se ha corregido un error en el puntero nulo al devolver los metadatos al cliente para determinadas consultas SQL. Estas consultas contenían parámetros dinámicos y subconsultas en las cláusulas `SELECT`.
- Se han corregido los resultados incorrectos cuando se utilizaba `GROUP BY` para escaneos de índices sueltos o escaneos de rangos no contiguos de un índice.
- Se ha corregido la pérdida de información de GTID en el bloqueo de MySQL durante la persistencia.
- Se ha corregido una condición de carrera que podía provocar que una transacción de InnoDB se bloqueara indefinidamente.
- Se ha corregido una condición de carrera en la limpieza de la información de certificación de Group Replication.
- Se ha corregido un problema al escanear un índice pasado con operaciones de página simultáneas.
- Se ha corregido un problema de estado de búsqueda de texto completo (FTS) incoherente en escenarios simultáneos.
- Se ha corregido un problema de aserción con búfer de cambio en la eliminación de tablas.
- Comportamiento unificado para llamar a la función `deinit` en todos los tipos de complementos.

Se han corregido los CVE:

- CVE-2024-20963
- CVE-2024-20993
- CVE-2024-20998
- CVE-2024-21009
- CVE-2024-21054

- CVE-2024-21055
- CVE-2024-21057
- CVE-2024-21062
- CVE-2024-21008
- CVE-2024-21013
- CVE-2024-21047
- CVE-2024-21087
- CVE-2024-21096

Soporte extendido de RDS para RDS para MySQL versión 5.7.44-RDS.20240408

Se encuentra disponible el soporte extendido de RDS para RDS para MySQL versión 5.7.44-RDS.20240408.

Esta versión contiene parches para los siguientes CVE:

- CVE-2024-20963

Trabajo con el entorno de vista previa de bases de datos

En julio de 2023, Oracle anunció un nuevo modelo de lanzamiento para MySQL. Este modelo incluye dos tipos de versiones: las versiones de innovación y las versiones LTS. Amazon RDS proporciona las versiones de innovación de MySQL en el entorno de versión preliminar de RDS. Para obtener más información sobre las versiones de innovación de MySQL, consulte Introducing MySQL Innovation and Long-Term Support (LTS) versions.

Las instancias de base de datos de RDS para MySQL en el entorno de vista previa de base de datos son funcionalmente similares a otras instancias de bases de datos de RDS para MySQL. Sin embargo, no puede usar el entorno de vista previa de bases de datos para las cargas de trabajo de producción.

Los entornos de vista previa presentan las siguientes limitaciones:

- Amazon RDS elimina todas las instancias de base de datos 60 días después de crearlas, junto con las copias de seguridad e instantáneas.
- Solo puede utilizar almacenamiento SSD de uso general y SSD IOPS provisionadas.

- No puede obtener ayuda de Soporte con instancias de bases de datos. En su lugar, puede publicar sus preguntas en la comunidad de preguntas y respuestas administrada de AWS, AWS re:Post.
- No puede copiar una instantánea de una instancia de base de datos en un entorno de producción.

Las siguientes opciones son compatibles con la vista previa.

- Puede crear instancias de base de datos con las clases de instancias de base de datos db.m6i, db.r6i, db.m6g, db.m5, db.t3, db.r6g y db.r5. Para obtener más información sobre las clases de instancias de RDS, consulte Clases de instancia de base de datos de .
- Puede utilizar implementaciones Single-AZ y Multi-AZ.
- Puede utilizar las funciones estándar de volcado y carga de MySQL para importar bases de datos desde el entorno de la vista previa de base de datos o para exportarlas a este.

Características no compatibles en el entorno de vista previa de bases de datos

Las siguientes características no están disponibles en el entorno de vista previa de bases de datos:

- Copia de instantáneas entre regiones
- Réplicas de lectura entre regiones
- RDS Proxy

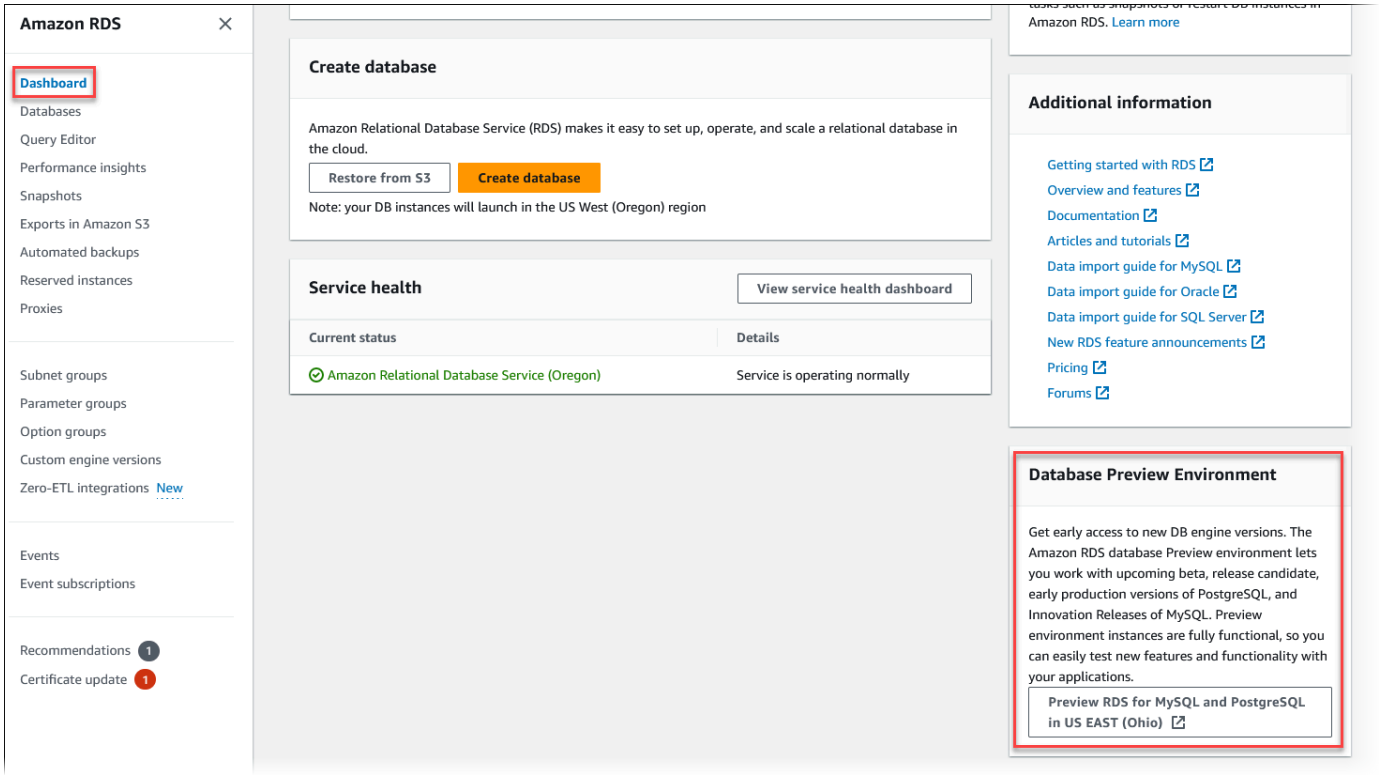
Creación de una nueva instancia de base de datos en el entorno de vista previa de bases de datos

Puede crear una instancia de base de datos en el entorno de vista previa de la base de datos utilizando AWS Management Console, AWS CLI o la API de RDS.

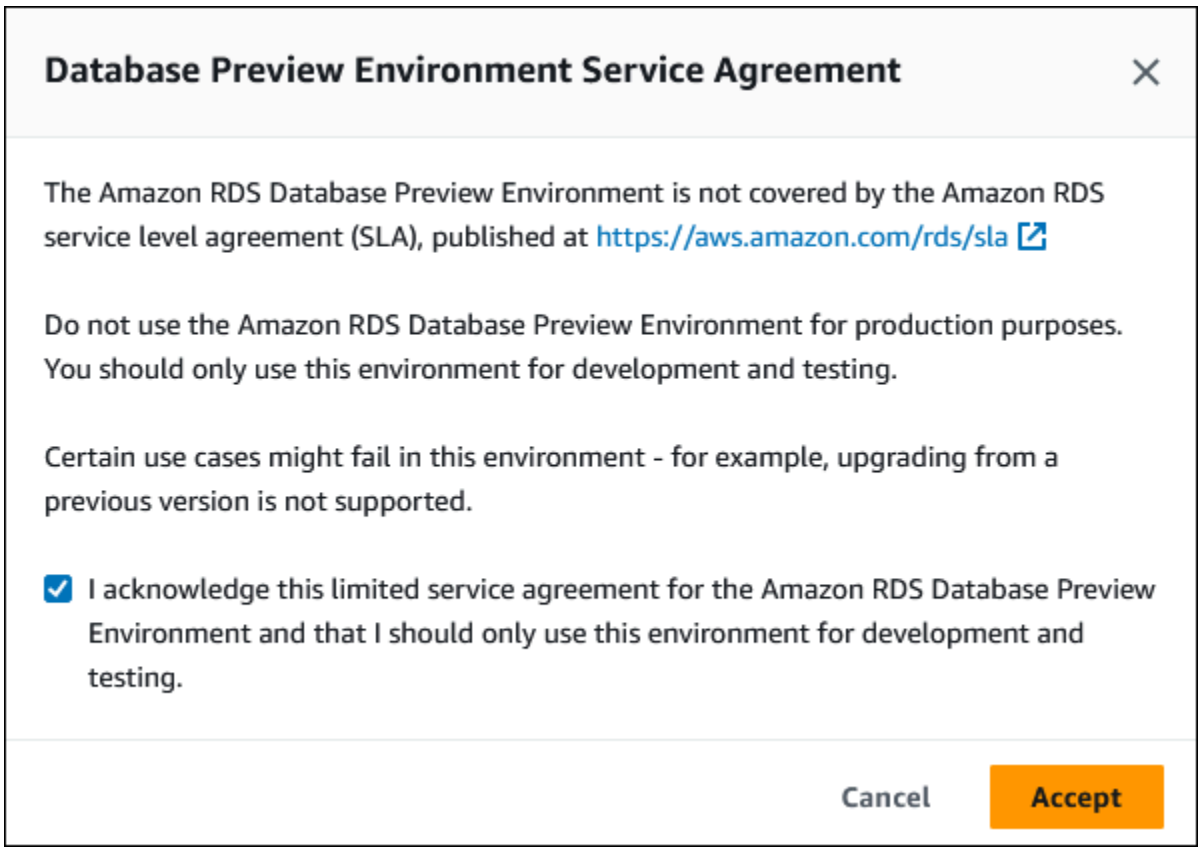
Consola

Para crear una instancia de base de datos en el entorno de vista previa de bases de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Dashboard (Panel) en el panel de navegación.
3. En la página Panel, busque la sección Database Preview Environment, tal y como se muestra en la siguiente imagen.



Puede navegar directamente a Database Preview Environment. Antes de continuar, debe reconocer y aceptar las limitaciones.



4. Para crear la instancia de base de datos de RDS para MySQL, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento Consola en Creación de una instancia de base de datos.

AWS CLI

Para crear una instancia de base de datos en el entorno de vista previa de base de datos mediante la AWS CLI, utilice el siguiente punto de conexión.

```
rds-preview.us-east-2.amazonaws.com
```

Para crear la instancia de base de datos de RDS para MySQL, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento AWS CLI en Creación de una instancia de base de datos.

API de RDS

Para crear una instancia de base de datos en el entorno de vista previa de base de datos mediante la API de RDS, utilice el siguiente punto de conexión.

```
rds-preview.us-east-2.amazonaws.com
```

Para crear la instancia de base de datos de RDS para MySQL, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento API de RDS en Creación de una instancia de base de datos.

MySQL versión 8.4 en el entorno de vista previa de bases de datos

MySQL versión 8.4 ya está disponible en el entorno de vista previa de bases de datos de Amazon RDS. MySQL versión 8.4 es la versión LTS más reciente de la comunidad, y contiene varias mejoras que se describen en Changes in MySQL 8.4.0. Puede usar el entorno de vista previa de bases de datos para probar sus cargas de trabajo con respecto a esta versión antes de que esté disponible en todas las Regiones de AWS para las cargas de trabajo de producción.

La versión 8.4 de MySQL en el entorno de vista previa de bases de datos puede diferir de la versión que Amazon RDS publica en todas las Regiones de AWS para cargas de trabajo de producción. En la siguiente lista, se incluyen las características que podrían cambiar. Esta lista no es exhaustiva.

- Definición del grupo de parámetros de RDS para MySQL 8.4. Por ejemplo, Amazon RDS podría añadir o eliminar parámetros, cambiarles el nombre o modificar sus valores predeterminados.
- El modelo de privilegios.
- La biblioteca TLS.

Para obtener información acerca del entorno de vista previa de base de datos, consulte the section called “ El entorno de vista previa de bases de datos”. Para acceder al entorno de vista previa desde la consola, seleccione https://console.aws.amazon.com/rds-preview/.

MySQL versión 8.3 en el entorno de vista previa de bases de datos

MySQL versión 8.3 ya está disponible en el entorno de vista previa de bases de datos de Amazon RDS. MySQL versión 8.3 contiene varias mejoras que se describen en Changes in MySQL 8.3.0.

Para obtener información acerca del entorno de vista previa de base de datos, consulte the section called “ El entorno de vista previa de bases de datos”. Para acceder al entorno de vista previa desde la consola, seleccione https://console.aws.amazon.com/rds-preview/.

MySQL versión 8.2 en el entorno de vista previa de bases de datos

MySQL versión 8.2 ya está disponible en el entorno de vista previa de bases de datos de Amazon RDS. MySQL versión 8.2 contiene varias mejoras que se describen en Changes in MySQL 8.2.0.

Para obtener información acerca del entorno de vista previa de base de datos, consulte the section called “ El entorno de vista previa de bases de datos”. Para acceder al entorno de vista previa desde la consola, seleccione https://console.aws.amazon.com/rds-preview/.

MySQL versión 8.1 en el entorno de vista previa de base de datos

MySQL versión 8.1 ya está disponible en el entorno de vista previa de bases de datos de Amazon RDS. MySQL versión 8.1 contiene varias mejoras que se describen en Changes in MySQL 8.1.0.

Para obtener información acerca del entorno de vista previa de base de datos, consulte the section called “ El entorno de vista previa de bases de datos”. Para acceder al entorno de vista previa desde la consola, seleccione https://console.aws.amazon.com/rds-preview/.

Versiones obsoleta para Amazon RDS for MySQL

Las versiones 5.1 y 5.5 y 5.6 Amazon RDS para MySQL están obsoletas.

Para obtener información sobre la política de obsolescencia de Amazon RDS for MySQL, consulte las preguntas frecuentes sobre Amazon RDS.

Conexión a la instancia de base de datos de MySQL

Antes de conectar a una instancia de base de datos que ejecute el motor de base de datos MySQL, debe crear a una instancia de base de datos. Para obtener información, consulte Creación de una instancia de base de datos de Amazon RDS. Después de que Amazon RDS aprovisione una instancia de base de datos, puede usar cualquier utilidad o aplicación cliente estándar de MySQL para conectarse a la instancia. En la cadena de conexión, especifique la dirección DNS del punto de enlace de la instancia de base de datos como parámetro del host y especifique el número de puerto del punto de enlace de la instancia de base de datos como parámetro del puerto.

Para autenticarse en la instancia de base de datos de RDS, puede usar uno de los métodos de autenticación de MySQL y la autenticación de base de datos AWS Identity and Access Management (IAM).

- Para conocer el procedimiento para autenticarse en MySQL usando uno de los métodos de autenticación de MySQL, consulte Authentication Method en la documentación de MySQL.
- Para conocer el procedimiento de autenticación en MySQL mediante la autenticación de base de datos de IAM, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

Puede conectarse a una instancia de base de datos de MySQL con herramientas como la utilidad de línea de comandos de MySQL. Para obtener más información sobre el uso de la utilidad de línea de comandos d MySQL, consulte mysql - the MySQL command-line client en la documentación de MySQL. MySQL Workbench es una de las aplicaciones basadas en interfaz gráfica de usuario (GUI) que puede utilizar para conectarse. Para obtener más información, consulte la página Download MySQL Workbench. Para obtener información sobre la instalación de MySQL (incluida la utilidad de línea de comandos de MySQL), consulte Installing and upgrading MySQL (Instalación y actualización de MySQL).

Para conectarse a una instancia de base de datos desde fuera de su Amazon VPC, la instancia de base de datos debe ser accesible públicamente, el acceso debe concederse mediante las reglas entrantes del grupo de seguridad de la instancia de base de datos y deben cumplirse otros requisitos. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Puede utilizar el cifrado de la capa de sockets seguros (SSL) o de la seguridad de la capa de transporte (TLS) en las conexiones a una instancia de base de datos MySQL. Para obtener más

información, consulta Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS. Si está utilizando la autenticación de base de datos AWS Identity and Access Management (IAM), asegúrese de utilizar una conexión SSL/TLS. Para obtener información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

También puede conectarse a una instancia de base de datos desde un servidor web. Para obtener más información, consulte Explicación: crear un servidor web y una instancia de base de datos de Amazon RDS.

> **Note**
>
> Para obtener más información acerca de la conexión a una instancia de base de datos de MariaDB, consulte Conexión a la instancia de base de datos de MariaDB.

Para buscar una instancia de base de datos de RDS para MySQL y conectarse a ella, consulte los temas siguientes.

Temas

- Búsqueda de información de conexión para una instancia de base de datos RDS para MySQL
- Instalación de cliente de línea de comandos de MySQL
- Conexión desde la utilidad de línea de comandos de MySQL (sin cifrar)
- Conexión desde MySQL Workbench
- Conexión a RDS para MySQL con el controlador JDBC de AWS, el controlador Python de AWS y el controlador ODBC de AWS para MySQL
- Solución de problemas de conexiones a la instancia de base de datos MySQL

Búsqueda de información de conexión para una instancia de base de datos RDS para MySQL

La información de conexión de una instancia de base de datos incluye su punto de enlace, puerto y un usuario de base de datos válido, como el usuario maestro. Por ejemplo, supongamos que un valor de punto de enlace es `mydb.123456789012.us-east-1.rds.amazonaws.com`. En este caso, el valor del puerto es `3306` y el usuario de la base de datos es `admin`. Dada esta información, se especifican los siguientes valores en una cadena de conexión:

- Para nombre de host o host o nombre DNS, especifique `mydb.123456789012.us-east-1.rds.amazonaws.com`.
- Para el puerto, especifique `3306`.
- Para el usuario, especifique `admin`.

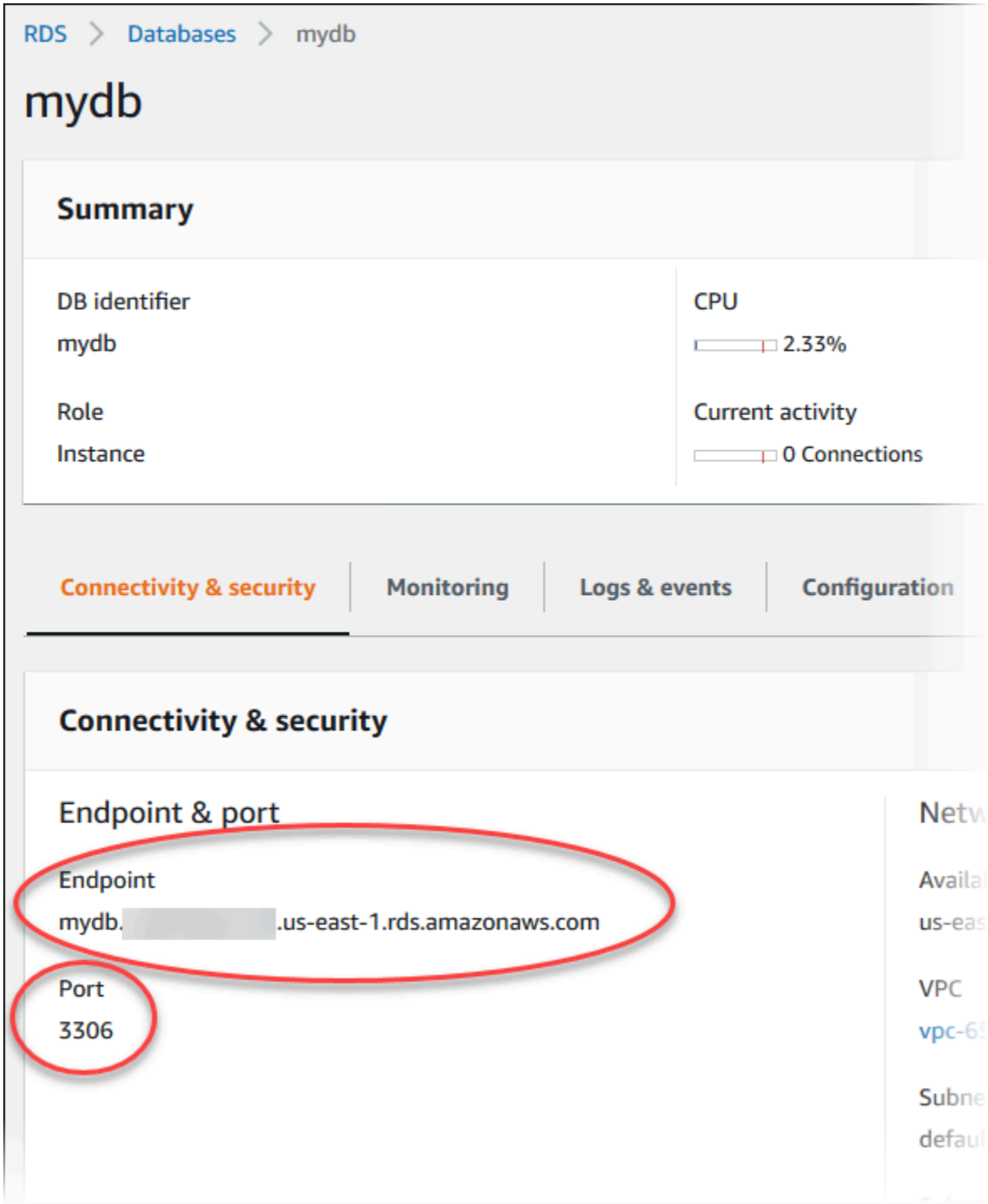
Para conectarse a una instancia de base de datos, utilice cualquier cliente para un motor de base de datos de MySQL. Por ejemplo, puede usar la utilidad de línea de comandos de MySQL o MySQL Workbench.

Para buscar la información de conexión de una instancia de base de datos, puede utilizar la AWS Management Console, el comando de AWS CLI describe-db-instances o la operación de la API de Amazon RDS DescribeDBInstances para enumerar sus detalles.

Consola

Para buscar la información de conexión para una instancia de base de datos en AWS Management Console

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) para ver una lista de las instancias de base de datos.
3. Seleccione el nombre de la instancia de base de datos MySQL para ver sus detalles.
4. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



5. Si necesita encontrar el nombre de usuario maestro, elija la ficha Configuration (Configuración) y vea el valor de Master username (Nombre de usuario maestro) .

AWS CLI

Para encontrar la información de conexión para una instancia de base de datos MySQL llame el AWS CLIcomando describe-db-instances. En la llamada, consulte el ID de instancia de base de datos, el punto de enlace, el puerto y el nombre de usuario maestro.

Para Linux, macOS o Unix:

```
aws rds describe-db-instances \
  --filters "Name=engine,Values=mysql" \
  --query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

Para Windows:

```
aws rds describe-db-instances ^
  --filters "Name=engine,Values=mysql" ^
  --query "*[].[DBInstanceIdentifier,Endpoint.Address,Endpoint.Port,MasterUsername]"
```

El resultado debería ser similar al siguiente.

```
[
    [
        "mydb1",
        "mydb1.123456789012.us-east-1.rds.amazonaws.com",
        3306,
        "admin"
    ],
    [
        "mydb2",
        "mydb2.123456789012.us-east-1.rds.amazonaws.com",
        3306,
        "admin"
    ]
]
```

API de RDS

Para buscar la información de conexión de una instancia de base de datos mediante la API Amazon RDS, llame a la operación DescribedBInstances . En el resultado, busque los valores de la dirección del punto de enlace, el puerto del punto de enlace y el nombre de usuario maestro.

Instalación de cliente de línea de comandos de MySQL

La mayoría de las distribuciones de Linux incluyen el cliente MariaDB en lugar del cliente Oracle MySQL. Para instalar el cliente de línea de comandos de MySQL en Amazon Linux 2023, ejecute el siguiente comando:

```
sudo dnf install mariadb105
```

Para instalar el cliente de línea de comandos de MySQL en Amazon Linux 2, ejecute el siguiente comando:

```
sudo yum install mariadb
```

Para instalar la utilidad de línea de comandos de MySQL en la mayoría de las distribuciones Linux basadas en DEB, ejecute el siguiente comando:

```
apt-get install mariadb-client
```

Para verificar la versión de la utilidad de línea de comandos de MySQL, ejecute el siguiente comando:

```
mysql --version
```

Para leer la documentación de MySQL de la versión actual del cliente, ejecute el siguiente comando:

```
man mysql
```

Conexión desde la utilidad de línea de comandos de MySQL (sin cifrar)

> **Important**
>
> Utilice sólo una conexión MySQL sin cifrar cuando el cliente y el servidor están en la misma VPC y la red es de confianza. Para obtener información sobre el uso de de conexiones cifradas, consulte Conexión a la instancia de base de datos de MySQL en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado).

Para conectarse a una instancia de base de datos mediante la utilidad de línea de comandos de MySQL, ingrese el siguiente comando en un símbolo del sistema. Para el parámetro -h, escriba el nombre de DNS (punto de enlace) de la instancia de base de datos. Para el parámetro -P, utilice el puerto de la instancia de base de datos. Para el parámetro -u, sustituya el nombre de usuario de un usuario de base de datos válido, como el usuario maestro. Escriba la contraseña del usuario maestro cuando se le pida.

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com -P 3306 -
u mymasteruser -p
```

Una vez especificada la contraseña del usuario, debería ver un resultado similar al siguiente.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9738
Server version: 8.0.28 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Conexión desde MySQL Workbench

Para conectar desde MySQL Workbench

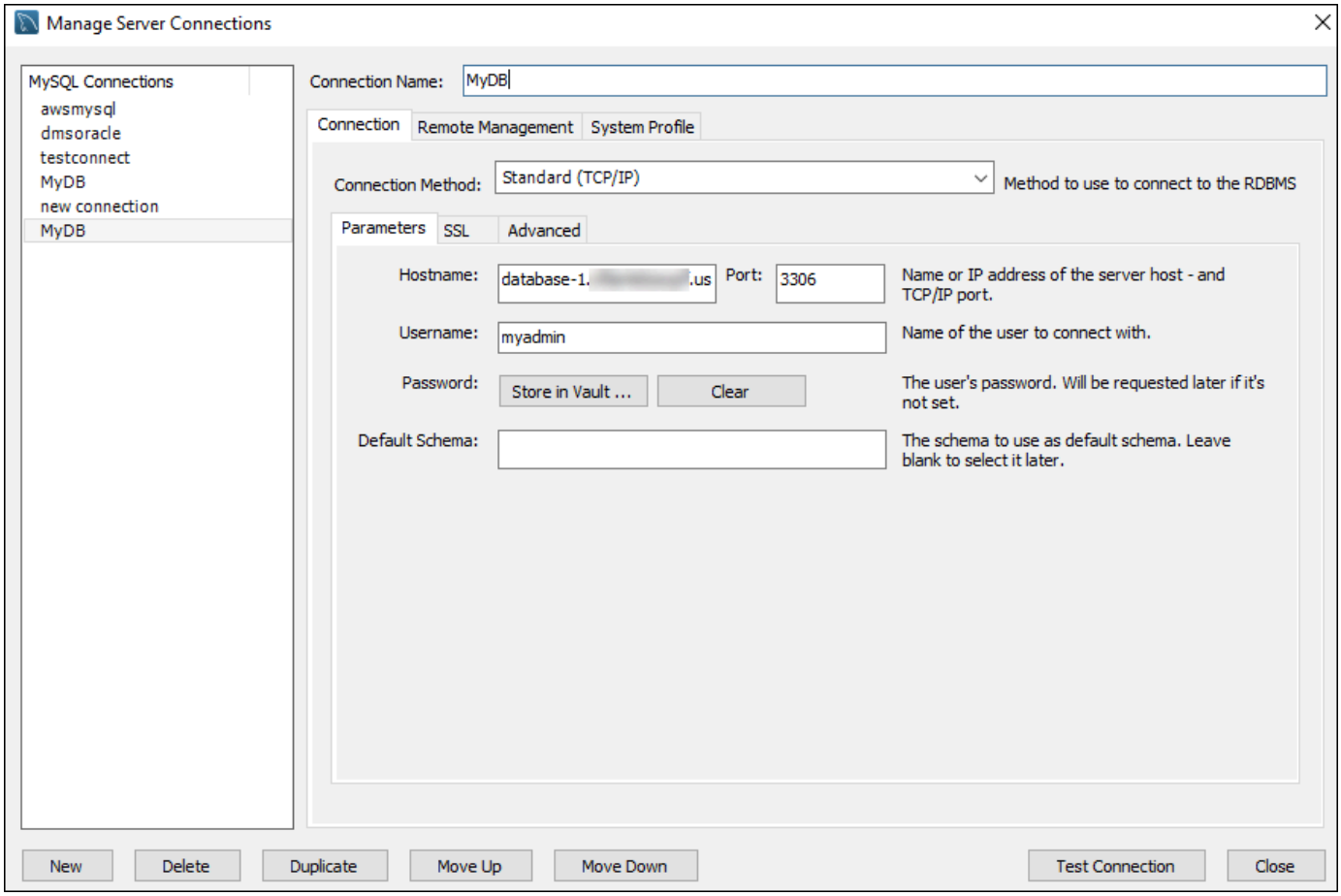
1. Descargue e instale MySQL Workbench en Download MySQL Workbench (Descargar MySQL Workbench).
2. Abra MySQL Workbench.



3. En Database (Base de datos), elija Manage Connections (Administrar conexiones).
4. En la ventana Manage Server Connections (Administrar conexiones de servidores) , elija New (Nueva).
5. En la ventana Connect to Database (Conectar a base de datos), introduzca la información siguiente:

   - Stored Connection (Conexión almacenada): escriba un nombre para la conexión, como por ejemplo **`MyDB`**.
   - Hostname (Nombre de host): escriba el punto de enlace de instancia de base de datos.
   - Port (Puerto): escriba el puerto utilizado por la instancia de base de datos.
   - Username (Nombre de usuario)–: escriba el nombre de usuario de base de datos válido, como el usuario maestro.
   - Password (Contraseña): opcionalmente, elija Store in Vault (Guardar en almacén) y escriba y guarde la contraseña del usuario.

   La ventana tendrá un aspecto similar al siguiente.



Puede utilizar las características de MySQL Workbench para personalizar las conexiones. Por ejemplo, puede utilizar la pestaña SSL para configurar las conexiones SSL/TLS. Para obtener información sobre el uso de MySQL Workbench, consulte la documentación de MySQL Workbench. Cifrado de conexiones de cliente con las instancias de base de datos MySQL con SSL/TLS; consulte Cifrado de conexiones de cliente con SSL/TLS a instancias de base de datos de MySQL en Amazon RDS.

6. Opcionalmente, elija Test Connection (Conexión de prueba) para confirmar que la conexión a la instancia de base de datos es correcta.
7. Elija Close.
8. En Database (Base de datos), elija Connect to Database (Conectar a base de datos).
9. En Stored Connection (Conexión almacenada), elija la conexión.
10. Seleccione OK.

Conexión a RDS para MySQL con el controlador JDBC de AWS, el controlador Python de AWS y el controlador ODBC de AWS para MySQL

Conéctese a las instancias de bases de datos de RDS para MySQL con el controlador JDBC de AWS, el controlador Python de AWS y el controlador ODBC de AWS para MySQL. Para obtener más información, consulte los siguientes temas.

Temas

- Conexión a RDS para MySQL con el controlador JDBC de Amazon Web Services (AWS)
- Conexión a RDS para MySQL con el controlador de Python de Amazon Web Services (AWS)
- Conexión a RDS para MySQL con el controlador ODBC de Amazon Web Services (AWS) para MySQL

Conexión a RDS para MySQL con el controlador JDBC de Amazon Web Services (AWS)

El controlador JDBC de Amazon Web Services (AWS) se ha diseñado como un contenedor JDBC avanzado. Este contenedor complementa y amplía la funcionalidad del controlador JDBC existente. El controlador se admite con el controlador Connector/J de la comunidad MySQL y el controlador Connector/J de la comunidad MariaDB.

Para instalar el controlador JDBC de AWS, añada el archivo .jar del controlador JDBC de AWS (ubicado en la aplicación `CLASSPATH`) y conserve las referencias al controlador de la comunidad correspondiente. Actualice el prefijo de la URL de conexión correspondiente de la siguiente manera:

- De `jdbc:mysql://` a `jdbc:aws-wrapper:mysql://`
- De `jdbc:mariadb://` a `jdbc:aws-wrapper:mariadb://`

Para obtener más información sobre el controlador JDBC de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador JDBC de Amazon Web Services (AWS).

Conexión a RDS para MySQL con el controlador de Python de Amazon Web Services (AWS)

El controlador de Python de Amazon Web Services (AWS) se ha diseñado como un contenedor Python avanzado. Este contenedor complementa y amplía la funcionalidad del controlador de Psycopg de código abierto. El controlador de Python de AWS se admite con las versiones 3.8 y

posteriores de Python. Puede instalar el paquete de `aws-advanced-python-wrapper` mediante el comando `pip`, junto con los paquetes de código abierto de `psycopg`.

Para obtener más información sobre el controlador de Python de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador de Python de Amazon Web Services (AWS).

Conexión a RDS para MySQL con el controlador ODBC de Amazon Web Services (AWS) para MySQL

El controlador ODBC de AWS para MySQL es un controlador de cliente diseñado para la alta disponibilidad de RDS para MySQL. El controlador puede existir junto con el conector MySQL/controlador ODBC y es compatible con los mismos flujos de trabajo.

Para obtener más información sobre el controlador ODBC de AWS para MySQL e instrucciones completas para instalarlo y utilizarlo, consulte el repositorio GitHub del controlador ODBC de Amazon Web Services (AWS) para MySQL.

Solución de problemas de conexiones a la instancia de base de datos MySQL

Hay dos causas frecuentes de errores de conexión a una nueva instancia de base de datos:

- La instancia de base de datos se creó usando un grupo de seguridad que no autoriza las conexiones desde el dispositivo o la instancia Amazon EC2 en los que se está ejecutando la utilidad o la aplicación de MySQL. La instancia de base de datos debe tener un grupo de seguridad de VPC que autorice las conexiones. Para obtener más información, consulte VPC de Amazon y Amazon RDS.

  Puede añadir o editar una regla de entrada en el grupo de seguridad. Para Source (Origen), elija My IP (Mi IP). Esto permite el acceso a la instancia de base de datos desde la dirección IP detectada en su navegador.
- La instancia de base de datos se creó con el puerto predeterminado 3306, y su compañía tiene reglas de firewall que bloquean las conexiones a ese puerto desde los dispositivos de la red de la organización. Para solucionar este error, vuelva a crear la instancia con un puerto diferente.

Para obtener más información sobre problemas de conexión, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Protección de las conexiones de instancias de base de datos MySQL

Puede implementar medidas de seguridad sólidas para proteger las instancias de base de datos de MySQL del acceso no autorizado y las posibles amenazas. Los grupos de seguridad, el cifrado SSL/TLS y la autenticación de bases de datos de IAM funcionan juntos para crear varias capas de seguridad de conexión para las instancias de base de datos de MySQL. Estos controles de seguridad le ayudan a cumplir los requisitos de conformidad, evitar filtraciones de datos y mantener canales de comunicación seguros entre las aplicaciones y las bases de datos. Puede proteger las instancias de base de datos de MySQL cifrando los datos en tránsito, restringiendo el acceso a rangos de IP específicos y gestionando la autenticación de los usuarios mediante roles de IAM en lugar de contraseñas de bases de datos.

La seguridad de las instancias de bases de datos de MySQL se administra en tres niveles:

- AWS Identity and Access Management controla quién puede realizar acciones de administración de Amazon RDS en las instancias de base de datos. Cuando se conecta a AWS con credenciales de IAM, la cuenta de IAM debe tener políticas de IAM que concedan los permisos necesarios para realizar operaciones de administración de Amazon RDS. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.
- Al crear una instancia de base de datos, se usa un grupo de seguridad de VPC para controlar qué dispositivos e instancias de Amazon EC2 pueden abrir conexiones al punto de conexión y al puerto de la instancia de base de datos. Estas conexiones se pueden establecer mediante la capa de sockets seguros (SSL) y la seguridad de la capa de transporte (TLS). Además, las reglas del firewall de su compañía pueden controlar si los dispositivos que se ejecutan en ella pueden abrir conexiones a la instancia de base de datos.
- Para autenticar el inicio de sesión y los permisos de una instancia de base de datos de MySQL, puede utilizar cualquiera de los siguientes enfoques o una combinación de ellos:
  - Puede seguir el mismo procedimiento que con una instancia independiente de MySQL. Los comandos como `CREATE USER`, `RENAME USER`, `GRANT`, `REVOKE` y `SET PASSWORD` funcionan de la misma forma que en las bases de datos locales, al igual que la modificación directa de las tablas de los esquemas de las bases de datos. Sin embargo, modificar directamente las tablas del esquema de la base de datos no es una práctica recomendada y, a partir de la versión 8.0.36 de RDS para MySQL, no se admite. Para obtener más información, consulte Access Control and Account Management en la documentación de MySQL.

- También puede utilizar la autenticación de base de datos de IAM. Si se utiliza la autenticación de bases de datos de IAM, la autenticación en la instancia de base de datos se realiza mediante un usuario o un rol de IAM y un token de autenticación. Un token de autenticación es un valor único que se genera utilizando el proceso de firma Signature Version 4. Mediante la autenticación de base de datos de IAM, puede utilizar las mismas credenciales para controlar el acceso a AWS los recursos y a las bases de datos. Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.
- Otra opción es la autenticación Kerberos para RDS para MySQL. La instancia de base de datos funciona con AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) para habilitar la autenticación Kerberos. Cuando los usuarios se autentican con una instancia de base de datos MySQL unida al dominio de confianza, las solicitudes de autenticación se reenvían. Las solicitudes reenviadas van al directorio de dominio con el que crea AWS Directory Service. Para obtener más información, consulte Uso de la autenticación de Kerberos para Amazon RDS para MySQL.

Cuando se crea una instancia de base de datos de Amazon RDS, el usuario maestro tiene los siguientes privilegios predeterminados:

Engine version (Versión del motor)	Privilegio del sistema	Rol de base de datos
RDS para MySQL versión 8.0 y versiones posteriores	`GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES ,INDEX, ALTER, SHOW DATABASES , CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, REPLICATION SLAVE , REPLICATION CLIENT , CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, EVENT, TRIGGER, CREATE ROLE, DROP ROLE, APPLICATION_PASSWORD_ADMIN , FLUSH_OPTIMIZER_COSTS , FLUSH_PRIVILEGES , FLUSH_STATUS , FLUSH_TABLES , FLUSH_USER_RESOURCES , ROLE_ADMIN , SENSITIVE_VARIABLE`	`rds_superuser_role` Para obtener más información acerca de `rds_superuser_role` , consulte Modelo de privilegios basado en roles de RDS para MySQL.

Engine version (Versión del motor)	Privilegio del sistema	Rol de base de datos
	`S_OBSERVER` , `SESSION_VARIABLES_ADMIN` , `SET_ANY_DEFINER` , `SHOW_ROUTINE` , `XA_RECOVER_ADMIN`	
RDS para MySQL versión 8. y versiones posteriores	`SELECT`, `INSERT`, `UPDATE`, `DELETE`, `CREATE`, `DROP`, `RELOAD`, `PROCESS`, `REFERENCES` , `INDEX`, `ALTER`, `SHOW DATABASES` , `CREATE TEMPORARY TABLES`, `LOCK TABLES`, `EXECUTE`, `REPLICATION SLAVE`, `REPLICATION CLIENT` , `CREATE VIEW`, `SHOW VIEW`, `CREATE ROUTINE`, `ALTER ROUTINE`, `CREATE USER`, `EVENT`, `TRIGGER`, `CREATE ROLE`, `DROP ROLE`, `APPLICATION_PASSWORD_ADMIN` , `ROLE_ADMIN` , `SET_USER_ID` , `XA_RECOVER_ADMIN`	`rds_superuser_role` Para obtener más información acerca de `rds_superuser_role` , consulte Modelo de privilegios basado en roles de RDS para MySQL.
Versiones de RDS para MySQL anteriores a 8.0.36	`SELECT`, `INSERT`, `UPDATE`, `DELETE`, `CREATE`, `DROP`, `RELOAD`, `PROCESS`, `REFERENCES` , `INDEX`, `ALTER`, `SHOW DATABASES` , `CREATE TEMPORARY TABLES`, `LOCK TABLES`, `EXECUTE`, `REPLICATION CLIENT` , `CREATE VIEW`, `SHOW VIEW`, `CREATE ROUTINE`, `ALTER ROUTINE`, `CREATE USER`, `EVENT`, `TRIGGER`, `REPLICATION SLAVE`	Ninguno

> **Note**
>
> Aunque es posible eliminar el usuario maestro de la instancia de base de datos, no se recomienda. Para volver a crear el usuario maestro, utilice la operación ModifyDBInstance de la API de RDS o ejecute el comando modify-db-instance de la AWS CLI y especifique una nueva contraseña del usuario maestro con el parámetro apropiado. Si no existe el usuario maestro en la instancia, se crea con la contraseña especificada.

Para proporcionar servicios de administración para cada instancia de base de datos, se crea el usuario `rdsadmin` al crear la instancia de base de datos. Al intentar eliminar, cambiar de nombre, cambiar la contraseña o cambiar los privilegios de la cuenta `rdsadmin`, se producirá un error.

Para permitir la administración de la instancia de base de datos, los comandos estándar `kill` y `kill_query` se han restringido. Se proporcionan los comandos de Amazon RDS `rds_kill` y `rds_kill_query` para permitir finalizar las sesiones de usuario o las consultas en las instancias de bases de datos.

Validación de contraseñas de RDS para MySQL

MySQL proporciona el complemento `validate_password` para ofrecer una seguridad mejorada. El complemento aplica políticas de contraseña mediante parámetros en el grupo de parámetros de base de datos para su instancia de base de datos de MySQL. El complemento es compatible con instancias de base de datos que ejecutan las versiones 5.7, 8.0 y 8.4 de MySQL. Para obtener más información sobre el complemento `validate_password`, consulte The Password Validation Plugin en la documentación de MySQL.

Habilitación del complemento **`validate_password`** para una instancia de base de datos de MySQL

1. Conéctese a la instancia de MySQL DB y ejecute el siguiente comando.

   ```
   INSTALL PLUGIN validate_password SONAME 'validate_password.so';
   ```

2. Configure los parámetros para el complemento en el grupo de parámetros de base de datos que utiliza la instancia de base de datos.

   Para obtener más información sobre los parámetros, consulte Opciones del complemento de validación de contraseñas y variables en la documentación de MySQL.

   Para obtener información sobre cómo modificar los parámetros de la instancia de base de datos, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

3. Reinicie la instancia de base de datos.

Después de habilitar el complemento `validate_password`, restablezca las contraseñas existentes para cumplir con las nuevas políticas de validación.

Amazon RDS no valida contraseñas. La instancia de base de datos de MySQL DB realiza la validación de contraseñas. Si establece una contraseña de usuario con la AWS Management Console, el comando de la `modify-db-instance` AWS CLI o la operación de la API de RDS `ModifyDBInstance`, puede realizarse el cambio correctamente incluso si la nueva contraseña no cumple con las políticas de contraseña. Sin embargo, se establece una nueva contraseña en la instancia de base de datos de MySQL solo si cumple las políticas de contraseña. En ese caso, Amazon RDS registra el siguiente evento.

```
   "RDS-EVENT-0067" - An attempt to reset the master password for the DB instance has
failed.
```

Para obtener más información acerca de los eventos de Amazon RDS, consulte Uso de notificaciones de eventos de Amazon RDS.

Cifrado de conexiones de cliente con SSL/TLS a instancias de base de datos de MySQL en Amazon RDS

La capa de conexión segura (SSL) es un protocolo estándar del sector que se utiliza para proteger las conexiones de red entre el cliente y el servidor. Después de la versión 3.0 de SSL, el nombre se cambió por seguridad de la capa de transporte (TLS). Amazon RDS admite el cifrado SSL/TLS para las instancias de base de datos MySQL. Con SSL/TLS puede cifrar una conexión entre el cliente de la aplicación y la instancia de base de datos MySQL. La compatibilidad con SSL/TLS está disponible en todas las Regiones de AWS para MySQL.

Con Amazon RDS, puede proteger los datos en tránsito cifrando las conexiones de los clientes a las instancias de base de datos de MySQL con SSL/TLS, exigiendo el uso de SSL/TLS para todas las conexiones a una instancia de base de datos de MySQL y conectándose desde el cliente de línea de comandos de MySQL con SSL/TLS (cifrado). En las siguientes secciones, se proporciona orientación sobre la configuración y el uso del cifrado SSL para las instancias de base de datos de MySQL en Amazon RDS.

Temas

- Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS
- Necesidad de uso de SSL/TLS para cuentas de usuario específicas en una instancia de base de datos de MySQL en Amazon RDS

- Necesidad de uso de SSL/TLS para todas las conexiones a una instancia de base de datos de MySQL en Amazon RDS
- Conexión a la instancia de base de datos de MySQL en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado)

Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS

Amazon RDS crea un certificado de SSL/TLS e instala el certificado en la instancia de base de datos cuando Amazon RDS aprovisiona la instancia. Estos certificados están firmados por una autoridad de certificación. El certificado SSL/TLS incluye el punto de enlace de la instancia de base de datos como nombre común (CN) que el certificado de SSL/TLS debe proteger frente a los ataques de suplantación.

Un certificado SSL/TLS creado por Amazon RDS es la entidad raíz de confianza y debería funcionar en la mayoría de los casos, pero podría fallar si la aplicación no acepta cadenas de certificados. Si la aplicación no acepta cadenas de certificados, intente utilizar un certificado intermedio para conectarse a la Región de AWS. Por ejemplo, debe utilizar un certificado intermedio para conectarse a las regiones de AWS GovCloud (US) con SSL/TLS.

Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener más información acerca de cómo usar SSL/TLS con MySQL, consulte Actualización de aplicaciones para la conexión a las instancias de base de datos de MySQL con los nuevos certificados SSL/TLS.

En el caso de MySQL versión 8.0 y anteriores, Amazon RDS para MySQL utiliza OpenSSL para garantizar las conexiones. Para la versión 8.4 y posteriores de MySQL, Amazon RDS para MySQL usa AWS-LC. La compatibilidad con TLS depende de la versión de MySQL. En la tabla siguiente se muestran la compatibilidad de TLS para versiones MySQL.

Versión de MySQL	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
MySQL 8.4	No admitido	No admitido	Soportado	Soportado
MySQL 8.0	No admitido	No admitido	Soportado	Soportado
MySQL 5.7	Soportado	Soportado	Soportado	No compatible

Necesidad de uso de SSL/TLS para cuentas de usuario específicas en una instancia de base de datos de MySQL en Amazon RDS

Puede exigir el uso del cifrado SSL/TLS para determinadas conexiones de cuentas de usuario a las instancias de base de datos de MySQL en Amazon RDS. Proteger la información confidencial del acceso o la interceptación no autorizados es fundamental para hacer cumplir las políticas de seguridad en los casos en los que la confidencialidad de los datos sea importante.

Para exigir el uso de conexiones SSL/TLS en determinadas cuentas de usuarios, utilice una de las siguientes instrucciones, en función de la versión de MySQL, para exigir conexiones SSL/TLS en la cuenta de usuario `encrypted_user`.

Para ello, utilice la siguiente instrucción.

```
ALTER USER 'encrypted_user'@'%' REQUIRE SSL;
```

Para obtener más información acerca de las conexiones SSL/TLS con MySQL, consulte Using Encrypted Connections (Uso de conexiones cifradas) en la documentación de MySQL.

Necesidad de uso de SSL/TLS para todas las conexiones a una instancia de base de datos de MySQL en Amazon RDS

Utilice el parámetro `require_secure_transport` para requerir que todas las conexiones de usuario a su instancia de base de datos de MySQL utilicen SSL/TLS. De forma predeterminada, el parámetro `require_secure_transport` está definido como `OFF`. Puede definir el parámetro `require_secure_transport` en `ON` (activado) para imponer SSL/TLS para las conexiones a la instancia de base de datos.

Puede definir el valor del parámetro `require_secure_transport` actualizando el grupo de parámetros de base de datos a su instancia de base de datos. No es necesario reiniciar la instancia de base de datos para que el cambio surta efecto.

Cuando el parámetro `require_secure_transport` se establece en `ON` para un clúster de base de datos, un cliente de base de datos puede conectarse a él si puede establecer una conexión cifrada. De lo contrario, se devuelve al cliente un mensaje de error similar al siguiente:

```
MySQL Error 3159 (HY000): Connections using insecure transport are prohibited while --
require_secure_transport=ON.
```

Para obtener información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Para obtener más información sobre el parámetro `require_secure_transport`, consulte la documentación de MySQL.

Conexión a la instancia de base de datos de MySQL en Amazon RDS con SSL/TLS desde el cliente de línea de comandos de MySQL (cifrado)

Los parámetros del programa `mysql` cliente varían ligeramente en función de la versión de MySQL o MariaDB que utilice.

Para saber qué versión tiene, ejecute el comando `mysql` con la opción de comando `--version`. En el ejemplo siguiente, el resultado muestra que el programa cliente es de MariaDB.

```
$ mysql --version
mysql  Ver 15.1 Distrib 10.5.15-MariaDB, for osx10.15 (x86_64) using readline 5.1
```

La mayoría de las distribuciones de Linux, como Amazon Linux, CentOS, SUSE y Debian han reemplazado MySQL por MariaDB, y la versión de `mysql` en ellos es de MariaDB.

Para conectarse a la instancia de base de datos mediante SSL/TLS, siga estos pasos:

Para conectarse a una instancia de base de datos mediante SSL/TLS con el cliente de la línea de comandos de MySQL

1. Descargue un certificado raíz que funcione para todas las Regiones de AWS.

   Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
2. Utilice un cliente de línea de comandos de MySQL para conectarse a una instancia de base de datos con cifrado SSL/TLS. Para el parámetro `-h`, escriba el nombre de DNS (punto de conexión) de la instancia de base de datos. Para el parámetro `--ssl-ca`, sustituya el nombre del archivo de certificado SSL/TLS. Para el parámetro `-P`, sustituya el puerto de la instancia de base de datos. Para el parámetro `-u`, sustituya el nombre de usuario de un usuario de base de datos válido, como el usuario maestro. Escriba la contraseña del usuario maestro cuando se le pida.

   En el siguiente ejemplo, se muestra cómo lanzar un cliente con el parámetro `--ssl-ca` con el cliente MySQL 5.7 y versiones posteriores.

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-bundle.pem --ssl-mode=REQUIRED -P 3306 -u myadmin -p
```

Para exigir que la conexión SSL/TLS verifique el punto de conexión de la instancia de la base de datos en el punto de conexión del certificado SSL/TLS, introduzca el siguiente comando:

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-bundle.pem --ssl-mode=VERIFY_IDENTITY -P 3306 -u myadmin -p
```

En el siguiente ejemplo, se muestra cómo lanzar un cliente con el parámetro `--ssl-ca` con el MariaDB.

```
mysql -h mysql-instance1.123456789012.us-east-1.rds.amazonaws.com --ssl-ca=global-bundle.pem --ssl -P 3306 -u myadmin -p
```

3. Escriba la contraseña del usuario maestro cuando se le pida.

Verá una salida similar a la siguiente.

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9738
Server version: 8.0.28 Source distribution

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Actualización de aplicaciones para la conexión a las instancias de base de datos de MySQL con los nuevos certificados SSL/TLS

El 13 de enero de 2023, Amazon RDS publicó nuevos certificados de entidades de certificación (CA) para la conexión a sus instancias de base de datos de RDS mediante la capa de sockets seguros o seguridad de la capa de transporte (SSL/TLS). Después, puede encontrar la información sobre la actualización de sus aplicaciones para utilizar los nuevos certificados.

Este tema puede ayudarle a determinar si las aplicaciones de cualquier cliente utilizan SSL/TLS para conectarse a sus instancias de base de datos. Si lo hacen, puede comprobar de manera adicional si esas aplicaciones precisan una verificación de certificados para conectarse.

> **Note**
>
> Algunas aplicaciones solo están configuradas para conectarse a las instancias de base de datos de MySQL solo si pueden verificar con éxito el certificado del servidor. Para esas aplicaciones, debe actualizar los almacenes de confianza de la aplicación de su cliente para incluir los nuevos certificados de CA.
>
> Puede especificar los siguientes modos SSL: `disabled`, `preferred` y `required`. Cuando utiliza el modo SSL `preferred` y el certificado de CA no existe o no está actualizado, la conexión vuelve a no utilizar SSL y se conecta sin cifrado.
>
> Recomendamos evitar el modo `preferred`. En modo `preferred`, si la conexión encuentra un certificado no válido, deja de usar el cifrado y continúa sin cifrar.

Después actualizar sus certificados de CA en los almacenes de confianza de la aplicación de su cliente, puede rotar los certificados en sus instancias de base de datos. Recomendamos encarecidamente probar estos procedimientos en un entorno de desarrollo o ensayo antes de implementarlos en sus entornos de producción.

Para obtener más información acerca de la rotación de certificados, consulte Rotar certificados SSL/TLS. Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener información sobre el uso de SSL/TLS con las instancias de base de datos de MySQL, consulte Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS.

Temas

- Determinación de si alguna aplicación se conecta a su instancia de base de datos de MySQL mediante SSL
- Determinación de si un cliente necesita una verificación de certificados para conectarse
- Actualización del almacén de confianza de su aplicación
- Ejemplo de código Java para el establecimiento de conexiones SSL

Determinación de si alguna aplicación se conecta a su instancia de base de datos de MySQL mediante SSL

Si utiliza Amazon RDS para MySQL versión 5.7, 8.0 u 8.4 y el esquema de rendimiento se activa, ejecute la siguiente consulta para comprobar si las conexiones utilizan SSL/TLS. Para obtener

información sobre la habilitación del esquema de rendimiento, consulte Inicio rápido del esquema de rendimiento en la documentación de MySQL.

```
mysql> SELECT id, user, host, connection_type
       FROM performance_schema.threads pst
       INNER JOIN information_schema.processlist isp
       ON pst.processlist_id = isp.id;
```

En estos resultados de ejemplo, puede ver que su propia sesión (`admin`) y una aplicación con sesión iniciada como `webapp1` utilizan SSL.

```
+----+-----------------+------------------+-----------------+
| id | user            | host             | connection_type |
+----+-----------------+------------------+-----------------+
|  8 | admin           | 10.0.4.249:42590 | SSL/TLS         |
|  4 | event_scheduler | localhost        | NULL            |
| 10 | webapp1         | 159.28.1.1:42189 | SSL/TLS         |
+----+-----------------+------------------+-----------------+
3 rows in set (0.00 sec)
```

Determinación de si un cliente necesita una verificación de certificados para conectarse

Puede comprobar si los cliente de JDBC y MySQL precisan la verificación de certificados para conectarse.

JDBC

El siguiente ejemplo con el conector de MySQL/J 8.0 muestra una manera de comprobar las propiedades de conexión de JDBC de una aplicación para determinar si las conexiones exitosas precisan un certificado válido. Para obtener más información sobre todas las opciones de conexión de JDBC para MySQL, consulte Propiedades de la configuración en la documentación de MySQL.

Al utilizar el conector de MySQL/J 8.0, una conexión requiere verificación con el certificado de servidor de base de datos si en sus propiedades de conexión se ha configurado `sslMode` en `VERIFY_CA` o `VERIFY_IDENTITY`, como en el siguiente ejemplo.

```
Properties properties = new Properties();
properties.setProperty("sslMode", "VERIFY_IDENTITY");
properties.put("user", DB_USER);
properties.put("password", DB_PASSWORD);
```

> **Note**
>
> Si utiliza MySQL Java Connector v5.1.38 o posterior, o MySQL Java Connector v8.0.9 o posterior para conectarse a sus bases de datos, incluso si no ha configurado explícitamente sus aplicaciones para usar SSL/TLS al conectarse a sus bases de datos, estos controladores cliente utilizan de forma predeterminada SSL/TLS. Además, al utilizar SSL/TLS, realizan una verificación parcial del certificado y producen un error al conectarse si el certificado del servidor de base de datos ha caducado.

MySQL

Los siguientes ejemplos con el cliente de MySQL muestran dos maneras de comprobar la conexión a MySQL de un script para determinar si las conexiones exitosas precisan un certificado válido. Para obtener más información sobre todas las opciones de conexión con el cliente de MySQL, consulte Configuración del lado del cliente para las conexiones cifradas en la documentación de MySQL.

Al utilizar el cliente de MySQL 5.7 o posterior, una conexión SSL precisa una verificación frente al certificado de CA del servidor si para la opción de `--ssl-mode` especifica `VERIFY_CA` o `VERIFY_IDENTITY`, como en el siguiente ejemplo.

```
mysql -h mysql-database.rds.amazonaws.com -uadmin -ppassword --ssl-ca=/tmp/ssl-cert.pem
 --ssl-mode=VERIFY_CA
```

Actualización del almacén de confianza de su aplicación

Para obtener información sobre la actualización del almacén de confianza para las aplicaciones de MySQL, consulte Instalación de certificados de SSL en la documentación de MySQL.

Para obtener información sobre la descarga del certificado raíz, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Para obtener secuencias de comandos de ejemplo que importan certificados, consulte Script de muestra para la importación de certificados en su almacén de confianza.

> **Note**
>
> Cuando actualice el almacén de confianza, puede retener certificados antiguos además de añadir los nuevos certificados.

Si utiliza el controlador de JDBC de MySQL en una aplicación, establezca las siguientes propiedades en la aplicación.

```
System.setProperty("javax.net.ssl.trustStore", certs);
System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

Cuando inicie la aplicación, establezca las siguientes propiedades.

```
java -Djavax.net.ssl.trustStore=/path_to_trust_store/MyTruststore.jks -
Djavax.net.ssl.trustStorePassword=my_trust_store_password com.companyName.MyApplication
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Ejemplo de código Java para el establecimiento de conexiones SSL

El siguiente ejemplo de código muestra cómo configurar la conexión SSL que valida el certificado del servidor mediante JDBC.

```
public class MySQLSSLTest {

        private static final String DB_USER = "username";
```

```
        private static final String DB_PASSWORD = "password";
        // This trust store has only the prod root ca.
        private static final String TRUST_STORE_FILE_PATH = "file-path-to-trust-store";
        private static final String TRUST_STORE_PASS = "trust-store-password";

        public static void test(String[] args) throws Exception {
            Class.forName("com.mysql.jdbc.Driver");

            System.setProperty("javax.net.ssl.trustStore", TRUST_STORE_FILE_PATH);
            System.setProperty("javax.net.ssl.trustStorePassword", TRUST_STORE_PASS);

            Properties properties = new Properties();
            properties.setProperty("sslMode", "VERIFY_IDENTITY");
            properties.put("user", DB_USER);
            properties.put("password", DB_PASSWORD);


            Connection connection = null;
            Statement stmt = null;
            ResultSet rs = null;
            try {
                connection =
 DriverManager.getConnection("jdbc:mysql://mydatabase.123456789012.us-
east-1.rds.amazonaws.com:3306",properties);
                stmt = connection.createStatement();
                rs=stmt.executeQuery("SELECT 1 from dual");
            } finally {
                if (rs != null) {
                    try {
                        rs.close();
                    } catch (SQLException e) {
                    }
                }
                if (stmt != null) {
                   try {
                        stmt.close();
                    } catch (SQLException e) {
                   }
                }
                if (connection != null) {
                    try {
                        connection.close();
                    } catch (SQLException e) {
                        e.printStackTrace();
```

```
                    }
                }
            }
            return;
        }
    }
```

> **Important**
>
> Después de que haya determinado que sus conexiones de base de datos utilizan SSL/TLS y haya actualizado el almacén de confianza de su aplicación, puede actualizar su base de datos para que utilice los certificados de rds-ca-rsa2048-g1. Para obtener instrucciones, consulte el paso 3 en Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos.
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Uso de la autenticación de Kerberos para Amazon RDS para MySQL

Puede usar la autenticación Kerberos para autenticar a los usuarios cuando estos se conecten a su instancia de base de datos de MySQL. La instancia de base de datos funciona con AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) para habilitar la autenticación Kerberos. Cuando los usuarios se autentican con una instancia de base de datos MySQL unida al dominio de confianza, las solicitudes de autenticación se reenvían. Las solicitudes reenviadas van al directorio de dominio con el que crea AWS Directory Service.

Mantener todas las credenciales en el mismo directorio puede ahorrarle tiempo y esfuerzo. Con este método, dispone de un lugar centralizado para almacenar y administrar credenciales de numerosas instancias de bases de datos. El uso de un directorio también puede mejorar su perfil de seguridad general.

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de Amazon RDS con autenticación Kerberos, consulte Regiones y motores de base de datos admitidos para autenticación de Kerberos en Amazon RDS.

Información general sobre la configuración de la autenticación Kerberos para instancias de base de datos MySQL

Para configurar la autenticación Kerberos para una instancia de base de datos de MySQL, complete los siguientes pasos generales, que se describen con más detalle más adelante:

1. Utilice AWS Managed Microsoft AD para crear un directorio de AWS Managed Microsoft AD. Puede utilizar la AWS Management Console, la AWS CLI o AWS Directory Service para crear el directorio. Para obtener más detalles sobre cómo hacerlo, consulte Creación de su directorio de AWS Managed Microsoft AD en la guía de administración de AWS Directory Service.
2. Cree un rol de AWS Identity and Access Management (IAM) que utilice la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. El rol permite a Amazon RDS realizar llamadas al directorio.

   Para que el rol permita el acceso, el punto de conexión AWS Security Token Service (AWS STS) debe activarse en la Región de AWS para su cuenta de AWS. Los puntos de conexión de AWS STS están activos de forma predeterminada en todas Regiones de AWS y puede usarlos sin ninguna acción posterior. Para obtener más información, consulte Activación y desactivación de AWS STS en una región de Región de AWS en la Guía del usuario de IAM.
3. Cree y configure usuarios en el directorio de AWS Managed Microsoft AD usando las herramientas de Microsoft Active Directory. Para obtener más información sobre la creación de usuarios en su Active Directory, consulte Administrar usuarios y grupos en AWS Managed Microsoft AD en la guía de administración de AWS Directory Service.
4. Cree o modifique una instancia de base de datos MySQL. Si utiliza la CLI o la API de RDS en la solicitud de creación, especifique un identificador de dominio con el parámetro `Domain`. Utilice el identificador `d-*` que se ha generado al crear el directorio y el nombre del rol que ha creado.

   Si modifica una instancia de base de datos MySQL ya existente para utilizar la autenticación Kerberos, establezca los parámetros de dominio y rol de IAM para la instancia de base de datos. Busque la instancia de base de datos en la misma VPC que el directorio de dominio.
5. Use las credenciales de usuario maestro de Amazon RDS para conectarse a la instancia de base de datos de MySQL. Cree el usuario en MySQL; para ello use la cláusula de `CREATE USER IDENTIFIED WITH 'auth_pam'`. Los usuarios que cree de esta manera pueden iniciar sesión en la instancia de base de datos MySQL con la autenticación Kerberos.

Configuración de la autenticación Kerberos para instancias de base de datos MySQL

Utilice AWS Managed Microsoft AD para configurar la autenticación Kerberos para una instancia de base de datos MySQL. Para configurar la autenticación Kerberos, siga los pasos que se indican a continuación:

Paso 1: crear un directorio con AWS Managed Microsoft AD

AWS Directory Service crea un directorio de Active Directory completamente administrado en la nube de AWS. Cuando crea un directorio de AWS Managed Microsoft AD, AWS Directory Service crea dos controladores de dominio y servidores del sistema de nombres de dominio (DNS) en su nombre. Los servidores de directorios se crean en diferentes subredes de una VPC. Esta redundancia ayuda a garantizar que su directorio permanezca accesible incluso si ocurre un error.

Cuando crea un directorio de AWS Managed Microsoft AD, AWS Directory Service realiza en su nombre las siguientes tareas:

- Configurar un Active Directory dentro de la VPC.
- Crea una cuenta de administrador para el directorio con el nombre de usuario Admin y la contraseña especificada. Esta cuenta le permite administrar el directorio.

  > **Note**
  >
  > Asegúrese de guardar esta contraseña. AWS Directory Service no la almacena. Es posible restablecerla, pero no recuperarla.

- Crea un grupo de seguridad para los controladores del directorio.

Al lanzar AWS Managed Microsoft AD, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa tiene el nombre de NetBIOS que escribió al crear el directorio y se encuentra en la raíz del dominio. La raíz del dominio es propiedad de , que también se encarga de su administració AWS.

La cuenta de administrador que se creó con el directorio AWS Managed Microsoft AD dispone de permisos para realizar las actividades administrativas más habituales para la unidad organizativa:

- Crear, actualizar o eliminar usuarios
- Añadir recursos a su dominio, como servidores de archivos o de impresión y, a continuación, asignar permisos para esos recursos a usuarios dentro de la unidad organizativa

- Crear unidades organizativas y contenedores adicionales
- Delegar autoridad
- Restaurar objetos eliminados de la papelera de reciclaje de Active Directory
- Ejecutar módulos de AD y DNS de Windows PowerShell en el servicio web de Active Directory

La cuenta de administrador también tiene derechos para realizar las siguientes actividades en todo el dominio:

- Administrar configuraciones DNS (agregar, quitar o actualizar registros, zonas y programas de envío).
- Ver logs de eventos DNS
- Ver logs de eventos de seguridad

Para crear un directorio con AWS Managed Microsoft AD

1. Inicie sesión en AWS Management Console y abra la consola de AWS Directory Service en https://console.aws.amazon.com/directoryservicev2/.
2. En el panel de navegación, elija Directories (Directorios) y, a continuación, Set up Directory (Configurar directorio).
3. Elija AWS Managed Microsoft AD. AWS Managed Microsoft AD es la única opción que puede usar actualmente con Amazon RDS.
4. Introduzca la información siguiente:

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo **`corp.example.com`**.

   Nombre NetBIOS del directorio

   El nombre abreviado del directorio, como **`CORP`**.

   Descripción del directorio

   (Opcional) Descripción del directorio.

   Contraseña de administrador

   Contraseña del administrador del directorio. El proceso de creación de directorios crea una cuenta de administrador con el nombre de usuario Admin y esta contraseña.

La contraseña del administrador del directorio no puede contener la palabra "admin".
La contraseña distingue entre mayúsculas y minúsculas y debe tener un mínimo de 864 caracteres y un máximo de 64. También debe contener al menos un carácter de tres de las siguientes categorías:

- Letras minúsculas (a–z)
- Letras mayúsculas (A–Z)
- Números (0–9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password

Vuelva a escribir la contraseña de administrador.

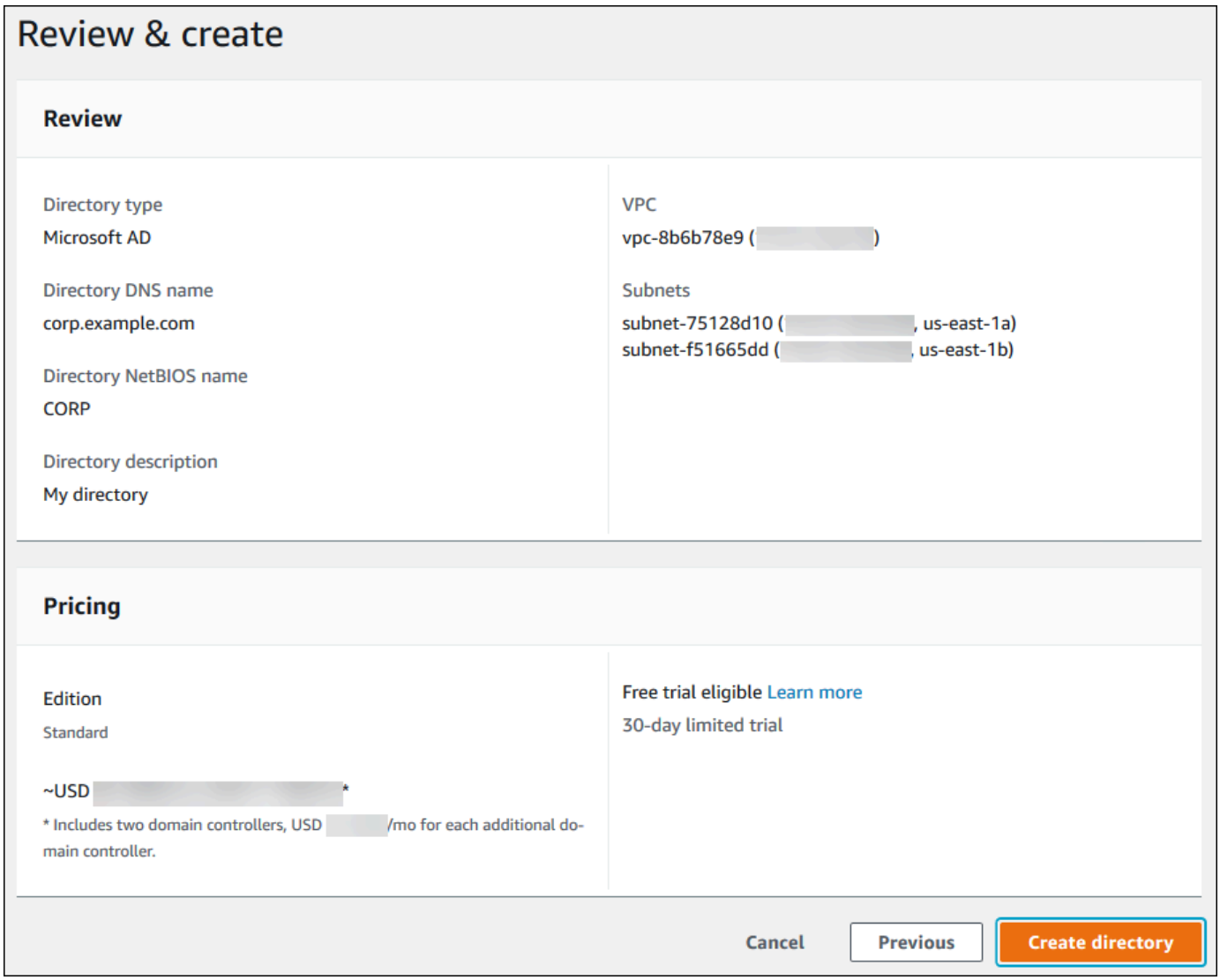
5. Elija Siguiente.
6. Escriba la siguiente información en la sección Networking (Redes) y luego seleccione Next (Siguiente):

   VPC

   VPC del directorio. Cree la instancia de base de datos MySQL en esta misma VPC.

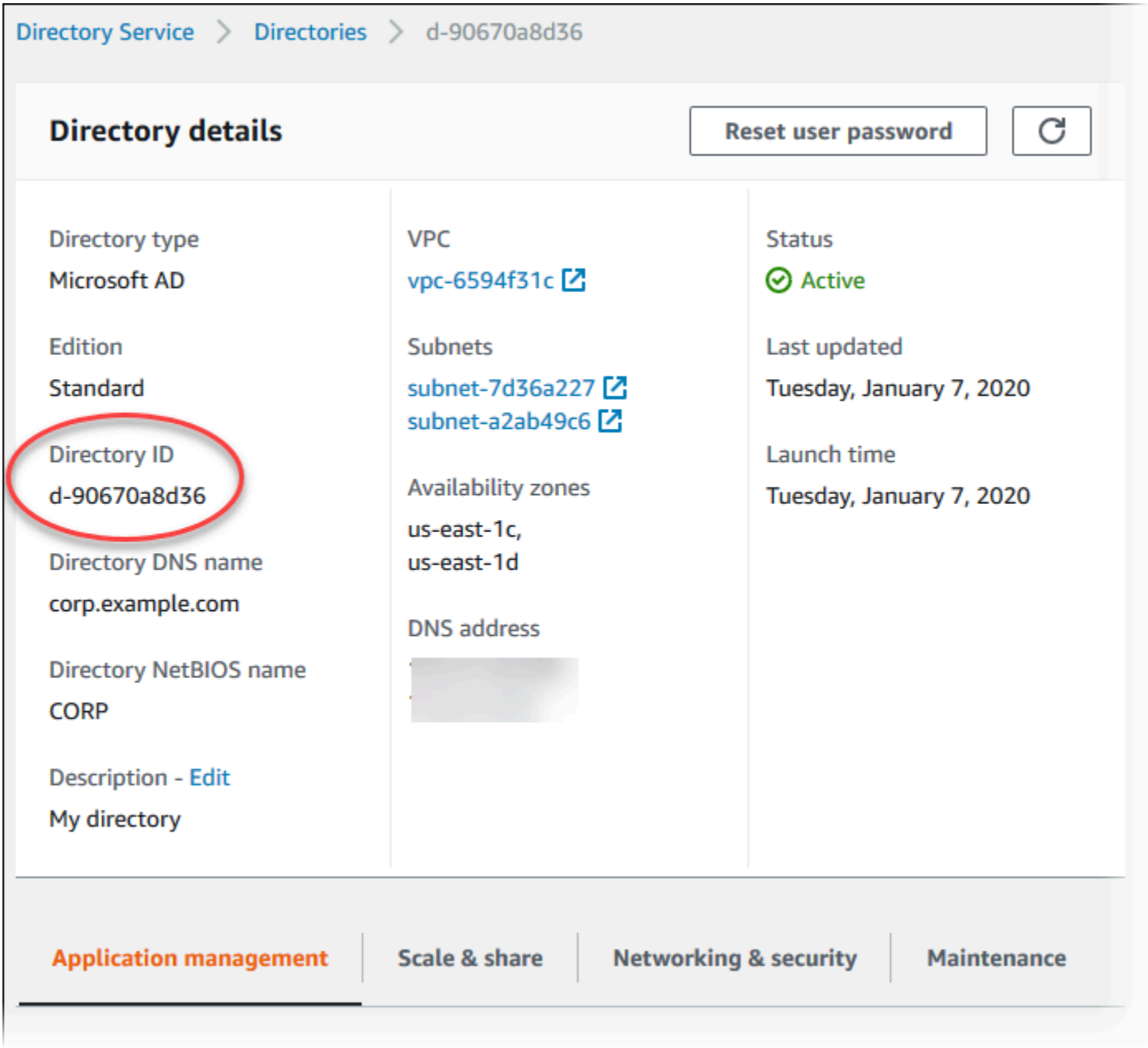
   Subredes

   Subredes de los servidores del directorio. Las dos subredes deben estar en diferentes zonas de disponibilidad.
7. Revise la información del directorio y haga los cambios necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio).



La creación del directorio tarda varios minutos. Cuando se haya creado correctamente, el valor de Status (Estado) cambiará a Active (Activo).

Para consultar información de su directorio, seleccione el nombre del directorio en la descripción de directorios. Tenga en cuenta el valor de Directory ID (ID de directorio) porque necesitará este valor cuando cree o modifique su instancia de base de datos MySQL.



Paso 2: crear el rol de IAM que usará Amazon RDS

Para que Amazon RDS llame a AWS Directory Service en su nombre, se precisa un rol de IAM que utilice la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. Este rol permite a Amazon RDS realizar llamadas a AWS Directory Service.

Cuando se crea una instancia de base de datos con la AWS Management Console y el usuario de la consola tiene el permiso `iam:CreateRole`, la consola crea este rol automáticamente. En este caso, el nombre del rol es `rds-directoryservice-kerberos-access-role`. De no ser así, debe

crear el rol de IAM manualmente. Cuando cree este rol de IAM, elija `Directory Service` y asocie la política administrada de AWS `AmazonRDSDirectoryServiceAccess` a este.

A fin de obtener más información acerca de la creación de roles de IAM para un servicio, consulte Creación de un rol para delegar permisos a un servicio de AWS en la guía del usuario de IAM.

> **Note**
>
> El rol de IAM utilizado para la autenticación de Windows en RDS para SQL Server no se puede usar en RDS para MySQL.

Opcionalmente, puede crear políticas con los permisos requeridos en vez de utilizar la política de IAM administrad `AmazonRDSDirectoryServiceAccess`. En este caso, el rol de IAM debe tener la siguiente política de confianza de IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El rol debe también tener la siguiente política de rol de IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Paso 3: crear y configurar usuarios

Puede crear usuarios con la herramienta Usuarios y equipos de Active Directory. Esta herramienta forma parte de las herramientas Active Directory Domain Services y Active Directory Lightweight Directory Services. Los usuarios representan a las personas físicas o entidades que tienen acceso al directorio.

Para crear usuarios en un directorio de AWS Directory Service, tiene que estar conectado a una instancia de Amazon EC2 basada en Microsoft Windows. Esta instancia tiene que ser miembro del directorio de AWS Directory Service y debe haber iniciado sesión como usuario con privilegios para crear usuarios. Para obtener más información, consulte Administrar usuarios y grupos de AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.

Paso 4: crear o modificar una instancia de base de datos MySQL

Cree o modifique una instancia de base de datos MySQL para usarla con su directorio. Puede utilizar la consola, CLI, o la API de RDS para asociar una instancia de base de datos con un directorio. Puede hacerlo de una de las siguientes formas:

- Cree una nueva instancia de base de datos de MySQL mediante la consola, el comando de la CLI create-db-instance o la operación CreateDBInstance de la API de RDS.

Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.

- Modifique una instancia de base de datos de MySQL existente mediante la consola, el comando de la CLI modify-db-instance o la operación ModifyDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.

- Restaure una instancia de base de datos de MySQL a partir de una instantánea de base de datos mediante la consola, el comando de la CLI restore-db-instance-from-db-snapshot o la operación RestoreDBInstanceFromDBSnapshot de la API de RDS.

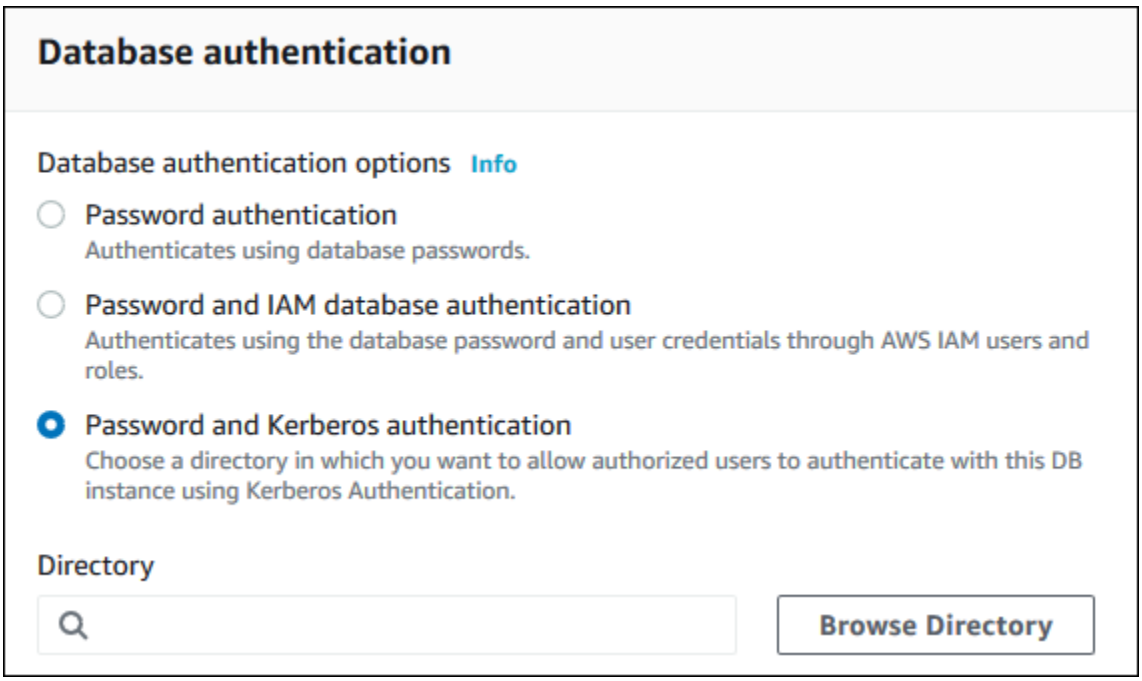
  Para obtener instrucciones, consulte Restauración a una instancia de base de datos.

- Restaure una instancia de base de datos de MySQL a partir de un punto en el tiempo mediante la consola, el comando de CLI la restore-db-instance-to-point-in-time o la operación RestoreDBInstanceToPointInTime de la API de RDS.

  Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

La autenticación Kerberos solo es compatible con instancias de base de datos de MySQL en una VPC. La instancia de DB puede estar en la misma VPC que el directorio o en una VPC diferente. La instancia de base de datos debe usar un grupo de seguridad que permita la salida dentro de la VPC del directorio, de modo que la instancia de base de datos pueda comunicarse con el directorio.

Si utiliza la consola para crear, modificar o restaurar una instancia de base de datos, elija Password and Kerberos authentication (Contraseña y autenticación de Kerberos) en la sección Database authentication (Autenticación de base de datos). Elija Browse Directory (Examinar directorio) y, a continuación, seleccione el directorio o elija Create a new directory (Crear un nuevo directorio).



Cuando use la AWS CLIo la API de RDS, asocie una instancia de base de datos a un directorio. Es obligatorio incluir los parámetros siguientes para que la instancia de base de datos pueda usar el directorio de dominio que ha creado:

- Para el parámetro `--domain`, utilice el identificador de dominio (identificador "d-*") que se generó cuando creó el directorio.
- Para el parámetro `--domain-iam-role-name`, utilice el rol que creó que usa la política `AmazonRDSDirectoryServiceAccess` de IAM administrada.

Por ejemplo, el siguiente comando de CLI modifica una instancia de base de datos para usar un directorio.

Para Linux, macOS, o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --domain d-ID \
    --domain-iam-role-name role-name
```

Para Windows:

```
aws rds modify-db-instance ^
```

```
    --db-instance-identifier mydbinstance ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

> **Important**
>
> Si modifica una instancia de base de datos para habilitar la autenticación Kerberos, reinicie la instancia de base de datos después de realizar el cambio.

Paso 5: crear inicios de sesión MySQL de autenticación Kerberos

Use las credenciales del usuario maestro de Amazon RDS para conectarse a la instancia de base de datos MySQL igual que con cualquier otra instancia de base de datos. La instancia de base de datos se une al dominio de AWS Managed Microsoft AD. Por lo tanto, puede aprovisionar inicios de sesión y usuarios de MySQL a partir de usuarios de Active Directory en su dominio. Los permisos de base de datos se administran mediante permisos estándar de MySQL que se conceden y revocan desde estos inicios de sesión.

Puede permitir que un usuario de Active Directory se autentique con MySQL. Para ello, primero use las credenciales de usuario maestro de Amazon RDS para conectarse a la instancia de base de datos MySQL igual que con cualquier otra instancia de base de datos. Después de haber iniciado sesión, cree un usuario autenticado externamente con PAM (Módulos de autenticación conectables) en MySQL ejecutando el siguiente comando. Sustituya *testuser* por el nombre de usuario.

```
CREATE USER 'testuser'@'%' IDENTIFIED WITH 'auth_pam';
```

Ahora, los usuarios (tanto humanos como aplicaciones) del dominio pueden conectarse a la instancia de base de datos desde un equipo cliente unido al dominio mediante la autenticación Herberos.

> **Important**
>
> Recomendamos encarecidamente que los clientes utilicen conexiones SSL/TLS cuando utilicen la autenticación PAM. Si no utilizan conexiones SSL/TLS, es posible que la contraseña se envíe como texto sin cifrar en algunos casos. Para exigir una conexión cifrada SSL/TLS para el usuario de AD, ejecute el siguiente comando y sustituya *testuser* con el nombre de usuario:

```
ALTER USER 'testuser'@'%' REQUIRE SSL;
```

Para obtener más información, consulte Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS.

Administración de una instancia de base de datos en un dominio

Puede usar la CLI o la API de RDS para administrar la instancia de base de datos y su relación con su Active Directory administrado. Por ejemplo, puede asociar un Active Directory para la autenticación Kerberos y desasociar un Active Directory para deshabilitar la autenticación Kerberos. También puede mover una instancia de base de datos para que sea autenticada externamente por un Active Directory a otro.

Por ejemplo, con la API de Amazon RDS puede hacer lo siguiente:

- Para volver a intentar habilitar la autenticación Kerberos en una pertenencia que ha dado un error, use la operación de API `ModifyDBInstance` y especifique el ID de directorio de la pertenencia actual.
- Para actualizar el nombre del rol de IAM para la suscripción, use la operación `ModifyDBInstance` de la API y especifique el ID del directorio de la suscripción actual y el nuevo rol de IAM.
- Para deshabilitar la autenticación Kerberos en una instancia de base de datos, utilice la operación `ModifyDBInstance` de la API y especifique `none` como parámetro de dominio.
- Para mover una instancia de base de datos de un dominio a otro, use la operación `ModifyDBInstance` de la API y especifique el identificador del nuevo dominio como parámetro del dominio.
- Para generar una lista de pertenencias de cada instancia de base de datos, utilice la operación `DescribeDBInstances` de la API.

Descripción de la pertenencia a los dominios

Una vez que haya creado o modificado una instancia de base de datos, esta se convierte en miembro del dominio. Si desea ver el estado de pertenencia al dominio de la instancia de base de datos, ejecute el comando de la CLI describe-db-instances. El estado de la instancia de base de datos puede ser uno de los siguientes:

- `kerberos-enabled`: la instancia de base de datos tiene habilitada la autenticación Kerberos.
- `enabling-kerberos` - AWS está en proceso de habilitar la autenticación Kerberos en esta instancia de base de datos.
- `pending-enable-kerberos`: la habilitación de la autenticación Kerberos está pendiente en esta instancia de base de datos.
- `pending-maintenance-enable-kerberos` - AWS intentará habilitar la autenticación Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `pending-disable-kerberos`: la deshabilitación de la autenticación Kerberos está pendiente en esta instancia de base de datos.
- `pending-maintenance-disable-kerberos` - AWS intentará desactivar la autenticación Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `enable-kerberos-failed`: un problema de configuración ha impedido que AWS habilite la autenticación Kerberos en la instancia de base de datos. Compruebe y corrija la configuración antes de volver a ejecutar el comando para modificar la instancia de base de datos.
- `disabling-kerberos` - AWS está en proceso de desactivar la autenticación Kerberos en esta instancia de base de datos.

Una solicitud para habilitar la autenticación Kerberos puede generar un error a causa de un problema de conectividad de la red o de un rol de IAM incorrecto. Por ejemplo, supongamos que crea una instancia de base de datos o modifica una instancia de base de datos ya existente y se produce un error en el intento de habilitar la autenticación Kerberos. Si esto sucede, vuelva a ejecutar el comando modify o modifique la instancia de base de datos recién creada para unirse al dominio.

Conexión a Oracle con autenticación Kerberos

Para conectarse a MySQL con autenticación Kerberos, inicie sesión con el tipo de autenticación Kerberos.

Para crear un usuario de base de datos al que pueda conectarse mediante la autenticación Kerberos, utilice una cláusula `IDENTIFIED WITH` en la instrucción `CREATE USER`. Para obtener instrucciones, consulte Paso 5: crear inicios de sesión MySQL de autenticación Kerberos.

Para evitar errores, utilice el cliente de `mysql` MariaDB. Puede descargar el software MariaDB en https://downloads.mariadb.org/.

En el símbolo del sistema, conéctese a uno de los puntos de enlace asociados a su instancia de base de datos MySQL. Siga el procedimiento general de Conexión a la instancia de base de datos de MySQL. Cuando se le pida la contraseña, escriba la contraseña de Kerberos asociada a ese nombre de usuario.

Restauración de una instancia de base de datos MySQL y adición de esta a un dominio

Puede restaurar una instantánea de base de datos o realizar una restauración a un momento dado de una instancia de base de datos MySQL y, a continuación, agregarla al dominio. Después de que la instancia de base de datos se haya restaurado, modifíquela mediante el proceso que se explica en la sección Paso 4: crear o modificar una instancia de base de datos MySQL para agregar la instancia de base de datos a un dominio.

Limitaciones de MySQL con la autenticación Kerberos

Las siguientes limitaciones se aplican a la autenticación Kerberos para MySQL:

- Solo se admite un AWS Managed Microsoft AD. Sin embargo, puede unir instancias de base de datos de RDS para MySQL a dominios compartidos de Managed Microsoft AD propiedad de distintas cuentas de la misma Región de AWS.
- Debe reiniciar la instancia de base de datos después de habilitar la característica.
- El nombre de dominio no puede tener más de 61 caracteres.
- No puede habilitar la autenticación Kerberos y la autenticación IAM al mismo tiempo. Elija uno u otro método de autenticación para su instancia de base de datos MySQL.
- No modifique el puerto de instancia de base de datos después de habilitar la característica.
- No utilice la autenticación Kerberos con réplicas de lectura.
- Si tiene activada la actualización automática de versiones secundarias para una instancia de base de datos de MySQL que utiliza la autenticación Kerberos, tiene que desactivar esta autenticación y volver a activarla después de una actualización automática. Para obtener más información acerca de las actualizaciones de versiones secundarias, consulte Actualizaciones de versiones secundarias automáticas de RDS para MySQL.
- Para eliminar una instancia de base de datos con esta característica habilitada, primero tiene que desactivar la característica. Para ello, ejecute el comando `modify-db-instance` de la CLI para la instancia de base de datos y especifique `none` para el parámetro `--domain`.

Si utiliza la CLI o la API de RDS para eliminar una instancia de base de datos con esta característica habilitada, espere un retraso.

- RDS para MySQL no admite la autenticación Kerberos en una confianza entre bosques entre su AD local o autohospedado y el AWS Managed Microsoft AD.

Mejora del rendimiento de las consultas de RDS para MySQL con lecturas optimizadas de Amazon RDS

Puede lograr un procesamiento de consultas más rápido en RDS para MySQL con las lecturas optimizadas de Amazon RDS. Una instancia de base de datos de RDS para MySQL o un clúster de base de datos Multi-AZ que utilicen lecturas optimizadas de RDS pueden procesar las consultas hasta dos veces más rápido en comparación con una instancia o clúster de base de datos que no las usa.

Temas

- Información general de las lecturas optimizadas de RDS
- Casos de uso de lecturas optimizadas para RDS
- Prácticas recomendadas para lecturas optimizadas de RDS
- Uso de lecturas optimizadas de RDS
- Supervisión de instancias de base de datos que utilizan lecturas optimizadas de RDS
- Limitaciones de las lecturas optimizadas de RDS

Información general de las lecturas optimizadas de RDS

Cuando utiliza una instancia de base de datos de RDS para MySQL o un clúster de base de datos Multi-AZ que tienen activadas las lecturas optimizadas de RDS, ambas realizan las consultas más rápido mediante el uso de un almacén de instancias. El almacén de instancias ofrece un almacenamiento de nivel de bloques temporal para la instancia de base de datos o el clúster de base de datos Multi-AZ. El almacenamiento se encuentra en unidades de estado sólido (SSD) de memoria rápida no volátil (NVMe) que están conectadas físicamente al servidor host. Este almacenamiento está optimizado para una latencia baja, un rendimiento de E/S aleatorio alto y un alto rendimiento de lectura secuencial.

Las lecturas optimizadas de RDS se activan de forma predeterminada cuando una instancia de base de datos o un clúster de base de datos Multi-AZ usa una clase de instancia de base de datos con un almacén de instancias, como db.m5d o db.m6gd. Con las lecturas optimizadas de RDS, algunos objetos temporales se almacenan en el almacén de instancias. Estos objetos temporales incluyen archivos temporales internos, tablas temporales internas en disco, archivos de mapas de memoria y archivos de caché de registros binarios (binlog). Para obtener más información sobre el almacén

de instancias, consulte Almacén de instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para las instancias de Linux.

Las cargas de trabajo que generan objetos temporales en MySQL para el procesamiento de consultas pueden aprovechar el almacén de instancias para procesar las consultas más rápido. Este tipo de carga de trabajo incluye consultas que implican ordenaciones, agregaciones de hash, uniones de alta carga, expresiones de tablas comunes (CTE) y consultas en columnas no indexadas. Estos volúmenes de almacenes de instancias proporcionan mayores IOPS y rendimiento, independientemente de las configuraciones de almacenamiento utilizadas para el almacenamiento persistente de Amazon EBS. Dado que RDS Optimized Reads descarga las operaciones de los objetos temporales al almacén de instancias, ahora las operaciones de entrada/salida por segundo (IOPS) o el rendimiento del almacenamiento persistente (Amazon EBS) se pueden utilizar para operaciones en objetos persistentes. Estas operaciones incluyen las lecturas y escrituras habituales de archivos de datos y las operaciones del motor en segundo plano, como vaciar e insertar combinaciones de búferes.

> **Note**
>
> Tanto las instantáneas de RDS manuales como las automatizadas solo contienen archivos de motor para objetos persistentes. Los objetos temporales creados en el almacén de instancias no se incluyen en las instantáneas de RDS.

Casos de uso de lecturas optimizadas para RDS

Si tiene cargas de trabajo que dependen en gran medida de objetos temporales, como tablas o archivos internos, para ejecutar consultas, puede beneficiarse de activar las lecturas optimizadas de RDS. Los siguientes casos de uso son candidatos a las lecturas optimizadas para RDS:

- Aplicaciones que ejecutan consultas analíticas con expresiones de tablas comunes (CTE) complejas, tablas derivadas y operaciones de agrupamiento
- Réplicas de lectura que atienden un tráfico de lectura intenso con consultas no optimizadas
- Aplicaciones que ejecutan consultas de generación de informes dinámicas o bajo demanda que implican operaciones complejas, como consultas con cláusulas `GROUP BY` y `ORDER BY`.
- Cargas de trabajo que utilizan tablas temporales internas para el procesamiento de consultas

Puede supervisar la variable de estado del motor `created_tmp_disk_tables` para determinar el número de tablas temporales basadas en discos que se han creado en la instancia de base de datos.

- Aplicaciones que crean tablas temporales de gran tamaño, ya sea directamente o en procedimientos, para almacenar resultados intermedios
- Consultas de bases de datos que agrupan u ordenan columnas no indexadas

Prácticas recomendadas para lecturas optimizadas de RDS

Utilice estas prácticas recomendadas para utilizar lecturas optimizadas de RDS:

- Añada una lógica de reintento para las consultas de solo lectura en caso de que fallen debido a que el almacén de instancias está lleno durante la ejecución.
- Supervise el espacio de almacenamiento disponible en el almacén de instancias con la métrica de CloudWatch `FreeLocalStorage`. Si el almacén de instancias alcanza su límite debido a la carga de trabajo de la instancia de base de datos, modifíquela para usar una clase de instancia de base de datos más grande.
- Cuando la instancia de base de datos o el clúster de base de datos Multi-AZ tenga memoria suficiente pero siga alcanzando el límite de almacenamiento del almacén de instancias, aumente el valor `binlog_cache_size` para mantener en la memoria las entradas del binlog específicas de la sesión. Esta configuración impide escribir las entradas de binlog en los archivos temporales de caché de binlog en el disco.

  El parámetro `binlog_cache_size` es específico de la sesión. Puede cambiar el valor para cada nueva sesión. La configuración de este parámetro puede aumentar la utilización de memoria en la instancia de base de datos durante los picos de carga de trabajo. Por lo tanto, considere aumentar el valor del parámetro en función del patrón de carga de trabajo de la aplicación y de la memoria disponible en la instancia de base de datos.
- Para la versión 8.0 y anteriores de MySQL, use el valor predeterminado `MIXED` del parámetro `binlog_format`. Según el tamaño de las transacciones, si se establece `binlog_format` en `ROW` se pueden generar archivos de caché binlog de gran tamaño en el almacén de instancias. Para la versión 8.4 y posteriores de MySQL, use el valor predeterminado `ROW` del parámetro `binlog_format`.

- Defina el parámetro internal_tmp_mem_storage_engine en `TempTable` y configure el parámetro temptable_max_mmap para que coincida con el tamaño del almacenamiento disponible en el almacén de instancias.
- Evite realizar cambios masivos en una sola transacción. Estos tipos de transacciones pueden generar archivos de caché binlog de gran tamaño en el almacén de instancias y pueden causar problemas cuando el almacén de instancias está lleno. Considere la posibilidad de dividir las escrituras en varias transacciones pequeñas para minimizar el uso de almacenamiento de los archivos de caché binlog.
- Utilice el valor predeterminado de `ABORT_SERVER` para el parámetro `binlog_error_action`. De este modo, se evitan problemas con el registro binario en las instancias de base de datos con las copias de seguridad habilitadas.

Uso de lecturas optimizadas de RDS

Al aprovisionar una instancia de base de datos de RDS para MySQL con una de las siguientes clases de instancia de base de datos en una implementación de instancia de base de datos Single-AZ, en una implementación de instancia de base de datos Multi-AZ o en una implementación de clúster de base de datos Multi-AZ, la instancia de base de datos utiliza automáticamente lecturas optimizadas de RDS.

Para activar las lecturas optimizadas de RDS, realice una de las siguientes acciones:

- Cree una instancia de base de datos de RDS para MySQL o un clúster de base de datos Multi-AZ utilizando una de estas clases de instancia de base de datos. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de RDS para MySQL o un clúster de base de datos Multi-AZ para utilizar una de estas clases de instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Las lecturas optimizadas de RDS están disponibles en todas las Regiones de AWS donde se admite una o más de las clases de instancia de base de datos con almacenamiento SSD NVMe local. Para obtener información acerca de las clases de instancia de base de datos, consulte the section called “Clases de instancia de base de datos”.

La disponibilidad de las clases de instancia de base de datos es diferente en las Regiones de AWS. Para determinar si una clase de instancia de base de datos se admite en una Región de AWS

específica, consulte the section called “Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS”.

Si no desea utilizar lecturas optimizadas de RDS, modifique la instancia de base de datos o el clúster de base de datos Multi-AZ para que no utilice una clase de instancia de base de datos que admita la característica.

Supervisión de instancias de base de datos que utilizan lecturas optimizadas de RDS

Puede supervisar las instancias de base de datos que utilizan lecturas optimizadas de RDS con las siguientes métricas de CloudWatch:

- `FreeLocalStorage`
- `ReadIOPSLocalStorage`
- `ReadLatencyLocalStorage`
- `ReadThroughputLocalStorage`
- `WriteIOPSLocalStorage`
- `WriteLatencyLocalStorage`
- `WriteThroughputLocalStorage`

Estas métricas proporcionan datos sobre el almacén de instancias disponible, las IOPS y el rendimiento. Para obtener más información sobre estas métricas, consulte Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS.

Limitaciones de las lecturas optimizadas de RDS

Las limitaciones siguientes se aplican a las lecturas optimizadas de RDS:

- Las lecturas optimizadas de RDS son compatibles con las siguientes versiones:
  - RDS para MySQL versión 8.0.28 y versiones principales y secundarias posteriores

  Para obtener más información acerca de las versiones de RDS para MySQL, consulte Versiones de MySQL en Amazon RDS.
- No puede cambiar la ubicación de los objetos temporales al almacenamiento persistente (Amazon EBS) en las clases de instancias de base de datos que admiten lecturas optimizadas de RDS.

- Cuando se habilita el registro binario en una instancia de base de datos, el tamaño máximo de transacción está limitado por el tamaño del almacén de instancias. En MySQL, cualquier sesión que requiera más almacenamiento que el valor de `binlog_cache_size` escribe los cambios de transacciones en archivos de caché binlog temporales, que se crean en el almacén de instancias.
- Las transacciones pueden fallar cuando el almacén de instancias está lleno.

Mejora del rendimiento de escritura con escrituras optimizadas para RDS para MySQL

Puede mejorar el rendimiento de las transacciones de escritura con escrituras optimizadas para RDS para MySQL. Cuando su base de datos de RDS para MySQL utiliza escrituras optimizadas de RDS, puede lograr un rendimiento de transacciones de escritura hasta dos veces mayor.

Temas

- Información general de las escrituras optimizadas de RDS
- Uso de escrituras optimizadas de RDS
- Habilitar las escrituras optimizadas para RDS en una base de datos existente
- Limitaciones de las escrituras optimizadas de RDS

Información general de las escrituras optimizadas de RDS

Al activar las escrituras optimizadas de RDS, las bases de datos de RDS para MySQL escriben solo una vez cuando vacían los datos en un almacenamiento duradero sin necesidad de utilizar un búfer de doble escritura. Las bases de datos siguen protegiendo las propiedades de ACID para realizar transacciones de bases de datos fiables, además de mejorar el rendimiento.

Las bases de datos relacionales, como MySQL, proporcionan las propiedades ACID de atomicidad, consistencia, aislamiento y durabilidad para transacciones de bases de datos fiables. Para ayudar a proporcionar estas propiedades, MySQL utiliza un área de almacenamiento de datos denominada búfer de escritura doble que evita errores de escritura parcial de páginas. Estos errores se producen cuando se produce un error de hardware mientras la base de datos actualiza una página, como en el caso de un corte de luz. Una base de datos MySQL puede detectar escrituras parciales de páginas y recuperarlas con una copia de la página en el búfer de doble escritura. Si bien esta técnica proporciona protección, también produce operaciones de escritura adicionales. Para obtener más información sobre el búfer de escritura doble de MySQL, consulte Doublewrite Buffer (Búfer de escritura doble) en la documentación de MySQL.

Con las escrituras optimizadas de RDS activadas, las bases de datos de RDS para MySQL escriben solo una vez cuando vacían los datos en un almacenamiento duradero sin utilizar el búfer de doble escritura. Las escrituras optimizadas de RDS son útiles si ejecuta cargas de trabajo con muchas escrituras en sus bases de datos de RDS para MySQL. Entre los ejemplos de bases de datos con

cargas de trabajo que requieren muchas escrituras, se incluyen las que admiten pagos digitales, operaciones financieras y aplicaciones de juegos.

Estas bases de datos se ejecutan en clases de instancias de base de datos que utilizan el sistema AWS Nitro. Gracias a la configuración del hardware de estos sistemas, la base de datos puede escribir páginas de 16 KiB directamente en archivos de datos de forma fiable y duradera en un solo paso. El sistema AWS Nitro permite las escrituras optimizadas de RDS.

Puede configurar el nuevo parámetro de base de datos `rds.optimized_writes` para controlar la característica de escrituras optimizadas para bases de datos RDS para MySQL. Acceda a este parámetro en los grupos de parámetros de base de datos de las versiones 8.0 y 8.4 de RDS para MySQL. Establezca el parámetro con uno de los siguientes valores:

- `AUTO`: activa las escrituras optimizadas de RDS si la base de datos las admite. Desactiva las escrituras optimizadas de RDS si la base de datos no las admite. Esta configuración es la predeterminada.
- `OFF`: desactiva las escrituras optimizadas de RDS aunque la base de datos las admita.

Si tiene una base de datos existente con una versión de motor, una clase de instancia de base de datos o un formato de sistema de archivos que no admiten las escrituras optimizadas de RDS, puede habilitar la función creando una implementación azul/verde. Para obtener más información, consulte the section called “Habilitación en una base de datos existente”.

Si migra una base de datos de RDS para MySQL que está configurada para utilizar escrituras optimizadas de RDS en una clase de instancia de base de datos que no admite la característica, RDS desactiva automáticamente las escrituras optimizadas de RDS para la base de datos.

Cuando las escrituras optimizadas de RDS están desactivadas, la base de datos utiliza el búfer de doble escritura de MySQL.

Para determinar si una base de datos de RDS para MySQL utiliza escrituras optimizadas de RDS, consulte el valor actual del parámetro `innodb_doublewrite` de la base de datos. Si la base de datos utiliza escrituras optimizadas de RDS, este parámetro se establece en `FALSE` (`0`).

Uso de escrituras optimizadas de RDS

Puede activar las escrituras optimizadas de RDS al crear una base de datos de RDS para MySQL con la consola de RDS, la AWS CLI o la API de RDS. Las escrituras optimizadas de RDS se activan

automáticamente cuando se cumplen las dos condiciones siguientes durante la creación de la base de datos:

- Debe especificar una clase de instancia de base de datos y una versión de motor de base de datos que admitan escrituras optimizadas de RDS.
  - Las escrituras optimizadas de RDS son compatibles con RDS para MySQL versión 8.0.30 y posteriores. Para obtener más información acerca de las versiones de RDS para MySQL, consulte Versiones de MySQL en Amazon RDS.
  - Las bases de datos RDS para MySQL que utilizan las siguientes clases de instancias de base de datos son compatibles con las escrituras optimizadas de RDS:
    - db.m7i
    - db.m7g
    - db.m6g
    - db.m6gd
    - db.m6i
    - db.m5
    - db.m5d
    - db.r7i
    - db.r7g
    - db.r6g
    - db.r6gd
    - db.r6i
    - db.r5
    - db.r5b
    - db.r5d
    - db.x2idn
    - db.x2iedn

    Para obtener información acerca de las clases de instancia de base de datos, consulte the section called “Clases de instancia de base de datos”.

    La disponibilidad de las clases de instancia de base de datos es diferente en las Regiones de AWS. Para determinar si una clase de instancia de base de datos se admite en una Región de

AWS específica, consulte the section called “Determinación de la compatibilidad de la clase de instancia de base de datos en Regiones de AWS”.

Para actualizar la base de datos a una clase de instancia de base de datos que sea compatible con las escrituras optimizadas de RDS, puede crear una implementación azul/verde. Para obtener más información, consulte the section called “Habilitación en una base de datos existente”.

- En el grupo de parámetros asociado a la base de datos, el parámetro `rds.optimized_writes` se establece en `AUTO`. En los grupos de parámetros predeterminados, este parámetro siempre se establece en `AUTO`.

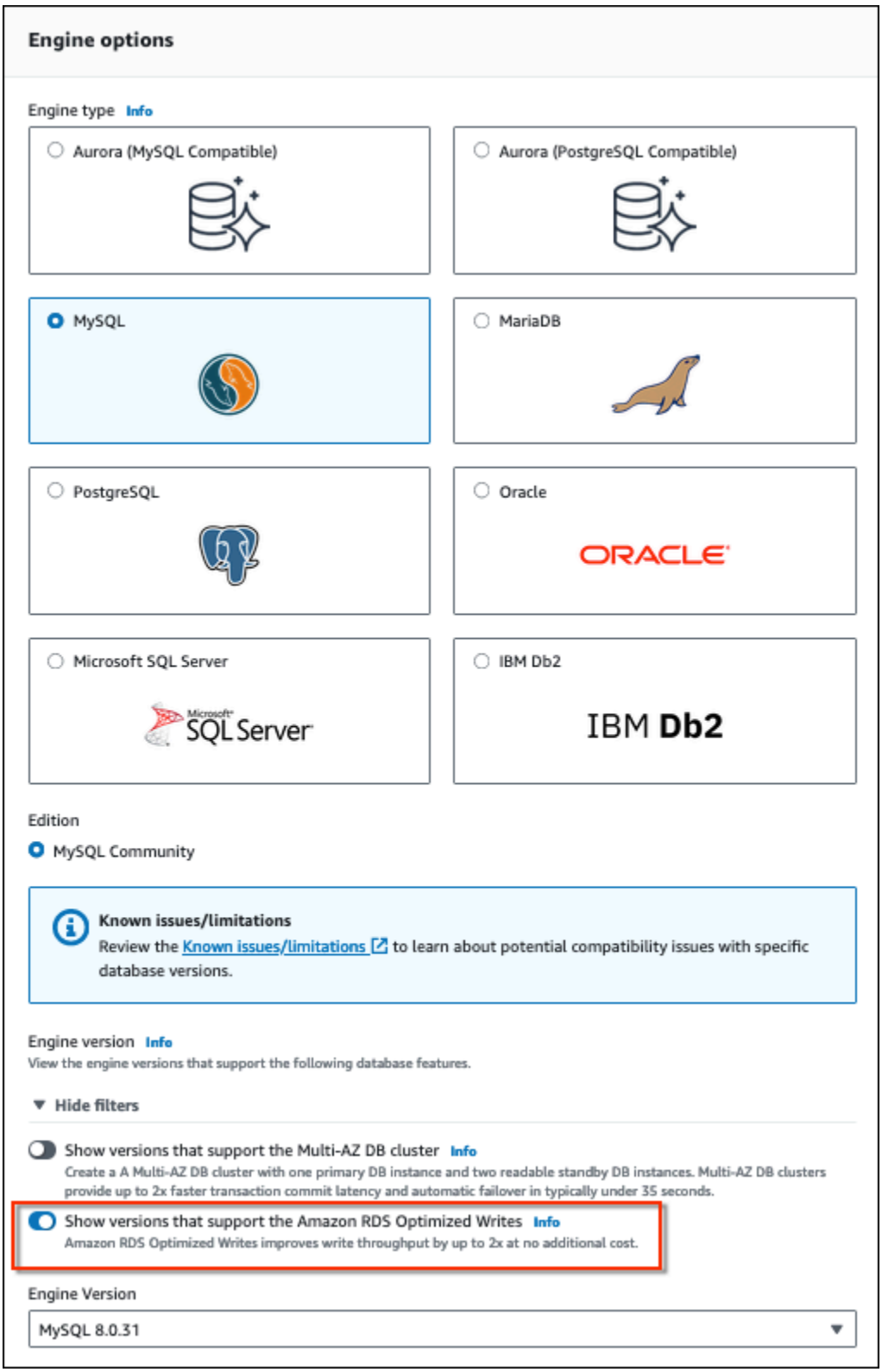
Si desea utilizar una versión del motor de base de datos y una clase de instancia de base de datos que admita las escrituras optimizadas para RDS, pero no quiere utilizar esta característica, especifique un grupo de parámetros personalizado al crear la base de datos. En este grupo de parámetros, defina el parámetro `rds.optimized_writes` en `OFF`. Si desea que la base de datos utilice las escrituras optimizadas de RDS más adelante, puede configurar el parámetro `AUTO` para activarla. Para obtener información sobre cómo trabajar con grupos de parámetros personalizados y establecer parámetros, consulte Grupos de parámetros para Amazon RDS.

Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

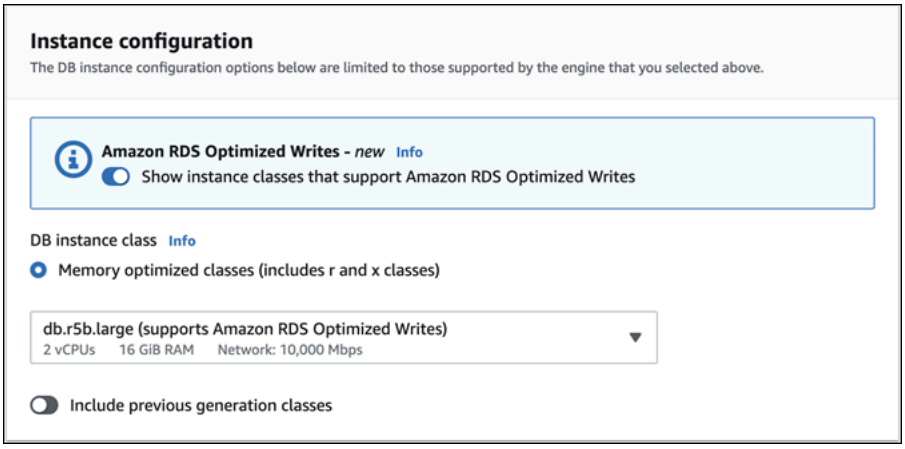
Consola

Al utilizar la consola de RDS para crear una base de datos de RDS para MySQL, puede filtrar las versiones del motor de base de datos y las clases de instancias de base de datos que admiten las escrituras optimizadas de RDS. Tras activar los filtros, puede elegir entre las clases de instancia de base de datos y las versiones del motor de base de datos disponibles.

Para elegir una versión del motor de base de datos que admita escrituras optimizadas de RDS, filtre las versiones del motor de base de datos de RDS para MySQL que la admitan en Engine version (Versión del motor) y, a continuación, elija una versión.



En la sección Instance configuration (Configuración de instancias), filtre las clases de instancias de base de datos que admiten escrituras optimizadas de RDS y, a continuación, elija una clase de instancia de base de datos.



Tras realizar estas selecciones, puede elegir otras configuraciones que cumplan sus requisitos y terminar de crear la base de datos RDS para MySQL con la consola.

AWS CLI

Para crear una instancia de base de datos con la AWS CLI, utilice el comando create-db-instance. Asegúrese de que los valores `--engine-version` y `--db-instance-class` admitan escrituras optimizadas de RDS. Además, asegúrese de que el grupo de parámetros asociado a la instancia de base de datos tiene el parámetro `rds.optimized_writes` configurado en AUT0. En este ejemplo, se asocia el grupo de parámetros predeterminado con la instancia de base de datos.

Example Creación de una instancia de base de datos que utilice escrituras optimizadas de RDS

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --engine mysql \
    --engine-version 8.0.30 \
    --db-instance-class db.r5b.large \
    --manage-master-user-password \
    --master-username admin \
    --allocated-storage 200
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --engine mysql ^
    --engine-version 8.0.30 ^
```

```
    --db-instance-class db.r5b.large ^
    --manage-master-user-password ^
    --master-username admin ^
    --allocated-storage 200
```

API de RDS

Puede crear una instancia de base de datos mediante la operación CreateDBInstance. Cuando realice esta operación, asegúrese de que los valores `EngineVersion` y `DBInstanceClass` admitan escrituras optimizadas de RDS. Además, asegúrese de que el grupo de parámetros asociado a la instancia de base de datos tiene el parámetro `rds.optimized_writes` configurado en `AUTO`.

Habilitar las escrituras optimizadas para RDS en una base de datos existente

Para modificar una base de datos de RDS para MySQL y activar las escrituras optimizadas de RDS, la base de datos debe haberse creado con una versión del motor de base de datos y una clase de instancia de base de datos compatibles. Además, la base de datos debe haberse creado después del lanzamiento de las escrituras optimizadas de RDS del 27 de noviembre de 2022, ya que la configuración del sistema de archivos subyacente requerida es incompatible con la de las bases de datos creadas antes de esa publicación. Si se cumplen estas condiciones, puede activar las escrituras optimizadas para RDS poniendo el parámetro `rds.optimized_writes` en `AUTO`.

Si la base de datos no se creó con una versión de motor, una clase de instancia o una configuración de sistema de archivos compatibles, puede usar las implementaciones azul/verde de RDS para migrar a una configuración compatible. Al crear la implementación azul/verde, haga lo siguiente:

- Seleccione Habilitar escrituras optimizadas en base de datos verde y especifique una versión del motor y una clase de instancia de base de datos que admitan escrituras optimizadas de RDS. Para ver una lista de las versiones de motor y las clases de instancias compatibles, consulte Uso de escrituras optimizadas de RDS.
- En Almacenamiento, seleccione Actualizar la configuración del sistema de archivos de almacenamiento. Esta opción actualiza la base de datos a una configuración de sistema de archivos subyacente compatible.

Al crear la implementación azul/verde, si el parámetro `rds.optimized_writes` se ha configurado en `AUTO`, las escrituras optimizadas de RDS se habilitarán automáticamente en el entorno verde. A

continuación, puede conmutar la implementación azul/verde para que el entorno verde sea el nuevo entorno de producción.

Para obtener más información, consulte the section called “Creación de una implementación azul/verde”.

Limitaciones de las escrituras optimizadas de RDS

Al restaurar una base de datos de RDS para MySQL a partir de una instantánea, solo puede activar las escrituras optimizadas de RDS para la base de datos si se cumplen todas las condiciones siguientes:

- La instantánea se creó a partir de una base de datos que admite escrituras optimizadas de RDS.
- La instantánea se ha creado a partir de una base de datos que se creó después del lanzamiento de las escrituras optimizadas para RDS.
- La instantánea se restaura en una base de datos que admite escrituras optimizadas de RDS.
- La base de datos restaurada está asociada a un grupo de parámetros que tiene el parámetro `rds.optimized_writes` establecido en `AUTO`.

Actualizaciones del motor de base de datos de RDS para MySQL

Cuando Amazon RDS admita una nueva versión de un motor de base de datos, podrá actualizar sus instancias de base de datos a la nueva versión. Hay dos tipos de actualizaciones para las bases de datos de MySQL: actualizaciones de versiones principales y actualizaciones de versiones secundarias.

Actualizaciones de la versión principal

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de las aplicaciones. Por lo tanto, debe realizar manualmente las actualizaciones de versiones principales de sus instancias de base de datos. Puede iniciar una actualización de versión principal modificando su instancia de base de datos. Antes de realizar una actualización de una versión principal, recomendamos que siga las instrucciones descritas en Actualizaciones de versiones principales de RDS para MySQL.

Para actualizaciones de versiones principales de implementaciones de instancias de base de datos multi-AZ, Amazon RDS actualiza simultáneamente las réplicas principal y en espera. La instancia de base de datos no estará disponible hasta que se complete la actualización. Para actualizaciones de versiones principales de implementaciones de clústeres de base de datos multi-AZ, Amazon RDS actualiza las instancias miembros del clúster de una en una.

> **Tip**
>
> Puede minimizar el tiempo de inactividad necesario para la actualización de una versión principal mediante una implementación azul/verde. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Actualizaciones de la versión secundaria

Las actualizaciones de versiones secundarias solo incluyen cambios compatibles con las versiones anteriores de las aplicaciones existentes. Puede iniciar manualmente una actualización de versiones secundarias modificando su instancia de base de datos. O puede habilitar la opción Actualización automática de versiones secundarias al crear o modificar una instancia de base de datos. Si lo hace, Amazon RDS actualizará automáticamente su instancia de base de datos tras probar y aprobar la nueva versión. Para obtener información sobre cómo realizar una actualización, consulte Actualización de una versión del motor de una instancia de base de datos.

Cuando se actualiza la versión secundaria de un clúster de base de datos multi-AZ, Amazon RDS actualiza las instancias de base de datos de lector una por una. A continuación, una de las instancias de base de datos de lector pasa a ser la nueva instancia de base de datos de escritor. Amazon RDS actualiza luego la antigua instancia de escritor (que ahora es una instancia de lector).

> **Note**
>
> El tiempo de inactividad para realizar una actualización de una versión secundaria de una implementación de una instancia de base de datos multi-AZ puede durar varios minutos. Los clústeres de bases de datos multi-AZ suelen reducir el tiempo de inactividad de las actualizaciones de versiones secundarias a aproximadamente 35 segundos. Cuando se utilizan con RDS Proxy, se puede reducir aún más el tiempo de inactividad a un segundo o menos. Para obtener más información, consulte Amazon RDS Proxy. Otra opción, puede utilizar un proxy de base de datos de código abierto como ProxySQL, PgBouncer o el controlador de contenedor JDBC avanzado de AWS.

Si la instancia de base de datos de MySQL usa las réplicas de lectura, debe actualizar todas las réplicas de lectura antes de actualizar la instancia de origen.

Temas

- Aspectos a tener en cuenta sobre las actualizaciones de MySQL
- Búsqueda de objetivos de actualización válidos
- Números de versión de MySQL
- Números de versión de RDS en RDS para MySQL
- Actualizaciones de versiones principales de RDS para MySQL
- Prueba de una actualización de RDS para MySQL
- Actualización de una instancia de base de datos MySQL
- Actualizaciones de versiones secundarias automáticas de RDS para MySQL
- Uso de una réplica de lectura para reducir el tiempo de inactividad al actualizar una base de datos de RDS para MySQL

Aspectos a tener en cuenta sobre las actualizaciones de MySQL

Amazon RDS toma dos o más instantáneas de la base de datos durante el proceso de actualización. Amazon RDS toma hasta dos instantáneas de la instancia de base de datos antes de realizar cualquier cambio en la actualización. Si la actualización de las bases de datos no funciona, puede restaurar una de estas instantáneas para crear una instancia de base de datos que ejecute la versión antigua. Amazon RDS toma otra instantánea de la instancia de base de datos cuando se completa la actualización. Amazon RDS toma estas instantáneas independientemente de si AWS Backup administra las copias de seguridad de la instancia de base de datos.

> **Note**
>
> Amazon RDS solo realiza instantáneas de base de datos si ha definido el periodo de retención de copia de seguridad de su instancia de base de datos en un número mayor que 0. Para cambiar el periodo de retención de copia de seguridad, consulte Modificación de una instancia de base de datos de Amazon RDS.

Después de completar la actualización, no puede volver a la versión anterior del motor de base de datos. Si desea volver a la versión anterior, restaure la primera instantánea de base de datos que se realizó para crear una nueva instancia de base de datos.

Puede controlar cuándo debe actualizar la instancia de base de datos a una nueva versión admitida por Amazon RDS. Este nivel de control le ayuda a mantener la compatibilidad con versiones de base de datos específicas y probar nuevas versiones con una aplicación antes de implementarlas en producción. Cuando esté listo, podrá efectuar actualizaciones de versiones en el momento que le resulte más conveniente.

Si la instancia de base de datos usa replicación de lectura, debe actualizar todas las réplicas de lectura antes de actualizar la instancia de origen.

Búsqueda de objetivos de actualización válidos

Cuando se utiliza la AWS Management Console para actualizar una instancia de base de datos, muestra los destinos de actualización válidos para la instancia de base de datos. También puede utilizar el siguiente comando de la AWS CLI para identificar los destinos de actualización válidos para una instancia de base de datos:

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
  --engine mysql \
  --engine-version version_number \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
  --engine mysql ^
  --engine-version version_number ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Por ejemplo, para identificar los destinos de actualización válidos para una instancia de base de datos de MySQL versión 8.0.28, ejecute el siguiente comando de la AWS CLI:

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
  --engine mysql \
  --engine-version 8.0.28 \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
  --engine mysql ^
  --engine-version 8.0.28 ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Números de versión de MySQL

La secuencia de numeración de versiones del motor de base de datos de RDS para MySQL tiene el formato principal.secundaria.parche.AAAAMMDD o principal.secundaria.parche (por ejemplo, 8.0.33.R2.20231201 o 5.7.44). El formato utilizado depende de la versión del motor de MySQL. Para obtener información sobre la numeración de versiones del Soporte extendido de RDS, consulte Nombre de versiones con el Soporte extendido de Amazon RDS.

principal

El número de versión principal es tanto el entero como la primera parte fraccional del número de versión (por ejemplo, 8.0). Una actualización de versión principal aumenta la parte principal del número de versión. Por ejemplo, una actualización de 5.7.44 a 8.0.33 es una actualización de versión principal, donde 5.7 y 8.0 son los números de la versión principal.

secundaria.

El número de versión secundaria es la tercera parte del número de versión (por ejemplo, el 33 en 8.0.33).

parche

El parche es la cuarta parte del número de versión (por ejemplo, el R2 en 8.0.33.R2). Una versión de parche de RDS incluye correcciones de errores importantes que se agregan a una versión secundaria después de su lanzamiento.

AAAAMMDD

La fecha es la quinta parte del número de versión (por ejemplo, 20231201 en 8.0.33.R2.20231201). Una versión de fecha de RDS es un parche de seguridad que incluye correcciones de seguridad importantes que se agregan a una versión secundaria después de su lanzamiento. No incluye ninguna corrección que pueda cambiar el comportamiento de un motor.

En la siguiente tabla, se explica el esquema de nomenclatura de RDS para MySQL versión 8.4.

Versión secundaria 8.4	Esquema de nomenclatura
≥ 3	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 8.4.3.R2.20241201). Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 8.4.3.R2) hasta la próxima actualización de la versión principal o secundaria.

La siguiente tabla explica el esquema de nomenclatura de RDS para MySQL versión 8.0.

Versión secundaria 8.0	Esquema de nomenclatura
≥ 33	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 8.0.33.R2.20231201). Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 8.0.33.R2) hasta la próxima actualización de la versión principal o secundaria.
< 33	Las instancias de base de datos existentes utilizan el formato principal.secundaria.parche (por ejemplo, 8.0.32.R2).

La siguiente tabla explica el esquema de nomenclatura de RDS para MySQL versión 5.7.

Versión secundaria 5.7	Esquema de nomenclatura
≥ 42	Las nuevas instancias de base de datos utilizan el formato principal.secundaria.parche.AAMMDD (por ejemplo, 5.7.42.R2.20231201). Las instancias de base de datos existentes pueden usar el formato principal.secundaria.parche (por ejemplo, 5.7.42.R2) hasta la próxima actualización de la versión principal o secundaria.

Números de versión de RDS en RDS para MySQL

Los números de versión de RDS utilizan el esquema de nomenclatura *major*.*minor*.*patch* o *major*.*minor*.*patch*.*YYYYMMDD*. Las versiones de Soporte extendido de Amazon RDS utilizan el esquema de nomenclatura de las versiones secundarias *minor-RDS*.*YYYYMMDD*.

Una versión de parche de RDS incluye correcciones de errores importantes que se agregan a una versión secundaria después de su lanzamiento. Una versión de fecha de RDS (*AAAAMMDD*) es un parche de seguridad. Un parche de seguridad no incluye ninguna corrección que pueda cambiar

el comportamiento de un motor. Para obtener información sobre la numeración de versiones del Soporte extendido de RDS, consulte Nombre de versiones con el Soporte extendido de Amazon RDS.

Puede averiguar el número de versión de RDS de su base de datos de RDS para MySQL con la siguiente consulta SQL:

```
mysql> select mysql.rds_version();
```

Por ejemplo, la consulta de una base de datos de RDS para MySQL 8.0.34 devuelve lo siguiente:

```
+---------------------+
| mysql.rds_version() |
+---------------------+
| 8.0.34.R2.20231201  |
+---------------------+
1 row in set (0.01 sec)
```

Actualizaciones de versiones principales de RDS para MySQL

Amazon RDS es compatible con las siguientes actualizaciones locales para versiones principales del motor de base de datos MySQL:

- MySQL 5.7 a MySQL 8.0
- MySQL 8.0 a MySQL 8.4

> **Note**
>
> Solo puede crear instancias de base de datos MySQL versión 5.7, 8.0 y 8.4 con clases de instancia de base de datos de última generación y generación actual.
> En algunos casos, desea actualizar una instancia de base de datos que se ejecuta en una clase de instancia de base de datos de una generación a una versión de motor MySQL posterior. En estos casos, modifique primero la instancia de base de datos para usar una clase de instancia de datos de última generación o generación actual. Una vez hecho esto, podrá modificar la instancia de base de datos para usar la versión posterior del motor de base de datos MySQL. Para obtener información acerca de las clases de instancia de base de datos de Amazon RDS, consulte Clases de instancia de base de datos de .

Temas

- Información general sobre las actualizaciones de la versión principal de MySQL
- Comprobaciones previas de actualizaciones
- Reversión tras un fallo en la actualización

Información general sobre las actualizaciones de la versión principal de MySQL

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de las aplicaciones. Como resultado, Amazon RDS no aplica automáticamente las actualizaciones de las versiones principales; es necesario modificar manualmente la instancia de base de datos. Recomendamos que pruebe exhaustivamente cualquier actualización antes de aplicarla a las instancias de producción.

Para realizar una actualización de versión principal, realice primero las actualizaciones de sistema operativo disponibles. Una vez que se completen las actualizaciones del sistema operativo, actualice a cada versión principal: de 5.7 a 8.0 y luego de 8.0. a 8.4. Para obtener más información sobre la actualización de un clúster de base de datos multi-AZ de RDS para MySQL, consulte Actualización de la versión del motor de un clúster de base de datos multi-AZ para Amazon RDS. Las instancias de base de datos MySQL creadas antes del 24 de abril de 2014, muestran una actualización del sistema operativo disponible hasta que se haya aplicado la actualización. Para obtener más información acerca de las actualizaciones del sistema operativo, consulte Aplicación de actualizaciones a una instancia de base de datos.

Durante una actualización de versión principal de MySQL, Amazon RDS ejecuta el comando `mysql_upgrade` binario de MySQL para actualizar tablas, si es necesario. Además, Amazon RDS vacía las tablas `slow_log` y `general_log` durante una actualización de versión principal. Para conservar información de registro, guarde el contenido de este antes de realizar la actualización de versión principal.

Las actualizaciones de versión principal de MySQL suelen realizarse en aproximadamente 10 minutos. Algunas actualizaciones podrían tardar algo más debido al tamaño de la clase de instancia de base de datos, o bien porque la instancia no sigue determinadas directrices de funcionamiento de Prácticas recomendadas para Amazon RDS. Si actualiza una instancia de base de datos desde la consola de Amazon RDS, el estado de la instancia indica cuándo finaliza la actualización. Si realiza la actualización utilizando la AWS Command Line Interface (AWS CLI), use el comando describe-db-instances y compruebe el valor de `Status`.

Comprobaciones previas de actualizaciones

Amazon RDS realiza comprobaciones previas antes de la actualización para comprobar si hay incompatibilidades. Estas incompatibilidades varían en función de la versión de MySQL a la que se vaya a actualizar.

Entre las comprobaciones previas se incluyen algunas que a su vez se incluyen con MySQL y otras que el equipo Amazon RDS creó específicamente. Para obtener información acerca de las comprobaciones previas que proporciona MySQL, consulte la sección sobre la utilidad del comprobador de actualización.

Las comprobaciones previas se ejecutan antes de detenerse la instancia de base de datos para la actualización, lo que quiere decir que no causan tiempos de inactividad al ejecutarse. Si las verificaciones previas encuentran una incompatibilidad, Amazon RDS cancela automáticamente la actualización antes de detenerse la instancia de base de datos. Amazon RDS también genera un evento por la incompatibilidad. Para obtener más información acerca de los eventos de Amazon RDS, consulte Uso de notificaciones de eventos de Amazon RDS.

Amazon RDS registra información detallada acerca de cada incompatibilidad en el archivo de registro `PrePatchCompatibility.log`. En la mayoría de los casos, la entrada de registro incluye un vínculo a la documentación de SQL para corregir la incompatibilidad. Para obtener más información acerca de cómo visualizar los archivos de registro, consulte Visualización y descripción de archivos de registro de base de datos.

Debido a la naturaleza de las comprobaciones previas, analizan objetos en su base de datos. Este análisis genera un consumo de recursos y aumenta el tiempo de ejecución de la actualización.

Temas

- Comprobaciones previas de actualizaciones de la versión 8.0 a la 8.4 de MySQL
- Comprobaciones previas de actualizaciones de la versión 5.7 a la 8.0 de MySQL

Comprobaciones previas de actualizaciones de la versión 8.0 a la 8.4 de MySQL

MySQL 8.4 presenta numerosas incompatibilidades con MySQL 8.0. Dichas incompatibilidades pueden causar problemas durante una actualización de MySQL 8.0 a MySQL 8.4. Así pues, puede requerirse cierta preparación con respecto a su base de datos para que la actualización se realice correctamente. A continuación, mostramos una lista general de dichas incompatibilidades:

- Ninguna tabla debe usar tipos o funciones de datos obsoletos.

- No debe haber un definidor vacío ni faltar un definidor en los disparadores, y el contexto de creación de los disparadores tiene que ser válido.
- No debe haber ninguna infracción de la palabra clave ni de la palabra reservada. Es posible que en MySQL 8.4 haya algunas palabras clave reservadas que no estaban reservadas previamente.

  Para obtener más información, consulte la página sobre Palabras clave y palabras reservadas en la documentación de MySQL.
- No tiene que haber tablas en la base de datos del sistema `mysql` de MySQL 8.0 que tengan el mismo nombre que una tabla usada por el diccionario de datos de MySQL 8.4.
- No tiene que haber modos SQL obsoletos en su configuración de variable del sistema `sql_mode`.
- No tiene que haber tablas ni procedimientos almacenados que tengan elementos de columna `ENUM` o `SET` individuales que superen los 255 caracteres o 1020 bytes de longitud.
- Su instalación de MySQL 8.0 no tiene que usar características que no sean compatibles con MySQL 8.4.

  Para obtener más información, consulte la sección Features removed in MySQL 8.4 en la documentación de MySQL.
- No tiene que haber nombres de restricción de clave externa que superen los 64 caracteres.
- Para la compatibilidad con Unicode mejorada, consulte la siguiente información:
  - Tenga en cuenta la conversión de objetos que usen el conjunto de caracteres `utf8mb3` para usar el conjunto de caracteres `utf8mb4`. El conjunto de caracteres `utf8mb3` ha quedado obsoleto.
  - Tenga en cuenta el uso de `utf8mb4` para referencias de conjuntos de caracteres, en vez de utilizar `utf8`, ya que actualmente `utf8` es un alias del conjunto de caracteres `utf8mb3`. Si es posible, cambie `utf8` a `utf8mb4` primero y, a continuación, actualice la base de datos.
  - Como los clientes antiguos pueden recibir un error de juego de caracteres desconocido para `utf8mb3`, actualice los clientes de la base de datos antes de actualizar la base de datos.

  Para obtener más información, consulte la sección sobre el conjunto de caracteres utf8mb3 (codificación Unicode UTF-8 de 3 bytes) en la documentación de MySQL.

  Para cambiar los conjuntos de caracteres, puede realizar manualmente una copia de seguridad, restauración y replicación de la base de datos. Puede utilizar las implementaciones azules/verdes de Amazon RDS. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Si inicia una actualización de MySQL de 8.0 a 8.4, Amazon RDS ejecutará comprobaciones previas de forma automática para detectar estas incompatibilidades. Para obtener información acerca de cómo actualizar a MySQL 8.4, consulte la sección sobre la actualización de MySQL en la documentación de MySQL.

Estas comprobaciones previas son obligatorias. No tiene la opción de omitirlas. Las comprobaciones previas proporcionan las siguientes ventajas:

- Le permiten evitar tiempos de inactividad no planeados durante la actualización.
- Si hay incompatibilidades, Amazon RDS impide la actualización y proporciona un registro para que se informe sobre ellas. Luego podrá usar el registro para preparar su base de datos para la actualización a MySQL 8.4 y reducir así las incompatibilidades. Para obtener información detallada acerca de cómo eliminar incompatibilidades, consulte Preparing your installation for upgrade en la documentación de MySQL.

Comprobaciones previas de actualizaciones de la versión 5.7 a la 8.0 de MySQL

MySQL 8.0 presenta numerosas incompatibilidades con MySQL 5.7. Dichas incompatibilidades pueden causar problemas durante una actualización de MySQL 5.7 a MySQL 8.0. Así pues, puede requerirse cierta preparación con respecto a su base de datos para que la actualización se realice correctamente. A continuación, mostramos una lista general de dichas incompatibilidades:

- Ninguna tabla debe usar tipos o funciones de datos obsoletos.
- No tiene que haber archivos *.frm huérfanos.
- No debe haber un definidor vacío ni faltar un definidor en los disparadores, y el contexto de creación de los disparadores tiene que ser válido.
- Ninguna tabla particionada debe usar un motor de almacenamiento que no tenga soporte de particiones nativo.
- No debe haber ninguna infracción de la palabra clave ni de la palabra reservada. Es posible que en MySQL 8.0 haya algunas palabras clave reservadas que no estaban reservadas previamente.

  Para obtener más información, consulte la página sobre Palabras clave y palabras reservadas en la documentación de MySQL.
- No tiene que haber tablas en la base de datos del sistema `mysql` de MySQL 5.7 que tengan el mismo nombre que una tabla usada por el diccionario de datos de MySQL 8.0.
- No tiene que haber modos SQL obsoletos en su configuración de variable del sistema `sql_mode`.

- No tiene que haber tablas ni procedimientos almacenados que tengan elementos de columna `ENUM` o `SET` individuales que superen los 255 caracteres o 1020 bytes de longitud.
- Antes de realizar la actualización a MySQL 8.0.13 o una versión superior, ninguna partición de tabla debe residir en espacios de tablas InnoDB compartidos.
- No tiene que haber consultas ni definiciones de programas almacenadas de MySQL 8.0.12 o versiones anteriores que usen calificadores `ASC` o `DESC` para cláusulas `GROUP BY`.
- Su instalación de MySQL 5.7 no tiene que usar características que no sean compatibles con MySQL 8.0.

  Para obtener más información, consulte la sección sobre características eliminadas en MySQL 8.0, en la documentación de MySQL.
- No tiene que haber nombres de restricción de clave externa que superen los 64 caracteres.
- Para la compatibilidad con Unicode mejorada, consulte la siguiente información:
  - Tenga en cuenta la conversión de objetos que usen el conjunto de caracteres `utf8mb3` para usar el conjunto de caracteres `utf8mb4`. El conjunto de caracteres `utf8mb3` ha quedado obsoleto.
  - Tenga en cuenta el uso de `utf8mb4` para referencias de conjuntos de caracteres, en vez de utilizar `utf8`, ya que actualmente `utf8` es un alias del conjunto de caracteres `utf8mb3`. Si es posible, cambie `utf8` a `utf8mb4` primero y, a continuación, actualice la base de datos.
  - Como los clientes antiguos pueden recibir un error de juego de caracteres desconocido para `utf8mb3`, actualice los clientes de la base de datos antes de actualizar la base de datos.

  Para obtener más información, consulte la sección sobre el conjunto de caracteres utf8mb3 (codificación Unicode UTF-8 de 3 bytes) en la documentación de MySQL.

  Para cambiar los conjuntos de caracteres, puede realizar manualmente una copia de seguridad, restauración y replicación de la base de datos. Puede utilizar las implementaciones azules/verdes de Amazon RDS. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Si inicia una actualización de MySQL 5.7 a 8.0, Amazon RDS ejecutará comprobaciones previas de forma automática para detectar estas incompatibilidades. Para obtener información acerca de cómo actualizar a MySQL 8.0, consulte la sección sobre la actualización de MySQL en la documentación de MySQL.

Estas comprobaciones previas son obligatorias. No tiene la opción de omitirlas. Las comprobaciones previas proporcionan las siguientes ventajas:

- Le permiten evitar tiempos de inactividad no planeados durante la actualización.
- Si hay incompatibilidades, Amazon RDS impide la actualización y proporciona un registro para que se informe sobre ellas. Luego podrá usar el registro para preparar su base de datos para la actualización a MySQL 8.0 y reducir así las incompatibilidades. Para obtener información detallada acerca de cómo eliminar incompatibilidades, consulte Preparing your installation for upgrade en la documentación de MySQL y Upgrading to MySQL 8.0? Here is what you need to know... en el blog de MySQL Server.

Reversión tras un fallo en la actualización

Cuando se actualiza una instancia de base de datos de la versión 5.7 a la 8.0 o de la versión 8.0 a la 8.4 de MySQL, la actualización puede fallar. En particular, puede fallar si el diccionario de datos contiene incompatibilidades que no fueron capturadas por las comprobaciones previas. En este caso, la base de datos no se puede iniciar correctamente en la nueva versión de MySQL 8.0 a la versión 8.4. En ese momento, Amazon RDS revierte los cambios realizados para la actualización. Tras la reversión, la instancia de base de datos de MySQL ejecuta la versión original.

- MySQL versión 8.0 (para una reversión desde la 8.4)
- MySQL versión 5.7 (para una reversión desde la 8.0)

Cuando se produce un error en una actualización y se revierte, Amazon RDS genera un evento con el ID de evento RDS-EVENT-0188.

Normalmente, una actualización falla porque existen incompatibilidades en los metadatos entre las bases de datos de la instancia de base de datos y la versión de MySQL de destino. Cuando falla una actualización, se pueden ver los detalles de dichas incompatibilidades en el archivo `upgradeFailure.log`. Resuelva las incompatibilidades antes de intentar actualizar nuevamente.

Durante un intento de actualización y de reversión fallidos, la instancia de base de datos se reinicia. Cualquier cambio de parámetros pendientes se aplica durante el reinicio y persiste después de la reversión.

Para obtener más información acerca de la actualización a MySQL 8.0, consulte los siguientes temas en la documentación de MySQL:

- Preparación de la instalación para la actualización
- ¿Actualizando a MySQL 8.0? Esto es lo que necesita saber…

Para obtener más información acerca de cómo actualizar a MySQL 8.4, consulte Preparing Your Installation for Upgrade en la documentación de MySQL.

Prueba de una actualización de RDS para MySQL

Antes de realizar una actualización de versión principal en su instancia de base de datos, realice una comprobación exhaustiva de su base de datos para determinar la compatibilidad con la versión nueva. Además, realice una comprobación exhaustiva de todas las aplicaciones que tienen acceso a la base de datos para determinar la compatibilidad con la versión nueva. Le recomendamos que utilice el siguiente procedimiento.

Para probar una actualización de versión principal

1. Revise la documentación de actualización relativa a la nueva versión del motor de base de datos para ver si hubiera problemas de compatibilidad que pudieran afectar a su base de datos o aplicaciones:
   - Cambios en MySQL 5.7
   - Cambios en MySQL 8.0
   - Cambios en MySQL 8.4
2. Si su instancia de base de datos forma parte de un grupo de parámetros de base de datos personalizado, cree un grupo nuevo con la configuración existente que sea compatible con la versión principal nueva. Especifique el grupo de parámetros de base de datos nuevo cuando actualice su instancia de prueba, para que la prueba de la actualización compruebe que funciona correctamente. Para obtener más información acerca de cómo crear un grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.
3. Cree una instantánea de base de datos de la instancia de base de datos que se va a actualizar. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
4. Restaure la instantánea de base de datos para crear una nueva instancia de base de datos de prueba. Para obtener más información, consulte Restauración a una instancia de base de datos.

5. Modifique esta instancia de base de datos de prueba nueva para actualizarla a la nueva versión, utilizando uno de los métodos que se detalla a continuación. Si creó un grupo de parámetros nuevo en el paso 2, especifíquelo.
6. Evalúe el almacenamiento utilizado por la instancia actualizada para determinar si la actualización necesita almacenamiento adicional.
7. Ejecute tantas pruebas de control de calidad en la instancia de base de datos actualizada como necesite para asegurarse de que la base de datos y la aplicación funcionan correctamente con la versión nueva. Implemente las pruebas nuevas que sean necesarias para evaluar el impacto de cualquier problema de compatibilidad que haya identificado en el paso 1. Pruebe todas las funciones y los procedimientos almacenados. Dirija las versiones de prueba de sus aplicaciones a la instancia de base de datos actualizada.
8. Si se superan todas las pruebas, realice la actualización de la instancia de base de datos de producción. Recomendamos que no permita operaciones de escritura en la instancia de base de datos hasta que confirme que todo funciona correctamente.

Actualización de una instancia de base de datos MySQL

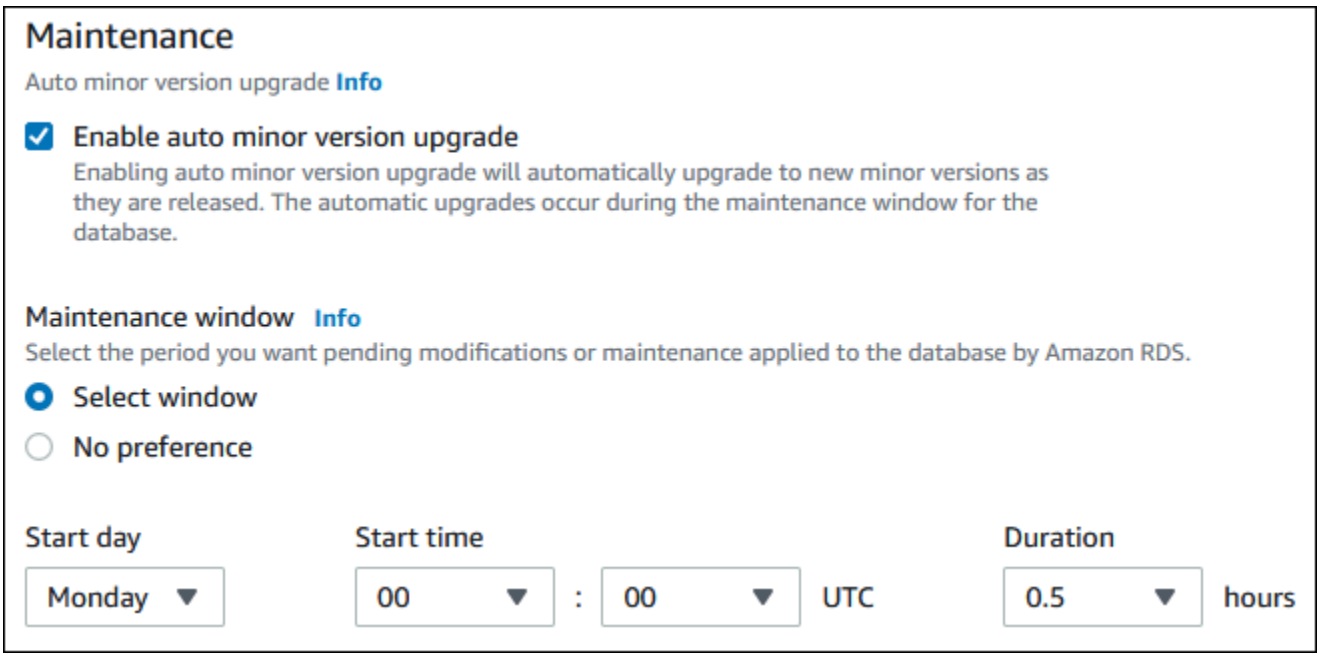
Para obtener más información acerca de la actualización automática o manual de una instancia de base de datos MySQL, consulte Actualización de una versión del motor de una instancia de base de datos.

Actualizaciones de versiones secundarias automáticas de RDS para MySQL

Si especifica la siguiente configuración al crear o modificar una instancia de base de datos, puede actualizar automáticamente la instancia de base de datos.

- La opción Auto minor version upgrade (Actualización automática de versión secundaria) está habilitada.
- La configuración del Backup retention period (periodo de retención de copia de seguridad) es mayor que 0.

En la AWS Management Console, esta configuración se encuentra en Additional configuration (Configuración adicional). En la siguiente imagen se muestra la configuración Auto minor version upgrade (Actualización automática de versiones secundarias).



Para obtener más información sobre estas opciones, consulte Configuración de instancias de base de datos.

Para algunas versiones principales de RDS para MySQL en algunas Regiones de AWS, RDS designa una versión secundaria como versión de actualización automática. Después de que Amazon RDS pruebe y apruebe una versión secundaria, la actualización de versión secundaria se produce automáticamente durante el periodo de mantenimiento. RDS no configura automáticamente versiones secundarias publicadas recientemente como la versión de actualización automática. Antes de que RDS asigne una versión de actualización automática más reciente, deben considerarse algunos criterios, como, por ejemplo, los que se indican a continuación:

- Problemas de seguridad conocidos
- Errores en la versión de la comunidad MySQL
- Estabilidad general de la flota desde que se publicó la versión secundaria

Puede utilizar el comando AWS CLI siguiente para determinar la versión secundaria actual de destino de actualización automática para una versión secundaria de MySQL especificada en una Región de AWS específica.

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
```

```
--engine-version minor_version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version minor_version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

Por ejemplo, el siguiente comando de la AWS CLI determina el destino de actualización secundaria automática para la versión secundaria 8.0.11 de MySQL en la Región de AWS de Este de EE. UU. (Ohio) (us-east-2).

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine mysql \
--engine-version 8.0.11 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine mysql ^
--engine-version 8.0.11 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Su resultado es similar al siguiente.

```
---------------------------------
|    DescribeDBEngineVersions    |
+--------------+-----------------+
|  AutoUpgrade |  EngineVersion  |
+--------------+-----------------+
|  False       |  8.0.15         |
|  False       |  8.0.16         |
|  False       |  8.0.17         |
|  False       |  8.0.19         |
|  False       |  8.0.20         |
|  False       |  8.0.21         |
|  True        |  8.0.23         |
|  False       |  8.0.25         |
+--------------+-----------------+
```

En este ejemplo, el valor `AutoUpgrade` es `True` para la versión 8.0.23 de MySQL. Por lo tanto, el destino de actualización secundaria automática es la versión 8.0.23 de MySQL, que está resaltado en el resultado.

Una instancia de base de datos de MySQL se actualiza automáticamente durante el periodo de mantenimiento si se cumplen los siguientes criterios:

- La opción Auto minor version upgrade (Actualización automática de versión secundaria) está habilitada.
- La configuración del Backup retention period (periodo de retención de copia de seguridad) es mayor que 0.
- La instancia de base de datos se ejecuta en una versión secundaria de motor de base de datos que es anterior a la versión secundaria de actualización automática actual.

Para obtener más información, consulte Actualización automática de la versión secundaria del motor.

Uso de una réplica de lectura para reducir el tiempo de inactividad al actualizar una base de datos de RDS para MySQL

En la mayoría de los casos, una implementación azul/verde es la mejor opción para reducir el tiempo de inactividad al actualizar una instancia de base de datos de MySQL. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.

Si no puede usar una implementación azul/verde y en la actualidad se está utilizando su instancia de base de datos de MySQL con una aplicación de producción, puede utilizar el siguiente procedimiento para actualizar la versión de base de datos de la instancia de base de datos. Este procedimiento puede reducir la duración del tiempo de inactividad de la aplicación.

Al utilizar una réplica de lectura, puede realizar la mayoría de los pasos de mantenimiento con anticipación y minimizar los cambios necesarios durante la interrupción real. Con esta técnica, puede probar y preparar la nueva instancia de base de datos sin realizar ningún cambio en su instancia de base de datos existente.

El siguiente procedimiento muestra un ejemplo de actualización de la versión 5.7 de MySQL a la versión 8.0 de MySQL. Puede usar los mismos pasos generales para actualizaciones a otras versiones principales. Puede usar los mismos pasos generales para actualizaciones a otras versiones principales.

> **Note**
>
> Cuando esté realizando la actualización de la versión 5.7 a la 8.0 o de la versión 8.0 a la 8.4 de MySQL, complete las comprobaciones previas antes de hacer la actualización. Para obtener más información, consulte Comprobaciones previas de actualizaciones de la versión 5.7 a la 8.0 de MySQL y Comprobaciones previas de actualizaciones de la versión 8.0 a la 8.4 de MySQL.

Para actualizar una base de datos MySQL mientras se está utilizando una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Cree una réplica de lectura para la instancia de base de datos de MySQL 5.7. Este proceso permite crear una copia actualizable de su base de datos. También pueden existir otras réplicas de lectura de la instancia de base de datos.
    a. En la consola, elija Databases (Bases de datos) y, después, seleccione la instancia de base de datos que desea actualizar.
    b. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).
    c. Proporcione un valor de DB instance identifier (Identificador de instancias de bases de datos) para su réplica de lectura y asegúrese de que el valor de DB instance class (Clase de

instancia de base de datos) y otros ajustes coincidan con su instancia de base de datos de MySQL 5.7.

d. Elija Create read replica (Crear réplica de lectura).

3. (Opcional) Cuando se ha creado la réplica de lectura y Status (Estado) se muestra como Available (Disponible), convierta la réplica de lectura en una implementación Multi-AZ y habilite las copias de seguridad.

   De forma predeterminada, una réplica de lectura se crea con copias de seguridad desactivadas. Dado que la réplica de lectura se convierte en la instancia de base de datos de producción, es una práctica recomendada configurar una implementación multi-AZ y habilitar las copias de seguridad.

   a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de crear.

   b. Elija Modify.

   c. Para Multi-AZ deployment (Implementación Multi-AZ), elija Create a standby instance (Crear una instancia en espera).

   d. En Backup Retention Period (Periodo de retención de copia de seguridad), elija un valor positivo distinto de cero, por ejemplo, 3 días y, después, elija Continue (Continuar).

   e. En Programación de modificaciones, elija Aplicar inmediatamente.

   f. Elija Modificar la instancia de base de datos.

4. Cuando el Status (Estado) de la réplica de lectura se muestra como Available (Disponible), actualice la réplica de lectura a MySQL 8.0:

   a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de crear.

   b. Elija Modify.

   c. Para DB engine version (versión de motor de base de datos), elija la versión de MySQL 8.0 a la que se realizará la actualización y, luego, elija Continue (Continuar).

   d. En Programación de modificaciones, elija Aplicar inmediatamente.

   e. Elija Modify DB instance (Modificar instancia de base de datos) para comenzar la actualización.

5. Cuando haya finalizado la actualización y el Status (Estado) se muestre como Available (Disponible), verifique que la réplica de lectura actualizada esté al día con la instancia de base de datos de MySQL 5.7 de origen. Para comprobarlo, conéctese a la réplica de lectura y ejecute

el comando `SHOW REPLICA STATUS`. Si el campo `Seconds_Behind_Master` muestra `0`, significa que la replicación está al día.

> **Note**
>
> Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

6. (Opcional) Cree una réplica de lectura de su réplica de lectura.

   Si desea que la instancia de base de datos tenga una réplica de lectura después de promocionarse a una instancia de base de datos independiente, puede crear la réplica de lectura ahora.

   a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de actualizar.

   b. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).

   c. Proporcione un valor de DB instance identifier (Identificador de instancias de bases de datos) para su réplica de lectura y asegúrese de que el valor de DB instance class (Clase de instancia de base de datos) y otros ajustes coincidan con su instancia de base de datos de MySQL 5.7.

   d. Elija Create read replica (Crear réplica de lectura).

7. (Opcional) Configure un grupo de parámetros de base de datos personalizado para la réplica de lectura.

   Si desea que la instancia de base de datos utilice un grupo de parámetros personalizado después de promocionarse a una instancia de base de datos independiente, puede crear el grupo de parámetros de base de datos ahora y asociarlo con la réplica de lectura.

   a. Cree un grupo de parámetros de base de datos personalizado para MySQL 8.0. Para obtener instrucciones, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS.

   b. Modifique los parámetros que desea cambiar en el grupo de parámetros de base de datos que acaba de crear. Para obtener instrucciones, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

   c. En la consola, elija Databases (Bases de datos) y, a continuación, elija la réplica de lectura.

d. Elija Modify.

e. Para el DB parameter group (grupo de parámetros de base de datos), elija el grupo de parámetros de base de datos de MySQL 8.0 que acaba de crear y, a continuación, elija Continue (Continuar).

f. En Programación de modificaciones, elija Aplicar inmediatamente.

g. Elija Modify DB instance (Modificar instancia de base de datos) para comenzar la actualización.

8. Haga que su réplica de lectura de MySQL 8.0 sea una instancia de base de datos independiente.

> **Important**
>
> Cuando promocione su réplica de lectura de MySQL 8.0 a instancia de base de datos independiente, dejará de ser una réplica de su instancia de base de datos de MySQL 5.7. Recomendamos que promocione su réplica de lectura de MySQL 8.0 durante un periodo de mantenimiento cuando su instancia de base de datos de MySQL 5.7 de origen esté en modo de solo lectura y se hayan suspendido todas las operaciones de escritura. Cuando haya finalizado la promoción, puede dirigir sus operaciones de escritura a la instancia de base de datos de MySQL 8.0 actualizada para asegurarse de que no se pierda ninguna operación de escritura.
> Además, recomendamos que antes de promocionar su réplica de lectura de MySQL 8.0 realice todas las operaciones de lenguaje de definición de datos (DDL) necesarias en la réplica de lectura de MySQL 8.0. Un ejemplo es la creación de índices. Este enfoque evita los efectos negativos en el rendimiento de la réplica de lectura de MySQL 8.0 después de su promoción. Para promocionar una réplica de lectura, siga este procedimiento.

a. En la consola, elija Databases (Bases de datos) y, después, seleccione la réplica de lectura que acaba de actualizar.

b. En Actions (Acciones), seleccione Promote (Promover).

c. Elija Yes (Sí) para habilitar las copias de seguridad automatizadas para la instancia de réplica de lectura. Para obtener más información, consulte Introducción a las copias de seguridad.

d. Elija Continue.

e. Elija Promote Read Replica.

9. Ahora tiene una versión actualizada de su base de datos MySQL. En este punto, puede dirigir sus aplicaciones a la nueva instancia de base de datos de MySQL 8.0.

Actualización de una versión del motor de instantáneas de base de datos de MySQL

Con Amazon RDS, puede crear una instantánea de base de datos de volumen de almacenamiento de su instancia de base de datos de MySQL. Cuando se crea una instantánea de base de datos, esta se basa en la versión del motor empleada por la instancia de base de datos. Puede actualizar la versión del motor para las instantáneas de base de datos.

Para RDS para MySQL, puede actualizar una instantánea de la versión 5.7 a la versión 8.0 o una instantánea de la versión 8.0. a la versión 8.4. Puede actualizar instantáneas de base de datos cifradas o no cifradas.

Para ver las versiones de motor disponibles para la instantánea de base de datos de RDS para MySQL, utilice el siguiente ejemplo de AWS CLI.

```
aws rds describe-db-engine-versions --engine mysql --include-all --engine-
version example-engine-version --query "DBEngineVersions[*].ValidUpgradeTarget[*].
{EngineVersion:EngineVersion}" --output text
```

Si no ve los resultados de la instantánea, es posible que la versión del motor esté obsoleta. Si la versión del motor ha quedado obsoleta, le recomendamos que actualice al destino de actualización de versión principal más reciente o a uno de los demás destinos de actualización disponibles para esa versión. Para obtener más información, consulte Opciones de actualización para instantáneas de bases de datos con versiones de motor no compatibles con RDS para MySQL.

Después de restaurar una instantánea de base de datos actualizada a una nueva versión del motor, asegúrese que la actualización se ha realizado correctamente. Para obtener más información acerca de una actualización de versión principal, consulte the section called “Actualizaciones del motor de base de datos de MySQL”. Para aprender a restaurar una instantánea de base de datos, consulte the section called “Restauración a una instancia de base de datos”.

> **Note**
>
> No puede actualizar las instantáneas de base de datos automatizadas que se hayan creado durante el proceso de copia de seguridad automatizado.

Puede actualizar una instantánea de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS.

Console

Para actualizar la versión del motor de una instantánea de base de datos mediante la AWS Management Console, siga el siguiente procedimiento.

Para actualizar una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea que desea actualizar.
4. En Actions (Acciones), seleccione Upgrade Snapshot (Actualizar instantánea). Aparece la página Upgrade snapshot.
5. Elija la New engine version (Nueva versión del motor) a la que actualizarse.
6. Elija Save changes (Guardar cambios) para actualizar la instantánea.

   Durante el proceso de actualización, todas las acciones están deshabilitadas para esta instantánea de base de datos. Además, el estado de la instantánea de base de datos cambia de Disponible a Actualizando y después cambia a Activo al completarse. Si la instantánea de base de datos no se puede actualizar porque se ha dañado, el estado cambia a No disponible. No puede recuperar el snapshot desde este estado.

   > **Note**
   >
   > Si la actualización de la base de datos falla, la instantánea se revierte al estado original con la versión original.

AWS CLI

Para actualizar una instantánea de base de datos a una nueva versión del motor de base de datos, ejecute el comando modify-db-snapshot de la AWS CLI.

Opciones

- `--db-snapshot-identifier`: identificador de la instantánea de base de datos que se va a actualizar. El identificador debe ser un Nombre de recurso de Amazon (ARN). Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

- `--engine-version`: versión del motor a la que se va a actualizar la instantánea de base de datos.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-snapshot \

    --db-snapshot-identifier my_db_snapshot \
    --engine-version new_version
```

Para Windows:

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier my_db_snapshot ^
    --engine-version new_version
```

Amazon RDS API

Para actualizar una instantánea de base de datos a una nueva versión del motor de base de datos, llame a la operación ModifyDBSnapshot de la API de RDS.

Parámetros

- `DBSnapshotIdentifier`: identificador de la instantánea de base de datos que se va a actualizar. El identificador debe ser un Nombre de recurso de Amazon (ARN). Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.
- `EngineVersion`: versión del motor a la que se va a actualizar la instantánea de base de datos.

Opciones de actualización para instantáneas de bases de datos con versiones de motor no compatibles con RDS para MySQL

En la siguiente tabla, se muestran las versiones de motor a las que puede actualizar desde una versión de motor no compatible con las instantáneas de base de datos de RDS para MySQL.

> **Note**
>
> Puede que tenga que actualizar la instantánea de base de datos más de una vez para actualizar a la versión de motor que haya elegido.

Versión del motor de instantáneas de base de datos	Versiones del motor disponibles para su actualización
5.5.8	5.5.62, 5.6.51
5.5.12	5.5.62, 5.6.51
5.5.20	5.5.62, 5.6.51
5.5.23	5.5.62, 5.6.51
5.5.25a	5.5.62, 5.6.51
5.5.27	5.5.62, 5.6.51
5.5.31	5.5.62, 5.6.51
5.5.33	5.5.62, 5.6.51
5.5.37	5.5.62, 5.6.51
5.5.38	5.5.62, 5.6.51
5.5.40	5.5.62, 5.6.51
5.5.40a	5.5.62, 5.6.51
5.5.40b	5.5.62, 5.6.51
5.5.41	5.5.62, 5.6.51
5.5.42	5.5.62, 5.6.51
5.5.59	5.5.62, 5.6.51

Versión del motor de instantáneas de base de datos	Versiones del motor disponibles para su actualización
5.6.12	5.6.51, 5.7.44
5.6.13	5.6.51, 5.7.44
5.6.17	5.6.51, 5.7.44
5.6.19	5.6.51, 5.7.44
5.6.19a	5.6.51, 5.7.44
5.6.19b	5.6.51, 5.7.44
5.6.21	5.6.51, 5.7.44
5.6.21b	5.6.51, 5.7.44
5.6.22	5.6.51, 5.7.44
5.6.23	5.6.51, 5.7.44
5.6.27	5.6.51, 5.7.44
5.6.27a	5.6.51, 5.7.44
5.7.10	5.7.44, 5.7.44-rds.20240408, 5.7.44-rds.20240529, 5.7.44-rds.20250103, 5.7.44-rds.20250213, 8.0.32, 8.0.33, 8.0.34, 8.0.35, 8.0.36, 8.0.37, 8.0.39, 8.0.40, 8.0.41
5.7.11	5.7.44, 5.7.44-rds.20240408, 5.7.44-rds.20240529, 5.7.44-rds.20250103, 5.7.44-rds.20250213, 8.0.32, 8.0.33, 8.0.34, 8.0.35, 8.0.36, 8.0.37, 8.0.39, 8.0.40, 8.0.41
5.7.12	5.7.44, 5.7.44-rds.20240408, 5.7.44-rds.20240529, 5.7.44-rds.20250103, 5.7.44-rds.20250213, 8.0.32, 8.0.33, 8.0.34, 8.0.35, 8.0.36, 8.0.37, 8.0.39, 8.0.40, 8.0.41

Importación de datos en una instancia de base de datos de Amazon RDS para MySQL

Puede usar varias técnicas diferentes para importar datos en una instancia de base de datos de RDS for MySQL. El mejor enfoque depende de varios factores:

- Origen de los datos
- Cantidad de datos
- Importar una vez o de forma continua
- Cantidad de tiempo de inactividad

Si también está migrando una aplicación con los datos, es importante tener en cuenta la cantidad de tiempo de inactividad.

En la tabla siguiente se muestran técnicas para la importación de datos en una instancia de base de datos de RDS para MySQL:

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Base de datos MySQL existente localmente o en Amazon EC2	Cualquiera	Una vez	Alguno	Crear una copia de seguridad de una base de datos local, almacenarlo en Amazon S3 y luego restaurar el archivo de copia de seguridad en una nueva instancia de base de datos de Amazon RDS que ejecute MySQL.	Restauración de una copia de seguridad en una instancia de base de

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
					datos MySQL.

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Base de datos MySQL existente localmente o en Amazon EC2	Cualquiera	Continuo	Mínima	Configurar la replicación con una base de datos de MySQL existente como origen de replicación.	Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa Importación de datos a una base de datos de Amazon RDS para MySQL con un

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
					tiempo de inactividad reducido

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Cualquier base de datos existente	Cualquiera	Una vez o continua	Mínima	Utilizar AWS Database Migration Service para migrar la base de datos con un tiempo de inactividad mínimo y, para numerosos motores de base de datos, continuar las replicaciones en curso.	Qué es AWS Database Migration Service y Uso de una base de datos compatible con MySQL como destino para AWS DMS en la Guía del usuario de AWS Database Migration Service

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Instancia de base de datos MySQL existente	Cualquiera	Una vez o continua	Mínima	Cree una réplica de lectura para la replicación continua. Promocione la réplica de lectura para la creación única de una nueva instancia de base de datos.	Trabajo con réplicas de lectura de instancias de base de datos

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Base de datos MySQL existente	Pequeña	Una vez	Alguno	Copie los datos directamente en la instancia de base de datos de MySQL utilizando una utilidad de línea de comandos.	Importación de datos de una base de datos MySQL externa a una instancia de base de datos de Amazon RDS para MySQL

Origen	Cantidad de datos	Una vez o continua	Tiempo de inactividad de las aplicaciones	Técnica	Más información
Datos no almacenados en una base de datos existente	Media	Una vez	Alguno	Cree archivos sin formato e impórtelos utilizando instrucciones `LOAD DATA LOCAL INFILE` de MySQL.	Importación de datos de cualquier origen a una instancia de base de datos de Amazon RDS para MySQL

> **Note**
>
> La base de datos del sistema `mysql` contiene la información de autenticación y autorización necesaria para iniciar sesión en la instancia de base de datos y obtener acceso a los datos. La eliminación, la modificación, el cambio de nombre o el truncamiento de tablas, datos u otros contenidos de la base de datos `mysql` de la instancia de base de datos puede provocar un error e impedir el acceso a la instancia de base de datos y a los datos. En ese caso, puede restaurar la instancia de base de datos desde una instantánea usando el comando AWS CLI de la restore-db-instance-from-db-snapshot. Puede recuperar la instancia de base de datos utilizando el comando AWS CLI de la restore-db-instance-to-point-in-time.

Consideraciones sobre la importación de datos para MySQL

En el siguiente contenido se encuentra información técnica relacionada con la carga de datos en MySQL. Este contenido está dirigido a usuarios familiarizados con la arquitectura del servidor de MySQL.

Registro binario

La habilitación del registro binario reduce el rendimiento de la carga de datos y requiere hasta cuatro veces más espacio en disco en comparación con el registro desactivado. El tamaño de la transacción utilizado para cargar los datos afecta directamente al rendimiento del sistema y a las necesidades de espacio en disco, las transacciones más grandes requieren más recursos.

Tamaño de la transacción

El tamaño de la transacción influye en los siguientes aspectos de las cargas de datos de MySQL:

- Consumo de recursos
- Utilización del espacio en disco
- Reanudación del proceso
- Tiempo de recuperación
- Formato de entrada (archivos sin formato o SQL)

En esta sección se describe el modo en que el tamaño de transacción afecta al registro binario y se argumentan los beneficios de desactivar el registro binario durante la carga de grandes volúmenes de datos. Puede habilitar y desactivar el registro binario estableciendo el periodo de retención de copia de seguridad automatizado de Amazon RDS. Un valor distinto de cero activa el registro binario y el valor cero lo desactiva. Para obtener más información, consulte Backup retention period (Periodo de retención de copia de seguridad).

En esta sección también se describe el impacto de las transacciones de gran tamaño en InnoDB y por qué es importante que los tamaños de transacción sean pequeños.

Transacciones pequeñas

En las transacciones pequeñas, el registro binario duplica el número de escrituras en disco requeridas para cargar los datos. Este efecto puede degradar el desempeño notablemente en otras

sesiones de base de datos y aumentar el tiempo requerido para cargar los datos. La degradación experimentada depende en parte de los siguientes factores:

- Tasa de carga
- Otra actividad de la base de datos que tenga lugar durante la carga
- Capacidad de la instancia de base de datos de Amazon RDS

Los registros binarios también consumen un espacio en disco aproximadamente igual al volumen de datos cargado hasta que se hace una copia de seguridad de los registros y se eliminan. Amazon RDS minimiza este impacto creando copias de seguridad de los registros binarios y retirándolos con frecuencia.

Transacciones grandes

En el caso de transacciones grandes, el registro binario triplica IOPS y el uso del disco por los siguientes motivos:

- La caché del registro binario almacena temporalmente los datos de las transacciones en el disco.
- Esta caché crece con el tamaño de la transacción, lo que consume espacio en disco.
- Cuando se completa la transacción (confirmación o reversión), el sistema copia la caché en el registro binario.

Este proceso crea tres copias de los datos:

- Los datos originales
- La caché en el disco
- La entrada del registro binario final

Cada operación de escritura implica una E/S adicional, lo que repercute aún más en el rendimiento.

Por este motivo, el registro binario requiere el triple de espacio en disco en comparación con el registro desactivado. Por ejemplo, si se cargan 10 GiB de datos en una sola transacción, se crean tres copias:

- 10 GiB para los datos de la tabla
- 10 GiB para la caché del registro binario
- 10 GiB para el archivo del registro binario

El espacio total en disco temporal necesario es 30 GiB.

Consideraciones importantes sobre el espacio en disco:

- El archivo de caché persiste hasta que finaliza la sesión o hasta que una nueva transacción crea otra caché.
- El registro binario permanece hasta que se realiza una copia de seguridad, lo que podría retener 20 GiB (caché y registro) durante un periodo prolongado.

Si se usa `LOAD DATA LOCAL INFILE` para cargar los datos, la recuperación de datos crea una cuarta copia en caso de que la base de datos deba recuperarse desde una copia de seguridad realizada antes de la carga. Durante la recuperación, MySQL extrae los datos desde el registro binario en un archivo sin formato. MySQL luego ejecuta `LOAD DATA LOCAL INFILE`. En función del ejemplo anterior, esta recuperación requiere un espacio total en disco temporal de 40 GiB o 10 GiB cada uno para la tabla, la caché, el registro y el archivo local. Sin al menos 40 GiB de espacio libre en disco, la recuperación produce un error.

Optimización de grandes cargas de datos

Para grandes cargas de datos, desactive el registro binario para reducir la sobrecarga y los requisitos de espacio en disco. Puede desactivar el registro binario estableciendo el periodo de retención de copias de seguridad en 0. Una vez completada la carga, restaure el periodo de retención de copias de seguridad al valor apropiado distinto de cero. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS y Periodo de retención de copia de seguridad en la tabla de configuración.

> **Note**
>
> Si la instancia de base de datos es una instancia de base de datos de origen para réplicas de lectura, no puede establecer el periodo de retención de copia de seguridad en 0.

Antes de cargar los datos, recomendamos que cree una instantánea de base de datos. Para obtener más información, consulte Administración de copias de seguridad manuales.

InnoDB

La siguiente información sobre las opciones de registro y recuperación para deshacer ayuda a mantener pequeñas las transacciones de InnoDB para optimizar el rendimiento de la base de datos.

Descripción del registro para deshacer InnoDB

Deshacer es un mecanismo de registro que permite la reversión de transacciones y admite el control de concurrencia multiversión (MVCC).

Para MySQL 5.7 y versiones anteriores, los registros para deshacer se almacenan en el espacio de tablas del sistema InnoDB (normalmente ibdata1) y se conservan hasta que el subproceso de purga los elimina. De este modo, las transacciones de carga de datos de gran tamaño pueden provocar que el espacio de tablas del sistema sea muy grande y consumir espacio en disco que no puede recuperar si no recrea la base de datos.

Para todas las versiones de MySQL, el subproceso de purga debe esperar para eliminar cualquier registro para deshacer hasta que la transacción activa más antigua se confirme o se revierta. Si la base de datos procesa otras transacciones durante la carga, los registros para deshacer también se acumulan y no pueden eliminarse, incluso si se confirman las transacciones y ninguna otra transacción necesita registros para deshacer MVCC. En esta situación, todas las transacciones, incluidas las de solo lectura, se ralentizan. Esta ralentización se produce porque todas las transacciones acceden a todas las filas que cualquier transacción (no solo la transacción de carga) cambia. En efecto, las transacciones deben examinar los registros para deshacer que las transacciones de carga de larga duración impidieron purgar durante una limpieza del registro para deshacer. Esto afecta al rendimiento de cualquier operación que acceda a las filas modificadas.

Opciones de recuperación de transacciones de InnoDB

Aunque InnoDB optimiza las operaciones de confirmación, las reversiones de transacciones grandes son lentas. Para una recuperación más rápida, realice una recuperación en un momento dado o restaure una instantánea de base de datos. Para obtener más información, consulte Recuperación a un momento dado y Restauración a una instancia de base de datos.

Formatos de importación de datos

MySQL admite dos formatos de importación de datos: archivos sin formato y SQL. Revise la información sobre cada formato para determinar cuál es la mejor opción para sus necesidades.

Archivos sin formato

Para transacciones pequeñas, cargue archivos sin formato con `LOAD DATA LOCAL INFILE`. Este formato de importación de datos puede proporcionar los siguientes beneficios en comparación con el uso de SQL:

- Menos tráfico de red
- Costos de transmisión de datos más bajos
- Menor sobrecarga de procesamiento de bases de datos
- Procesamiento más rápido

`LOAD DATA LOCAL INFILE` carga todo el archivo sin formato en una sola transacción. Mantenga pequeño el tamaño de los archivos individuales para obtener las siguientes ventajas:

- Posibilidad de reanudación: puede hacer un seguimiento de los archivos que se han cargado. Si surge un problema durante la carga, puede continuar donde se detuvo. Es posible que sea necesario volver a transmitir algunos datos a Amazon RDS, pero con los archivos pequeños, el volumen es mínimo.
- Carga de datos en paralelo: si tiene IOPS y ancho de banda de la red suficiente para la carga de un solo archivo, la carga en paralelo podría ahorrar tiempo.
- Control de la velocidad de carga: si la carga de datos tiene un impacto negativo en otros procesos, puede controlar la velocidad de carga aumentando el intervalo entre los archivos.

Las transacciones de gran tamaño reducen los beneficios de usar `LOAD DATA LOCAL INFILE` para importar datos. Cuando no pueda dividir una gran cantidad de datos en archivos más pequeños, considere la posibilidad de utilizar SQL.

SQL

SQL tiene una ventaja fundamental con respecto a los archivos sin formato: puede mantener pequeños los tamaños de transacción. Sin embargo, SQL puede tardar mucho más en cargar que los archivos sin formato. Además, después de un error, puede ser difícil determinar dónde reanudar, ya que no se pueden reiniciar los archivos mysqldump. Si se produce un error durante la carga de un archivo mysqldump, debe modificarlo o sustituirlo antes de poder reanudar la carga. Otra opción, después de corregir la causa del error, puede restaurar a un momento anterior a la carga antes de cargar y volver a enviar el archivo. Para obtener más información, consulte Recuperación a un momento dado.

Uso de instantáneas de base de datos de Amazon RDS para puntos de comprobación de la base de datos

Si carga datos durante periodos prolongados, como horas o días, sin registro binario, utilice las instantáneas de base de datos para proporcionar puntos de comprobación periódicos para garantizar

la seguridad de los datos. Cada instantánea de base de datos crea una copia coherente de la instancia de base de datos que sirve como punto de recuperación durante errores del sistema o eventos de corrupción de datos. Como las instantáneas de base de datos son rápidas, los puntos de comprobación frecuentes tienen un impacto mínimo en el rendimiento de la carga. Puede eliminar las instantáneas de base de datos anteriores sin que ello afecte a la durabilidad de la base de datos ni a las capacidades de recuperación. Para obtener más información acerca de las instantáneas de base de datos, consulte Administración de copias de seguridad manuales.

Reducción de los tiempos de carga de bases de datos

Los siguientes elementos son consejos adicionales para reducir los tiempos de carga:

- Cree todos los índices secundarios antes de cargar los datos en las bases de datos MySQL. A diferencia de otros sistemas de bases de datos, MySQL reconstruye toda la tabla al agregar o modificar índices secundarios. Este proceso crea una nueva tabla con los cambios de índice, copia todos los datos y elimina la tabla original.
- Cargue los datos en el orden de la clave principal. Para las tablas de InnoDB, esto puede reducir los tiempos de carga entre un 75 % y un 80 % y reducir el tamaño del archivo de datos en un 50 %.
- Desactive las restricciones de clave externa estableciendo `foreign_key_checks` en `0`. Esto es obligatorio en muchos casos para archivos sin formato cargados con `LOAD DATA LOCAL INFILE`. Para cualquier carga, desactivar las comprobaciones de claves externas acelera la carga de datos. Una vez completada la carga, vuelva a habilitar las restricciones configurando `foreign_key_checks` en 1 y verifique los datos.
- Cargue datos en paralelo a no ser que se aproxime al límite de los recursos. Para habilitar la carga simultánea en varios segmentos de la tabla, use tablas particionadas cuando sea apropiado.
- Para reducir la sobrecarga de ejecución de SQL, combine varias instrucciones `INSERT` en operaciones `INSERT` únicas con varios valores. `mysqldump` implementa esta optimización automáticamente.
- Reduzca las operaciones de E/S de registro de InnoDB estableciendo `innodb_flush_log_at_trx_commit` en `0`. Una vez completada la carga, restaure `innodb_flush_log_at_trx_commit` a 1.

> **Warning**
>
> Si se establece `innodb_flush_log_at_trx_commit` en `0`, InnoDB vaciará sus registros cada segundo en lugar de hacerlo con cada confirmación. Esta configuración

aumenta el rendimiento, pero puede conllevar el riesgo de perder transacciones si se produce un error en el sistema.

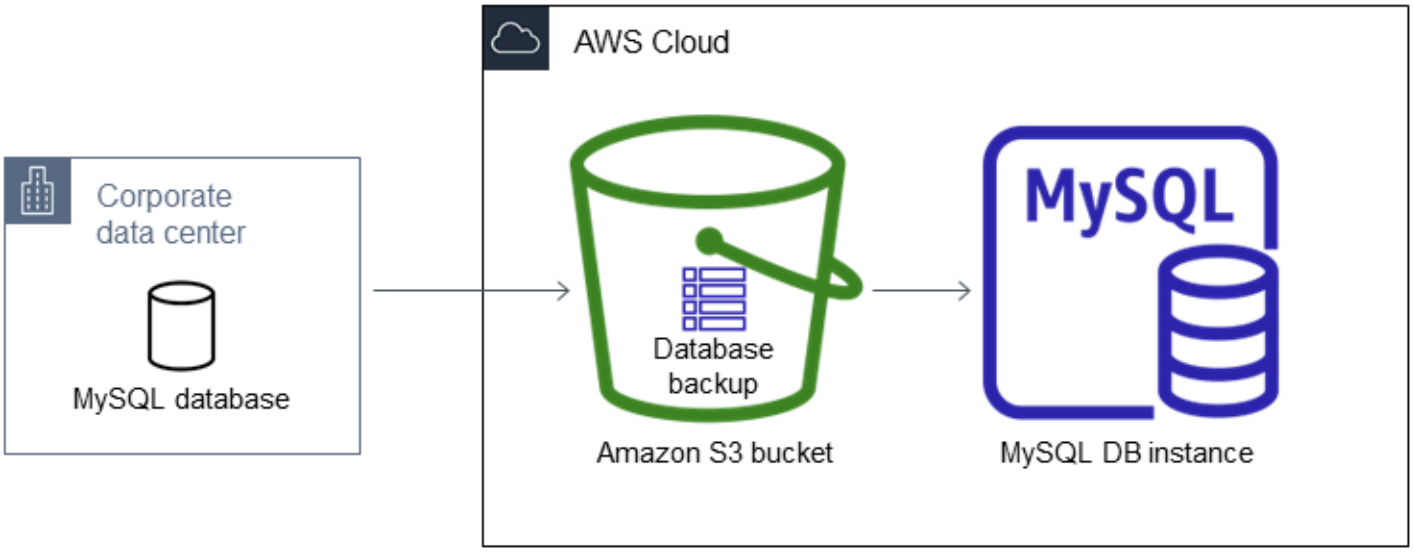
- Si va a cargar datos en una instancia de base de datos que no tiene réplicas de lectura, establezca `sync_binlog` en `0`. Una vez completada la carga, restaure `sync_binlog parameter` a `1`.
- Cargue los datos en una instancia de base de datos de Single-AZ antes de convertir la instancia de base de datos en una implementación Multi-AZ. Si la instancia de base de datos ya usa una implementación Multi-AZ, no se recomienda cambiar a una implementación Single-AZ para la carga de datos. Hacerlo solo proporciona mejoras marginales.

Restauración de una copia de seguridad en una instancia de base de datos MySQL.

Amazon RDS admite la importación de bases de datos MySQL mediante archivos de copia de seguridad. Puede crear una copia de seguridad de la base de datos y, a continuación, almacenarla en Amazon S3 y luego restaurar el archivo de copia de seguridad en una nueva instancia de base de datos de Amazon RDS que ejecuta MySQL.

La situación descrita en esta sección restaura una copia de seguridad de una base de datos en las instalaciones. Puede utilizar esta técnica para bases de datos en otras ubicaciones, como Amazon EC2 o los servicios en la nube que no son de AWS, siempre que se pueda acceder a la base de datos.

Puede encontrar la situación admitida en el siguiente diagrama.



La importación de archivos de copia de seguridad desde Amazon S3 es compatible con MySQL en todas las Regiones de AWS.

Recomendamos importar la base de datos a Amazon RDS mediante archivos de copia de seguridad si la base de datos en las instalaciones puede estar sin conexión mientras se crea, se copia y se restaura el archivo de copia de seguridad. Si la base de datos no puede estar sin conexión, puede usar la replicación de registro binario (binlog) para actualizar su base de datos una vez que haya migrado a Amazon RDS a través de Amazon S3 tal como se explica en este tema. Para obtener más información, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa. También puede utilizar AWS Database Migration Service para migrar su base de datos a Amazon RDS. Para obtener más información, consulte ¿Qué es AWS Database Migration Service?

Limitaciones y recomendaciones para importar archivos de copia de seguridad de Amazon S3 a Amazon RDS

A continuación se muestran algunas limitaciones y recomendaciones para importar archivos de copia de seguridad de Amazon S3:

- Solo puede importar sus datos a una nueva instancia de base de datos y no a una existente.
- Debe usar Percona XtraBackup para crear la copia de seguridad de su base de datos local.
- No puede importar datos de una exportación de instantáneas de base de datos a Amazon S3.
- No puede migrar de una base de datos de origen que tenga tablas definidas fuera del directorio de datos de MySQL predeterminado.
- Percona Server for MySQL no se admite como base de datos de origen, ya que puede contener tablas `compression_dictionary*` en el esquema `mysql`.
- Debe importar sus datos a la versión secundaria predeterminada de su versión principal de MySQL en su Región de AWS. Por ejemplo, si su versión principal es MySQL 8.0 y la versión secundaria predeterminada para su Región de AWS es 8.0.28, debe importar los datos en una instancia de base de datos de MySQL versión 8.0.28. Puede actualizar su instancia de base de datos después de la importación. Para obtener información acerca de cómo determinar la versión secundaria predeterminada, consulte Versiones de MySQL en Amazon RDS.
- No se admite la migración a versiones anteriores en el caso de las versiones principales y secundarias. Por ejemplo, no puede migrar de la versión 8.0 a la 5.7 ni migrar de la versión 8.0.32 a la versión 8.0.31.
- No puede importar la versión 5.5 o 5.6 de una base de datos MySQL.

- No puede importar una base de datos de MySQL en las instalaciones desde una versión principal a otra. Por ejemplo, no puede importar una base de datos de MySQL 5.7 a una base de datos de RDS para MySQL 8.0. Puede actualizar su instancia de base de datos una vez que complete la importación.
- No puede restaurar desde una base de datos de origen cifrada, pero puede restaurar a una instancia de base de datos de Amazon RDS cifrada.
- No puede restaurar desde una copia de seguridad cifrada en el bucket de Amazon S3.
- No se puede restaurar desde un bucket de Amazon S3 en una Región de AWS que no coincide con la de la instancia de base de datos de Amazon RDS.
- La importación de Amazon S3 no es compatible en la clase de instancia de base de datos db.t2.micro. Sin embargo, puede restaurar en otra clase de instancia de base de datos y, a continuación, cambiar la clase de instancia de base de datos posteriormente. Para obtener más información sobre las clases de instancias, consulte Especificaciones de hardware para clases de instancia de base de datos .
- Amazon S3 limita el tamaño de un archivo cargado en un bucket de Amazon S3 a 5 TB. Si un archivo de copia de seguridad supera los 5 TB, debe dividir el archivo de copia de seguridad en archivos más pequeños.
- Al restaurar la base de datos, la copia de seguridad se copia y, a continuación, se extrae en la instancia de base de datos. Por lo tanto, aprovisione un espacio de almacenamiento para la instancia de base de datos que sea igual o mayor que la suma del tamaño de la copia de seguridad, más el tamaño de la base de datos original en el disco.
- Amazon RDS limita el número de archivos cargados en un bucket de Amazon S3 a 1 millón. Si los datos de copia de seguridad de su base de datos, con todas las copias de seguridad completas e incrementales, superan 1 millón de archivos, use un archivo Gzip (.gz), tar (.tar.gz) o Percona xbstream (.xbstream) para almacenar archivos de copia de seguridad completas e incrementales en el bucket de Amazon S3. Percona XtraBackUp 8.0 solo admite Percona xbstream para la compresión.
- Las cuentas de usuario no se importan automáticamente. Guarde sus cuentas de usuario de su base de datos de origen y añádalas a su nueva instancia de base de datos posteriormente.
- Las funciones no se importan automáticamente. Guarde sus funciones de su base de datos de origen y añádalas a su nueva instancia de base de datos posteriormente.
- Los procedimientos almacenados no se importan automáticamente. Guarde sus procedimientos almacenados de su base de datos de origen y añádalos a su nueva instancia de base de datos posteriormente.

- La información de zona horaria no se importa automáticamente. Registre la información de zona horaria para su base de datos de origen y establezca la zona horaria de su nueva instancia de base de datos posteriormente. Para obtener más información, consulte Zona horaria local para las instancias de bases de datos MySQL.
- El parámetro `innodb_data_file_path` debe configurarse con un solo archivo de datos que utilice el nombre de archivo de datos predeterminado `"ibdata1:12M:autoextend"`. Las bases de datos con dos archivos de datos, o con un archivo de datos con un nombre diferente, no se pueden migrar con este método.

  A continuación se muestran ejemplos de nombres de archivo no permitidos: `"innodb_data_file_path=ibdata1:50M; ibdata2:50M:autoextend"` y `"innodb_data_file_path=ibdata01:50M:autoextend"`.
- El tamaño máximo de la base de datos restaurada es el tamaño máximo admitido menos el tamaño de la copia de seguridad. Por lo tanto, si el tamaño máximo de la base de datos admitido es 64 TiB y el tamaño de la copia de seguridad es 30 TiB, el tamaño máximo de la base de datos restaurada será de 34 TiB, como en el ejemplo siguiente:

  ```
  64 TiB - 30 TiB = 34 TiB
  ```

  Para obtener información sobre el tamaño máximo de base de datos admitido en Amazon RDS for MySQL, consulte Almacenamiento de SSD de uso general y Almacenamiento de SSD de IOPS aprovisionadas.

Información general de configuración para importar archivos de copia de seguridad de Amazon S3 a Amazon RDS

Estos son los componentes que necesita configurar para importar archivos de copia de seguridad de Amazon S3 a Amazon RDS:

- Un bucket de Amazon S3 para almacenar los archivos de copia de seguridad.
- una copia de seguridad de su base de datos local creada por Percona XtraBackup.
- Un rol de AWS Identity and Access Management (IAM) para permitir a Amazon RDS el acceso al bucket.

Si ya tiene un bucket de Amazon S3, puede utilizarlo. Si no dispone de un bucket de Amazon S3, puede crear uno nuevo. Si desea crear un bucket, consulte Creación de un bucket.

Use la herramienta Percona XtraBackup para crear su copia de seguridad. Para obtener más información, consulte Creación de su copia de seguridad de base de datos.

Si ya tiene un rol de IAM, puede utilizarlo. Si no dispone de un rol de IAM, puede crear uno manualmente. También puede elegir que el asistente cree automáticamente un rol de IAM nuevo en su cuenta cuando restaure la base de datos desde la AWS Management Console. Si desea crear un nuevo rol de IAM manualmente o asociar políticas de confianza y de permisos a un rol de IAM existente, consulte Creación manual de un rol de IAM. Si desea hacer que se cree un nuevo rol de IAM automáticamente, siga el procedimiento en Consola.

Creación de su copia de seguridad de base de datos

Use el software Percona XtraBackup para crear su backup. Le recomendamos que utilice la última versión de Percona XtraBackup. Puede instalar Percona XtraBackup desde el artículo sobre cómo descargar Percona XtraBackup.

> **Warning**
>
> Cuando crea una copia de seguridad de base de datos, es posible que XtraBackup guarde credenciales en el archivo xtrabackup_info. Asegúrese de examinar ese archivo para que la configuración `tool_command` no contenga información confidencial.

> **Note**
>
> Para la migración de MySQL 8.0, debe usar Percona XtraBackup 8.0. Percona XtraBackup 8.0.12 y versiones posteriores admiten la migración de todas las versiones de MySQL.
> Si migra a RDS for MySQL 8.0.20 o posterior, debe usar Percona XtraBackup 8.0.12 o posterior.
> Para las migraciones de MySQL 5.7, también puede usar Percona XtraBackup 2.4. Para migraciones de versiones de MySQL anteriores, también puede usar Percona XtraBackup 2.3 o 2.4.

Puede crear una copia de seguridad completa de sus archivos de base de datos MySQL mediante Percona XtraBackup. Como alternativa, si ya usa Percona XtraBackup para realizar las copias de seguridad de los archivos de la base de datos MySQL, puede cargar los archivos y los directorios de backup completos e incrementales.

Para obtener más información acerca de cómo realizar una copia de seguridad de su base de datos con Percona XtraBackup, consulte la documentación de Percona XtraBackup y el artículo sobre el archivo binario xtrabackup en el sitio web de Percona.

Creación de una copia de seguridad completa con Percona XtraBackup

Si desea crear una copia de seguridad completa de los archivos de base de datos de MySQL que se pueda restaurar desde Amazon S3, use la utilidad Percona XtraBackup (`xtrabackup`) para crear una copia de seguridad de la base de datos.

Por ejemplo, el siguiente comando crea un backup de una base de datos MySQL y almacena los archivos en la carpeta `/on-premises/s3-restore/backup`.

```
xtrabackup --backup --user=<myuser> --password=<password> --target-dir=</on-premises/
s3-restore/backup>
```

Si desea comprimir su backup en un solo archivo (que se puede dividir posteriormente si es necesario), puede guardar el backup en uno de los siguientes formatos:

- Gzip (.gz)
- tar (.tar)
- Percona xbstream (.xbstream)

> **Note**
>
> Percona XtraBackUp 8.0 solo admite Percona xbstream para la compresión.

El siguiente comando crea una copia de seguridad de la base de datos MySQL dividido en varios archivos Gzip.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=tar \
   --target-dir=</on-premises/s3-restore/backup> | gzip - | split -d --bytes=500MB \
   - </on-premises/s3-restore/backup/backup>.tar.gz
```

El siguiente comando crea una copia de seguridad de la base de datos MySQL dividido en varios archivos tar.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=tar \
   --target-dir=</on-premises/s3-restore/backup> | split -d --bytes=500MB \
   - </on-premises/s3-restore/backup/backup>.tar
```

El siguiente comando crea una copia de seguridad de la base de datos MySQL dividido en varios archivos xbstream.

```
xtrabackup --backup --user=<myuser> --password=<password> --stream=xbstream \
   --target-dir=</on-premises/s3-restore/backup> | split -d --bytes=500MB \
   - </on-premises/s3-restore/backup/backup>.xbstream
```

> **Note**
>
> Si aparece el siguiente error, puede deberse a que se han mezclado formatos de archivo en el comando:
>
> ```
> ERROR:/bin/tar: This does not look like a tar archive
> ```

Uso de copias de seguridad incrementales con Percona XtraBackup

Si ya usa Percona XtraBackup para realizar copias de seguridad completas e incrementales de sus archivos de base de datos MySQL, no tiene que crear una copia de seguridad completa y cargar los archivos del backup en Amazon S3. En lugar de eso, puede ahorrar una cantidad considerable de tiempo copiando los directorios y archivos de backup existentes en su bucket de Amazon S3. Para obtener más información acerca de la creación de copias de seguridad incrementales con Percona XtraBackup, consulte el artículo acerca de la copia de seguridad incremental.

Cuando copie los archivos de backup completos o incrementales en un bucket de Amazon S3, debe copiar repetidamente el contenido del directorio base. Esos contenidos incluyen el backup completo y también todos los directorios y archivos del backup incremental. Esta copia debe mantener la estructura de directorios en el bucket de Amazon S3. Amazon RDS realiza iteraciones por todos los archivos y directorios. Amazon RDS utiliza el archivo `xtrabackup-checkpoints` incluido con cada copia de seguridad progresiva para identificar el directorio base y ordenar las copias de seguridad progresivas por rango del número de secuencia del registro (LSN).

Consideraciones sobre copias de seguridad para Percona XtraBackup

Amazon RDS consume sus archivos de copia de seguridad en función del nombre de archivo. Asigne la extensión de archivo adecuada a los archivos de copia de seguridad según el formato de archivo: por ejemplo, `.xbstream` para archivos almacenados con el formato xbstream de Percona.

Amazon RDS consume sus archivos de backup en orden alfabético, así como según la numeración natural. Utilice la opción `split` al ejecutar el comando `xtrabackup` para asegurarse de que la escritura y la asignación de nombre de sus archivos de backup se realice en el orden correcto.

Amazon RDS no admite copias de seguridad parciales creados con Percona XtraBackup. No puede utilizar las siguientes opciones para crear una copia de seguridad parcial al realizar copias de seguridad de los archivos de origen de su base de datos: `--tables`, `--tables-exclude`, `--tables-file`, `--databases`, `--databases-exclude` o `--databases-file`.

Amazon RDS admite copias de seguridad incrementales creadas con Percona XtraBackup. Para obtener más información acerca de la creación de copias de seguridad incrementales con Percona XtraBackup, consulte el artículo acerca de la copia de seguridad incremental.

Creación manual de un rol de IAM

Si no dispone de un rol de IAM, puede crear uno manualmente. Sin embargo, si restaura la base de datos mediante la AWS Management Console, le recomendamos que siga el procedimiento descrito en Consola y elija que RDS cree este nuevo rol de IAM por usted.

Para crear manualmente un nuevo rol de IAM para importar su base de datos desde Amazon S3, debe crear un rol para delegar permisos de Amazon RDS al bucket de Amazon S3. Cuando cree un rol de IAM, debe asociar políticas de confianza y de permisos. Para importar sus archivos de copia de seguridad desde Amazon S3, utilice políticas de confianza y permisos similares a los siguientes ejemplos. Para obtener más información acerca de cómo crear un rol, consulte Crear un rol para delegar permisos a un servicio AWS.

Para utilizar las políticas de confianza y de permisos es necesario proporcionar un nombre de recurso de Amazon (ARN). Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Example política de confianza para importar desde Amazon S3

```
{
    "Version": "2012-10-17",
    "Statement":
```

```
    [{
        "Effect": "Allow",
        "Principal": {"Service":  "rds.amazonaws.com"},
        "Action": "sts:AssumeRole"
    }]
}
```

Example política de permisos para importar desde Amazon S3: permisos de usuario de IAM

En el siguiente ejemplo, sustituya *iam_user_id* por su propio valor.

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Sid":"AllowS3AccessRole",
            "Effect":"Allow",
            "Action":"iam:PassRole",
            "Resource":"arn:aws:iam::iam_user_id:role/S3Access"
        }
    ]
}
```

Example política de permisos para importar desde Amazon S3: permisos de rol

En el siguiente ejemplo, sustituya *amzn-s3-demo-bucket* y *prefix* con sus propios valores.

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
        "Effect": "Allow",
        "Action":
            [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
        "Effect": "Allow",
```

```
        "Action":
            [
                "s3:GetObject"
            ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix*"
        },
        { // If your bucket is encrypted, include the following permission. This
 permission allows decryption of your AWS KMS key.
        "Effect": "Allow",
        "Action":
            [
                "kms:Decrypt"
            ],
        "Resource": [
            "arn:aws:kms:region:customer_id:key/key_id*"
            ]
        }
    ]
}
```

> **Note**
>
> Si incluye un prefijo del nombre de archivo, incluya el asterisco (*) después del prefijo. Si no desea especificar ningún prefijo, especifique únicamente un asterisco.

Importación de datos desde Amazon S3 a una nueva instancia de base de datos de MySQL

Puede importar datos desde Amazon S3 a una nueva instancia de base de datos de MySQL mediante la AWS Management Console, la AWS CLI o la API de RDS.

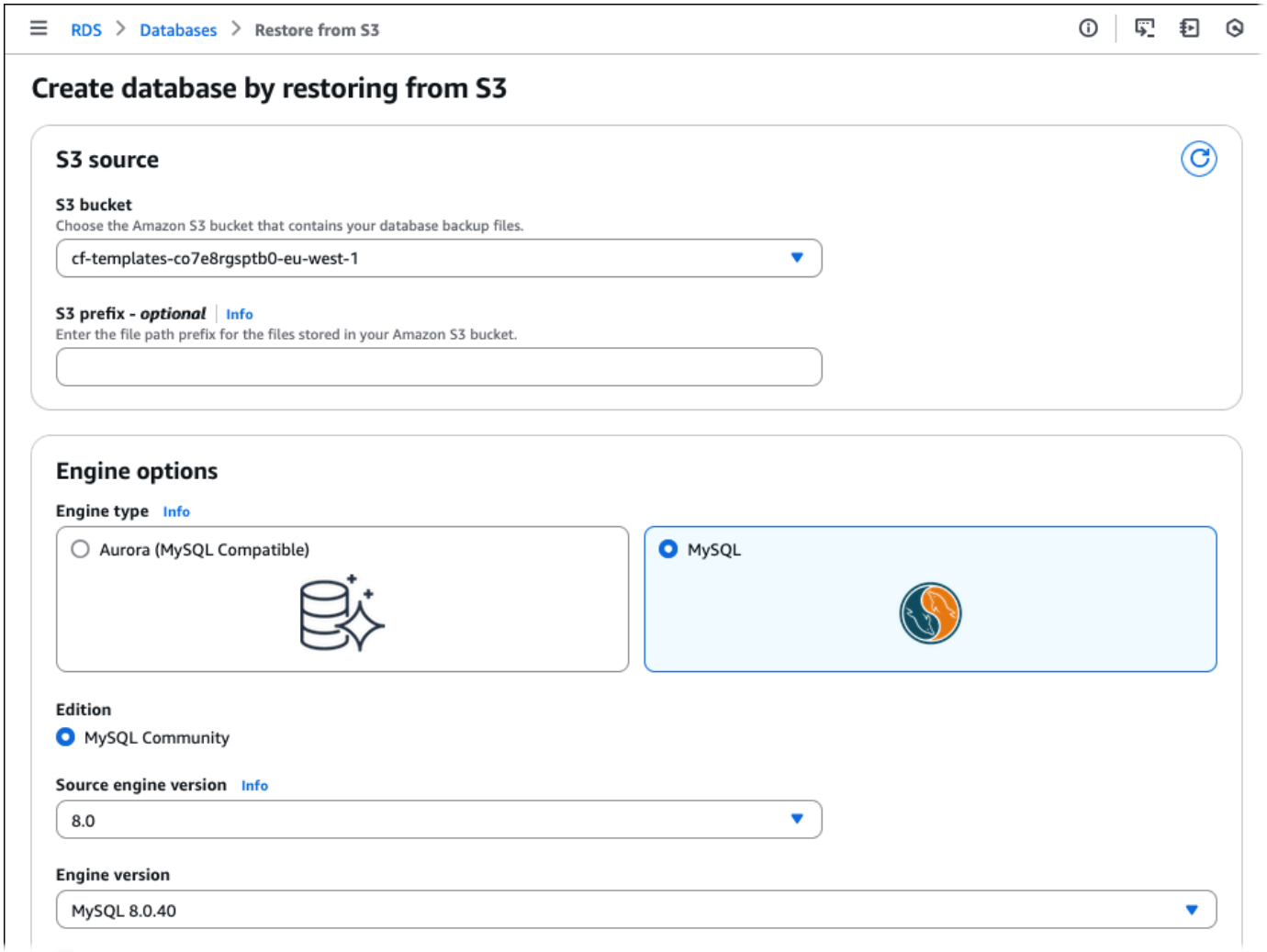
Consola

Para importar datos desde Amazon S3 a una nueva instancia de base de datos MySQL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que se va a crear su instancia de base de datos. Elija la misma Región de AWS que el bucket de Amazon S3 que contiene su copia de seguridad de base de datos.

3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Elija Restore from S3 (Restaurar de S3).

   Aparecerá la página Create database by restoring from S3 (Crear base de datos restaurando desde S3).



5. En S3 destination (destino de S3):

   a. Elija el bucket de S3 que contiene la copia de seguridad.

   b. (Opcional) Para prefijo de S3, escriba un prefijo de ruta de archivo para los archivos almacenados en el bucket de Amazon S3.

      Si no especifica un prefijo, RDS creará su instancia de base de datos con todos los archivos y carpetas de la carpeta raíz del bucket de S3. Si especifica un prefijo, RDS creará su instancia de base de datos con los archivos y carpetas del bucket de S3 cuya ruta completa del archivo empieza con el prefijo especificado.

Por ejemplo, suponga que almacena los archivos de backup en S3 en una subcarpeta denominada copias de seguridad y que tiene varios conjuntos de archivos de backup, cada uno en su propio directorio (gzip_backup1, gzip_backup2, etc.). En este caso, debe especificar un prefijo de backups/gzip_backup1 para restaurar a partir de los archivos de la carpeta gzip_backup1.

6. En Engine options (Opciones del motor):

   a. En Engine type (Tipo de motor), seleccione MySQL.

   b. En Source engine version (Versión del motor de origen), seleccione la versión principal de MySQL de su base de datos de origen.

   c. Para Version de motor, elija la versión secundaria predeterminada de su versión principal de MySQL en su Región de AWS.

      En AWS Management Console, solo está disponible la versión secundaria predeterminada. Puede actualizar su instancia de base de datos después de la importación.

7. Para el rol de IAM, cree o selección el rol de IAM con la política de confianza y la política de permisos requeridas que permitan a Amazon RDS acceder a su bucket de Amazon S3. Lleve a cabo una de las siguientes acciones:

   - (Recomendado) Elija Crear un nuevo rol e introduzca el Nombre de rol de IAM. Con esta opción, RDS crea automáticamente el rol con la política de confianza y la política de permisos.
   - Elija un rol de IAM existente. Asegúrese de que este rol cumpla con todos los criterios de the section called “Creación manual de un rol de IAM”.

8. Especifique la información de la instancia de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.

   > **Note**
   >
   > Asegúrese de asignar memoria suficiente para su nueva instancia de base de datos de modo que la operación de restauración pueda realizarse correctamente.
   > También puede elegir Enable storage autoscaling (Habilitar el escalado automático del almacenamiento) para permitir el crecimiento futuro automáticamente.

9. Elija ajustes adicionales según sea necesario.

10. Elija Create database (Crear base de datos).

AWS CLI

Para importar datos desde Amazon S3 a una nueva instancia de base de datos de MySQL mediante la AWS CLI, llame el comando restore-db-instance-from-s3 con los siguientes parámetros. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.

> **Note**
>
> Asegúrese de asignar memoria suficiente para su nueva instancia de base de datos de modo que la operación de restauración pueda realizarse correctamente.
> También puede utilizar el parámetro `--max-allocated-storage` para habilitar el escalado automático del almacenamiento y permitir el crecimiento futuro automáticamente.

- `--allocated-storage`
- `--db-instance-identifier`
- `--db-instance-class`
- `--engine`
- `--master-username`
- `--manage-master-user-password`
- `--s3-bucket-name`
- `--s3-ingestion-role-arn`
- `--s3-prefix`
- `--source-engine`
- `--source-engine-version`

Example

Para Linux, macOS o:Unix

```
aws rds restore-db-instance-from-s3 \
    --allocated-storage 250 \
    --db-instance-identifier myidentifier \
    --db-instance-class db.m5.large \
    --engine mysql \
    --master-username admin \
```

```
    --manage-master-user-password \
    --s3-bucket-name amzn-s3-demo-bucket \
    --s3-ingestion-role-arn arn:aws:iam::account-number:role/rolename \
    --s3-prefix bucketprefix \
    --source-engine mysql \
    --source-engine-version 8.0.32 \
    --max-allocated-storage 1000
```

En:Windows

```
aws rds restore-db-instance-from-s3 ^
    --allocated-storage 250 ^
    --db-instance-identifier myidentifier ^
    --db-instance-class db.m5.large ^
    --engine mysql ^
    --master-username admin ^
    --manage-master-user-password ^
    --s3-bucket-name amzn-s3-demo-bucket ^
    --s3-ingestion-role-arn arn:aws:iam::account-number:role/rolename ^
    --s3-prefix bucketprefix ^
    --source-engine mysql ^
    --source-engine-version 8.0.32 ^
    --max-allocated-storage 1000
```

API de RDS

Para importar datos desde Amazon S3 a una nueva instancia de base de datos de MySQL mediante la API de Amazon RDS, llame a la operación RestoreDBInstanceFromS3.

Importación de datos de una base de datos MySQL externa a una instancia de base de datos de Amazon RDS para MySQL

Puede importar datos desde una base de datos de MariaDB o MySQL existente a una instancia de base de datos de RDS para MariaDB o RDS para MySQL. Esto se lleva a cabo copiando la base de datos con mysqldump y canalizándola de forma directa en la instancia de base de datos de RDS para MariaDB o RDS para MySQL. La utilidad de línea de comandos `mysqldump` suele utilizarse para crear copias de seguridad y transferir datos de un servidor de MySQL o MariaDB a otro. Se incluye con el software cliente de MySQL y MariaDB.

En MariaDB 10.5, el cliente se llama mariadb-dump. A partir de MariaDB 11.0.1, debe usar `mariadb-dump` en lugar de `mysqldump`.

> **Note**
>
> Si importa o exporta grandes cantidades de datos con una instancia de base de datos de MySQL, lo más fiable y rápido para introducir y sacar los datos de Amazon RDS es mediante archivos de copia de seguridad `xtrabackup` y Amazon S3. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..
>
> Amazon RDS no admite `xtrabackup` para MariaDB o `mariabackup`. Amazon RDS solo admite la importación de Amazon S3 para MySQL.

Un comando `mysqldump` típico para mover datos de una base de datos externa a una instancia de base de datos de Amazon RDS tiene el aspecto del ejemplo siguiente. Sustituya valores con su propia información. Para MariaDB 11.0.1 y versiones posteriores, sustituya `mysqldump` por `mariadb-dump` y `mysql` por `mariadb`.

```
mysqldump -u local_user \
    --databases database_name \
    --single-transaction \
    --compress \
    --order-by-primary  \
    --routines=0 \
    --triggers=0 \
    --events=0 \
    -plocal_password | mysql -u RDS_user \
        --port=port_number \
        --host=host_name \
        -pRDS_password
```

> **Important**
>
> Asegúrese de no dejar un espacio entre la opción `-p` y la contraseña especificada.
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en este ejemplo.

Asegúrese de conocer las siguientes recomendaciones y consideraciones:

- Excluya los siguientes esquemas del archivo de volcado:

  - `sys`
  - `performance_schema`
  - `information_schema`

  La utilidad `mysqldump` y `mariadb-dump` excluye estos esquemas de forma predeterminada.
- Si necesita migrar usuarios y privilegios, considere la posibilidad de usar una herramienta que genere el lenguaje de control de datos (DCL) para volver a crearlos, como la utilidad pt-show-grants.
- Para realizar la importación, asegúrese de que el usuario que lo haga tenga acceso a la instancia de base de datos. Para obtener más información, consulte Control de acceso con grupos de seguridad.

Los parámetros son los siguientes:

- `-u` *`local_user`*: use este parámetro para especificar un nombre de usuario. La primera vez que utilice este parámetro, especifique el nombre de una cuenta de usuario en la base de datos de MariaDB o MySQL local que identifique con el parámetro `--databases`.
- `--databases` *`database_name`*: use este parámetro para especificar el nombre de la base de datos en la instancia de MySQL o MariaDB local que desea importar a Amazon RDS.
- `--single-transaction`: use este parámetro para asegurarse de que todos los datos cargados desde la base de datos local sean coherentes en un momento determinado. Si hay otros procesos que modifican los datos mientras `mysqldump` los lee, el uso de este parámetro ayuda a mantener la integridad de los datos.
- `--compress`: use este parámetro para reducir el consumo de ancho de banda mediante la compresión de los datos de la base de datos local antes de su envío a Amazon RDS.
- `--order-by-primary`: use este parámetro para reducir el tiempo de carga mediante la ordenación de los datos de cada tabla según su clave primaria.
- `--routines`: Úselo si existen rutinas como procedimientos almacenados o funciones en la base de datos que está copiando. Establezca el parámetro en `0`, lo que excluye las rutinas durante el proceso de importación. Después, vuelva a crear manualmente las rutinas en la base de datos de Amazon RDS.
- `--triggers`: Úselo si existen desencadenadores en la base de datos que va a copiar. Establezca el parámetro en `0`, lo que excluye los desencadenadores durante el proceso de importación.

Después, vuelva a crear manualmente los desencadenadores en la base de datos de Amazon RDS.

- `--events`: Úselo si existen eventos en la base de datos que está copiando. Establezca el parámetro en `0`, lo que excluye los eventos durante el proceso de importación. Después, vuelva a crear manualmente los eventos en la base de datos de Amazon RDS.
- `-p`*`local_password`*: use este parámetro para especificar una contraseña. La primera vez que use este parámetro, especifique la contraseña de la cuenta de usuario identificada con el primer parámetro `-u`.
- `-u` *`RDS_user`*: use este parámetro para especificar un nombre de usuario. La segunda vez que utilice este parámetro, especifique el nombre de una cuenta de usuario en la base de datos predeterminada de la instancia de base de datos de MariaDB o MySQL identificada con el parámetro `--host`.
- `--port` *`port_number`*: se utiliza para especificar el puerto de la instancia de base de datos de MySQL o MariaDB. El valor predeterminado es 3306, salvo que se haya cambiado al crear la instancia de base de datos.
- `--host` *`host_name`*: se utiliza para especificar el nombre del sistema de nombres de dominio (DNS) del punto de conexión de la instancia de base de datos de Amazon RDS, por ejemplo, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la instancia de base de datos en la consola de Amazon RDS.
- `-p`*`RDS_password`*: use este parámetro para especificar una contraseña. La segunda vez que use este parámetro, debe especificar la contraseña de la cuenta de usuario identificada por el segundo parámetro `-u`.

Asegúrese de crear de forma manual procedimientos almacenados, desencadenadores, funciones o eventos en su base de datos de Amazon RDS. Si hay alguno de estos objetos en la base de datos que va a copiar, exclúyalo cuando ejecute `mysqldump` o `mariadb-dump`. Para hacerlo, incluya los siguientes parámetros con el comando `mysqldump` o `mariadb-dump`:

- `--routines=0`
- `--triggers=0`
- `--events=0`

Ejemplo

En el siguiente ejemplo se copia la base de datos de ejemplo `world` del host local en una instancia de base de datos de RDS para MySQL. Sustituya valores con su propia información. Para copiar la base de datos de ejemplo en una instancia de base de datos de RDS para MariaDB, sustituya `mysqldump` por `mariadb-dump` y `mysql` por `mariadb`.

Para Linux, macOS o Unix:

```
sudo mysqldump -u local_user \
    --databases world \
    --single-transaction \
    --compress \
    --order-by-primary  \
    --routines=0 \
    --triggers=0 \
    --events=0 \
    -plocal_password | mysql -u rds_user \
        --port=3306 \
        --host=my_instance.123456789012.us-east-1.rds.amazonaws.com \
        -pRDS_password
```

Para Windows:

Ejecute el siguiente comando en un símbolo del sistema que se haya abierto con un clic con el botón derecho en Símbolo del sistema del menú de programas de Windows y con la selección de Ejecutar como administrador. Sustituya valores con su propia información. Para copiar la base de datos de ejemplo en una instancia de base de datos de RDS para MariaDB, sustituya `mysqldump` por `mariadb-dump` y `mysql` por `mariadb`.

```
mysqldump -u local_user ^
    --databases world ^
    --single-transaction ^
    --compress ^
    --order-by-primary  ^
    --routines=0 ^
    --triggers=0 ^
    --events=0 ^
    -plocal_password | mysql -u RDS_user ^
        --port=3306 ^
        --host=my_instance.123456789012.us-east-1.rds.amazonaws.com ^
        -pRDS_password
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.

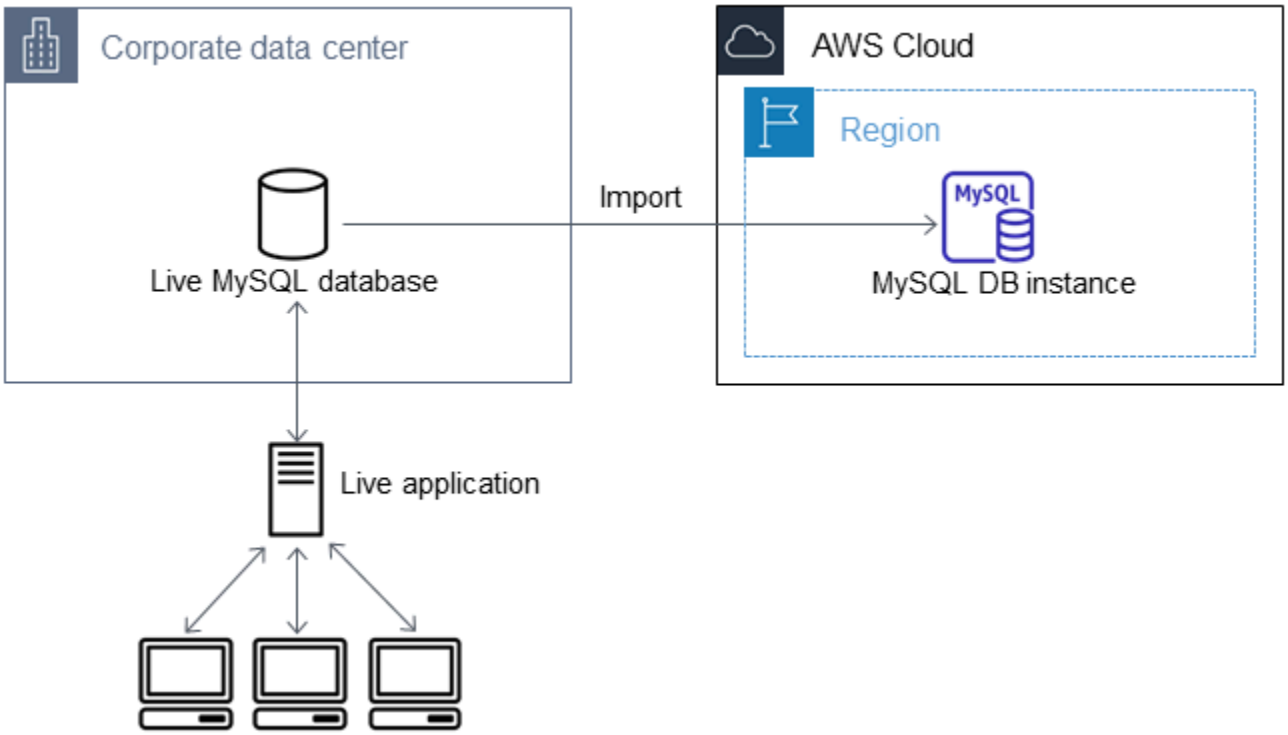
Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido

En algunos casos, es posible que sea necesario importar datos de una base de datos de MySQL o MariaDB externa, que sea compatible con una aplicación activa, a una instancia de base de datos de RDS para MariaDB o un clúster de base de datos de Multi-AZ de RDS para MySQL. Utilice el siguiente procedimiento para minimizar el impacto en la disponibilidad de las aplicaciones. Este procedimiento también puede resultar útil al trabajar con una base de datos de gran tamaño. Con este procedimiento, puede reducir el coste de la importación al reducir la cantidad de datos que se transfieren a través de la red a AWS.

En el procedimiento, se transfiere primero una copia de los datos de la base de datos a una instancia de Amazon EC2 y después se importan los datos a una nueva base de datos de Amazon RDS. A continuación, se usa la replicación para actualizar la base de datos de Amazon RDS al estado de la instancia externa activa, antes de redirigir la aplicación a la base de datos de Amazon RDS. Si la instancia externa es MariaDB 10.0.24 o superior y la instancia de destino es RDS para MariaDB, configure la replicación de MariaDB en función de los identificadores de transacción globales (GTID). De lo contrario, debe configurar la replicación en función de las coordenadas de los registros binarios. Si la base de datos externa la admite, recomendamos la replicación basada en GTID porque es un método más fiable. Para obtener más información, consulte Global Transaction ID en la documentación de MariaDB.

> **Note**
>
> Si desea importar datos a una instancia de base de datos de RDS para MySQL y el escenario lo admite, recomendamos importar y exportar los datos de Amazon RDS mediante el uso de archivos de copia de seguridad y Amazon S3. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..

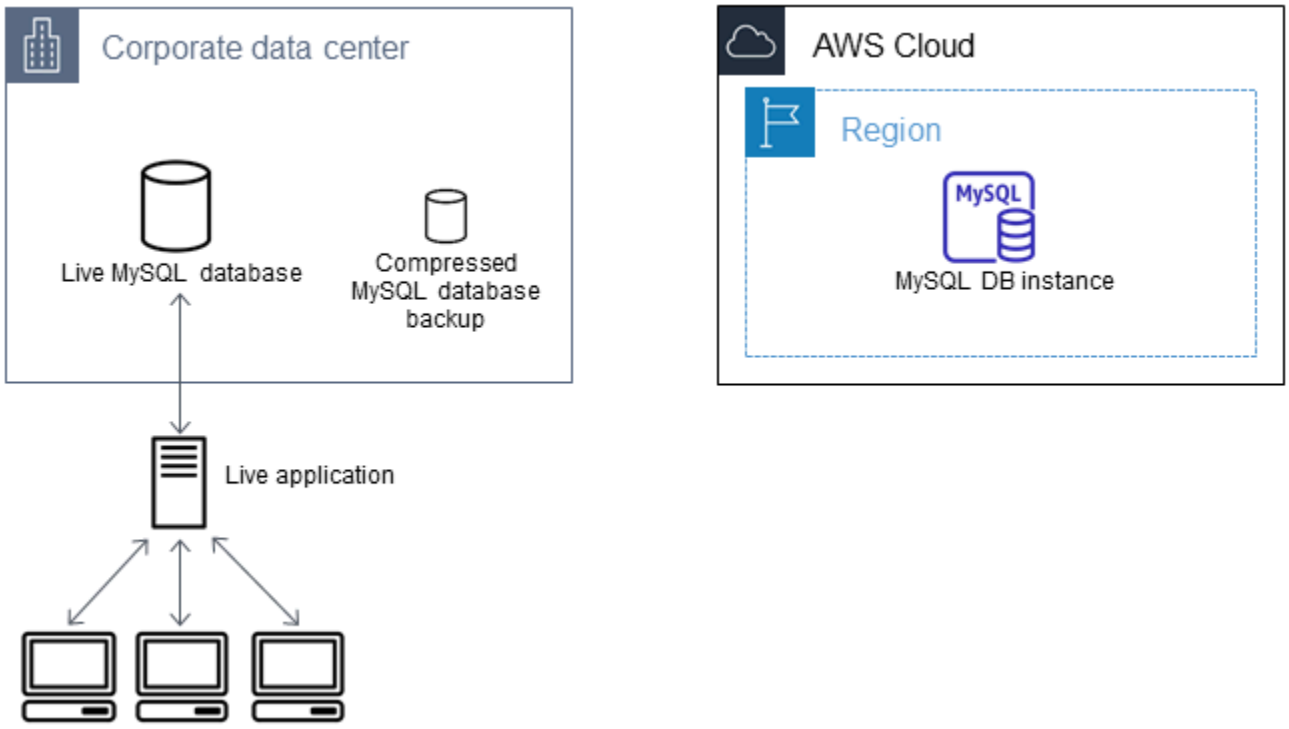
El siguiente diagrama muestra la importación de una base de datos de MySQL externa a una base de datos de MySQL en Amazon RDS.



Tarea 1: Crear una copia de la base de datos existente

El primer paso del proceso de migración de una gran cantidad de datos a una base de datos de RDS para MariaDB o RDS para MySQL con un tiempo de inactividad mínimo es crear una copia de los datos de origen.

El siguiente diagrama muestra la creación de una copia de seguridad de la base de datos de MySQL.



Con la utilidad `mysqldump` puede crear una copia de seguridad de la base de datos, ya sea en formato SQL o como texto delimitado. En MariaDB 10.5, el cliente se llama mariadb-dump. A partir de MariaDB 11.0.1, debe usar `mariadb-dump` en lugar de `mysqldump`. Se recomienda hacer una prueba con cada formato en un entorno que no sea de producción para determinar con qué método tarda menos la ejecución de mysqldump.

También se recomienda comparar el rendimiento de `mysqldump` con el beneficio que ofrece el uso del formato de texto delimitado para la carga. Una copia de seguridad con formato de texto delimitado crea un archivo de texto separado por tabuladores por cada tabla volcada. Los archivos obtenidos pueden cargarse en paralelo con el comando `LOAD DATA LOCAL INFILE` para reducir el tiempo necesario para importar la base de datos. Para obtener más información, consulte Cargar los datos para MariaDB o Cargar los datos para MySQL.

Antes de iniciar la operación de copia de seguridad, asegúrese de configurar las opciones de replicación para la base de datos de MySQL o MariaDB que va a copiar en Amazon RDS. Las opciones de replicación incluyen la activación del registro binario y la configuración de un ID de servidor único. La activación de estas opciones hace que el servidor comience a registrar las transacciones de la base de datos y la prepare para ser una instancia de replicación de origen en una fase posterior del proceso.

Asegúrese de conocer las siguientes recomendaciones y consideraciones:

- Utilice la opción `--single-transaction` con `mysqldump` porque vuelca un estado coherente de la base de datos. Para garantizar un archivo de volcado válido, no ejecute instrucciones de lenguaje de definición de datos (DDL) mientras `mysqldump` se está ejecutando. Puede programar un periodo de mantenimiento para estas operaciones.
- Excluya los siguientes esquemas del archivo de volcado:
  - `sys`
  - `performance_schema`
  - `information_schema`

  La utilidad `mysqldump` y `mariadb-dump` excluye estos esquemas de forma predeterminada.
- Si necesita migrar usuarios y privilegios, considere la posibilidad de usar una herramienta que genere el lenguaje de control de datos (DCL) para volver a crearlos, como la utilidad pt-show-grants.

Para establecer las opciones de replicación

1. Edite el archivo `my.cnf`. Este archivo se suele encontrar en `/etc`.

   ```
   sudo vi /etc/my.cnf
   ```

   Añada las opciones `log_bin` y `server_id` a la sección `[mysqld]`. La opción `log_bin` proporciona un identificador de nombre de archivo para los archivos de log binarios. La opción `server_id` proporciona un identificador único para el servidor en las relaciones origen-réplica.

   El siguiente ejemplo muestra la sección `[mysqld]` actualizada de un archivo `my.cnf`:

   ```
   [mysqld]
   log-bin=mysql-bin
   server-id=1
   ```

   Para obtener más información, consulte Setting the Replication Source Configuration en la documentación de MySQL.
2. Para la replicación con un clúster de base de datos Multi-AZ, establezca `ENFORCE_GTID_CONSISTENCY` y el parámetro `GTID_MODE` en `ON`.

   ```
   mysql> SET @@GLOBAL.ENFORCE_GTID_CONSISTENCY = ON;
   ```

```
mysql> SET @@GLOBAL.GTID_MODE = ON;
```

Esta configuración no es necesaria para la replicación con una instancia de base de datos.

3. Reinicie el servicio `mysql`.

```
sudo service mysqld restart
```

Para crear una copia de seguridad de la base de datos existente

1. Cree una copia de seguridad de los datos con la utilidad `mysqldump` o la utilidad `mariadb-dump`, especificando el formato SQL o de texto delimitado.

   Para MySQL 8.0.25 y versiones anteriores, especifique `--master-data=2` para crear un archivo de copia de seguridad que se pueda utilizar para iniciar la replicación entre servidores. Para MySQL 8.0.26 y versiones posteriores, especifique `--source-data=2` para crear un archivo de copia de seguridad que se pueda utilizar para iniciar la replicación entre servidores. Para obtener más información, consulte mysqldump - Un programa de copia de seguridad de base de datos en la documentación de MySQL.

   Para mejorar el desempeño y asegurar la integridad de los datos, use las opciones `--order-by-primary` y `--single-transaction` para `mysqldump`.

   Para evitar incluir la base de datos de sistema de MySQL en la copia de seguridad, no use la opción `--all-databases` con `mysqldump`. Para obtener más información, consulte Creating a Data Snapshot Using mysqldump en la documentación de MySQL.

   Use `chmod`, si es necesario, para asegurarse de que es posible escribir en el directorio donde se va a crear el archivo de copia de seguridad.

   > **Important**
   >
   > En Windows, ejecute el símbolo del sistema como administrador.

   - Para generar la salida en formato SQL, use el siguiente comando:

     Para Linux, macOS o Unix:

```
sudo mysqldump \
    --databases database_name \
    --master-data=2  \
    --single-transaction \
    --order-by-primary \
    -r backup.sql \
    -u local_user \
    -ppassword
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.

Para Windows:

```
mysqldump ^
    --databases database_name ^
    --master-data=2  ^
    --single-transaction ^
    --order-by-primary ^
    -r backup.sql ^
    -u local_user ^
    -ppassword
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.

- Para generar la salida en formato de texto delimitado, ejecute el siguiente comando:

  Para Linux, macOS o Unix:

```
sudo mysqldump \
    --tab=target_directory \
    --fields-terminated-by ',' \
    --fields-enclosed-by '"' \
```

```
    --lines-terminated-by 0x0d0a \
    database_name \
    --master-data=2 \
    --single-transaction \
    --order-by-primary \
    -ppassword
```

Para Windows:

```
mysqldump ^
    --tab=target_directory ^
    --fields-terminated-by "," ^
    --fields-enclosed-by """ ^
    --lines-terminated-by 0x0d0a ^
    database_name ^
    --master-data=2 ^
    --single-transaction ^
    --order-by-primary ^
    -ppassword
```

> **Note**
>
> Como práctica recomendada de seguridad, especifique credenciales distintas de las que se muestran en el ejemplo.
> Asegúrese de crear de forma manual procedimientos almacenados, desencadenadores, funciones o eventos en su base de datos de Amazon RDS. Si hay alguno de estos objetos en la base de datos que va a copiar, exclúyalos cuando ejecute `mysqldump`. Para hacerlo, incluya los siguientes argumentos con el comando `mysqldump`:
>
> - `--routines=0`
> - `--triggers=0`
> - `--events=0`

Para MySQL 8.0.22 y versiones anteriores y versiones de MariaDB, al ejecutar `mysqldump` y especificar el formato de texto delimitado, se devuelve un comentario `CHANGE MASTER TO`. Este comentario contiene el nombre y la ubicación del archivo de registro maestro. Para MySQL 8.0.23 y versiones posteriores, cuando ejecuta `mysqldump` con el formato de texto delimitado, se devuelve un comentario `CHANGE REPLICATION SOURCE TO`. Este comentario contiene

el nombre y la ubicación del archivo de registro de origen. Si la instancia externa es distinta de MariaDB versión 10.0.24 y posteriores o MySQL 8.0.23 y versiones posteriores, tenga en cuenta los valores de `MASTER_LOG_FILE` y `MASTER_LOG_POS`. Necesita estos valores al configurar la replicación.

Se devuelve la siguiente salida para las versiones de MariaDB y para MySQL 8.0.22 y versiones anteriores:

```
-- Position to start replication or point-in-time recovery from
--
-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031',
 MASTER_LOG_POS=107;
```

Se devuelve la siguiente salida para MySQL 8.0.23 y versiones posteriores:

```
-- Position to start replication or point-in-time recovery from
--
-- CHANGE SOURCE TO SOURCE_LOG_FILE='mysql-bin-changelog.000031',
 SOURCE_LOG_POS=107;
```

Para MySQL 8.0.22 y versiones anteriores, si utiliza el formato SQL, puede obtener el nombre y la posición del archivo de registro principal en el comentario `CHANGE MASTER TO` del archivo de copia de seguridad. Para MySQL 8.0.23 y versiones posteriores, si utiliza el formato SQL, puede obtener el nombre y la posición del archivo de registro de origen en el comentario `CHANGE REPLICATION SOURCE TO` del archivo de copia de seguridad. Si la instancia externa corresponde a MariaDB versión 10.0.24 o posterior, puede obtener el GTID en el paso siguiente.

2. Si la instancia externa que utiliza es MariaDB versión 10.0.24 o posterior, use la reproducción basada en GTID. Ejecute `SHOW MASTER STATUS` en la instancia de MariaDB externa para obtener el nombre y ubicación del archivo de registro binario y, a continuación, conviértalos en un GTID ejecutando `BINLOG_GTID_POS` en la instancia de MariaDB externa.

   ```
   SELECT BINLOG_GTID_POS('binary_log_file_name', binary_log_file_position);
   ```

   Tenga en cuenta el GTID devuelto. Necesita GTID para configurar la replicación.

3. Comprima los datos copiados para reducir los recursos de red necesarios para copiarlos a la base de datos de Amazon RDS. Tenga en cuenta el tamaño del archivo de copia de seguridad.

Necesitará esta información para determinar el tamaño de la instancia de Amazon EC2 que se debe crear. Cuando haya terminado, comprima el archivo de copia de seguridad con GZIP o la utilidad de compresión que prefiera.

- Para comprimir la salida en formato SQL, ejecute el siguiente comando:

```
gzip backup.sql
```

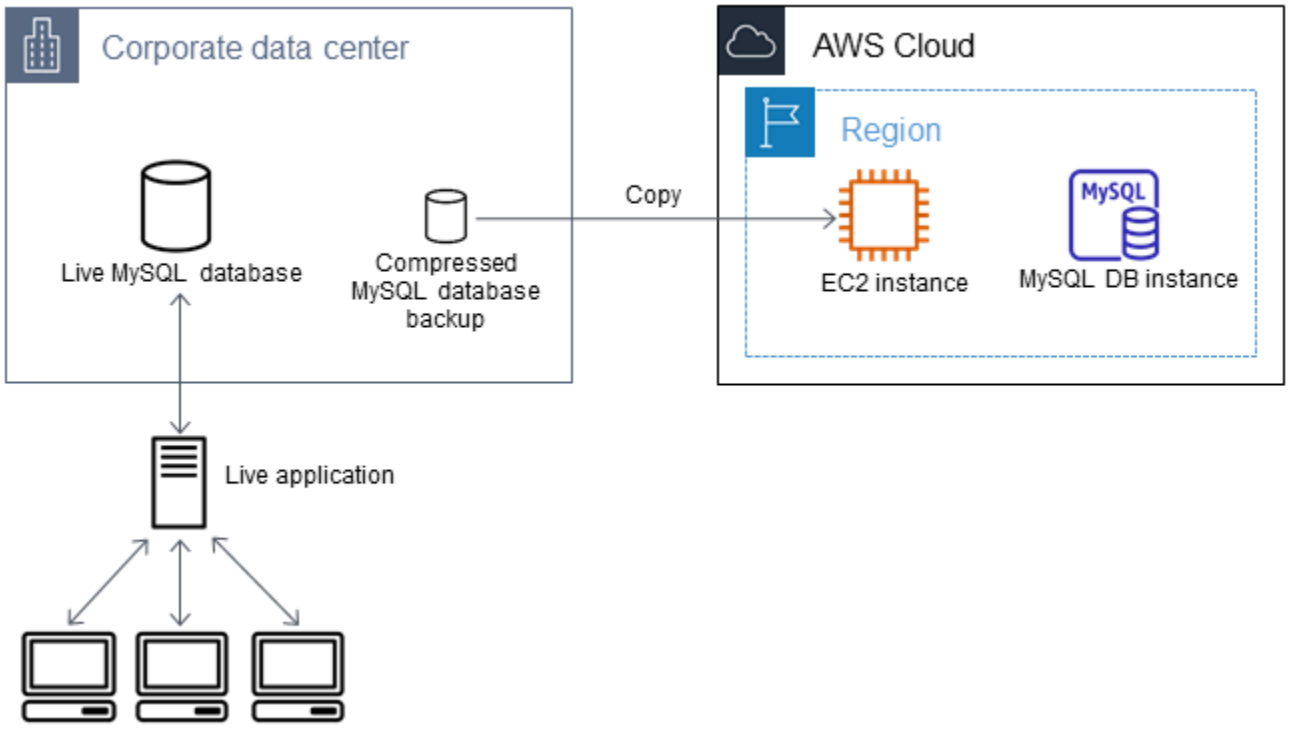
- Para comprimir la salida en formato de texto delimitado, ejecute el siguiente comando:

```
tar -zcvf backup.tar.gz target_directory
```

Tarea 2: Crear una instancia de Amazon EC2 y copiar la base de datos comprimida

La copia del archivo de copia de seguridad comprimido a una instancia Amazon EC2 requiere menos recursos de red que una copia directa de los datos sin comprimir entre las instancias de base de datos. Una vez que los datos se encuentran en Amazon EC2, puede copiarlos desde allí directamente a la base de datos de MySQL o MariaDB. Para ahorrar en el costo de los recursos de red, la instancia de Amazon EC2 debe estar en la misma Región de AWS que la instancia de base de datos de Amazon RDS. Tener la instancia de Amazon EC2 en la misma Región de AWS que la base de datos de Amazon RDS también reduce la latencia de red durante la importación.

El siguiente diagrama muestra cómo copiar la copia de seguridad de la base de datos a una instancia de Amazon EC2.



Para crear una instancia Amazon EC2 y copiar los datos

1. En la Región de AWS donde tiene pensado crear la base de datos de Amazon RDS, cree una nube privada virtual (VPC), un grupo de seguridad de VPC y una subred de VPC. Asegúrese de que las reglas de entrada del grupo de seguridad de VPC permiten las direcciones IP necesarias para que la aplicación se conecte a AWS. Puede especificar un intervalo de direcciones IP, por ejemplo, `203.0.113.0/24`, u otro grupo de seguridad de VPC. Puede usar la Consola de Amazon VPC para crear y administrar VPC, subredes y grupos de seguridad. Para obtener más información, consulte Introducción a Amazon VPC en la Guía del usuario de Amazon Virtual Private Cloud.
2. Abra la consola de Amazon EC2 y elija la Región de AWS que contendrá la instancia de Amazon EC2 y la base de datos de Amazon RDS. Lance una instancia Amazon EC2 utilizando la VPC, la subred y el grupo de seguridad que creó en el paso 1. Asegúrese de seleccionar un tipo de instancia con suficiente espacio de almacenamiento para el archivo de copia de seguridad de base de datos sin comprimir. Para obtener más información sobre las instancias de Amazon EC2, consulte Introducción a Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud.
3. Para conectarse a la base de datos de Amazon RDS desde la instancia de Amazon EC2, edite el grupo de seguridad de VPC. Agregue una regla de entrada que especifique la dirección IP privada de la instancia de EC2. La dirección IP privada aparece en la pestaña Details (Detalles) del panel Instance (Instancia) de la consola de EC2. Para editar el grupo de seguridad de VPC y agregar

una regla de entrada, elija Security Groups (Grupos de seguridad) en el panel de navegación de la consola de EC2, elija el grupo de seguridad y, luego, agregue una regla de entrada para MySQL o Aurora que especifique la dirección IP privada de la instancia de EC2. Para obtener información sobre cómo agregar una regla de entrada a un grupo de seguridad de VPC, consulte Reglas de grupo de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

4. Copie el archivo de copia de seguridad de base de datos comprimido del sistema local a la instancia Amazon EC2. Use `chmod`, si es necesario, para asegurarse de que tiene permiso de escritura para el directorio de destino de la instancia de Amazon EC2. Puede utilizar `scp` o un cliente de Secure Shell (SSH) para copiar el archivo. El siguiente comando es un comando `scp` de ejemplo:

```
scp -r -i key pair.pem backup.sql.gz ec2-user@EC2 DNS:/target_directory/backup.sql.gz
```

> **Important**
>
> Al copiar la información confidencial, asegúrese de usar un protocolo de transferencia de red seguro.

5. Establezca una conexión con la instancia Amazon EC2 e instale las últimas actualizaciones y las herramientas de cliente MySQL con los comandos siguientes:

```
sudo yum update -y
sudo yum install mysql -y
```

Para obtener más información, consulte Conexión a la instancia para instancias de Linux en la Guía del usuario de Amazon Elastic Compute Cloud.

> **Important**
>
> En este ejemplo se instala el cliente de MySQL en una imagen de máquina de Amazon (AMI) para una distribución de Amazon Linux. Este ejemplo no instala el cliente de MySQL en una distribución diferente, como Ubuntu o Red Hat Enterprise Linux. Para obtener información sobre la instalación de MySQL, consulte Instalación de MySQL en la documentación de MySQL.

6. Una vez establecida la conexión la instancia Amazon EC2 descomprima el archivo de copia de seguridad de base de datos. Los siguientes comandos son ejemplos.

- Para descomprimir la salida en formato SQL, ejecute el siguiente comando:

```
gzip backup.sql.gz -d
```

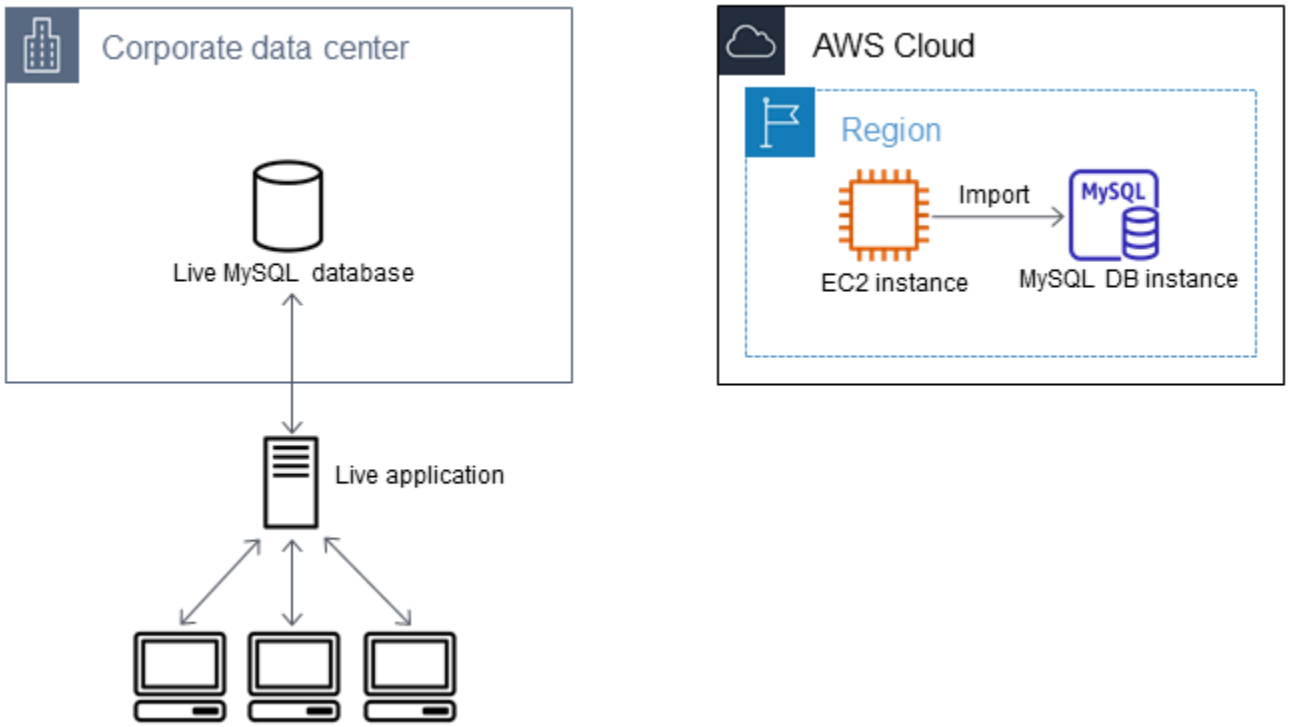
- Para descomprimir la salida en formato de texto delimitado, ejecute el siguiente comando:

```
tar xzvf backup.tar.gz
```

Tarea 3: Crear una base de datos de MySQL o MariaDB e importar los datos desde la instancia de Amazon EC2

Al crear una instancia de base de datos de RDS para MariaDB, una instancia de base de datos de RDS para MySQL o un clúster de base de datos Multi-AZ de MySQL en la misma Región de AWS que la instancia de Amazon EC2, puede importar el archivo de copia de seguridad de la base de datos desde Amazon EC2 más rápido que a través de Internet.

El siguiente diagrama muestra la importación de la copia de seguridad desde una instancia de Amazon EC2 a una base de datos de MySQL.



Para crear una base de datos de MySQL o MariaDB e importar los datos

1. Determine la clase de la instancia de base de datos y la cantidad de espacio de almacenamiento requeridas para atender la carga de trabajo prevista para esta base de datos de Amazon RDS. Como parte de este proceso, decida cuánto espacio y qué capacidad de procesamiento requieren los procedimientos de carga de datos. Decida también lo que se necesita para manejar la carga de trabajo de producción. Puede estimar esto en función del tamaño y los recursos de la base de datos de MySQL o MariaDB de origen. Para obtener más información, consulte Clases de instancia de base de datos de .
2. Cree una instancia de base de datos o un clúster de base de datos Multi-AZ en la Región de AWS que contenga la instancia de Amazon EC2.

   Para crear un clúster de base de datos Multi-AZ de RDS para MySQL, siga las instrucciones de Creación de un clúster de base de datos multi-AZ para Amazon RDS.

   Para crear una instancia de base de datos de RDS para MariaDB o RDS para MySQL, siga las instrucciones en Creación de una instancia de base de datos de Amazon RDS y use las siguientes directrices:

   - Especifique una versión del motor de base de datos compatible con la instancia de base de datos de origen.
     - Si la instancia de origen es MySQL 5.5.x, la instancia de base de datos de Amazon RDS debe ser MySQL.
     - Si la instancia de origen es MySQL 5.6.x o 5.7.x, la instancia de base de datos de Amazon RDS debe ser MySQL o MariaDB.
     - Si la instancia de origen es MySQL 8.0.x, la instancia de base de datos de Amazon RDS debe ser MySQL 8.0.x.
     - Si la instancia de origen es MySQL 8.4.x, la instancia de base de datos de Amazon RDS debe ser MySQL 8.4.x.
     - Si la instancia de origen es MariaDB 5.5 o superior, la instancia de base de datos de Amazon RDS debe ser MariaDB.
   - Especifique la misma nube privada virtual (VPC) y el mismo grupo de seguridad de VPC que para la instancia de Amazon EC2. De este modo se asegura de que la instancia Amazon EC2 y la instancia de Amazon RDS sean visibles mutuamente a través de la red. Asegúrese de que la instancia de base de datos sea de acceso público. Para configurar la replicación con la base

de datos de origen como se describe en la siguiente sección, la instancia de base de datos debe ser accesible públicamente.

- No configure varias zonas de disponibilidad, retenciones de copia de seguridad ni réplicas de lectura hasta haber importado la copia de seguridad de la base de datos. Una vez completada la importación, puede configurar Multi-AZ y la retención de copia de seguridad para la instancia de producción.

3. Revise las opciones de configuración predeterminadas para la base de datos de Amazon RDS. Si el grupo de parámetros predeterminado para la base de datos no tiene las opciones de configuración que desea, busque otro que sea adecuado o cree un grupo de parámetros nuevo. Para obtener más información acerca de cómo crear un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.
4. Conéctese a la nueva base de datos de Amazon RDS como usuario maestro. Cree los usuarios necesarios para admitir a los administradores, las aplicaciones y los servicios que necesitan acceso a la instancia de base de datos. El nombre de host para la base de datos de Amazon RDS es el valor de Punto de conexión para esta instancia de base de datos, sin el número de puerto; por ejemplo, `mysampledb.123456789012.us-west-2.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la base de datos en la consola de Amazon RDS.
5. Conéctese a la instancia de Amazon EC2. Para obtener más información, consulte Conexión a la instancia para instancias de Linux en la Guía del usuario de Amazon Elastic Compute Cloud.
6. Conecte con la base de datos de Amazon RDS como host remoto desde la instancia de Amazon EC2 con el comando `mysql`. El siguiente comando es un ejemplo:

   ```
   mysql -h host_name -P 3306 -u db_master_user -p
   ```

   El *`host_name`* es el punto de conexión de la base de datos de Amazon RDS.
7. En la petición de `mysql`, ejecute el comando `source` y pásele el nombre del archivo de volcado de la base de datos. Este comando carga los datos en la instancia de base de datos de Amazon RDS.

   - Para el formato SQL, utilice el siguiente comando:

     ```
     mysql> source backup.sql;
     ```

   - Para el formato de texto delimitado, cree primero la base de datos, si no es la predeterminada que se creó cuando se configuró la base de datos de Amazon RDS.

```
mysql> create database database_name;
mysql> use database_name;
```

A continuación, cree las tablas.

```
mysql> source table1.sql
mysql> source table2.sql
etc...
```

Importe entonces los datos.

```
mysql> LOAD DATA LOCAL INFILE 'table1.txt' INTO TABLE table1 FIELDS TERMINATED BY
 ',' ENCLOSED BY '"' LINES TERMINATED BY '0x0d0a';
mysql> LOAD DATA LOCAL INFILE 'table2.txt' INTO TABLE table2 FIELDS TERMINATED BY
 ',' ENCLOSED BY '"' LINES TERMINATED BY '0x0d0a';
etc...
```

Para mejorar el rendimiento, puede ejecutar estas operaciones en paralelo desde varias conexiones, de modo que todas las tablas se creen y luego se carguen al mismo tiempo.

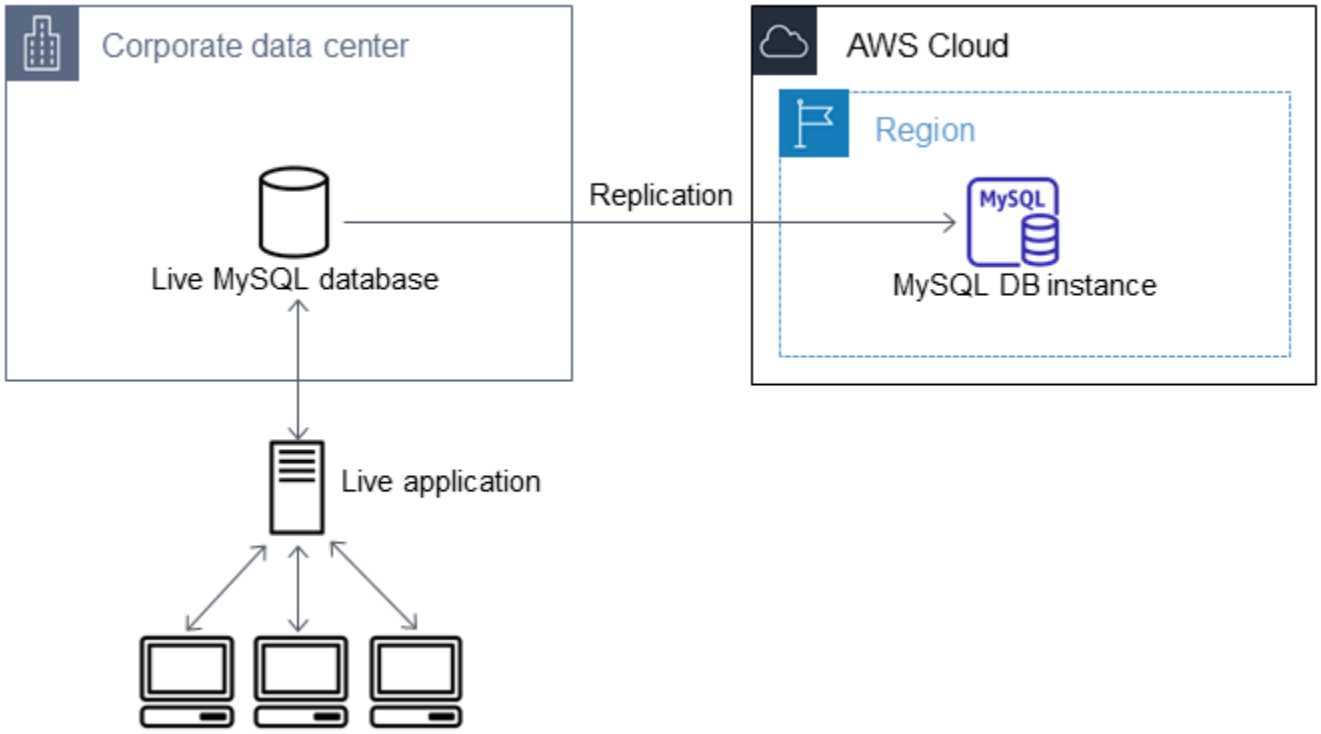
> **Note**
>
> Si utilizó alguna opción de formato de datos con `mysqldump` en el volcado inicial de la tabla, asegúrese de utilizar las mismas opciones con `LOAD DATA LOCAL INFILE` para garantizar una interpretación adecuada del contenido del archivo de datos.

8. Ejecute una consulta `SELECT` sencilla en una o dos de las tablas de la base de datos importada para comprobar que la importación se ha completado correctamente.

Si ya no necesita la instancia de Amazon EC2 utilizada en este procedimiento, termine la instancia de EC2 para reducir el uso de recursos de AWS. Para terminar una instancia de EC2, consulte Terminación de una instancia en la Guía del usuario de Amazon Elastic Compute Cloud.

Tarea 4: Replicar los datos de la base de datos externa a la nueva base de datos de Amazon RDS

Es probable que su base de datos de origen se haya actualizado durante el tiempo que tardó en copiar y transferir los datos a la base de datos MariaDB o MySQL. Por tanto, puede utilizar la replicación para actualizar la base de datos copiada con la base de datos de origen.



Los permisos requeridos para comenzar la replicación en una base de datos de Amazon RDS están restringidos y no están disponibles para el usuario principal de Amazon RDS. Por ello, utilice el procedimiento almacenado de Amazon RDS adecuado para la versión principal del motor:

- mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_external_master_gtid para configurar la replicación y mysql.rds_start_replication para iniciar la replicación

Para iniciar la replicación

En la tarea 1, cuando estableció las opciones de replicación, activó el registro binario y estableció un ID de servidor único para la base de datos de origen. Ahora puede configurar la base de datos de

Amazon RDS como réplica estableciendo la base de datos activa como instancia de replicación de origen.

1. En la consola de Amazon RDS, agregue la dirección IP del servidor que aloja la base de datos de origen al grupo de seguridad de VPC configurado para la base de datos de Amazon RDS. Para obtener más información sobre la configuración de un grupo de seguridad de VPC, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

   Es posible que también necesite configurar la red local para permitir las conexiones desde la dirección IP de la base de datos de Amazon RDS para que se pueda comunicar con la instancia de origen. Para encontrar la dirección IP de la base de datos de Amazon RDS, use el comando `host`:

   ```
   host host_name
   ```

   El *`host_name`* es el nombre de DNS del punto de conexión de la base de datos de Amazon RDS, por ejemplo, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la instancia de base de datos en la consola de Amazon RDS.

2. Con el cliente que prefiera, conecte con la instancia de origen y cree un usuario para la replicación. Esta cuenta se usa únicamente para la replicación y debe estar limitada a su dominio para mejorar la seguridad. El siguiente comando es un ejemplo:

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

   > **Note**
   >
   > Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

3. En la instancia de origen, conceda al usuario de replicación los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE`. Por ejemplo, para conceder los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` referidos a todas las bases de datos al usuario "`repl_user`" del dominio, ejecute el siguiente comando:

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
   ```

4. Si utilizó el formato SQL para crear el archivo de copia de seguridad y la instancia externa no es MariaDB 10.0.24 o posterior, observe el contenido de ese archivo ejecutando el siguiente comando:

```
cat backup.sql
```

El archivo contiene un comentario `CHANGE MASTER TO` que contiene el nombre y la posición del archivo de registro maestro. Este comentario se incluye en el archivo de copia de seguridad cuando se usa la opción `--master-data` con `mysqldump`. Tenga en cuenta los valores de `MASTER_LOG_FILE` y `MASTER_LOG_POS`.

```
--
-- Position to start replication or point-in-time recovery from
--

-- CHANGE MASTER TO MASTER_LOG_FILE='mysql-bin-changelog.000031', MASTER_LOG_POS=107;
```

Si utilizó el formato de texto delimitado para crear el archivo de copia de seguridad y la instancia externa no es MariaDB 10.0.24 o posterior, ya debe haber obtenido las coordenadas del registro binario del paso 1 del procedimiento descrito en “Creación de una copia de seguridad de la base de datos existente” en la tarea 1.

Si la instancia externa es MariaDB 10.0.24 o posterior, ya debe haber obtenido el GTID desde el que inicia la replicación en el paso 2 del procedimiento descrito en “Creación de una copia de seguridad de la base de datos existente” en la tarea 1.

5. Convertir la base de datos de Amazon RDS en la réplica. Si la instancia externa no es MariaDB 10.0.24 o una versión posterior, conéctese a la base de datos de Amazon RDS como usuario principal e identifique la base de datos de origen como la instancia de replicación de origen con el procedimiento almacenado de Amazon RDS adecuado:

   - mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
   - mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)

   Si tiene un archivo de copia de seguridad con formato SQL, utilice el nombre de archivo de registro y la ubicación del registro principal que determinó en el paso 4. Si utilizó formato de texto delimitado, utilice el nombre y la posición que determinó cuando se crearon los archivos de copia de seguridad. Los siguientes comandos son ejemplos:

MySQL 8.4 y versiones posteriores

```
CALL mysql.rds_set_external_source ('myserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
```

MariaDB y MySQL 8.0 y versiones anteriores

```
CALL mysql.rds_set_external_master ('myserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
```

> **Note**
>
> Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

Si la instancia externa no es MariaDB 10.0.24 o una versión posterior, conéctese a la base de datos de Amazon RDS como usuario maestro e identifique la base de datos de origen como la instancia de replicación de origen con el comando mysql.rds_set_external_master_gtid. Utilice el GTID que determinó en el paso 2 del procedimiento descrito en “Creación de una copia de seguridad de la base de datos existente” en la tarea 1. El siguiente comando es un ejemplo:

```
CALL mysql.rds_set_external_master_gtid ('source_server_ip_address', 3306,
 'ReplicationUser', 'password', 'GTID', 1);
```

source_server_ip_address es la dirección IP de la instancia de replicación de origen. Una dirección DNS privada de EC2 no se admite actualmente.

> **Note**
>
> Especifique credenciales distintas de las que se muestran aquí como práctica recomendada de seguridad.

6. En la base de datos de Amazon RDS, para empezar la replicación, ejecute el comando mysql.rds_start_replication siguiente:

```
CALL mysql.rds_start_replication;
```

7. En la base de datos de Amazon RDS, para determinar si la réplica está actualizada con la instancia de replicación de origen, ejecute el comando SHOW REPLICA STATUS. Los resultados del comando `SHOW REPLICA STATUS` incluyen el campo `Seconds_Behind_Master`. Cuando el campo `Seconds_Behind_Master` devuelve 0, la réplica está actualizada con la instancia de replicación de origen.

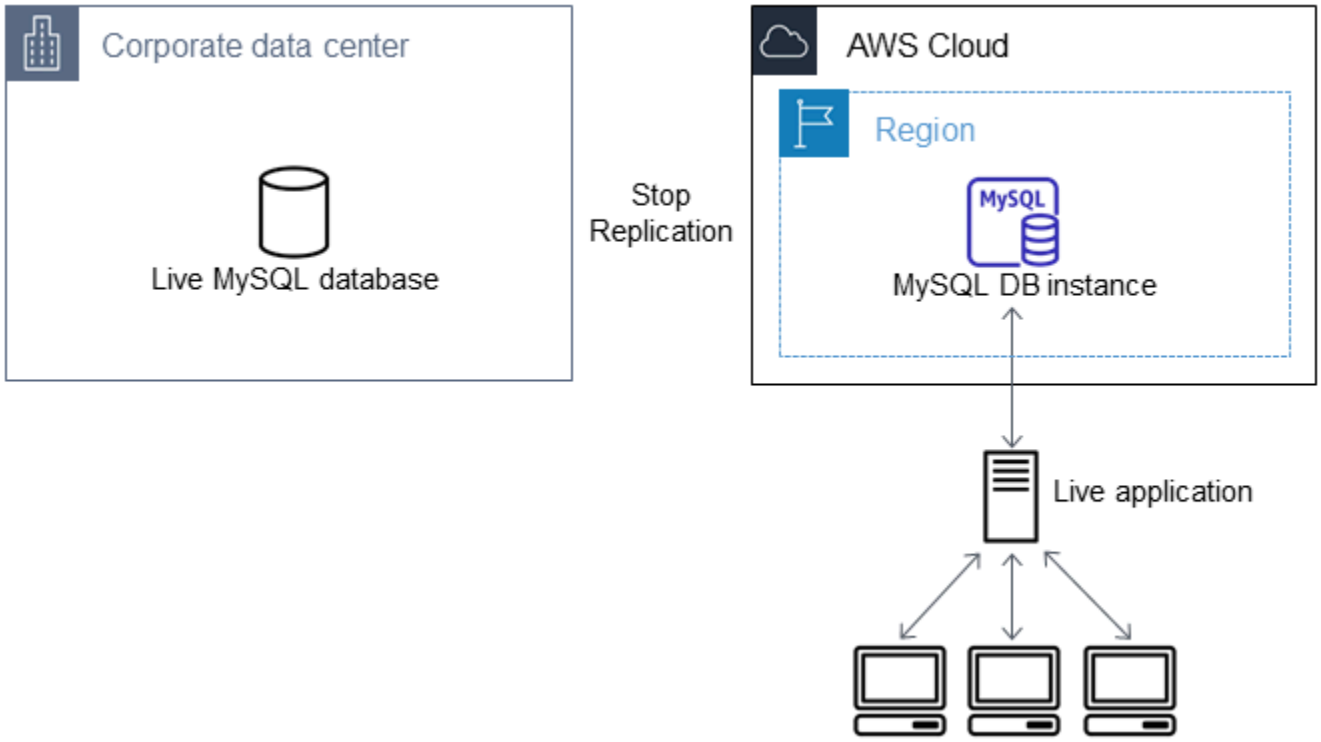
   > **Note**
   >
   > Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

   Para una instancia de base de datos de MariaDB 10.5, 10.6 o 10.11, ejecute el procedimiento almacenado mysql.rds_replica_status en lugar del comando de MySQL.

8. Una vez que la base de datos de Amazon RDS esté actualizada, active las copias de seguridad automatizadas para poder restaurar la base de datos si es necesario. Puede activar o modificar copias de seguridad automatizadas para la base de datos de Amazon RDS mediante la consola de Amazon RDS. Para obtener más información, consulte Introducción a las copias de seguridad.

Tarea 5: Redirigir la aplicación en funcionamiento a la instancia de Amazon RDS

Una vez que la base de datos de MySQL o MariaDB esté actualizada con la instancia de replicación de origen, puede actualizar la aplicación activa para utilizar la instancia de Amazon RDS.



Para redirigir una aplicación activa a una base de datos de MySQL o MariaDB y detener la replicación

1. Para añadir el grupo de seguridad de VPC para la base de datos de Amazon RDS, añada la dirección IP del servidor que aloja la aplicación. Para obtener más información sobre la modificación de un grupo de seguridad de VPC, consulte Configuración de reglas de grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.
2. Compruebe que el valor del campo `Seconds_Behind_Master` en el comando SHOW REPLICA STATUS sea 0, lo que indica que la réplica está actualizada con la instancia de replicación de origen.

```
SHOW REPLICA STATUS;
```

> **Note**
>
> Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

Para una instancia de base de datos de MariaDB 10.5 o 10.6 o 10.11 ejecute el procedimiento mysql.rds_replica_status en lugar del comando de MySQL.

3. Cierre todas las conexiones con el origen cuando se completen las transacciones.
4. Actualice la aplicación para que use la base de datos de Amazon RDS. Normalmente, la actualización implicará cambar la configuración de conexión para identificar el nombre de host y el puerto de la base de datos de Amazon RDS, la cuenta de usuario y la contraseña con las que conectarse y la base de datos que se debe emplear.
5. Conéctese a la instancia de base de datos.

   Para un clúster de base de datos Multi-AZ, conéctese a la instancia de base de datos de escritor.
6. Detenga la replicación para la instancia de Amazon RDS con el comando mysql.rds_stop_replication siguiente:

   ```
   CALL mysql.rds_stop_replication;
   ```
7. Ejecute el procedimiento almacenado de Amazon RDS adecuado en la base de datos de Amazon RDS para restablecer la configuración de replicación y que la instancia deje de considerarse una réplica.

   - mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
   - mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)

   MySQL 8.4 y versiones posteriores

   ```
   CALL mysql.rds_reset_external_source;
   ```

   MariaDB y MySQL 8.0 y versiones anteriores

   ```
   CALL mysql.rds_reset_external_master;
   ```
8. Active las características adicionales de Amazon RDS, como la compatibilidad con Multi-AZ y las réplicas de lectura. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS y Trabajo con réplicas de lectura de instancias de base de datos.

Importación de datos de cualquier origen a una instancia de base de datos de Amazon RDS para MySQL

Los siguientes pasos le guiarán a través del proceso de importación de datos a una instancia de base de datos de Amazon RDS:

Paso 1: crear archivos sin formato con los datos que se van a cargar

Utilice un formato habitual, como valores separados por comas (CSV), para almacenar los datos que se deben cargar. Cada tabla debe tener su propio archivo. No puede combinar los datos de varias tablas en el mismo archivo. Dé a cada archivo el nombre de la tabla correspondiente. Puede elegir la extensión que desee para el nombre de los archivos. Por ejemplo, si el nombre de la tabla es `sales`, el nombre del archivo podría ser `sales.csv` o `sales.txt`.

Si es posible, ordene los datos según la clave principal de la tabla que se va a cargar. Esto mejorará drásticamente los tiempos de carga y minimizará los requisitos de almacenamiento en disco.

La velocidad y la eficiencia de este procedimiento dependen de que el tamaño de los archivos sea pequeño. Si el tamaño sin comprimir de algún archivo es mayor de 1 GiB, divídalo en varios archivos y cárguelos por separado.

En los sistemas de tipo Unix (incluido Linux), utilice el comando `split`. Por ejemplo, el siguiente comando divide el archivo `sales.csv` en varios archivos de menos de 1 GiB y los divide solo en los saltos de línea (-C 1024m). Los nombres de los nuevos archivos incluyen sufijos numéricos ascendentes. El siguiente comando genera archivos con nombres como `sales.part_00` y `sales.part_01`.

```
split -C 1024m -d sales.csv sales.part_
```

Otros sistemas operativos disponen de utilidades similares.

Puede almacenar los archivos sin formato en cualquier lugar. No obstante, cuando cargue los datos en el paso 5, debe invocar el intérprete de comandos de `mysql` desde la misma ubicación donde existen los archivos o utilizar la ruta absoluta de los archivos cuando ejecute `LOAD DATA LOCAL INFILE`.

Paso 2: Detener las aplicaciones con acceso a la instancia de base de datos de destino

Antes de iniciar una carga grande, detenga toda la actividad de aplicaciones de acceder a la instancia de base de datos de destino que prevé cargar. Se recomienda esto en particular si otras sesiones modificarán las tablas que se cargan o las tablas a las que hacen referencia. Hacer esto reduce el riesgo de violaciones de restricciones que se producen durante la carga y mejoran el desempeño de carga. También permite restaurar la instancia de base de datos al estado inmediatamente anterior a la carga sin perder los cambios efectuados por los procesos no implicados en la carga.

Por supuesto, en ocasiones esto no será posible o no resultará práctico. Si no puede detener el acceso de las aplicaciones con acceso a la instancia de base de datos antes de la carga, tome las medidas oportunas para asegurar la disponibilidad e integridad de los datos. Los pasos específicos requeridos varían mucho en función de cada caso y de los requisitos del sitio.

Paso 3: crear una instantánea de base de datos

Si tiene previsto cargar los datos en una nueva instancia de base de datos que aún está vacía, puede omitir este paso. De lo contrario, recomendamos crear instantáneas de bases de datos de la instancia de base de datos de Amazon RDS elegida como destino antes y después de la carga de los datos. Las instantáneas de base de datos de Amazon RDS son copias de seguridad completas de la instancia de base de datos que puede usar para restaurar la instancia de base de datos a un estado conocido. Cuando se inicia una instantánea de base de datos, las operaciones de E/S de la instancia de base de datos se suspenden de forma temporal mientras se crea una copia de seguridad de la base de datos.

La creación de una instantánea de base de datos inmediatamente antes de la carga permite restaurar la base de datos al estado previo a la carga, si es necesario. Una instantánea de base de datos tomada inmediatamente después de la carga le evita tener que volver a cargar los datos en caso de error. También puede usar instantáneas de bases de datos después de la carga para importar datos a nuevas instancias de bases de datos.

En el ejemplo siguiente se ejecuta el comando create-db-snapshot de la AWS CLI para crear una instantánea de base de datos de la instancia `AcmeRDS` y se otorga el identificador `"preload"` a la instantánea de base de datos.

Para Linux, macOS o Unix:

```
aws rds create-db-snapshot \
    --db-instance-identifier AcmeRDS \
    --db-snapshot-identifier preload
```

Para Windows:

```
aws rds create-db-snapshot ^
    --db-instance-identifier AcmeRDS ^
    --db-snapshot-identifier preload
```

También puede utilizar la funcionalidad de restauración de instantáneas de bases de datos para crear instancias de bases de datos de prueba para simulacros o para deshacer cambios realizados durante la carga.

Tenga en cuenta que al restaurar una base de datos a partir de una instantánea de base de datos se crea una instancia nueva de base de datos que, como todas las instancias de base de datos, tiene un identificador y un punto de conexión únicos. Para restaurar la instancia de base de datos sin cambiar de punto de conexión, primero, elimine la instancia de base de datos para poder reutilizar el mismo punto de conexión.

Por ejemplo, para crear una instancia de base de datos para simulacros u otras pruebas, asigne a la instancia de base de datos su propio identificador. En el ejemplo, el identificador es `AcmeRDS-2`. El ejemplo se conecta a la instancia de base de datos mediante el punto de conexión asociado con `AcmeRDS-2`. Para obtener más información, consulte restore-db-instance-from-db-snapshot.

Para Linux, macOS o Unix:

```
aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier AcmeRDS-2 \
    --db-snapshot-identifier preload
```

Para Windows:

```
aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier AcmeRDS-2 ^
    --db-snapshot-identifier preload
```

Para reutilizar el punto de conexión existente, es necesario eliminar primero la instancia de base de datos y, luego, asignar el mismo identificador a la base de datos restaurada. Para obtener más información, consulte delete-db-instance.

En el ejemplo siguiente se toma una instantánea de base de datos final de la instancia de base de datos antes de eliminarla. Esto es opcional, pero recomendable.

Para Linux, macOS o Unix:

```
aws rds delete-db-instance \
    --db-instance-identifier AcmeRDS \
    --final-db-snapshot-identifier AcmeRDS-Final

aws rds restore-db-instance-from-db-snapshot \
    --db-instance-identifier AcmeRDS \
    --db-snapshot-identifier preload
```

Para Windows:

```
aws rds delete-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --final-db-snapshot-identifier AcmeRDS-Final

aws rds restore-db-instance-from-db-snapshot ^
    --db-instance-identifier AcmeRDS ^
    --db-snapshot-identifier preload
```

Paso 4 (opcional): Desactivar copias de seguridad automatizadas de Amazon RDS

> **Warning**
>
> No desactive las copias de seguridad automatizadas si necesita realizar una recuperación en un momento dado.

La desactivación de las copias de seguridad automatizadas es una optimización del rendimiento y no es un requisito para las cargas de datos. La desactivación de las copias de seguridad automatizadas elimina todas las copias de seguridad existentes. Como resultado, después de desactivar las copias de seguridad automatizadas, no es posible la recuperación en un momento dado. Las instantáneas de base de datos manuales no se ven afectadas por la desactivación de las copias de seguridad automatizadas. Todas las instantáneas de base de datos manuales existentes seguirán estando disponibles para su restauración.

La desactivación de las copias de seguridad automatizadas reduce el tiempo de carga en aproximadamente un 25 % y reduce el espacio de almacenamiento necesario durante la carga. Si planea cargar los datos en una instancia de base de datos nueva que no contiene datos, desactivar las copias de seguridad es una forma sencilla de acelerar la carga y evitar utilizar el almacenamiento adicional que las copias de seguridad necesitan. Sin embargo, en algunos casos, es posible que tenga previsto cargar en una instancia de base de datos que ya contiene datos. Si es así, evalúe los beneficios de la desactivación de las copias de seguridad frente al impacto de perder la capacidad de realizar una recuperación a un momento dado.

Las instancias de base de datos tienen copias de seguridad automatizadas activadas de forma predeterminada (con un periodo de retención de un día). Para desactivar las copias de seguridad automatizadas, configure el periodo de retención de copia de seguridad en cero. Después de la carga, puede volver a activar las copias de seguridad mediante la configuración del periodo de retención de copia de seguridad en un valor distinto de cero. Para activar o desactivar las copias de seguridad, Amazon RDS apaga la instancia de base de datos y, a continuación, la reinicia para activar o desactivar el registro de MariaDB o MySQL.

Ejecute el comando `modify-db-instance` de la AWS CLI para establecer el valor cero como período de retención de copia de seguridad y aplicar el cambio inmediatamente. Al configurar cero como periodo de retención es necesario reiniciar la instancia de base de datos, por lo que debe esperar a que la operación se complete para poder continuar. Para obtener más información, consulte modify-db-instance.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier AcmeRDS \
    --apply-immediately \
    --backup-retention-period 0
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --apply-immediately ^
    --backup-retention-period 0
```

Puede comprobar el estado de la instancias de base de datos con el comando describe-db-instances de la AWS CLI. En el siguiente ejemplo se muestra el estado de la instancia de base de datos de la instancia de base de datos `AcmeRDS`:

```
aws rds describe-db-instances --db-instance-identifier AcmeRDS --query "*[].
{DBInstanceStatus:DBInstanceStatus}"
```

Cuando el estado de la instancia de base de datos es `available`, está listo para continuar con el siguiente paso.

Paso 5: cargar los datos

Para leer las filas de los archivos sin formato en las tablas de base de datos, use la instrucción `LOAD DATA LOCAL INFILE` de MySQL.

> **Note**
>
> Debe invocar el intérprete de comandos de `mysql` desde la misma ubicación donde existen los archivos o utilizar la ruta absoluta de los archivos cuando ejecute `LOAD DATA LOCAL INFILE`.

En el siguiente ejemplo, se muestra cómo cargar datos de un archivo denominado `sales.txt` en una tabla denominada `Sales` en la base de datos:

```
mysql> LOAD DATA LOCAL INFILE 'sales.txt' INTO TABLE Sales FIELDS TERMINATED BY ' '
 ENCLOSED BY '' ESCAPED BY '\\';
Query OK, 1 row affected (0.01 sec)
Records: 1  Deleted: 0  Skipped: 0  Warnings: 0
```

Para obtener más información sobre la instrucción `LOAD DATA`, consulte la instrucción LOAD DATA en la documentación de MySQL.

Paso 6: Activar las copias de seguridad automatizadas de Amazon RDS

Si desactiva las copias de seguridad automatizadas de Amazon RDS en el paso 4, una vez terminada la carga, active las copias de seguridad automatizadas estableciendo nuevamente el periodo de retención de copia de seguridad en el valor que había antes de la carga. Como se ha

indicado en el paso 4, Amazon RDS reinicia la instancia de base de datos, por lo que debe estar preparado para una breve interrupción del servicio.

El siguiente ejemplo ejecuta el comando modify-db-instance de la AWS CLI para activar las copias de seguridad automatizadas para la instancia de base de datos `AcmeRDS` y establecer el periodo de retención en un día:

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier AcmeRDS \
    --backup-retention-period 1 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier AcmeRDS ^
    --backup-retention-period 1 ^
    --apply-immediately
```

Uso de la replicación de MySQL en Amazon RDS

Normalmente se utilizan réplicas de lectura para configurar la replicación entre instancias de base de datos de Amazon RDS. Para obtener información general acerca de las réplicas de lectura, consulte Trabajo con réplicas de lectura de instancias de base de datos. Para obtener información específica acerca de cómo utilizar las réplicas de lectura en Amazon RDS para MySQL, consulte Uso de réplicas de lectura de MySQL.

Puede usar identificadores de transacciones globales (GTID) para la replicación con RDS para MySQL. Para obtener más información, consulte Uso de la replicación basada en GTID.

También puede configurar la replicación entre una instancia de base de datos de RDS para MySQL y una instancia de MariaDB o MySQL externa a Amazon RDS. Para obtener más información sobre cómo configurar la replicación con un origen externo, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

Para cualquiera de estas opciones de replicación, puede utilizar replicación basada en filas, basada en instrucciones o mixta. La replicación basada en filas solo replica las filas cambiadas que resulten de una instrucción SQL. La replicación basada en instrucciones replica toda la instrucción SQL. La replicación mixta utiliza la replicación basada en instrucciones siempre que sea posible, pero alterna a la replicación basada en filas cuando se ejecutan las instrucciones SQL que no son seguras para la replicación basada en instrucciones. En la mayoría de los casos, se recomienda la replicación mixta. El formato de registro binario de la instancia de base de datos determina si la replicación se basa en filas, instrucciones o mixta. Para obtener información acerca de la configuración del formato de registro binario, consulte Configuración del registro binario de RDS para MySQL para bases de datos de Single-AZ.

> **Note**
>
> Puede configurar la replicación para importar bases de datos desde una instancia de MariaDB o MySQL que sea externa a Amazon RDS, o para exportar bases de datos a dichas instancias. Para obtener más información, consulte Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido y Exportación de datos desde una instancia de base de datos MySQL mediante replicación.

Tras restaurar la instancia de base de datos a partir de una instantánea o realizar una recuperación en un momento dado, puede ver la última posición de binlog recuperada de la base de datos de

origen en la consola de RDS. En Registros y eventos, ingrese binlog. La posición del binlog aparece en Notas del sistema.

Temas

- Uso de réplicas de lectura de MySQL
- Uso de la replicación basada en GTID
- Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa
- Configuración de la replicación de varios orígenes de Amazon RDS para MySQL

Uso de réplicas de lectura de MySQL

A continuación, encontrará información específica acerca de cómo utilizar las réplicas de lectura en RDS para MySQL. Para obtener información general sobre las réplicas de lectura e instrucciones sobre cómo usarlas, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Para obtener más información sobre las réplicas de lectura de MySQL, consulte los siguientes temas.

- Configuración de filtros de replicación con MySQL
- Configuración de la replicación retrasada con MySQL
- Eliminación de réplicas de lectura con MySQL
- Implementaciones de réplicas de lectura Multi-AZ con MySQL
- Uso de réplicas de lectura en cascada con RDS para MySQL
- Supervisión del retardo de replicación para réplicas de lectura de MySQL
- Inicio y detención de replicaciones con réplicas de lectura de MySQL
- Solución de problemas de réplicas de lectura de MySQL

Configuración de réplicas con MySQL

Para que una instancia de base de datos de MySQL pueda servir como origen de replicación, asegúrese de habilitar las copias de seguridad automáticas en la instancia de base de datos de origen. Para ello, debe establecer el periodo de retención de copia de seguridad en un valor distinto de 0. Este requisito también es válido para una réplica de lectura que sea la instancia de base de datos de origen de otra réplica de lectura. Las copias de seguridad automáticas se admiten para las

réplicas de lectura en las que se ejecuta cualquier versión de MySQL. Puede configurar la replicación en función de las coordenadas de los registros binarios para las instancias de base de datos MySQL.

Puede configurar la replicación mediante identificadores de transacciones globales (GTIDS) en las siguientes versiones:

- RDS para MySQL versión 5.7.44 y versiones 5.7 posteriores
- RDS para MySQL versión 8.0.28 y versiones 8.0 posteriores
- RDS para MySQL versión 8.4.3 y versiones 8.4 posteriores

Para obtener más información, consulte Uso de la replicación basada en GTID.

Puede crear hasta 15 réplicas de lectura a partir de una instancia de base de datos de dentro de la misma región. Para que la replicación sea eficaz, cada réplica de lectura debe tener la misma cantidad de recursos de computación y de almacenamiento que la instancia de base de datos de origen. Si modifica la escala de la instancia de base de datos de origen, debe ajustar también la escala de las réplicas de lectura.

RDS para MySQL admite réplicas de lectura en cascada. Para obtener información sobre cómo configurar réplicas de lectura en cascada, consulte Uso de réplicas de lectura en cascada con RDS para MySQL.

Puede ejecutar varias acciones de creación y eliminación de réplicas de lectura al mismo tiempo que hagan referencia a la misma instancia de base de datos de origen. Al realizar estas acciones, permanezca dentro del límite de 15 réplicas de lectura para cada instancia de origen.

Una réplica de lectura de una instancia de base de datos MySQL no puede usar una versión de motor de base de datos inferior que su instancia de base de datos de origen.

Preparación de instancias de base de datos de MySQL que usan MyISAM

Si una instancia de base de datos MySQL usa un motor no transaccional como MyISAM, debe llevar a cabo los siguientes pasos para configurar la réplica de lectura. Estos pasos son necesarios para garantizar que la réplica de lectura tiene una copia coherente de los datos. Los pasos no son necesarios si todas las tablas usan un motor transaccional como InnoDB.

1. Detenga todas las operaciones de lenguaje de manipulación de datos (DML) y lenguaje de definición de datos (DDL) que se lleven a cabo en las tablas no transaccionales de la instancia de base de datos de origen y espere a que se completen. Las declaraciones SELECT pueden seguir ejecutándose.

2. Vacíe y bloquee las tablas de la instancia de base de datos de origen.
3. Cree la réplica de lectura usando uno de los métodos que se describen en las siguientes secciones.
4. Compruebe el progreso de la creación de la réplica de lectura usando, por ejemplo, la operación de la API `DescribeDBInstances`. Una vez que la réplica de lectura esté disponible, desbloquee las tablas de la instancia de base de datos de origen y reanude las operaciones normales de la base de datos.

Configuración de filtros de replicación con MySQL

Puede utilizar filtros de replicación para especificar qué bases de datos y tablas se replican con una réplica de lectura. Los filtros de replicación pueden incluir bases de datos y tablas en la replicación o excluirlas de la replicación.

Los siguientes son algunos casos de uso para filtros de replicación:

- Para reducir el tamaño de una réplica de lectura. Con el filtrado de replicación, puede excluir las bases de datos y las tablas que no son necesarias en la réplica de lectura.
- Para excluir bases de datos y tablas de réplicas de lectura por razones de seguridad.
- Para replicar diferentes bases de datos y tablas para casos de uso específicos en diferentes réplicas de lectura. Por ejemplo, puede utilizar réplicas de lectura específicas para análisis o fragmentación.
- Con una instancia de base de datos que tiene réplicas de lectura en diferentes Regiones de AWS, para replicar diferentes bases de datos o tablas en diferentes regiones de Regiones de AWS.

> **Note**
>
> También puede utilizar filtros de reproducción para especificar qué bases de datos y tablas se reproducen con una instancia de base de datos primaria de MySQL que está configurada como una réplica en una topología de reproducción entrante. Para obtener más información acerca de esta configuración, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

Temas

- Configurar parámetros de filtrado de replicación de RDS for MySQL

- Limitaciones del filtrado de replicación de RDS fopara r MySQL
- Ejemplos de filtrado de replicación de RDS para MySQL
- Visualización de los filtros de replicación para una réplica de lectura

Configurar parámetros de filtrado de replicación de RDS for MySQL

Para configurar filtros de replicación, establezca los siguientes parámetros de filtrado de replicación en la réplica de lectura:

- `replicate-do-db` – Replicar los cambios en las bases de datos especificadas. Cuando se establece este parámetro para una réplica de lectura, solo se replican las bases de datos especificadas en el parámetro.
- `replicate-ignore-db` – No replicar los cambios en las bases de datos especificadas. Cuando el parámetro `replicate-do-db` se establece para una réplica de lectura, este parámetro no se evalúa.
- `replicate-do-table` – Replicar los cambios en las tablas especificadas. Cuando se establece este parámetro para una réplica de lectura, solo se replican las tablas especificadas en el parámetro. Además, cuando se establece el parámetro `replicate-do-db` o `replicate-ignore-db`, asegúrese de incluir la base de datos que incluye las tablas especificadas en la replicación con la réplica de lectura.
- `replicate-ignore-table` – No replicar los cambios en las tablas especificadas. Cuando el parámetro `replicate-do-table` se establece para una réplica de lectura, este parámetro no se evalúa.
- `replicate-wild-do-table` – Replicar tablas en función de la base de datos y los patrones de nombre de tabla especificados. Se admiten los caracteres comodín `%` y `_`. Cuando se establece el parámetro `replicate-do-db` o `replicate-ignore-db`, asegúrese de incluir la base de datos que incluye las tablas especificadas en la replicación con la réplica de lectura.
- `replicate-wild-ignore-table` – No replicar tablas en función de la base de datos y los patrones de nombre de tabla especificados. Se admiten los caracteres comodín `%` y `_`. Cuando el parámetro `replicate-do-table` o `replicate-wild-do-table` se establece para una réplica de lectura, este parámetro no se evalúa.

Los parámetros se evalúan en el orden en que se enumeran. Para obtener más información sobre cómo funcionan estos parámetros, consulte la documentación de MySQL.

- Para obtener información general, consulte Opciones y variables del servidor de réplica.
- Para obtener información acerca de cómo se evalúan los parámetros de filtrado de replicación de bases de datos, consulte Evaluación de opciones de registros binarios y replicación a nivel de base de datos.
- Para obtener información acerca de cómo se evalúan los parámetros de filtrado de replicación de tablas, consulte Evaluación de las opciones de replicación a nivel de tabla.

Por defecto, cada uno de estos parámetros tiene un valor vacío. En cada réplica de lectura, puede utilizar estos parámetros para establecer, cambiar y eliminar los filtros de replicación. Cuando establezca uno de estos parámetros, separe cada filtro de los demás con una coma.

Puede utilizar los caracteres comodín `%` y `_` en los parámetros `replicate-wild-do-table` y `replicate-wild-ignore-table`. El comodín `%` coincide con cualquier número de caracteres y el comodín `_` solo coincide con un carácter.

El formato de registro binario de la instancia de base de datos de origen es importante para la replicación, ya que determina el registro de los cambios en los datos. La configuración del parámetro `binlog_format` determina si la replicación está basada en filas o en instrucciones. Para obtener más información, consulte Configuración del registro binario de RDS para MySQL para bases de datos de Single-AZ.

> **Note**
>
> Todas las instrucciones de lenguaje de definición de datos (DDL) se replican como instrucciones, independientemente de la configuración de `binlog_format` en la instancia de base de datos de origen.

Limitaciones del filtrado de replicación de RDS fopara r MySQL

Las siguientes limitaciones se aplican al filtrado de replicación de RDS para MySQL:

- Cada parámetro de filtrado de replicación tiene un límite de 2000 caracteres.
- No se admiten comas en los filtros de replicación para los valores de los parámetros. En una lista de parámetros, las comas solo se pueden usar como separadores de valores. Por ejemplo, no se admite `ParameterValue='`a,b`'`, pero sí `ParameterValue='a,b'`.
- Las opciones `--binlog-do-db` y `--binlog-ignore-db` de MySQL para el filtrado de registros binarios no son compatibles.

- El filtrado de replicación no es compatible con transacciones XA.

  Para obtener más información, consulte Restricciones a las transacciones XA en la documentación de MySQL.

Ejemplos de filtrado de replicación de RDS para MySQL

Para configurar el filtrado de replicación para una réplica de lectura, modifique los parámetros de filtrado de replicación en el grupo de parámetros asociado a la réplica de lectura.

> **Note**
>
> No puede modificar un grupo de parámetros predeterminado. Si la réplica de lectura emplea un grupo de parámetros predeterminado, cree un nuevo grupo de parámetros y asócielo con la réplica de lectura. Para obtener más información acerca de los grupos de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.

Puede establecer parámetros en un grupo de parámetros mediante la API de RDS, AWS Management Console o AWS CLI. Para obtener información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS. Cuando se establecen parámetros en un grupo de parámetros, todas las instancias de base de datos asociadas al grupo de parámetros utilizan la configuración de los parámetros. Si establece los parámetros de filtrado de replicación en un grupo de parámetros, asegúrese de que el grupo de parámetros está asociado solo con réplicas de lectura. Deje los parámetros de filtrado de replicación vacíos para las instancias de base de datos de origen

En los siguientes ejemplos se establecen los parámetros mediante el uso de AWS CLI. Estos ejemplos establecen `ApplyMethod` en `immediate` para que los cambios de los parámetros se produzcan inmediatamente después de que se complete el comando de la CLI. Si desea que se aplique un cambio pendiente después de reiniciar la réplica de lectura, establezca `ApplyMethod` en `pending-reboot`.

Los siguientes ejemplos establecen filtros de replicación:

- Including databases in replication
- Including tables in replication
- Including tables in replication with wildcard characters

- Excluding databases from replication
- Excluding tables from replication
- Excluding tables from replication using wildcard characters

Example Inclusión de bases de datos en la replicación

En el ejemplo siguiente se incluyen las bases de datos `mydb1` y `mydb2` en la replicación.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-do-
db,ParameterValue='mydb1,mydb2',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-do-
db,ParameterValue='mydb1,mydb2',ApplyMethod=immediate"
```

Example Inclusión de tablas en la replicación

En el siguiente ejemplo se incluyen las tablas `table1` y `table2` en la base de datos `mydb1` en la replicación.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-do-
table,ParameterValue='mydb1.table1,mydb1.table2',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
```

```
  --db-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-do-
table,ParameterValue='mydb1.table1,mydb1.table2',ApplyMethod=immediate"
```

Example Inclusión de tablas en la replicación mediante el uso de caracteres comodín

En el ejemplo siguiente se incluyen tablas con nombres que empiezan con `order` y `return` en la base de datos `mydb` en la replicación.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-wild-do-table,ParameterValue='mydb.order
%,mydb.return%',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-wild-do-table,ParameterValue='mydb.order
%,mydb.return%',ApplyMethod=immediate"
```

Example Exclusión de bases de datos de la replicación

En el siguiente ejemplo se excluyen las bases de datos `mydb5` y `mydb6` de la replicación.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-ignore-
db,ParameterValue='mydb5,mydb6',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
```

```
  --parameters "ParameterName=replicate-ignore-
db,ParameterValue='mydb5,mydb6',ApplyMethod=immediate"
```

Example Exclusión de tablas de la replicación

En el siguiente ejemplo, se excluyen de la replicación las tablas `table1` en la base de datos `mydb5` y `table2` en la base de datos `mydb6`.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-ignore-
table,ParameterValue='mydb5.table1,mydb6.table2',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-ignore-
table,ParameterValue='mydb5.table1,mydb6.table2',ApplyMethod=immediate"
```

Example Exclusión de tablas de la replicación mediante el uso de caracteres comodín

En el siguiente ejemplo se excluyen las tablas con nombres que empiezan con `order` y `return` en la base de datos `mydb7` de la replicación.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myparametergroup \
  --parameters "ParameterName=replicate-wild-ignore-table,ParameterValue='mydb7.order
%,mydb7.return%',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myparametergroup ^
  --parameters "ParameterName=replicate-wild-ignore-table,ParameterValue='mydb7.order
%,mydb7.return%',ApplyMethod=immediate"
```

Visualización de los filtros de replicación para una réplica de lectura

Puede ver los filtros de replicación para una réplica de lectura de las siguientes maneras:

- Verifique la configuración de los parámetros de filtrado de replicación en el grupo de parámetros asociado a la réplica de lectura.

  Para obtener instrucciones, consulte Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS.
- En un cliente de MySQL, conéctese a la réplica de lectura y ejecute la instrucción `SHOW REPLICA STATUS`.

  En la salida, los siguientes campos muestran los filtros de replicación para la réplica de lectura:
  - `Replicate_Do_DB`
  - `Replicate_Ignore_DB`
  - `Replicate_Do_Table`
  - `Replicate_Ignore_Table`
  - `Replicate_Wild_Do_Table`
  - `Replicate_Wild_Ignore_Table`

  Para obtener más información acerca de estos campos, consulte Comprobación del estado de replicación en la documentación de MySQL.

Configuración de la replicación retrasada con MySQL

Puede utilizar la replicación retrasada como estrategia de recuperación de desastres. Con la replicación retardada, se especifica el tiempo mínimo, en segundos, que se retardará la replicación desde la instancia de origen a la réplica de lectura. En caso de desastre, por ejemplo, si se elimina una tabla involuntariamente, el procedimiento siguiente permite recuperarse rápidamente del desastre:

- Detenga la replicación en la réplica de lectura antes de que se envíe a ella el cambio que provocó el desastre.

  Utilice el procedimiento almacenado mysql.rds_stop_replication para detener la replicación.
- Inicie la replicación y especifique que esta se detenga automáticamente en una ubicación del archivo registro.

Para especificar una ubicación justo anterior al desastre, se utiliza el procedimiento almacenado mysql.rds_start_replication_until.

- Promocione la réplica de lectura para que sea la nueva instancia de base de datos de origen; para ello, siga las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

> **Note**
>
> - En Amazon RDS para MySQL 8.4, la replicación retrasada es compatible con MySQL 8.4.3 y versiones posteriores. En Amazon RDS para MySQL 8.0, la replicación retrasada es compatible con MySQL 8.0.28 y versiones posteriores. En Amazon RDS para MySQL 5.7, la replicación retardada es compatible con MySQL 5.7.44 y versiones posteriores.
> - Use procedimientos almacenados para configurar la replicación retardada. La reproducción retrasada no se puede configurar con la AWS Management Console, la AWS CLI o la API de Amazon RDS.
> - Puede usar la replicación basada en identificadores de transacciones globales (GTID) en una configuración de replicación retrasada para las versiones siguientes.
>   - RDS para MySQL versión 5.7.44 y versiones 5.7 posteriores
>   - RDS para MySQL versión 8.0.28 y versiones 8.0 posteriores
>   - RDS para MySQL versión 8.4.3 y versiones 8.4 posteriores
>
>   Si usa una replicación basada en GTID, use el procedimiento almacenado mysql.rds_start_replication_until_gtid en lugar del procedimiento almacenado mysql.rds_start_replication_until. Para obtener más información sobre la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

Temas

- Configuración de la replicación retrasada durante la creación de réplicas de lectura
- Modificación de la replicación retrasada para una réplica de lectura existente
- Establecimiento de una ubicación para detener la replicación en una réplica de lectura
- Promoción de una réplica de lectura

Configuración de la replicación retrasada durante la creación de réplicas de lectura

Para configurar la replicación retardada para cualquier réplica de lectura futura creada a partir de una instancia de base de datos, ejecute el procedimiento almacenado mysql.rds_set_configuration con el parámetro `target delay`.

Para configurar la replicación retardada durante la creación de réplicas de lectura

1. Utilice un cliente de MySQL para conectarse como usuario maestro a la instancia de base de datos MySQL que vaya a ser el origen de las réplicas de lectura.
2. Ejecute el procedimiento almacenado mysql.rds_set_configuration con el parámetro `target delay`.

   Por ejemplo, ejecute el siguiente procedimiento almacenado para especificar que la replicación se retardará al menos una hora (3600 segundos) para todas las réplicas de lectura creadas desde la instancia de base de datos actual.

   ```
   call mysql.rds_set_configuration('target delay', 3600);
   ```

   > **Note**
   >
   > Después de ejecutar este procedimiento almacenado, todas las réplicas de lectura que cree mediante la AWS CLI o la API de Amazon RDS se configurarán con la reproducción retardada el número de segundos especificado.

Modificación de la replicación retrasada para una réplica de lectura existente

Para modificar la replicación retardada para una réplica de lectura existente, ejecute el procedimiento almacenado mysql.rds_set_source_delay.

Para modificar la replicación retardada de una réplica de lectura existente

1. Use un cliente de MySQL para conectarse como usuario maestro a la réplica de lectura.
2. Utilice el procedimiento almacenado mysql.rds_stop_replication para detener la replicación.
3. Ejecute el procedimiento almacenado mysql.rds_set_source_delay.

   Por ejemplo, ejecute el siguiente procedimiento almacenado para especificar que la replicación en la réplica de lectura se retardará al menos una hora (3600 segundos).

```
call mysql.rds_set_source_delay(3600);
```

4. Utilice el procedimiento almacenado mysql.rds_start_replication para iniciar la replicación.

Establecimiento de una ubicación para detener la replicación en una réplica de lectura

Después de detener la replicación en la réplica de lectura, puede utilizar el procedimiento almacenado mysql.rds_start_replication_until para iniciar la replicación y volver a detenerla en una ubicación concreta del registro binario.

Para iniciar la replicación en una réplica de lectura y detenerla en una ubicación concreta

1. Use un cliente de MySQL para conectarse como usuario maestro a la instancia de base de datos MySQL de origen.
2. Ejecute el procedimiento almacenado mysql.rds_start_replication_until.

   En el ejemplo siguiente se inicia la replicación y se replican los cambios hasta que alcanza la ubicación `120` del archivo registro binario `mysql-bin-changelog.000777`. En una situación de recuperación de desastres, supongamos que la ubicación `120` es justo anterior al desastre.

   ```
   call mysql.rds_start_replication_until(
     'mysql-bin-changelog.000777',
     120);
   ```

La replicación se detiene automáticamente cuando se alcanza el punto de detención. Se genera el siguiente evento de RDS: `Replication has been stopped since the replica reached the stop point specified by the rds_start_replication_until stored procedure`.

Promoción de una réplica de lectura

Después de que se detenga la replicación, en una situación de recuperación de desastres, puede promocionar una réplica de lectura para que sea la nueva instancia de base de datos de origen. Para obtener información acerca de la promoción de una réplica de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Eliminación de réplicas de lectura con MySQL

Las réplicas de lectura se han diseñado para permitir las consultas de lectura, pero puede necesitar actualizaciones ocasionales. Por ejemplo, puede necesitar añadir un índice para optimizar los tipos concretos de consultas que obtienen acceso a la réplica.

Aunque puede habilitar las actualizaciones configurando el parámetro `read_only` en `0` en el grupo de parámetros de base de datos de la réplica de lectura, se recomienda no hacerlo porque puede provocar problemas si la réplica de lectura es incompatible con la instancia de base de datos de origen. Para las operaciones de mantenimiento, se recomienda utilizar la implementación azul/verde. Para obtener más información, consulte Uso de las implementaciones azul/verde para actualizar las bases de datos.

Si deshabilita el modo de solo lectura en una réplica de lectura, cambie el valor del parámetro `read_only` a `1` de nuevo lo antes posible.

Implementaciones de réplicas de lectura Multi-AZ con MySQL

Puede crear una réplica de lectura a partir de implementaciones de instancia de base de datos Single-AZ o Multi-AZ. Puede usar implementaciones Multi-AZ para mejorar la durabilidad y la disponibilidad de los datos críticos, pero no puede usar la implementación Multi-AZ secundaria para responder a consultas de solo lectura. En lugar de ello, puede crear réplicas de lectura a partir de una instancia de base de datos Multi-AZ con un tráfico elevado para descargar las consultas de solo lectura. Si la instancia de origen de una implementación Multi-AZ conmuta a la secundaria, las réplicas de lectura asociadas cambian automáticamente para usar la secundaria (ahora principal) como origen de replicación. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Puede crear una réplica de lectura como instancia de base de datos de Multi-AZ. Amazon RDS crea una réplica en espera en otra zona de disponibilidad para permitir la conmutación por error de la réplica. La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.

Uso de réplicas de lectura en cascada con RDS para MySQL

RDS para MySQL admite réplicas de lectura en cascada. Con réplicas de lectura en cascada, puede escalar las lecturas sin agregar sobrecarga a su instancia de base de datos de origen de RDS para MySQL.

Con réplicas de lectura en cascada, la instancia de base de datos de RDS para MySQL envía datos a la primera réplica de lectura de la cadena. Esa réplica de lectura envía datos a la segunda réplica de la cadena, etc. El resultado final es que todas las réplicas de lectura de la cadena tienen los cambios de la instancia de base de datos de RDS para MySQL, pero sin la sobrecarga únicamente en la instancia de base de datos de origen.

Puede crear una serie de hasta tres réplicas de lectura en cadena a partir de una instancia de base de datos de origen de RDS para MySQL. Por ejemplo, suponga que tiene una instancia de base de datos de RDS para MySQL: `mysql-main`. Puede hacer lo siguiente:

- A partir de `mysql-main`, cree la primera réplica de lectura de la cadena, `read-replica-1`.
- A continuación, a partir de `read-replica-1`, cree la siguiente réplica de lectura de la cadena, `read-replica-2`.
- Por último, a partir de `read-replica-2`, cree la tercera réplica de lectura de la cadena, `read-replica-3`.

No se puede crear otra réplica de lectura más allá de esta tercera réplica de lectura en cascada de la serie para `mysql-main`. Una serie completa de instancias de una instancia de base de datos de origen de RDS para MySQL hasta el final de una serie de réplicas de lectura en cascada puede constar de cuatro instancias de base de datos como máximo.

Para que las réplicas de lectura en cascada funcionen, cada instancia de base de datos de origen de RDS para MySQL debe tener las copias de seguridad automáticas activadas. Para habilitar las copias de seguridad automáticas en una réplica de lectura, primero debe crear la réplica de lectura y modificarla a continuación para habilitar las copias de seguridad automáticas. Para obtener más información, consulte Creación de una réplica de lectura.

Al igual que con cualquier réplica de lectura, puede promocionar una réplica de lectura que forma parte de una cascada. La promoción de una réplica de lectura desde dentro de una cadena de réplicas de lectura elimina esa réplica de la cadena. Por ejemplo, suponga que desea trasladar parte de la carga de trabajo de su Instancia de base de datos de `mysql-main` a una nueva instancia para que la utilice únicamente el departamento de contabilidad. Tomando la cadena de tres réplicas de lectura del ejemplo, decide promocionar `read-replica-2`. La cadena se ve afectada de la siguiente manera:

- Promover `read-replica-2` la elimina de la cadena de replicación.
  - Ahora es una instancia de base de datos de lectura o escritura completa.

  - Continúa replicando en `read-replica-3`, tal como hacía antes de la promoción.
- Su `mysql-main` sigue replicándose en `read-replica-1`.

Para obtener más información acerca de la promoción de réplicas de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Supervisión del retardo de replicación para réplicas de lectura de MySQL

Para las réplicas de lectura de MySQL, puede monitorear el retraso de replicación en Amazon CloudWatch mediante la visualización de la métrica `ReplicaLag` de Amazon RDS. La métrica `ReplicaLag` indica el valor del campo `Seconds_Behind_Master` del comando `SHOW REPLICA STATUS`.

Los motivos comunes de retardo de la replicación para MySQL son los siguientes:

- Una interrupción de la red.
- Escritura en tablas con índices diferentes en una réplica de lectura. Si el parámetro `read_only` se establece en `0` en la réplica de lectura, la replicación puede bloquearse si la réplica de lectura es incompatible con la instancia de base de datos de origen. Una vez que haya realizado las tareas de mantenimiento en la réplica de lectura, le recomendamos que vuelva a establecer el parámetro `read_only` en `1`.
- Uso de un motor de almacenamiento no transaccional como MyISAM. La replicación solo se admite para el motor de almacenamiento InnoDB en MySQL.

Cuando la métrica `ReplicaLag` llegue a 0, la réplica estará funcionando al mismo ritmo que la instancia de base de datos de origen. Si la métrica `ReplicaLag` devuelve -1, la replicación no está activa. `ReplicaLag` = -1 es equivalente a `Seconds_Behind_Master` = `NULL`.

Inicio y detención de replicaciones con réplicas de lectura de MySQL

Puede detener y reiniciar el proceso de replicación en una instancia de base de datos de Amazon RDS llamando a los procedimientos mysql.rds_stop_replication y mysql.rds_start_replication almacenados en el sistema. Puede hacerlo cuando replique entre dos instancias de Amazon RDS para las operaciones de larga duración, como la creación de índices grandes. También debe detener y comenzar la replicación cuando importe o exporte bases de datos. Para obtener más información, consulte Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de

inactividad reducido y Exportación de datos desde una instancia de base de datos MySQL mediante replicación.

Si la replicación se detiene durante más de 30 días consecutivos, ya sea manualmente o a causa de un error de replicación, Amazon RDS termina la replicación entre la instancia de base de datos de origen y todas las réplicas de lectura Realiza ese procedimiento para impedir que aumenten los requisitos de almacenamiento en la instancia de base de datos de origen y que se incrementen los tiempos de conmutación por error. La instancia de base de datos de la réplica de lectura seguirá estando disponible. Sin embargo, la replicación no se podrá reanudar porque los registros binarios requeridos por la réplica de lectura se eliminan de la instancia de base de datos de origen cuando termina la replicación. Puede crear una nueva réplica de lectura para la instancia de base de datos de origen si desea restablecer la replicación.

Solución de problemas de réplicas de lectura de MySQL

Para las instancias de base de datos MySQL, en algunos casos, las réplicas de lectura tienen errores de replicación o incoherencias de datos (o ambos) entre la réplica de lectura y su instancia de base de datos de origen. Este problema se produce cuando algunos eventos de binglog o registros redo de InnoDB no se vacían durante un error de la réplica de lectura o la instancia de base de datos de origen. En estos casos, elimine y vuelva a crear manualmente las réplicas de lectura. Puede reducir la probabilidad de que esto ocurra al establecer los siguientes valores de parámetro: `sync_binlog=1` y `innodb_flush_log_at_trx_commit=1`. Estos ajustes pueden reducir el desempeño, así que es aconsejable probar su impacto antes de implementar los cambios en un entorno de producción.

> **Warning**
>
> En el grupo de parámetros asociado con la instancia de base de datos de origen, recomendamos mantener estos valores de parámetros: `sync_binlog=1` y `innodb_flush_log_at_trx_commit=1`. Estos parámetros son dinámicos. Si no quiere utilizar esta configuración, le recomendamos configurar temporalmente esos valores antes de ejecutar cualquier operación en la instancia de base de datos de origen que pueda provocar que se reinicie. Estas operaciones incluyen, entre otras, el reinicio, el reinicio con conmutación por error, la actualización de la versión de la base de datos y el cambio de la clase de la instancia de base de datos o su almacenamiento. La misma recomendación se aplica a la creación de nuevas réplicas de lectura de la instancia de base de datos de origen.

Si no se siguen estas recomendaciones, se aumenta el riesgo de que las réplicas de lectura tengan errores de replicación o incoherencias de datos (o ambos) entre la réplica de lectura y su instancia de base de datos de origen.

Las tecnologías de replicación para MySQL son asíncronas. Como son asíncronas, cabe esperar aumentos ocasionales de `BinLogDiskUsage` en la instancia de base de datos de origen y de `ReplicaLag` en la réplica de lectura. Por ejemplo, en paralelo se pueden realizar gran volumen de operaciones de escritura en la instancia de base de datos de origen. En cambio, las operaciones de escritura en la réplica de lectura se serializan con un único subproceso E/S que puede provocar un retraso entre la instancia de origen y la réplica de lectura. Para obtener más información acerca de las réplicas de solo lectura en la documentación de MySQL, consulte Replication Implementation Details.

Puede hacer varias cosas para reducir el retraso entre las actualizaciones de una instancia de base de datos de origen y las actualizaciones posteriores de la réplica de lectura. Por ejemplo, puede hacer lo siguiente:

- Dimensionar una réplica de lectura para que tenga un tamaño de almacenamiento y una clase de instancia de base de datos comparables a los de la instancia de base de datos de origen.
- Asegurarse de que los valores de los parámetros de los grupos de parámetros de base de datos utilizados en la instancia de base de datos de origen y la réplica de lectura son compatibles. Para obtener más información y un ejemplo, consulte el análisis del parámetro `max_allowed_packet` que se puede encontrar más adelante en esta sección.

Amazon RDS monitorea el estado de la replicación de las réplicas de lectura y actualiza el campo `Replication State` de la instancia de la réplica de lectura a `Error` si la replicación se detiene por cualquier motivo. Un ejemplo de ello pueden ser las consultas DML que se ejecutan en la réplica de lectura y que entran en conflicto con las actualizaciones realizadas en la instancia de base de datos de origen.

Puede revisar los detalles del error asociado mostrado por el motor de MySQL visualizando el campo `Replication Error`. También se generan eventos que indican el estado de la réplica de lectura, entre los que se incluyen RDS-EVENT-0045, RDS-EVENT-0046 y RDS-EVENT-0047. Para obtener más información acerca de los eventos y la suscripción a ellos, consulte Uso de notificaciones de eventos de Amazon RDS. Si aparece un mensaje de error de MySQL, revise el número del error en la documentación sobre los mensajes de error de MySQL.

Un problema frecuente que puede causar errores de replicación es que el valor del parámetro `max_allowed_packet` de una réplica de lectura sea inferior al parámetro `max_allowed_packet` de la instancia de base de datos de origen. El parámetro `max_allowed_packet` es un parámetro personalizado que puede establecer en un grupo de parámetros de base de datos. Utilice `max_allowed_packet` para especificar el tamaño máximo del código DML que se puede ejecutar en la base de datos. En algunos casos, el valor de `max_allowed_packet` en el grupo de parámetros de base de datos asociado a una réplica de lectura es inferior al valor de `max_allowed_packet` del grupo de parámetros de base de datos asociado a la instancia de base de datos de origen. En estos casos, el proceso de replicación puede generar el error `Packet bigger than 'max_allowed_packet' bytes` y detener la replicación. Para resolver el error, haga que la instancia de base de datos de origen y la réplica de lectura usen grupos de parámetros de base de datos con los mismos valores del parámetro `max_allowed_packet`.

Entre las situaciones comunes que pueden causar errores de replicación se incluyen las siguientes:

- Escritura en tablas en una réplica de lectura. En algunos casos, puede crear índices en una réplica de lectura que sean diferentes de los índices de la instancia de base de datos de origen. Si lo hace, establezca el parámetro `read_only` en `0` para crear los índices. Si escribe en tablas en la réplica de lectura, la replicación puede bloquearse si la réplica de lectura es incompatible con la instancia de base de datos de origen. Una vez que haya realizado las tareas de mantenimiento en la réplica de lectura, le recomendamos que vuelva a establecer el parámetro `read_only` en `1`.
- Uso de un motor de almacenamiento no transaccional como MyISAM. Las réplicas de lectura requieren un motor de almacenamiento transaccional. La replicación solo se admite para el motor de almacenamiento InnoDB en MySQL.
- Uso de consultas no deterministas que no sean seguras, como `SYSDATE()`. Para obtener más información, consulte Determinación de instrucciones seguras e inseguras en el registro binario.

Si decide que es seguro hacer caso omiso de un error, puede seguir los pasos que se describen en la sección Omisión del error de replicación actual de RDS para MySQL. De no ser así, primero puede eliminar la réplica de lectura. A continuación, cree una instancia que use el mismo identificador de instancias de bases de datos para que el punto de conexión siga siendo el mismo que en la réplica de lectura antigua. Si se corrige un error de replicación, `Replication State` cambia a replicating.

Uso de la replicación basada en GTID

El siguiente contenido explica cómo utilizar los identificadores de transacciones globales (GTID) con replicación de registro binario (binlog) entre instancias de base de datos de Amazon RDS para MySQL

Si utiliza la replicación del binlog y no conoce la replicación basada en GTID con MySQL, consulte Replication with global transaction identifiers en la documentación de MySQL.

La replicación basada en GTID no es compatible con las versiones siguientes:

- Todas las versiones de RDS para MySQL 8.4
- Todas las versiones de RDS para MySQL 8.0
- Todas las versiones de RDS para MySQL 5.7

Todas las instancias de base de datos de MySQL en una configuración de replicación deben cumplir este requisito.

Temas

- Información general de identificadores de transacciones globales (GTID)
- Parámetros de replicación basada en GTID
- Activación de la replicación basada en GTID de las nuevas réplicas de lectura para RDS para MySQL
- Activación de la replicación basada en GTID de las réplicas de lectura existentes para RDS para MySQL
- Desactivación de la reproducción basada en GTID para una instancia de base de datos de MySQL de RDS con réplicas de lectura

Información general de identificadores de transacciones globales (GTID)

Los identificadores de transacciones globales (GTID) son indentificadores únicos generados por transacciones confirmadas por MySQL. Puede utilizar GTID para que la replicación del binlog sea más simple y sencilla para la solución de problemas.

MySQL usa dos tipos distintos de transacciones para la replicación del binlog:

- Transacciones de GTID: transacciones que se identifican mediante GTID.

- Transacciones anónimas: transacciones que no tienen un GTID asignado.

En una configuración de replicación, los GTID son únicos en todas las instancias de base de datos. Los GTID simplifican la configuración de replicación porque cuando se usan no es necesario hacer referencia a las posiciones de los archivos de registro. Los GTID también simplifican el seguimiento de las transacciones replicadas y determinan si las instancias de origen y las réplicas son coherentes.

Puede usar una replicación basada en GTID para replicar los datos con réplicas de lectura de RDS for MySQL. Puede configurar la replicación basada en GTID cuando cree réplicas de lectura nuevas o puede convertir las réplicas de lectura existentes para que usen la replicación basada en GTID.

También puede usar la replicación basada en GTID en una configuración de replicación retrasada con RDS for MySQL. Para obtener más información, consulte Configuración de la replicación retrasada con MySQL.

Parámetros de replicación basada en GTID

Use los parámetros siguientes para configurar replicación basada en GTID.

Parámetro	Valores válidos	Descripción
`gtid_mode`	`OFF`, `OFF_PERMISSIVE` , `ON_PERMISSIVE` , `ON`	`OFF` especifica que las nuevas transacciones son anónimas (es decir, no tienen GTID) y que una transacción debe ser anónima para replicarse. `OFF_PERMISSIVE` especifica que las nuevas transacciones son anónimas, pero que todas las transacciones pueden replicarse. `ON_PERMISSIVE` especifica que las nuevas transacciones son de GTID, pero que todas las transacciones pueden replicarse. `ON` especifica que las nuevas transacciones son de GTID y que una transacción debe ser de GTID para poder replicarse.

Parámetro	Valores válidos	Descripción
`enforce_gtid_consistency`	`OFF`, `ON`, `WARN`	`OFF` permite que las transacciones infrinjan la uniformidad de GTID. `ON` evita que las transacciones infrinjan la uniformidad de GTID. `WARN` permite que las transacciones infrinjan la uniformidad de GTID, pero genera un aviso cuando se proudce una infracción.

> **Note**
>
> En la AWS Management Console, el parámetro `gtid_mode` aparece como `gtid-mode`.

Para la replicación basada en GTID, utilice esta configuración para el grupo de parámetros para su instancia de base de datos o réplica de lectura:

- `ON` y `ON_PERMISSIVE` se aplican solo a la replicación saliente de una instancia de base de datos de RDS. Estos valores provocan que su instancia de base de datos de RDS utilicen GTID para transacciones que se replican. `ON` requiere que la base de datos externa también utilice la replicación basada en GTID. `ON_PERMISSIVE` hace que la replicación basada en GTID sea opcional en la base de datos externa.
- Si se establece `OFF_PERMISSIVE`, significa que sus instancias de base de datos de RDS pueden aceptar la replicación entrante de una base de datos externa. Esto se puede realizar sin importar si la base de datos de origen utiliza la replicación basada en GTID.
- Si se establece `OFF`, significa que su instancia de base de datos de RDS solo acepta la replicación entrante desde bases de datos externas que no utilizan la replicación basada en GTID.

Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

Activación de la replicación basada en GTID de las nuevas réplicas de lectura para RDS para MySQL

Cuando la reproducción basada en GTID esté habilitada para una instancia de base de datos de MySQL de RDS, la reproducción basada en GTID se configura automáticamente para las réplicas de lectura de la instancia de base de datos.

Para habilitar la replicación basada en GTID para nuevas réplicas de lectura

1. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos tiene la siguiente configuración de parámetros:

   - `gtid_mode` – `ON` o `ON_PERMISSIVE`
   - `enforce_gtid_consistency` – `ON`

   Para obtener más información sobre el establecimiento de parámetros de configuración con grupos de consultas, consulte Grupos de parámetros para Amazon RDS.
2. Si ha cambiado el grupo de parámetros de la instancia de base de datos, reinicie la instancia de base de datos. Para obtener más información acerca de cómo hacerlo, consulte Reinicio de una instancia de base de datos.
3. Cree una o varias réplicas de lectura de la instancia de base de datos. Para obtener más información acerca de cómo hacerlo, consulte Creación de una réplica de lectura.

Amazon RDS intenta establecer la replicación basada en GTID entre la instancia de base de datos de MySQL y las réplicas de lectura usando `MASTER_AUTO_POSITION`. Si el intento produce un error, Amazon RDS usa las posiciones de los archivos de registro para la replicación con las réplicas de lectura. Para obtener más información acerca de `MASTER_AUTO_POSITION`, consulte GTID Auto-Positioning en la documentación de MySQL.

Activación de la replicación basada en GTID de las réplicas de lectura existentes para RDS para MySQL

Para una instancia de base de datos de MySQL existente con réplicas de lectura que no utilice la reproducción basada en GTID, puede configurar la reproducción basada en GTID entre la instancia de base de datos y las réplicas de lectura.

Habilitación de la replicación basada en GTID para las réplicas de lectura existentes

1. Si la instancia de base de datos o cualquier réplica de lectura utiliza RDS para MySQL 8.0 o versiones anteriores a 8.0.26, actualice la instancia de base de datos o la réplica de lectura a la versión 8.0.26 o a versiones posteriores a MySQL 8.0. Todas las versiones de RDS para MySQL 8.4 y 5.7 admiten la replicación basada en GTID.

   Para obtener más información, consulte Actualizaciones del motor de base de datos de RDS para MySQL.

2. De manera opcional, restablezca los parámetros de GTID y pruebe el comportamiento de la instancia de base de datos y las réplicas de lectura:

   a. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos y cada réplica de lectura tiene el parámetro `enforce_gtid_consistency` establecido en `WARN`.

      Para obtener más información sobre el establecimiento de parámetros de configuración con grupos de consultas, consulte Grupos de parámetros para Amazon RDS.

   b. Si ha cambiado el grupo de parámetros de la instancia de base de datos, reinicie la instancia de base de datos. Si ha cambiado el grupo de parámetros de una réplica de lectura, reinicie la réplica de lectura.

      Para obtener más información, consulte Reinicio de una instancia de base de datos.

   c. Ejecute la instancia de base de datos y las réplicas de lectura con su carga de trabajo normal y monitoree los archivos de registro.

      Si ve advertencias sobre las transacciones incompatibles con GTID, ajuste su aplicación de forma que solo use características compatibles con GTID. Asegúrese de que la instancia de base de datos no está generando ningún aviso sobre transacciones incompatibles con GTID antes de continuar al paso siguiente.

3. Restablezca los parámetros de GTID para la replicación basada en GTID que permite las transacciones anónimas hasta que las réplicas de lectura las hayan procesado todas.

   a. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos y cada réplica de lectura tienen la siguiente configuración de parámetros:

      - `gtid_mode` – `ON_PERMISSIVE`
      - `enforce_gtid_consistency` – `ON`

b. Si ha cambiado el grupo de parámetros de la instancia de base de datos, reinicie la instancia de base de datos. Si ha cambiado el grupo de parámetros de una réplica de lectura, reinicie la réplica de lectura.

4. Espere a que todas las transacciones anónimas se hayan replicado. Para comprobar que se han replicado, haga lo siguiente:

   a. Ejecute la siguiente instrucción en su instancia de base de datos de origen:

      MySQL 8.4

      ```
      SHOW BINARY LOG STATUS;
      ```

      MySQL 5.7 y 8.0

      ```
      SHOW MASTER STATUS;
      ```

      Anote los valores de las columnas `File` y `Position`.

   b. En cada réplica de lectura, use la información de archivo y posición de su instancia de origen en el paso anterior para ejecutar la siguiente consulta.

      ```
      SELECT MASTER_POS_WAIT('file', position);
      ```

      Por ejemplo, si el nombre del archivo es `mysql-bin-changelog.000031` y la posición es `107`, ejecute la siguiente instrucción.

      ```
      SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
      ```

      Si la réplica de lectura está después de la posición especificada, la consulta devuelve resultados inmediatamente. De no hacerlo, la función espera. Continúe al siguiente paso cuando la consulta haya devuelto resultados para todas las réplicas de lectura.

5. Restablezca los parámetros de GTID solo para la replicación basada en GTID.

   a. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos y cada réplica de lectura tienen la siguiente configuración de parámetros:

      - `gtid_mode` – `ON`
      - `enforce_gtid_consistency` – `ON`

b. Reinicie la instancia de base de datos y cada réplica de lectura.

6. En cada réplica de lectura, ejecute el siguiente procedimiento.

MySQL 8.4 y versiones principales superiores

```
CALL mysql.rds_set_source_auto_position(1);
```

MySQL 8.0 y versiones secundarias superiores

```
CALL mysql.rds_set_master_auto_position(1);
```

Desactivación de la reproducción basada en GTID para una instancia de base de datos de MySQL de RDS con réplicas de lectura

Puede desactivar la reproducción basada en GTID para una instancia de base de datos de MySQL con réplicas de lectura.

Para desactivar la replicación basada en GTID para una instancia de base de datos de MySQL con réplicas de lectura

1. En cada réplica de lectura, ejecute el siguiente procedimiento:

MySQL 8.4 y versiones principales superiores

```
CALL mysql.rds_set_source_auto_position(0);
```

MySQL 8.0 y versiones secundarias superiores

```
CALL mysql.rds_set_master_auto_position(0);
```

2. Restablezca `gtid_mode` en `ON_PERMISSIVE` .

a. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos de MySQL y cada réplica de lectura tiene el parámetro `gtid_mode` establecido en `ON_PERMISSIVE`.

Para obtener más información sobre el establecimiento de parámetros de configuración con grupos de consultas, consulte Grupos de parámetros para Amazon RDS.

b. Reinicie la instancia de base de datos de MySQL y cada réplica de lectura. Para obtener más información acerca del reinicio, consulte Reinicio de una instancia de base de datos.

3. Restablezca `gtid_mode` en `OFF_PERMISSIVE` .

   a. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos de MySQL y cada réplica de lectura tiene el parámetro `gtid_mode` establecido en `OFF_PERMISSIVE`.

   b. Reinicie la instancia de base de datos de MySQL y cada réplica de lectura.

4. Espere a que todas las transacciones de GTID se hayan replicado a todas las réplicas de lectura. Para comprobar que se hayan aplicado, realice los siguientes pasos:

   a. En la instancia de base de datos de MySQL, ejecute el siguiente comando:

      MySQL 8.4

      ```
      SHOW BINARY LOG STATUS
      ```

      MySQL 5.7 y 8.0

      ```
      SHOW MASTER STATUS
      ```

      El resultado debería ser similar al que se indica a continuación.

      ```
      File                        Position
      ------------------------------------
      mysql-bin-changelog.000031      107
      ------------------------------------
      ```

      Tenga en cuenta el archivo y la posición en su resultado.

   b. En cada réplica de lectura, use la información de archivo y posición de su instancia de origen en el paso anterior para ejecutar la siguiente consulta:

      Versiones de MySQL 8.4 y 8.0.26 y versiones superiores de MySQL 8.0

      ```
      SELECT SOURCE_POS_WAIT('file', position);
      ```

      MySQL 5.7

```
SELECT MASTER_POS_WAIT('file', position);
```

Por ejemplo, si el nombre del archivo es `mysql-bin-changelog.000031` y la posición es `107`, ejecute la siguiente instrucción:

Versiones de MySQL 8.4 y 8.0.26 y versiones superiores de MySQL 8.0

```
SELECT SOURCE_POS_WAIT('mysql-bin-changelog.000031', 107);
```

MySQL 5.7

```
SELECT MASTER_POS_WAIT('mysql-bin-changelog.000031', 107);
```

5. Restablezca los parámetros de GTID para deshabilitar la replicación basada en GTID.
   a. Asegúrese de que el grupo de parámetros asociado a la instancia de base de datos de MySQL y cada réplica de lectura tienen la siguiente configuración de parámetros:
      - `gtid_mode` – `OFF`
      - `enforce_gtid_consistency` – `OFF`
   b. Reinicie la instancia de base de datos de MySQL y cada réplica de lectura.

Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Puede configurar la replicación entre una instancia de base de datos de RDS for MySQL o MariaDB y una instancia MySQL o MariaDB externa a Amazon RDS usando la replicación del archivo de registro binario.

Temas

- Antes de empezar
- Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Antes de empezar

Puede configurar la replicación usando la posición de los archivos de registro binarios de transacciones replicadas.

Los permisos requeridos para comenzar la replicación en una instancia de base de datos de Amazon RDS están restringidos y no están disponibles para el usuario maestro de Amazon RDS. Por este motivo, asegúrese de usar los comandos mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) o mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) y mysql.rds_start_replication de Amazon RDS para configurar la replicación entre la base de datos en funcionamiento y la base de datos de Amazon RDS.

Para establecer el formato de registro binario para una base de datos MySQL o MariaDB, actualice el parámetro `binlog_format`. Si su instancia de base de datos usa el grupo de parámetros de instancia de base de datos predeterminado, cree un nuevo grupo de parámetros de base de datos para modificar el parámetro `binlog_format`. En MariaDB y MySQL 8.0 y versiones anteriores, el valor predeterminado de `binlog_format` es `MIXED`. Sin embargo, también puede configurar `binlog_format` como `ROW` o `STATEMENT` si necesita un formato de registro binario (binlog) concreto. Reinicie la instancia de base de datos para que el cambio entre en vigor. En MySQL 8.4 y versiones posteriores, el valor predeterminado de `binlog_format` es `ROW`.

Para obtener más información sobre configurar el parámetro `binlog_format`, consulte Configuración del registro binario de RDS para MySQL para bases de datos de Single-AZ. Para obtener más información acerca de las implicaciones de distintos tipos de replicación de MySQL, consulte Advantages and Disadvantages of Statement-Based and Row-Based Replication en la documentación de MySQL.

Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa

Siga estas directrices al configurar una instancia de origen externa y una réplica en Amazon RDS:

- Monitorice los eventos de conmutación por error para la instancia de base de datos de Amazon RDS que usa como réplica. Si se produce una conmutación por error, la instancia de base de datos que es la réplica se puede volver a crear en un nuevo host con una dirección de red diferente. Para obtener información acerca de la monitorización de los eventos de conmutación por error, consulte Uso de notificaciones de eventos de Amazon RDS.

- Mantenga los binlogs en la instancia de origen hasta que haya verificado que se han aplicado a la réplica. Este mantenimiento garantiza que se pueda restaurar la instancia de origen en caso de error.
- Active las copias de seguridad automatizadas para la instancia de base de datos de Amazon RDS. La activación de las copias de seguridad automatizadas garantiza que puede restaurar su réplica a un momento dado si necesita volver a sincronizar la instancia de origen y la réplica. Para obtener información acerca de las copias de seguridad y la restauración a un momento dado, consulte Copia de seguridad, restauración y exportación de datos.

Para configurar la replicación de archivos de registro binario con una instancia de origen externa

1. Configure la instancia de base de datos MySQL o MariaDB de origen como de solo lectura.

```
mysql> FLUSH TABLES WITH READ LOCK;
mysql> SET GLOBAL read_only = ON;
```

2. Ejecute el comando `SHOW MASTER STATUS` en la instancia de base de datos MySQL o MariaDB para determinar la ubicación del binlog.

   Se recibe un resultado similar al del siguiente ejemplo.

```
File                        Position
------------------------------------
 mysql-bin-changelog.000031      107
------------------------------------
```

3. Copie la base de datos de la instancia externa a la instancia de Amazon RDS con `mysqldump`. Para las bases de datos muy grandes, puede usar el procedimiento que se describe en Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido.

   Para Linux, macOS o Unix:

```
mysqldump --databases database_name \
    --single-transaction \
    --compress \
    --order-by-primary \
    -u local_user \
    -plocal_password | mysql \
        --host=hostname \
```

```
        --port=3306 \
        -u RDS_user_name \
        -pRDS_password
```

Para Windows:

```
mysqldump --databases database_name ^
    --single-transaction ^
    --compress ^
    --order-by-primary ^
    -u local_user ^
    -plocal_password | mysql ^
        --host=hostname ^
        --port=3306 ^
        -u RDS_user_name ^
        -pRDS_password
```

> **Note**
>
> Asegúrese de que no haya ningún espacio entre la opción `-p` y la contraseña que haya escrito.

Para especificar el nombre de host, el nombre de usuario, el puerto y la contraseña para conectarse a su instancia de base de datos en Amazon RDS, use las opciones `--host`, `--user (-u)`, `--port` y `-p` en el comando `mysql`. El nombre de host es el nombre del servicio de nombre de dominio (DNS) tomado del punto de enlace de la instancia de base de datos de Amazon RDS, por ejemplo, `myinstance.123456789012.us-east-1.rds.amazonaws.com`. Puede encontrar el valor del punto de conexión en los detalles de la instancia en la AWS Management Console.

4. Haga que la instancia MySQL o MariaDB de origen vuelvan a admitir la escritura.

```
mysql> SET GLOBAL read_only = OFF;
mysql> UNLOCK TABLES;
```

Para obtener más información sobre cómo hacer copias de seguridad para su uso con replicación, consulte la documentación de MySQL.

5. En la AWS Management Console, agregue la dirección IP del servidor que aloja la base de datos externa al grupo de seguridad de la nube virtual privada (VPC) para la instancia de base de datos de Amazon RDS. Para obtener más información acerca de la modificación de un grupo de seguridad de VPC, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon Virtual Private Cloud.

   La dirección IP puede cambiar cuando se cumplen las siguientes condiciones:

   - Está usando una dirección IP pública para la comunicación entre la instancia de origen externa y la instancia de base de datos.
   - La instancia de origen externa se detuvo y se reinició.

   Si se cumplen esas condiciones, compruebe la dirección IP antes de añadirla.

   Es posible que también necesite configurar su red local para permitir las conexiones desde la dirección IP de la instancia de base de datos de Amazon RDS. Eso se hace para que la red local se pueda comunicar con la instancia de MySQL o MariaDB externa. Para encontrar la dirección IP de la instancia de base de datos de Amazon RDS, use el comando `host`.

   ```
   host db_instance_endpoint
   ```

   El nombre de host es el nombre de DNS tomado del punto de conexión de la instancia de base de datos de Amazon RDS.

6. Con el cliente que prefiera, conecte con la instancia externa y cree un usuario para la replicación. Use esta cuenta únicamente para la replicación y limítela a su dominio para mejorar la seguridad. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

   > **Note**
   >
   > Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

7. Para la instancia externa, conceda los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` al usuario de replicación. Por ejemplo, para conceder los privilegios `REPLICATION`

`CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario "`repl_user`" del dominio, ejecute el siguiente comando.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

8. Defina la instancia de base de datos de Amazon RDS como réplica, Para ello, en primer lugar, conéctese a la instancia de base de datos de Amazon RDS como usuario maestro. A continuación, identifique la base de datos de MySQL o MariaDB externa como instancia de origen usando el comando mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) o mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores). Use el nombre del archivo de registro maestro y la posición del registro maestro que determinó en el paso 2. Los siguientes comandos son ejemplos.

   MySQL 8.4

   ```
   CALL mysql.rds_set_external_source ('mysourceserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
   ```

   MariaDB y MySQL 8.0 y 5.7

   ```
   CALL mysql.rds_set_external_master ('mymasterserver.mydomain.com', 3306,
    'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1);
   ```

   > **Note**
   >
   > En RDS para MySQL, puede aplicar la replicación retrasada si lo desea ejecutando el procedimiento mysql.rds_set_external_source_with_delay (RDS para las versiones principales de MySQL 8.4 y superiores) o mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) almacenado en su lugar. Un motivo para usar la replicación retrasada en RDS para MySQL es activar la recuperación de desastres con el procedimiento almacenado mysql.rds_start_replication_until. En la actualidad, RDS para MariaDB es compatible con la replicación retrasada, pero no con el procedimiento `mysql.rds_start_replication_until`.

9. En la instancia de base de datos de Amazon RDS, ejecute el comando mysql.rds_start_replication para comenzar la replicación.

```
CALL mysql.rds_start_replication;
```

Configuración de la replicación de varios orígenes de Amazon RDS para MySQL

Con la replicación de varios orígenes, puede configurar una instancia de base de datos de Amazon RDS para MySQL como una réplica que reciba eventos de registros binarios de más de una instancia de base de datos de origen de RDS para MySQL. Las instancias de base de datos de RDS para MySQL que ejecutan las siguientes versiones de motor admiten la replicación de varios orígenes:

- Todas las versiones MySQL 8.4
- 8.0.35 y versiones secundarias posteriores
- 5.7.44 y versiones secundarias posteriores

Para obtener información acerca de la replicación varios orígenes de MySQL, consulte MySQL Multi-Source Replication en la documentación de MySQL. La documentación de MySQL contiene información detallada sobre esta característica, mientras que en este tema se describe cómo configurar y administrar canales de replicación de varios orígenes en las instancias de base de datos de RDS para MySQL.

Casos de uso de la replicación de varios orígenes

Los siguientes casos son buenos candidatos para utilizar la replicación de varios orígenes en RDS para MySQL:

- Aplicaciones que necesitan fusionar o combinar varias particiones de instancias de base de datos independientes en una sola.
- Aplicaciones que necesitan generar informes a partir de datos consolidados de varios orígenes.
- Requisitos para crear copias de seguridad consolidadas de los datos a largo plazo que se distribuyen entre varias instancias de base de datos de RDS para MySQL.

Requisitos previos para la replicación de varios orígenes

Antes de configurar la replicación de varios orígenes, se deben completar los siguientes requisitos previos.

- Asegúrese de que cada instancia de base de datos de RDS para MySQL de origen tenga habilitadas las copias de seguridad automáticas. Al habilitar las copias de seguridad automáticas, se habilita el registro binario. Para obtener información acerca de cómo habilitar las copias de seguridad automáticas, consulte the section called “Habilitar las copias de seguridad automatizadas”.
- Para evitar errores de replicación, se recomienda bloquear las operaciones de escritura en las instancias de base de datos de origen. Para ello, defina el parámetro `read-only` en `ON` en un grupo de parámetros personalizado asociado a la instancia de base de datos de origen de RDS para MySQL. Puede utilizar la AWS Management Console o la AWS CLI para crear un nuevo grupo de parámetros personalizado o modificar uno existente. Para obtener más información, consulte the section called “Creación de un grupo de parámetros de base de datos” y the section called “Modificación de parámetros de un grupo de parámetros de base de datos”.
- Para cada instancia de base de datos de origen, agregue la dirección IP de la instancia al grupo de seguridad de la nube privada virtual (VPC) de Amazon para la instancia de base de datos de varios orígenes. Para identificar la dirección IP de una instancia de base de datos de origen, puede ejecutar el comando `dig` *`RDS Endpoint`*. Ejecute el comando desde una instancia de Amazon EC2 en la misma VPC que la instancia de base de datos de varios orígenes de destino.
- Para cada instancia de base de datos de origen, utilice un cliente para conectarse a la instancia de base de datos y cree un usuario de base de datos con los privilegios necesarios para la replicación, como en el siguiente ejemplo.

```
CREATE USER 'repl_user' IDENTIFIED BY 'password';
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user';
```

> **Note**
>
> A partir de MySQL 8.4, el privilegio `REPLICATION SLAVE` ha quedado obsoleto y se ha reemplazado por `REPLICATION REPLICA`. Para MySQL 8.4 y versiones posteriores, utilice la siguiente sintaxis:
>
> ```
> CREATE USER 'repl_user' IDENTIFIED BY 'password';
> GRANT REPLICATION CLIENT, REPLICATION REPLICA ON *.* TO 'repl_user';
> ```

Configuración de canales de replicación de varios orígenes en instancias de base de datos de RDS para MySQL

La configuración de los canales de replicación de varios orígenes es similar a la configuración de la replicación de un solo origen. Para la replicación de varios orígenes, primero habilite el registro binario en la instancia de origen. A continuación, importe los datos desde los orígenes a la réplica de varios orígenes. A continuación, se inicia la replicación desde cada origen utilizando las coordenadas del registro binario o el posicionamiento automático de GTID.

Para configurar una instancia de base de datos de RDS para MySQL como una réplica de varios orígenes de dos o más instancias de base de datos de RDS para MySQL, realice estos pasos.

Temas

- Paso 1: importe datos de las instancias de base de datos de origen a la réplica de varios orígenes
- Paso 2: inicie la replicación desde las instancias de base de datos de origen a la réplica de varios orígenes

Paso 1: importe datos de las instancias de base de datos de origen a la réplica de varios orígenes

Realice los siguientes pasos en cada instancia de base de datos de origen.

Antes de importar los datos de un origen a la réplica de varios orígenes, ejecute el comando `SHOW MASTER STATUS` para determinar el archivo de registro binario actual y su posición. Tome nota de estos datos para usarlos en el paso siguiente. En este ejemplo de salida, el archivo es `mysql-bin-changelog.000031` y la posición es `107`.

> **Note**
>
> A partir de MySQL 8.4, el comando `SHOW MASTER STATUS` ha quedado obsoleto y se ha reemplazado por `SHOW BINARY LOG STATUS`. Para MySQL 8.4 y versiones posteriores, utilice `SHOW BINARY LOG STATUS`.

```
File                        Position
-----------------------------------
mysql-bin-changelog.000031      107
-----------------------------------
```

Ahora copie la base de datos desde la instancia de base de datos de origen a la réplica de varios orígenes utilizando `mysqldump`, como en el ejemplo siguiente.

```
mysqldump --databases database_name \
 --single-transaction \
 --compress \
 --order-by-primary \
 -u RDS_user_name \
 -p RDS_password \
 --host=RDS Endpoint | mysql \
 --host=RDS Endpoint \
 --port=3306 \
 -u RDS_user_name \
-p RDS_password
```

Tras copiar la base de datos, puede establecer el parámetro de solo lectura en `OFF` en la instancia de base de datos de origen.

Paso 2: inicie la replicación desde las instancias de base de datos de origen a la réplica de varios orígenes

Para cada instancia de base de datos de origen, use las credenciales de usuario administrativo para conectarse a la instancia y ejecute los siguientes dos procedimientos almacenados. Estos procedimientos almacenados configuran la replicación en un canal e inician la replicación. En este ejemplo, se utilizan el nombre y la posición del archivo binlog de la salida del ejemplo del paso anterior.

```
CALL mysql.rds_set_external_source_for_channel('mysourcehost.example.com', 3306,
 'repl_user', 'password', 'mysql-bin-changelog.000031', 107, 1, 'channel_1');
CALL mysql.rds_start_replication_for_channel('channel_1');
```

Para obtener más información acerca del uso de estos procedimientos almacenados y otros para configurar y administrar los canales de replicación, consulte the section called “Administración de la replicación de varios orígenes”.

Uso de filtros con la replicación de varios orígenes

Puede utilizar filtros de replicación para especificar qué bases de datos y tablas se replican con una réplica de varios orígenes. Los filtros de replicación pueden incluir bases de datos y tablas en la replicación o excluirlas de la replicación. Para obtener información sobre los filtros de replicación, consulte the section called “Configuración de filtros de replicación”.

Con la replicación de varios orígenes, puede configurar los filtros de replicación de forma global o en el nivel del canal. El filtrado en el nivel del canal solo está disponible con las instancias de base de datos compatibles que ejecutan la versión 8.0 o la versión 8.4. Los siguientes ejemplos muestran cómo configurar filtros globalmente o en el nivel del canal.

Tenga en cuenta los siguientes requisitos y comportamiento con el filtrado en la replicación de varios orígenes:

- Los nombres de los canales deben ir entre comillas inversas (``).
- Si cambia los filtros de replicación en el grupo de parámetros, el `sql_thread` de la réplica de varios orígenes de todos los canales con actualizaciones se reinicia para aplicar los cambios de forma dinámica. Si una actualización incluye un filtro global, se reinician todos los canales de replicación en estado de ejecución.
- Todos los filtros globales se aplican antes que cualquier filtro específico del canal.
- Si un filtro se aplica globalmente y en el ámbito del canal, el filtro solo se aplica en el nivel del canal. Por ejemplo, si los filtros son `replicate_ignore_db="db1,`channel_22`:db2"`, `replicate_ignore_db` configurado en `db1` se aplica a todos los canales excepto a `channel_22` y solo `channel_22` omite los cambios efectuados desde `db2`.

Ejemplo 1: configuración de un filtro global

En el ejemplo siguiente, la base de datos `temp_data` se excluye de la replicación en todos los canales.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "ParameterName=replicate-ignore-
db,ParameterValue='temp_data',ApplyMethod=immediate"
```

Ejemplo 2: configuración de un filtro en el nivel del canal

En el siguiente ejemplo, los cambios efectuados desde la base de datos `sample22` solo se incluyen en el canal `channel_22`. Del mismo modo, los cambios efectuados desde la base de datos `sample99` solo se incluyen en el canal `channel_99`.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
--db-parameter-group-name myparametergroup \
--parameters "ParameterName=replicate-do-db,ParameterValue='\`channel_22\`:sample22,
\`channel_99\`:sample99',ApplyMethod=immediate"
```

Monitorización de canales de replicación de varios orígenes

Puede monitorizar canales individuales en una réplica de varios orígenes mediante los siguientes métodos:

- Para monitorizar el estado de todos los canales o de un canal específico, conéctese a la réplica de varios orígenes y ejecute el comando `SHOW REPLICA STATUS` o `SHOW REPLICA STATUS FOR CHANNEL 'channel_name'`. Para obtener más información, consulte Checking Replication Status en la documentación de MySQL.
- Para recibir una notificación cuando se inicie, detenga o elimine un canal de replicación, utilice la notificación de eventos de RDS. Para obtener más información, consulte the section called “Uso de notificaciones de eventos de Amazon RDS”.
- Para monitorizar el retardo de un canal específico, compruebe la métrica `ReplicationChannelLag` correspondiente. Los puntos de datos de esta métrica tienen un periodo de 60 segundos (1 minuto) y están disponibles 15 días. Para localizar el retardo del canal de replicación de un canal, utilice el identificador de instancia y el nombre del canal de replicación. Para recibir una notificación cuando este retardo supere un umbral determinado, puede configurar una alarma de CloudWatch. Para obtener más información, consulte the section called “Supervisión de RDS con CloudWatch”.

Consideraciones y prácticas recomendadas para la replicación de varios orígenes

Antes de utilizar la replicación de varios orígenes en RDS para MySQL, revise las siguientes consideraciones y prácticas recomendadas:

- Asegúrese de que una instancia de base de datos configurada como réplica de varios orígenes cuente con recursos suficientes, como rendimiento, memoria, CPU e IOPS, para gestionar la carga de trabajo de varias instancias de origen.
- Monitorice periódicamente el uso de los recursos en su réplica de varios orígenes y ajuste la configuración de la instancia o el almacenamiento para gestionar la carga de trabajo sin agotar los recursos.

- Para configurar la replicación de varios subprocesos en una réplica de varios orígenes, configure la variable del sistema `replica_parallel_workers` en un valor superior a `0`. En este caso, el número de subprocesos asignados a cada canal es el valor de esta variable, más un subproceso coordinador para administrar los subprocesos del aplicador.
- Configure los filtros de replicación de la forma adecuada para evitar conflictos. Para replicar una base de datos completa en otra base de datos en una réplica, puede usar la opción `--replicate-rewrite-db`. Por ejemplo, puede replicar todas las tablas de la base de datos A en la base de datos B en una instancia de réplica. Este enfoque puede resultar útil cuando todas las instancias de origen utilizan la misma convención de nomenclatura de esquemas. Para obtener información sobre la opción `--replicate-rewrite-db`, consulte Replica Server Options and Variables en la documentación de MySQL.
- Para evitar errores de replicación, evite escribir en la réplica. Se recomienda activar el parámetro `read_only` en réplicas de varios orígenes para bloquear las operaciones de escritura. Esto ayuda a eliminar los problemas de replicación causados por operaciones de escritura conflictivas.
- Para aumentar el rendimiento de las operaciones de lectura, como las ordenaciones y las uniones de carga elevada que se ejecutan en la réplica de varios orígenes, considere la posibilidad de utilizar lecturas optimizadas para RDS. Esta característica puede ayudar con las consultas que dependen de tablas temporales o archivos de ordenación de gran tamaño. Para obtener más información, consulte the section called “Mejora del rendimiento de las consultas con lecturas optimizadas de RDS”.
- Para minimizar el retardo en la replicación y mejorar el rendimiento de una réplica de varios orígenes, considere la posibilidad de habilitar escrituras optimizadas. Para obtener más información, consulte the section called “Mejora del rendimiento de escritura con escrituras optimizadas para RDS para MySQL”.
- Realice operaciones de administración (como cambiar la configuración) en un canal a la vez y evite realizar cambios en varios canales desde varias conexiones. Estas prácticas pueden provocar conflictos en las operaciones de replicación. Por ejemplo, la ejecución de los procedimientos `rds_skip_repl_error_for_channel` y `rds_start_replication_for_channel` de forma simultánea desde varias conexiones puede provocar la omisión de eventos en un canal diferente al previsto.
- Puede habilitar las copias de seguridad en una instancia de replicación de varios orígenes y exportar los datos de esa instancia a un bucket de Amazon S3 para almacenarlos a largo plazo. Sin embargo, también es importante configurar las copias de seguridad con la retención adecuada en las instancias de origen individuales. Para obtener más información acerca de la exportación

de datos de instantáneas a Amazon S3, consulte the section called “Exportación de datos de instantáneas de bases de datos a Amazon S3”.

- Para distribuir la carga de trabajo de lectura en una réplica de varios orígenes, puede crear réplicas de lectura a partir de una réplica de varios orígenes. Puede ubicar estas réplicas de lectura en diferentes Regiones de AWS según los requisitos de su aplicación. Para obtener más información acerca de las réplicas de lectura, consulte the section called “Réplicas de lectura de MySQL”.

Limitaciones de la replicación de varios orígenes en RDS para MySQL

Las siguientes limitaciones se aplican a la replicación de varios orígenes en RDS para MySQL:

- Actualmente, RDS para MySQL admite la configuración de un máximo de 15 canales para una réplica de varios orígenes.
- Una instancia de réplica de lectura no se puede configurar como una réplica de varios orígenes.
- Para configurar la replicación de varios orígenes en RDS para MySQL con el motor que ejecuta la versión 5.7, Performance Schema debe estar habilitado en la instancia de réplica. La habilitación de Performance Schema es opcional en la versión 8.0 u 8.4 del motor de ejecución de RDS para MySQL.
- En el caso del motor que ejecuta la versión 5.7 de RDS para MySQL, los filtros de replicación se aplican a todos los canales de replicación. Para el motor que ejecuta la versión 8.0 u 8.4 de RDS para MySQL, puede configurar filtros que se apliquen a todos los canales de replicación o a canales individuales.
- Al restaurar una instantánea de RDS o realizar una restauración a un momento dado (PITR), no se restauran las configuraciones de los canales de réplica de varios orígenes.
- Cuando se crea una réplica de lectura de una réplica de varios orígenes, solo se replican los datos de la instancia de varios orígenes. No se restaura la configuración de ningún canal.
- MySQL no admite la configuración de un número diferente de trabajadores paralelos para cada canal. Cada canal recibe el mismo número de trabajadores paralelos en función del valor de `replica_parallel_workers`.

Si su objetivo de replicación de varios orígenes es un clúster de base de datos multi-AZ, se aplican las siguientes limitaciones adicionales:

- Se debe configurar un canal para una instancia de RDS para MySQL de origen antes de que se produzca cualquier escritura en esa instancia.
- Cada instancia de RDS para MySQL de origen debe tener la replicación basada en GTID habilitada.
- Un evento de conmutación por error en el clúster de base de datos elimina la configuración de replicación de varios orígenes. Para restaurar esa configuración, es necesario repetir los pasos de configuración.

Configuración de clústeres activo-activo para RDS para MySQL

Un clúster activo-activo en Amazon RDS es una configuración de base de datos en la que varios nodos gestionan activamente las operaciones de lectura y escritura, distribuyendo la carga de trabajo entre las instancias para mejorar la disponibilidad y la escalabilidad. Cada nodo del clúster está sincronizado para mantener la coherencia de datos, lo que permite una alta disponibilidad y una conmutación por error más rápida en caso de que se produzca un error en el nodo.

Puede configurar un clúster activo-activo para RDS para MySQL mediante el complemento MySQL Group Replication. El complemento de replicación de grupos es compatible con RDS para MySQL que ejecutan las siguientes versiones:

- Todas las versiones MySQL 8.4
- MySQL 8.0.35 y versiones secundarias posteriores

Para obtener información acerca de MySQL Group Replication, consulte Group Replication en la documentación de MySQL. La documentación de MySQL contiene información detallada sobre esta característica, mientras que en este tema se describe cómo configurar y administrar el complemento en las instancias de base de datos de RDS para MySQL.

> **Note**
>
> En aras de la brevedad, todas las menciones a clúster “activo-activo” que se realicen en este tema se refieren a clústeres activo-activo que utilizan el complemento Group Replication de MySQL.

Casos de uso de clústeres activo-activo

Los siguientes casos son buenos candidatos para usar clústeres activo-activo:

- Aplicaciones que necesitan todas las instancias de base de datos del clúster para admitir operaciones de escritura. El complemento Group Replication mantiene la coherencia de datos en cada instancia de base de datos del clúster activo-activo. Para obtener más información acerca de su funcionamiento, consulte Group Replication en la documentación de MySQL.
- Aplicaciones que requieren una disponibilidad continua de la base de datos. Con un clúster activo-activo, los datos se conservan en todas las instancias de base de datos del clúster. Si se produce

un error en una instancia de base de datos, la aplicación puede redirigir el tráfico a otra instancia de base de datos del clúster.

- Aplicaciones que podrían necesitar dividir las operaciones de lectura y escritura entre distintas instancias de base de datos del clúster para equilibrar la carga. Con un clúster activo-activo, sus aplicaciones pueden enviar tráfico de lectura a instancias de base de datos específicas y tráfico de escritura a otras. También puede cambiar las instancias de base de datos a las que desea enviar lecturas o escrituras en cualquier momento.

Temas

- Limitaciones y aspectos a tener en cuenta de los clústeres activo-activo
- Preparación de un clúster activo-activo entre VPC
- Configuración de parámetros obligatorios para los clústeres activo-activo
- Conversión de una instancia de base de datos existente en un clúster activo-activo
- Configuración de un clúster activo-activo con nuevas instancias de base de datos
- Adición de una instancia de base de datos en un clúster activo-activo
- Monitorización de clústeres activo-activo
- Detención de Group Replication en una instancia de base de datos de un clúster activo-activo
- Cambio de nombre de una instancia de base de datos en un clúster activo-activo
- Eliminación de una instancia de base de datos de un clúster activo-activo

Limitaciones y aspectos a tener en cuenta de los clústeres activo-activo

Los clústeres activo-activo de Amazon RDS ofrecen una mayor disponibilidad y escalabilidad al distribuir las cargas de trabajo entre varias instancias. Sin embargo, hay limitaciones y aspectos importantes que se deben tener en cuenta al utilizar esta arquitectura.

En las siguientes secciones se describen los factores clave, como, por ejemplo, los retrasos en la replicación, la resolución de conflictos, la asignación de recursos y el comportamiento de la conmutación por error. Conocer estos aspectos puede ayudar a garantizar un rendimiento y una fiabilidad óptimos en las implementaciones de clústeres activo-activo.

Temas

- Limitaciones de los clústeres activo-activo de RDS para MySQL

- Aspectos a tener en cuenta y prácticas recomendadas de los clústeres activo-activo de RDS para MySQL

Limitaciones de los clústeres activo-activo de RDS para MySQL

Las siguientes limitaciones se aplican a los clústeres activo-activo de RDS para MySQL:

- El nombre de usuario maestro no puede ser `rdsgrprepladmin` para las instancias de base de datos de un clúster activo-activo. Este nombre de usuario está reservado para las conexiones de Group Replication.
- En el caso de las instancias de base de datos con réplicas de lectura en clústeres activo-activo, un estado de replicación prolongado que no sea `Replicating` puede provocar que los archivos de registro superen los límites de almacenamiento. Para obtener más información acerca del estado de las réplicas de lectura, consulte Monitoreo de la replicación de lectura.
- Las implementaciones azul/verde no son compatibles con instancias de base de datos en un clúster activo-activo. Para obtener más información, consulte Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos.
- La autenticación Kerberos no es compatible con las instancias de base de datos en un clúster activo-activo. Para obtener más información, consulte Uso de la autenticación de Kerberos para Amazon RDS para MySQL.
- Las instancias de base de datos de un clúster de base de datos multi-AZ no se pueden agregar a un clúster activo-activo. Sin embargo, las instancias de base de datos en una implementación de instancias de base de datos multi-AZ se pueden agregar a un clúster activo-activo. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.
- Las tablas que no tienen una clave principal no se replican en un clúster activo-activo porque el complemento Group Replication rechaza las escrituras.
- Las tablas que no son de InnoDB no se replican en un clúster activo-activo.
- Los clústeres activo-activo no admiten instrucciones DML y DDL simultáneas en distintas instancias de base de datos del clúster.
- No puede configurar un clúster activo-activo para que utilice el modo principal único para el modo de replicación del grupo. Para esta configuración, se recomienda utilizar en su lugar un clúster de base de datos multi-AZ. Para obtener más información, consulte Implementaciones de clústeres de base de datos multi-AZ para Amazon RDS.

- Las instancias de base de datos de un clúster activo-activo no admiten la replicación de varios orígenes.
- Un clúster activo-activo entre regiones no puede aplicar la verificación de la autoridad de certificación (CA) en las conexiones de Group Replication.

Aspectos a tener en cuenta y prácticas recomendadas de los clústeres activo-activo de RDS para MySQL

Antes de utilizar clústeres activo-activo de RDS para MySQL, revise las siguientes consideraciones y prácticas recomendadas:

- Los clústeres activo-activo no pueden tener más de nueve instancias de base de datos.
- Con el complemento Group Replication, puede controlar las garantías de coherencia de las transacciones del clúster activo-activo. Para obtener más información, consulte Transaction Consistency Guarantees en la documentación de MySQL.
- Es posible que surjan conflictos cuando distintas instancias de base de datos actualizan la misma fila de un clúster activo-activo. Para obtener información sobre conflictos y resolución de conflictos, consulte Group Replication en la documentación de MySQL.
- Para garantizar la tolerancia a errores, incluya al menos tres instancias de base de datos en el clúster activo-activo. Es posible configurar un clúster activo-activo con solo una o dos instancias de base de datos, pero el clúster no tolerará errores. Para obtener información acerca de la tolerancia a errores, consulte Fault-tolerance en la documentación de MySQL.
- Cuando una instancia de base de datos se une a un clúster activo-activo existente y ejecuta la misma versión del motor que la versión de motor más antigua del clúster, la instancia de base de datos se une en modo de lectura-escritura.
- Cuando una instancia de base de datos se une a un clúster activo-activo existente y ejecuta una versión de motor posterior a la versión de motor más antigua del clúster, la instancia de base de datos debe permanecer en modo de solo lectura.
- Si habilita Group Replication para una instancia de base de datos configurando su parámetro `rds.group_replication_enabled` en `1` en el grupo de parámetros de base de datos, pero la replicación no se ha iniciado, la instancia de base de datos se coloca en modo de solo superlectura para evitar incoherencias en los datos. Para obtener información sobre el modo de solo superlectura, consulte la documentación de MySQL.
- Puede actualizar una instancia de base de datos de un clúster activo-activo, pero la instancia de base de datos será de solo lectura hasta que todas las demás instancias de base de datos

del clúster activo-activo se actualicen a la misma versión del motor o a una versión del motor posterior. Al actualizar una instancia de base de datos, esta se une automáticamente al mismo clúster activo-activo cuando se completa la actualización. Para evitar que una instancia de base de datos cambie involuntariamente al modo de solo lectura, desactive las actualizaciones automáticas de las versiones secundarias en ella. Para obtener información acerca de la actualización de una instancia de base de datos MySQL, consulte Actualizaciones del motor de base de datos de RDS para MySQL.

- Puede añadir una instancia de base de datos en una implementación de instancia de base de datos multi-AZ a un clúster activo-activo existente. También puede convertir una instancia de base de datos single-AZ de un clúster activo-activo en una implementación de instancia de base de datos multi-AZ. Si se produce un error en una instancia de base de datos principal de una implementación multi-AZ, esa instancia principal realiza una conmutación por error a la instancia en espera. La nueva instancia de base de datos principal se une automáticamente al mismo clúster una vez finalizada la conmutación por error. Para obtener más información acerca de las implementaciones de instancias de base de datos multi-AZ, consulte Habilitación de implementaciones de instancias de bases de datos multi-AZ para Amazon RDS.
- Recomendamos que las instancias de base de datos de un clúster activo-activo tengan intervalos de tiempo diferentes para sus períodos de mantenimiento. Esta práctica evita que varias instancias de base de datos del clúster se desconecten al mismo tiempo para realizar tareas de mantenimiento. Para obtener más información, consulte La ventana de mantenimiento de Amazon RDS.
- Los clústeres activo-activo pueden usar SSL para las conexiones entre instancias de base de datos. Para configurar las conexiones SSL, defina los parámetros group_replication_recovery_use_ssl y group_replication_ssl_mode. Los valores de estos parámetros deben ser iguales para todas las instancias de base de datos del clúster activo-activo.

  Actualmente, los clústeres activo-activo no admiten la verificación por parte de la autoridad de certificación (CA) para las conexiones entre Regiones de AWS. Por lo tanto, el parámetro group_replication_ssl_mode debe estar establecido en `DISABLED` (el valor predeterminado) o `REQUIRED` para los clústeres entre regiones.
- Un clúster activo-activo de RDS para MySQL se ejecuta en modo multiprimario. El valor predeterminado de group_replication_enforce_update_everywhere_checks es `ON` y el parámetro es estático. Si este parámetro está establecido en `ON`, las aplicaciones no pueden insertarlo en una tabla que tenga restricciones de clave externa en cascada.

- Un clúster activo-activo de RDS para MySQL utiliza la pila de comunicación de MySQL para garantizar la seguridad de la conexión en lugar de XCOM. Para obtener más información, consulte Communication Stack for Connection Security Management en la documentación de MySQL.
- Cuando un grupo de parámetros de base de datos está asociado a una instancia de base de datos de un clúster activo-activo, recomendamos asociar este grupo de parámetros de base de datos únicamente a otras instancias de base de datos que estén en el clúster.
- Los clústeres activo-activo solo admiten instancias de base de datos de RDS para MySQL. Estas instancias de base de datos deben ejecutar versiones compatibles del motor de base de datos.
- Cuando una instancia de base de datos de un clúster activo-activo sufre un error inesperado, RDS inicia la recuperación de la instancia de base de datos automáticamente. Si la instancia de base de datos no se recupera, le recomendamos que la sustituya por una nueva instancia de base de datos mediante una recuperación a un momento dado con una instancia de base de datos en buen estado del clúster. Para obtener instrucciones, consulte Adición de una instancia de base de datos a un clúster activo-activo mediante la recuperación a un momento dado.
- Puede eliminar una instancia de base de datos de un clúster activo-activo sin que ello afecte a las demás instancias de base de datos del clúster. Para obtener más información sobre la eliminación de instancias de base de datos, consulte Eliminación de una instancia de base de datos.
- Cuando una instancia de base de datos abandona un clúster activo-activo, el parámetro `group_replication_exit_state_action` cambia de forma predeterminada a `OFFLINE_MODE`. En este estado, no se puede acceder a la instancia de base de datos y debe reiniciarla para volver a ponerla en línea y volver a unirse al clúster. Este comportamiento se puede modificar cambiando el parámetro `group_replication_exit_state_action` en un grupo de parámetros personalizado. Al configurar el parámetro en `READ_ONLY`, cuando la instancia de base de datos abandone un clúster de forma involuntaria, adopta un estado de super solo lectura en lugar de quedar sin conexión.

Preparación de un clúster activo-activo entre VPC

Puede configurar un clúster activo-activo con instancias de base de datos de Amazon RDS para MySQL en más de una VPC. Las VPC pueden estar en la misma Región de AWS o en diferentes Regiones de AWS.

> **Note**
>
> El envío de tráfico entre varias Regiones de AWS puede conllevar costos adicionales. Para obtener más información, consulte Overview of Data Transfer Costs for Common Architectures.

Si va a configurar un clúster activo-activo en una sola VPC, puede omitir estos pasos y pasar a Configuración de un clúster activo-activo con nuevas instancias de base de datos.

Preparación para un clúster activo-activo con instancias de base de datos en más de una VPC

1. Asegúrese de que los rangos de direcciones IPv4 de los bloques CIDR cumplan los siguientes requisitos:

   - Los rangos de direcciones IPv4 de los bloques CIDR de las VPC no se pueden superponer.
   - Todos los rangos de direcciones IPv4 de los bloques CIDR deben ser inferiores a `128.0.0.0/subnet_mask` o superiores a 128.0.0.0/`subnet_mask`.

   Los siguientes rangos ilustran estos requisitos:

   - Se admite `10.1.0.0/16` en una VPC y `10.2.0.0/16` en la otra VPC.
   - Se admite `172.1.0.0/16` en una VPC y `172.2.0.0/16` en la otra VPC.
   - No se admite `10.1.0.0/16` en una VPC y `10.1.0.0/16` en la otra VPC porque los rangos se superponen.
   - No se admite `10.1.0.0/16` en una VPC y `172.1.0.0/16` en la otra VPC porque una está por debajo de `128.0.0.0/subnet_mask` y la otra por encima de `128.0.0.0/subnet_mask`.

   Para obtener información acerca de los bloques de CIDR, consulte Bloques de CIDR de VPC en la Guía del usuario de Amazon VPC.
2. En cada VPC, asegúrese de que tanto la resolución de DNS como los nombres de host DNS están habilitados.

   Para obtener instrucciones, consulte Ver y actualizar los atributos de DNS de su VPC en la Guía del usuario de Amazon VPC.

3. Configure las VPC para poder enrutar el tráfico entre ellas de una de las siguientes maneras:

   - Cree una conexión de emparejamiento de VPC entre las VPC.

     Para obtener instrucciones, consulte Create a VPC peering connection en la Guía de emparejamiento de Amazon VPC. En cada VPC, asegúrese de que haya reglas entrantes para los grupos de seguridad que hagan referencia a grupos de seguridad de la VPC emparejada. De este modo, garantizará el tráfico entrante y saliente de las instancias asociadas al grupo de seguridad al que se hace referencia en la VPC del mismo nivel. Para obtener instrucciones, consulte Update your security groups to reference peer security groups en la Guía de interconexión de Amazon VPC.

   - Cree una puerta de enlace de tránsito entre las VPC.

     Para obtener instrucciones, consulte Getting started with transit gateways en Amazon VPC Transit Gateways. En cada VPC, asegúrese de que haya reglas de entrada para sus grupos de seguridad que permitan el tráfico desde la otra VPC, como reglas de entrada que especifiquen el CIDR de la otra VPC. De este modo, garantizará el tráfico entrante y saliente de las instancias asociadas al grupo de seguridad al que se hace referencia en el clúster activo-activo. Para obtener más información, consulte Controlar el tráfico hacia los recursos de AWS mediante grupos de seguridad en la Guía del usuario de Amazon VPC.

Configuración de parámetros obligatorios para los clústeres activo-activo

La configuración de los parámetros de los clústeres activo-activo en Amazon RDS para MySQL es fundamental para mantener un rendimiento y una estabilidad operativa uniformes. En esta tabla, se indican los parámetros clave que controlan la replicación, la resolución de conflictos y la distribución de la carga de trabajo. La configuración correcta garantiza una sincronización eficaz entre los nodos, minimiza el retardo en la replicación y optimiza la utilización de los recursos en entornos distribuidos o de alto tráfico.

Parámetro	Descripción	Configuración necesaria
`binlog_format`	Permite configurar el formato de registro binario. El valor predeterminado de las versiones RDS para MySQL 8.0 y anteriores es `MIXED`.	`ROW`

Parámetro	Descripción	Configuración necesaria
	El valor predeterminado de RDS para MySQL 8.4 es `ROW`. Para obtener más información, consulte la documentación de MySQL.	
`enforce_gtid_consistency`	Aplica la coherencia de GTID en la ejecución de las instrucciones. El valor predeterminado de RDS para MySQL es `OFF`. Para obtener más información, consulte la documentación de MySQL.	`ON`
`group_replication_group_name`	Permite establecer el nombre de Group Replication en un UUID. El formato de UUID es `11111111-2222-3333-4444-555555555555`. Para generar un UUID de MySQL, conéctese a una instancia de base de datos MySQL y ejecute `SELECT UUID()`. El valor debe ser el mismo para todas las instancias de base de datos del clúster activo-activo. Para obtener más información, consulte la documentación de MySQL.	Un UUID de MySQL

Parámetro	Descripción	Configuración necesaria
`gtid-mode`	Controla el registro basado en GTID. El valor predeterminado de RDS para MySQL es `OFF_PERMISSIVE` . Para obtener más información, consulte la documentación de MySQL.	`ON`
`rds.custom_dns_resolution`	Especifica si se permite la resolución de DNS desde el servidor DNS de Amazon en la VPC. La resolución de DNS debe estar habilitada cuando Group Replication está habilitado con el parámetro `rds.group_replication_enabled` . La resolución de DNS no puede estar habilitada cuando Group Replication está deshabilitado con el parámetro `rds.group_replication_enabled` . Para obtener más información, consulte Servidor DNS de Amazon en la Guía del usuario de Amazon VPC.	1
`rds.group_replication_enabled`	Especifica si Group Replication está habilitado para una instancia de base de datos. Group Replication debe estar habilitado en una instancia de base de datos de un clúster activo-activo.	1

Parámetro	Descripción	Configuración necesaria
`replica_preserve_commit_order` (RDS para MySQL 8.4 y versiones posteriores) o `slave_preserve_commit_order` (RDS para MySQL versiones 8.0)	Controla el orden en que se confirman las transacciones en una réplica. El valor predeterminado de RDS para MySQL es `ON`. Para obtener más información, consulte la documentación de MySQL.	`ON`

Conversión de una instancia de base de datos existente en un clúster activo-activo

La versión del motor de base de datos de la instancia de base de datos que desea migrar a un clúster activo-activo debe ser una de las versiones siguientes:

- Todas las versiones MySQL 8.4
- MySQL 8.0.35 y versiones secundarias posteriores

Si necesita actualizar la versión del motor, consulte Actualizaciones del motor de base de datos de RDS para MySQL.

Si va a configurar un clúster activo-activo con instancias de base de datos en más de una VPC, asegúrese de completar los requisitos previos que se indican en Preparación de un clúster activo-activo entre VPC.

Realice los siguientes pasos para migrar una instancia de base de datos existente a un clúster activo-activo para RDS para MySQL.

Temas

- Paso 1: defina los parámetros del clúster activo-activo en uno o más grupos de parámetros personalizados
- Paso 2: asocie la instancia de base de datos a un grupo de parámetros de base de datos que tenga configurados los parámetros de Group Replication necesarios
- Paso 3: cree el clúster activo-activo

- Paso 4: cree instancias de base de datos de RDS para MySQL adicionales para el clúster activo-activo
- Paso 5: inicialice el grupo en la instancia de base de datos que va a convertir
- Paso 6: inicie la replicación en las demás instancias de base de datos del clúster activo-activo
- Paso 7: (recomendado) compruebe el estado del clúster activo-activo

Paso 1: defina los parámetros del clúster activo-activo en uno o más grupos de parámetros personalizados

Las instancias de base de datos de RDS para MySQL de un clúster activo-activo deben estar asociadas a un grupo de parámetros personalizado que tenga la configuración correcta para los parámetros necesarios. Para obtener más información sobre los parámetros y la configuración necesaria para cada uno, consulte Configuración de parámetros obligatorios para los clústeres activo-activo.

Puede configurar estos parámetros en grupos de parámetros nuevos o en grupos de parámetros existentes. Sin embargo, para evitar que afecte accidentalmente a las instancias de base de datos que no forman parte del clúster activo-activo, le recomendamos encarecidamente que cree un nuevo grupo de parámetros personalizado. Las instancias de base de datos de un clúster activo-activo se pueden asociar al mismo grupo de parámetros de base de datos o a diferentes grupos de parámetros de base de datos.

Puede utilizar la AWS Management Console o la AWS CLI para crear un nuevo grupo de parámetros personalizado. Para obtener más información, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS. En el siguiente ejemplo, se ejecuta el comando create-db-parameter-group de la AWS CLI para crear un grupo de parámetros de base de datos personalizado denominado *myactivepg* para RDS para MySQL 8.0:

Para Linux, macOS o Unix:

```
aws rds create-db-parameter-group \
  --db-parameter-group-name myactivepg \
  --db-parameter-group-family mysql8.0 \
  --description "Parameter group for active-active clusters"
```

Para Windows:

```
aws rds create-db-parameter-group ^
```

```
  --db-parameter-group-name myactivepg ^
  --db-parameter-group-family mysql8.0 ^
  --description "Parameter group for active-active clusters"
```

También puede utilizar la AWS Management Console o la AWS CLI para establecer los parámetros del grupo de parámetros personalizado. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

En el siguiente ejemplo, se ejecuta el comando de la modify-db-parameter-group de la AWS CLI para establecer los parámetros de RDS para MySQL 8.0: Para usar este ejemplo con RDS para MySQL 8.4, cambie `slave_preserve_commit_order` a `replica_preserve_commit_order`.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myactivepg \
  --parameters
 "ParameterName='rds.group_replication_enabled',ParameterValue='1',ApplyMethod=pending-
reboot" \

 "ParameterName='rds.custom_dns_resolution',ParameterValue='1',ApplyMethod=pending-
reboot" \

 "ParameterName='enforce_gtid_consistency',ParameterValue='ON',ApplyMethod=pending-
reboot" \
               "ParameterName='gtid-mode',ParameterValue='ON',ApplyMethod=pending-
reboot" \

 "ParameterName='binlog_format',ParameterValue='ROW',ApplyMethod=immediate" \

 "ParameterName='slave_preserve_commit_order',ParameterValue='ON',ApplyMethod=immediate"
 \

 "ParameterName='group_replication_group_name',ParameterValue='11111111-2222-3333-4444-55555555
reboot"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myactivepg ^
```

```
  --parameters
 "ParameterName='rds.group_replication_enabled',ParameterValue='1',ApplyMethod=pending-
reboot" ^

 "ParameterName='rds.custom_dns_resolution',ParameterValue='1',ApplyMethod=pending-
reboot" ^

 "ParameterName='enforce_gtid_consistency',ParameterValue='ON',ApplyMethod=pending-
reboot" ^
               "ParameterName='gtid-mode',ParameterValue='ON',ApplyMethod=pending-
reboot" ^

 "ParameterName='binlog_format',ParameterValue='ROW',ApplyMethod=immediate" ^

 "ParameterName='slave_preserve_commit_order',ParameterValue='ON',ApplyMethod=immediate"
 ^

 "ParameterName='group_replication_group_name',ParameterValue='11111111-2222-3333-4444-55555555
reboot"
```

Paso 2: asocie la instancia de base de datos a un grupo de parámetros de base de datos que tenga configurados los parámetros de Group Replication necesarios

Asocie la instancia de base de datos a un grupo de parámetros que haya creado o modificado en el paso anterior. Para obtener instrucciones, consulte Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS.

Reinicie la instancia de base de datos para que se aplique la nueva configuración de los parámetros. Para obtener instrucciones, consulte Reinicio de una instancia de base de datos.

Paso 3: cree el clúster activo-activo

En el grupo de parámetros de base de datos asociado a la instancia de base de datos, defina el parámetro `group_replication_group_seeds` en el punto de conexión de la instancia de base de datos que va a convertir.

Puede usar la AWS Management Console o la AWS CLI para establecer el parámetro. No es necesario reiniciar la instancia de base de datos después de configurar este parámetro. Para obtener más información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

En el siguiente ejemplo, se ejecuta el comando de la AWS CLI modify-db-parameter-group para establecer los parámetros:

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myactivepg \
  --parameters
 "ParameterName='group_replication_group_seeds',ParameterValue='myactivedb1.123456789012.us-east-1.rds.amazonaws.com:3306',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myactivepg ^
  --parameters
 "ParameterName='group_replication_group_seeds',ParameterValue='myactivedb1.123456789012.us-east-1.rds.amazonaws.com:3306',ApplyMethod=immediate"
```

Paso 4: cree instancias de base de datos de RDS para MySQL adicionales para el clúster activo-activo

Para crear instancias de base de datos adicionales para el clúster activo-activo, realice una recuperación en un momento dado de la instancia de base de datos que va a convertir. Para obtener instrucciones, consulte Adición de una instancia de base de datos a un clúster activo-activo mediante la recuperación a un momento dado.

Los clústeres activo-activo pueden tener hasta nueve instancias de base de datos. Realice una recuperación a un momento dado de la instancia de base de datos hasta que tenga el número de instancias de base de datos que desea para el clúster. Cuando realice una recuperación en un momento dado, asegúrese de asociar la instancia de base de datos que va a añadir a un grupo de parámetros de base de datos que tenga `rds.group_replication_enabled` establecido en 1. De lo contrario, Group Replication no se iniciará en la instancia de base de datos recién agregada.

Paso 5: inicialice el grupo en la instancia de base de datos que va a convertir

Inicialice el grupo e inicie la replicación:

1. Conéctese a la instancia de base de datos que va a convertir en un cliente SQL. Para obtener más información sobre la conexión a una instancia de base de datos de RDS para MySQL, consulte Conexión a la instancia de base de datos de MySQL.

2. En el cliente de SQL, ejecute los siguientes procedimientos almacenados y sustituya *group_replication_user_password* por la contraseña del usuario `rdsgrprepladmin`. El usuario `rdsgrprepladmin` está reservado para las conexiones de Group Replication de un clúster activo-activo. La contraseña de este usuario debe ser la misma en todas las instancias de base de datos de un clúster activo-activo.

```
call mysql.rds_set_configuration('binlog retention hours', 168); -- 7 days binlog
call mysql.rds_group_replication_create_user('group_replication_user_password');
call
 mysql.rds_group_replication_set_recovery_channel('group_replication_user_password');
call mysql.rds_group_replication_start(1);
```

   En este ejemplo, se establece el valor de `binlog retention hours` en 168, lo que significa que los archivos de registro binarios se conservan durante siete días en la instancia de base de datos. Puede ajustar este valor de acuerdo con sus requisitos.

   En este ejemplo, se especifica 1 en el procedimiento almacenado `mysql.rds_group_replication_start` para que se inicialice un grupo nuevo con la instancia de base de datos actual.

   Para obtener más información acerca de los procedimientos almacenados a los que se hace referencia en el ejemplo, consulte Administración de clústeres activo-activo.

Paso 6: inicie la replicación en las demás instancias de base de datos del clúster activo-activo

Para cada una de las instancias de base de datos del clúster activo-activo, utilice un cliente de SQL para conectarse a la instancia y ejecute los siguientes procedimientos almacenados. Sustituya *group_replication_user_password* por la contraseña del usuario `rdsgrprepladmin`.

```
call mysql.rds_set_configuration('binlog retention hours', 168); -- 7 days binlog
call mysql.rds_group_replication_create_user('group_replication_user_password');
call
 mysql.rds_group_replication_set_recovery_channel('group_replication_user_password');
call mysql.rds_group_replication_start(0);
```

En este ejemplo, se establece el valor de `binlog retention hours` en 168, lo que significa que los archivos de registro binarios se conservan durante siete días en cada instancia de base de datos. Puede ajustar este valor de acuerdo con sus requisitos.

En este ejemplo, se especifica `0` en el procedimiento almacenado `mysql.rds_group_replication_start` para que se una la instancia de base de datos actual a un grupo existente.

> **Tip**
>
> Asegúrese de ejecutar estos procedimientos almacenados en todas las demás instancias de base de datos del clúster activo-activo.

Paso 7: (recomendado) compruebe el estado del clúster activo-activo

Para asegurarse de que cada miembro del clúster esté configurado correctamente, compruebe el estado del clúster conectándose a una instancia de base de datos del clúster activo-activo y ejecutando el siguiente comando SQL:

```
SELECT * FROM performance_schema.replication_group_members;
```

En el resultado se debería mostrar `ONLINE` para el `MEMBER_STATE` de cada instancia de base de datos, como en el siguiente ejemplo de salida:

```
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+----------------
+----------------------------+
| CHANNEL_NAME              | MEMBER_ID                            | MEMBER_HOST    |
 MEMBER_PORT | MEMBER_STATE | MEMBER_ROLE | MEMBER_VERSION | MEMBER_COMMUNICATION_STACK
 |
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+----------------
+----------------------------+
| group_replication_applier | 9854d4a2-5d7f-11ee-b8ec-0ec88c43c251 | ip-10-15-3-137 |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
| group_replication_applier | 9e2e9c28-5d7f-11ee-8039-0e5d58f05fef | ip-10-15-3-225 |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
| group_replication_applier | a6ba332d-5d7f-11ee-a025-0a5c6971197d | ip-10-15-1-83  |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+----------------
+----------------------------+
3 rows in set (0.00 sec)
```

Para obtener información acerca de los valores posibles de `MEMBER_STATE`, consulte Group Replication Server States en la documentación de MySQL.

Configuración de un clúster activo-activo con nuevas instancias de base de datos

Realice los siguientes pasos para configurar un clúster activo-activo mediante las nuevas instancias de base de datos de Amazon RDS para MySQL.

Si va a configurar un clúster activo-activo con instancias de base de datos en más de una VPC, asegúrese de completar los requisitos previos que se indican en Preparación de un clúster activo-activo entre VPC.

Temas

- Paso 1: defina los parámetros del clúster activo-activo en uno o más grupos de parámetros personalizados
- Paso 2: cree nuevas instancias de base de datos de RDS para MySQL para el clúster activo-activo
- Paso 3: especifique las instancias de base de datos del clúster activo-activo
- Paso 4: inicialice el grupo en una instancia de base de datos e inicie la replicación
- Paso 5: inicie la replicación en las demás instancias de base de datos del clúster activo-activo
- Paso 6: (recomendado) compruebe el estado del clúster activo-activo
- Paso 7: (opcional) importe los datos a una instancia de base de datos del clúster activo-activo

Paso 1: defina los parámetros del clúster activo-activo en uno o más grupos de parámetros personalizados

Las instancias de base de datos de RDS para MySQL de un clúster activo-activo deben estar asociadas a un grupo de parámetros personalizado que tenga la configuración correcta para los parámetros necesarios. Para obtener más información sobre los parámetros y la configuración necesaria para cada uno, consulte Configuración de parámetros obligatorios para los clústeres activo-activo.

Puede configurar estos parámetros en grupos de parámetros nuevos o en grupos de parámetros existentes. Sin embargo, para evitar que afecte accidentalmente a las instancias de base de datos que no forman parte del clúster activo-activo, le recomendamos encarecidamente que cree un nuevo grupo de parámetros personalizado. Las instancias de base de datos de un clúster activo-

activo se pueden asociar al mismo grupo de parámetros de base de datos o a diferentes grupos de parámetros de base de datos.

Puede utilizar la AWS Management Console o la AWS CLI para crear un nuevo grupo de parámetros personalizado. Para obtener más información, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS. En el siguiente ejemplo, se ejecuta el comando create-db-parameter-group de la AWS CLI para crear un grupo de parámetros de base de datos personalizado denominado *myactivepg* para RDS para MySQL 8.0:

Para Linux, macOS o Unix:

```
aws rds create-db-parameter-group \
  --db-parameter-group-name myactivepg \
  --db-parameter-group-family mysql8.0 \
  --description "Parameter group for active-active clusters"
```

Para Windows:

```
aws rds create-db-parameter-group ^
  --db-parameter-group-name myactivepg ^
  --db-parameter-group-family mysql8.0 ^
  --description "Parameter group for active-active clusters"
```

También puede utilizar la AWS Management Console o la AWS CLI para establecer los parámetros del grupo de parámetros personalizado. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

En el siguiente ejemplo, se ejecuta el comando de la modify-db-parameter-group de la AWS CLI para establecer los parámetros de RDS para MySQL 8.0: Para usar este ejemplo con RDS para MySQL 8.4, cambie `slave_preserve_commit_order` a `replica_preserve_commit_order`.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myactivepg \
  --parameters
 "ParameterName='rds.group_replication_enabled',ParameterValue='1',ApplyMethod=pending-
reboot" \

 "ParameterName='rds.custom_dns_resolution',ParameterValue='1',ApplyMethod=pending-
reboot" \
```

```
 "ParameterName='enforce_gtid_consistency',ParameterValue='ON',ApplyMethod=pending-
reboot" \
               "ParameterName='gtid-mode',ParameterValue='ON',ApplyMethod=pending-
reboot" \

 "ParameterName='binlog_format',ParameterValue='ROW',ApplyMethod=immediate" \

 "ParameterName='slave_preserve_commit_order',ParameterValue='ON',ApplyMethod=immediate"
 \

 "ParameterName='group_replication_group_name',ParameterValue='11111111-2222-3333-4444-55555555
reboot"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myactivepg ^
  --parameters
 "ParameterName='rds.group_replication_enabled',ParameterValue='1',ApplyMethod=pending-
reboot" ^

 "ParameterName='rds.custom_dns_resolution',ParameterValue='1',ApplyMethod=pending-
reboot" ^

 "ParameterName='enforce_gtid_consistency',ParameterValue='ON',ApplyMethod=pending-
reboot" ^
               "ParameterName='gtid-mode',ParameterValue='ON',ApplyMethod=pending-
reboot" ^

 "ParameterName='binlog_format',ParameterValue='ROW',ApplyMethod=immediate" ^

 "ParameterName='slave_preserve_commit_order',ParameterValue='ON',ApplyMethod=immediate"
 ^

 "ParameterName='group_replication_group_name',ParameterValue='11111111-2222-3333-4444-55555555
reboot"
```

Paso 2: cree nuevas instancias de base de datos de RDS para MySQL para el clúster activo-activo

Los clústeres activo-activo son compatibles con las versiones siguientes de las instancias de base de datos de RDS para MySQL:

- Todas las versiones de MySQL 8.4
- Aurora MySQL versión 8.0.35 y versiones secundarias posteriores

Puede crear hasta nueve instancias de base de datos nuevas para el clúster.

Puede utilizar la AWS Management Console o la AWS CLI para crear las nuevas instancias de base de datos. Para obtener más información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS. Al crear la instancia de base de datos, asóciela a un grupo de parámetros de base de datos que haya creado o modificado en el paso anterior.

Paso 3: especifique las instancias de base de datos del clúster activo-activo

En el grupo de parámetros de base de datos asociado a cada instancia de base de datos, defina el parámetro `group_replication_group_seeds` en los puntos de conexión de las instancias de base de datos que desee incluir en el clúster.

Puede usar la AWS Management Console o la AWS CLI para establecer el parámetro. No es necesario reiniciar la instancia de base de datos después de configurar este parámetro. Para obtener más información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

En el siguiente ejemplo, se ejecuta el comando de la AWS CLI modify-db-parameter-group para establecer los parámetros:

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
  --db-parameter-group-name myactivepg \
  --parameters
 "ParameterName='group_replication_group_seeds',ParameterValue='myactivedb1.123456789012.us-
east-1.rds.amazonaws.com:3306,myactivedb2.123456789012.us-
east-1.rds.amazonaws.com:3306,myactivedb3.123456789012.us-
east-1.rds.amazonaws.com:3306',ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
  --db-parameter-group-name myactivepg ^
  --parameters
 "ParameterName='group_replication_group_seeds',ParameterValue='myactivedb1.123456789012.us-
east-1.rds.amazonaws.com:3306,myactivedb2.123456789012.us-
east-1.rds.amazonaws.com:3306,myactivedb3.123456789012.us-
east-1.rds.amazonaws.com:3306',ApplyMethod=immediate"
```

> **Tip**
>
> Asegúrese de configurar el parámetro `group_replication_group_seeds` en cada grupo de parámetros de base de datos que esté asociado a una instancia de base de datos del clúster activo-activo.

Paso 4: inicialice el grupo en una instancia de base de datos e inicie la replicación

Puede elegir cualquier base de datos nueva para inicializar el grupo e iniciar la replicación. Para ello, complete los siguientes pasos.

1. Elija una instancia de base de datos en el clúster activo-activo y conéctese a esa instancia de base de datos en un cliente de SQL. Para obtener más información sobre la conexión a una instancia de base de datos de RDS para MySQL, consulte Conexión a la instancia de base de datos de MySQL.
2. En el cliente de SQL, ejecute los siguientes procedimientos almacenados y sustituya *group_replication_user_password* por la contraseña del usuario `rdsgrprepladmin`. El usuario `rdsgrprepladmin` está reservado para las conexiones de Group Replication de un clúster activo-activo. La contraseña de este usuario debe ser la misma en todas las instancias de base de datos de un clúster activo-activo.

   ```
   call mysql.rds_set_configuration('binlog retention hours', 168); -- 7 days binlog
   call mysql.rds_group_replication_create_user('group_replication_user_password');
   call
    mysql.rds_group_replication_set_recovery_channel('group_replication_user_password');
   call mysql.rds_group_replication_start(1);
   ```

En este ejemplo, se establece el valor de `binlog retention hours` en 168, lo que significa que los archivos de registro binarios se conservan durante siete días en la instancia de base de datos. Puede ajustar este valor de acuerdo con sus requisitos.

En este ejemplo, se especifica 1 en el procedimiento almacenado `mysql.rds_group_replication_start` para que se inicialice un grupo nuevo con la instancia de base de datos actual.

Para obtener más información acerca de los procedimientos almacenados a los que se hace referencia en el ejemplo, consulte Administración de clústeres activo-activo.

Paso 5: inicie la replicación en las demás instancias de base de datos del clúster activo-activo

Para cada una de las instancias de base de datos del clúster activo-activo, utilice un cliente de SQL para conectarse a la instancia y ejecute los siguientes procedimientos almacenados. Sustituya *`group_replication_user_password`* por la contraseña del usuario `rdsgrprepladmin`.

```
call mysql.rds_set_configuration('binlog retention hours', 168); -- 7 days binlog
call mysql.rds_group_replication_create_user('group_replication_user_password');
call
 mysql.rds_group_replication_set_recovery_channel('group_replication_user_password');
call mysql.rds_group_replication_start(0);
```

En este ejemplo, se establece el valor de `binlog retention hours` en 168, lo que significa que los archivos de registro binarios se conservan durante siete días en cada instancia de base de datos. Puede ajustar este valor de acuerdo con sus requisitos.

En este ejemplo, se especifica `0` en el procedimiento almacenado `mysql.rds_group_replication_start` para que se una la instancia de base de datos actual a un grupo existente.

> **Tip**
>
> Asegúrese de ejecutar estos procedimientos almacenados en todas las demás instancias de base de datos del clúster activo-activo.

Paso 6: (recomendado) compruebe el estado del clúster activo-activo

Para asegurarse de que cada miembro del clúster esté configurado correctamente, compruebe el estado del clúster conectándose a una instancia de base de datos del clúster activo-activo y ejecutando el siguiente comando SQL:

```
SELECT * FROM performance_schema.replication_group_members;
```

En el resultado se debería mostrar `ONLINE` para el `MEMBER_STATE` de cada instancia de base de datos, como en el siguiente ejemplo de salida:

```
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+---------------
+----------------------------+
| CHANNEL_NAME              | MEMBER_ID                            | MEMBER_HOST    |
 MEMBER_PORT | MEMBER_STATE | MEMBER_ROLE | MEMBER_VERSION | MEMBER_COMMUNICATION_STACK
 |
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+---------------
+----------------------------+
| group_replication_applier | 9854d4a2-5d7f-11ee-b8ec-0ec88c43c251 | ip-10-15-3-137 |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
| group_replication_applier | 9e2e9c28-5d7f-11ee-8039-0e5d58f05fef | ip-10-15-3-225 |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
| group_replication_applier | a6ba332d-5d7f-11ee-a025-0a5c6971197d | ip-10-15-1-83  |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+---------------
+----------------------------+
3 rows in set (0.00 sec)
```

Para obtener información acerca de los valores posibles de `MEMBER_STATE`, consulte Group Replication Server States en la documentación de MySQL.

Paso 7: (opcional) importe los datos a una instancia de base de datos del clúster activo-activo

Puede importar datos desde una base de datos MySQL a una instancia de base de datos del clúster activo-activo. Una vez importados los datos, Group Replication los replica en las demás instancias de base de datos del clúster.

Para obtener información acerca de cómo importar los datos, consulte Importación de datos a una base de datos de Amazon RDS para MySQL con un tiempo de inactividad reducido.

Adición de una instancia de base de datos en un clúster activo-activo

Para añadir una instancia de base de datos a un clúster activo-activo de Amazon RDS para MySQL, restaure una instantánea de base de datos o una instancia de base de datos a un momento determinado. Un clúster activo-activo puede incluir hasta nueve instancias de base de datos.

Cuando recupera una instancia de base de datos a un momento dado, normalmente incluye transacciones más recientes que las de una instancia de base de datos que se haya restaurado a partir de una instantánea de base de datos. Cuando la instancia de base de datos tiene transacciones más recientes, es necesario aplicar menos transacciones al iniciar la replicación. Por lo tanto, suele ser más rápido utilizar la recuperación a un momento dado para agregar una instancia de base de datos a un clúster que realizar la restauración a partir de una instantánea de base de datos.

Temas

- Adición de una instancia de base de datos a un clúster activo-activo mediante la recuperación a un momento dado
- Adición de una instancia de base de datos en un clúster activo-activo mediante una instantánea de base de datos

Adición de una instancia de base de datos a un clúster activo-activo mediante la recuperación a un momento dado

Para agregar una instancia de base de datos a un clúster activo-activo, realice una recuperación a un momento dado en una instancia de base de datos del clúster.

Para obtener información sobre la recuperación de una instancia de base de datos a un momento dado en una Región de AWS diferente, consulte Replicación de las copias de seguridad automatizadas en otra Región de AWS.

Adición de una instancia de base de datos a un clúster activo-activo mediante la recuperación a un momento dado

1. Cree una nueva instancia de base de datos realizando una recuperación a momento dado en una instancia de base de datos del clúster activo-activo.

Puede realizar una recuperación a un momento dado en cualquier instancia de base de datos del clúster para crear la nueva instancia de base de datos. Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

> **Important**
>
> Durante la recuperación a un momento dado, asocie la nueva instancia de base de datos a un grupo de parámetros de base de datos que tenga establecidos los parámetros del clúster activo-activo. De lo contrario, Group Replication no se iniciará en la nueva instancia de base de datos. Para obtener más información sobre los parámetros y la configuración necesaria para cada uno, consulte Configuración de parámetros obligatorios para los clústeres activo-activo.

> **Tip**
>
> Si realiza una instantánea de la instancia de base de datos antes de iniciar la recuperación a un momento dado, es posible que pueda reducir el tiempo necesario para aplicar las transacciones en la nueva instancia de base de datos.

2. Agregue la instancia de base de datos al parámetro `group_replication_group_seeds` de cada grupo de parámetros de base de datos asociado a una instancia de base de datos en el clúster activo-activo, incluido el grupo de parámetros de base de datos que asoció a la nueva instancia de base de datos.

   Para obtener más información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

3. En un cliente SQL, conéctese a la nueva instancia de base de datos y llame al procedimiento almacenado mysql.rds_group_replication_set_recovery_channel. Sustituya *`group_replication_user_password`* por la contraseña del usuario `rdsgrprepladmin`.

```
call
 mysql.rds_group_replication_set_recovery_channel('group_replication_user_password');
```

4. Con el cliente SQL, llame al procedimiento almacenado mysql.rds_group_replication_start para iniciar la replicación:

```
call mysql.rds_group_replication_start(0);
```

Adición de una instancia de base de datos en un clúster activo-activo mediante una instantánea de base de datos

Para agregar una instancia de base de datos a un clúster activo-activo, cree una instantánea de base de datos de una instancia de base de datos del clúster y, a continuación, restaure la instantánea de base de datos.

Para obtener más información acerca de cómo copiar una instantánea en una Región de AWS diferente, consulte the section called “Copias entre regiones”.

Adición de una instancia de base de datos en un clúster activo-activo mediante una instantánea de base de datos

1. Cree una instantánea de base de datos de una instancia de base de datos en el clúster activo-activo.

   Puede crear una instantánea de base de datos de una instancia de base de datos en el clúster. Para obtener instrucciones, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
2. Restaure una instancia de base de datos a partir de una instantánea de base de datos.

   Durante la operación de restauración de la instantánea, asocie la nueva instancia de base de datos a un grupo de parámetros de base de datos que tenga establecidos los parámetros del clúster activo-activo. Para obtener más información sobre los parámetros y la configuración necesaria para cada uno, consulte Configuración de parámetros obligatorios para los clústeres activo-activo.

   Para obtener información acerca de cómo restaurar una instancia de base de datos a partir una instantánea de base de datos, consulte Restauración a una instancia de base de datos.
3. Agregue la instancia de base de datos al parámetro `group_replication_group_seeds` de cada grupo de parámetros de base de datos asociado a una instancia de base de datos en el clúster activo-activo, incluido el grupo de parámetros de base de datos que asoció a la nueva instancia de base de datos.

Para obtener más información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

4. En un cliente SQL, conéctese a la nueva instancia de base de datos y llame al procedimiento almacenado mysql.rds_group_replication_set_recovery_channel. Sustituya *group_replication_user_password* por la contraseña del usuario `rdsgrprepladmin`.

```
call
 mysql.rds_group_replication_set_recovery_channel('group_replication_user_password');
```

5. Con el cliente SQL, llame al procedimiento almacenado mysql.rds_group_replication_start para iniciar la replicación:

```
call mysql.rds_group_replication_start(0);
```

Monitorización de clústeres activo-activo

La supervisión de los clústeres activo-activo en Amazon RDS para MySQL es fundamental para realizar un seguimiento del rendimiento, la integridad de la replicación y la sincronización de los nodos. Puede monitorizar el clúster activo-activo conectándose a una instancia de base de datos del clúster y ejecutando el siguiente comando SQL:

```
SELECT * FROM performance_schema.replication_group_members;
```

En el resultado se debería mostrar `ONLINE` para el `MEMBER_STATE` de cada instancia de base de datos, como en el siguiente ejemplo de salida:

```
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+----------------
+----------------------------+
| CHANNEL_NAME              | MEMBER_ID                            | MEMBER_HOST    |
 MEMBER_PORT | MEMBER_STATE | MEMBER_ROLE | MEMBER_VERSION | MEMBER_COMMUNICATION_STACK
 |
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+----------------
+----------------------------+
| group_replication_applier | 9854d4a2-5d7f-11ee-b8ec-0ec88c43c251 | ip-10-15-3-137 |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                      |
```

```
| group_replication_applier | 9e2e9c28-5d7f-11ee-8039-0e5d58f05fef | ip-10-15-3-225 |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
| group_replication_applier | a6ba332d-5d7f-11ee-a025-0a5c6971197d | ip-10-15-1-83  |
      3306 | ONLINE       | PRIMARY     | 8.0.35         | MySQL                       |
+---------------------------+--------------------------------------
+---------------+-------------+--------------+-------------+---------------
+----------------------------+
3 rows in set (0.00 sec)
```

Para obtener información acerca de los valores posibles de `MEMBER_STATE`, consulte Group Replication Server States en la documentación de MySQL.

Detención de Group Replication en una instancia de base de datos de un clúster activo-activo

Puede detener Group Replication en una instancia de base de datos de un clúster activo-activo. Al detener Group Replication, la instancia de base de datos pasa al modo de solo superlectura hasta que se reinicie la replicación o se elimine la instancia de base de datos del clúster activo-activo. Para obtener información sobre el modo de solo superlectura, consulte la documentación de MySQL.

Detención temporal de Group Replication para un clúster activo-activo

1. Conéctese a una instancia de base de datos en el clúster activo-activo utilizando un cliente SQL.

   Para obtener más información sobre la conexión a una instancia de base de datos de RDS para MySQL, consulte Conexión a la instancia de base de datos de MySQL.
2. En el cliente SQL, llame al procedimiento almacenado mysql.rds_group_replication_stop:

   ```
   call mysql.rds_group_replication_stop();
   ```

Cambio de nombre de una instancia de base de datos en un clúster activo-activo

Puede cambiar el nombre de una instancia de base de datos en un clúster activo-activo. Para cambiar el nombre de más de una instancia de base de datos en un clúster activo-activo, debe hacerlo de una en una. Por lo tanto, cambie el nombre de una instancia de base de datos y vuelva a unirla al clúster antes de cambiar el nombre de la siguiente.

Cambio de nombre de una instancia de base de datos en un clúster activo-activo

1. Conéctese a la instancia de base de datos en un cliente SQL y llame al procedimiento almacenado mysql.rds_group_replication_stop.

   ```
   call mysql.rds_group_replication_stop();
   ```

2. Para cambiar el nombre de la instancia de base de datos, siga las instrucciones que se indican en Cambio del nombre de una instancia de base de datos.
3. Modifique el parámetro `group_replication_group_seeds` en cada grupo de parámetros de base de datos asociado a una instancia de base de datos del clúster activo-activo.

   En la configuración de los parámetros, sustituya el punto de conexión de la instancia de base de datos anterior por el nuevo punto de conexión de la instancia de base de datos. Para obtener más información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.
4. Conéctese a la instancia de base de datos en un cliente SQL y llame al procedimiento almacenado mysql.rds_group_replication_start.

   ```
   call mysql.rds_group_replication_start(0);
   ```

Eliminación de una instancia de base de datos de un clúster activo-activo

Al eliminar una instancia de base de datos de un clúster activo-activo, esta se convierte en una instancia de base de datos independiente.

Eliminación de una instancia de base de datos de un clúster activo-activo

1. Conéctese a la instancia de base de datos en un cliente SQL y llame al procedimiento almacenado mysql.rds_group_replication_stop.

   ```
   call mysql.rds_group_replication_stop();
   ```

2. Modifique el parámetro `group_replication_group_seeds` de las instancias de base de datos que permanecerán en el clúster activo-activo.

   En el parámetro `group_replication_group_seeds`, elimine la instancia de base de datos que va a eliminar del clúster activo-activo. Para obtener más información acerca de cómo

configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

3. Modifique los parámetros de la instancia de base de datos que va a eliminar del clúster activo-activo para que deje de formar parte del clúster.

   Puede asociar la instancia de base de datos a un grupo de parámetros diferente o modificar los parámetros del grupo de parámetros de base de datos asociado a la instancia de base de datos. Los parámetros que se van a modificar incluyen `group_replication_group_name`, `rds.group_replication_enabled` y `group_replication_group_seeds`. Para obtener más información acerca de los parámetros de clúster activo-activo, consulte Configuración de parámetros obligatorios para los clústeres activo-activo.

   Si modifica los parámetros de un grupo de parámetros de base de datos, asegúrese de que el grupo de parámetros de base de datos no esté asociado a otras instancias de base de datos del clúster activo-activo.

4. Reinicie la instancia de base de datos que ha eliminado del clúster activo-activo para que se aplique la nueva configuración de parámetros.

   Para obtener instrucciones, consulte Reinicio de una instancia de base de datos.

Exportación de datos desde una instancia de base de datos MySQL mediante replicación

Puede usar la replicación para exportar datos desde una instancia de base de datos RDS para MySQL o posterior a una instancia MySQL que se ejecuta fuera de Amazon RDS. En esta situación, la instancia de base de datos MySQL es la instancia de base de datos MySQL de origen y la instancia de MySQL que se ejecuta fuera de Amazon RDS es la base de datos MySQL externa.

La base de datos MySQL externa puede ejecutarse en las instalaciones en su centro de datos o en una instancia Amazon EC2. La base de datos MySQL externa debe ejecutar la misma versión que la instancia de base de datos MySQL de origen o una versión posterior.

La replicación a una base de datos MySQL externa solo se admite durante el tiempo que se tarda en exportar una base de datos desde la instancia de base de datos MySQL de origen. La replicación deberá haber terminado cuando se hayan exportado los datos y las aplicaciones pueden empezar a acceder a la instancia MySQL externa.

La siguiente lista muestra los pasos que se deben dar. Cada paso se describe más detalladamente en las siguientes posteriores.

1. Prepare una instancia externa de base de datos MySQL.
2. Prepare la instancia de base de datos MySQL de origen para replicación.
3. Utilice la utilidad mysqldump para transferir la base de datos desde la instancia de base de datos MySQL de origen a la base de datos MySQL externa.
4. Inicie la replicación a la base de datos MySQL externa.
5. Una vez completada la exportación, detener la replicación.

Preparar una base de datos MySQL externa

Realice los siguientes pasos para preparar la base de datos MySQL externa.

Para preparar la base de datos MySQL externa

1. Instale la base de datos MySQL externa.
2. Conéctese a la base de datos MySQL externa como usuario maestro. A continuación, cree los usuarios que requieran los administradores, aplicaciones y servicios que acceden a la base de datos.

3. Siga las instrucciones de la documentación de MySQL para preparar la base de datos MySQL externa como réplica. Para obtener más información, consulte Setting the Replica Configuration en la documentación de MySQL.
4. Configure una regla de salida para que la base de datos MySQL externa funcione como réplica de lectura durante la exportación. La regla de salida permite que la base de datos MySQL externa se conecte a la instancia de base de datos MySQL de origen durante la replicación. Especifique una regla de salida que permita conexiones de Protocolo de control de transmisión (TCP) al puerto y la dirección IP de la instancia de base de datos MySQL.

   Especifique las reglas de salida adecuadas para su entorno:

   - Si la base de datos MySQL externa se está ejecutando en una instancia Amazon EC2 en una nube privada virtual (VPC) basada en el servicio Amazon VPC, especifique las reglas de salida en un grupo de seguridad de VPC. Para obtener más información, consulte Control de acceso con grupos de seguridad.
   - Si la base de datos MySQL externa está instalada en las instalaciones, especifique las reglas de salida en un firewall.
5. Si la base de datos MySQL externa se está ejecutando en una VPC, configure reglas para las reglas de la lista de control de acceso (ACL) de la VPC además de la regla de salida del grupo de seguridad:

   - Configure una regla ACL de entrada que permite tráfico TCP hacia los puertos 1024–65535 desde la dirección IP de la instancia de base de datos MySQL de origen.
   - Configure una regla ACL de salida que permita tráfico TCP saliente hacia el puerto y la dirección IP de la instancia de base de datos MySQL de origen.

   Para obtener más información acerca de las ACL de red de Amazon VPC, consulte ACL de red en la Guía del usuario de Amazon VPC.
6. (Opcional) Configure el parámetro `max_allowed_packet`en el tamaño máximo para evitar que se produzcan errores de replicación. Recomendamos este ajuste.

Preparar la instancia de base de datos MySQL de origen

Realice los siguientes pasos para preparar la instancia de base de datos MySQL de origen como origen de replicación.

Para preparar la instancia de base de datos MySQL de origen

1. Asegúrese de que el equipo cliente tenga suficiente espacio en disco disponible para guardar los registros binarios mientras se configura la replicación.
2. Conéctese a la instancia de base de datos de MySQL de origen y cree una cuenta de replicación siguiendo las instrucciones de Creating a User for Replication en la documentación de MySQL.
3. Configure reglas de ingreso en el sistema que ejecuta la instancia de base de datos MySQL de origen para permitir que la base de datos MySQL externa se conecte durante la replicación. Especifique una regla de entrada que permita conexiones TCP al puerto que utiliza la instancia de base de datos MySQL desde la dirección IP de la base de datos MySQL externa.
4. Especifique las reglas de salida:

   - Si la instancia de base de datos MySQL se ejecuta en una VPC, especifique las reglas de entrada en un grupo de seguridad de VPC. Para obtener más información, consulte Control de acceso con grupos de seguridad.
5. Si la instancia de base de datos MySQL se ejecuta en una VPC, configure reglas ACL de VPC además de la regla de entrada del grupo de seguridad.

   - Configure una regla ACL de entrada para permitir conexiones TCP hacia el puerto que utiliza la instancia de Amazon RDS desde la dirección IP de la base de datos MySQL externa.
   - Configure una regla ACL de salida para permitir conexiones TCP desde los puertos 1024–65535 hacia la dirección IP de la base de datos MySQL externa.

   Para obtener más información acerca de las ACL de red de Amazon VPC, consulte ACL de red en la Guía del usuario de Amazon VPC.
6. Asegúrese de que el periodo de retención de copia de seguridad configurado es lo bastante largo para que no se purguen logs binarios durante la exportación. Si se vacía alguno de los registros antes de que termine la exportación, deberá reiniciar la replicación desde el principio. Para obtener más información acerca de la configuración del periodo de retención de copia de seguridad, consulte Introducción a las copias de seguridad.
7. Utilice el procedimiento almacenado `mysql.rds_set_configuration` para configurar un periodo de retención de registro binario lo bastante largo como para que no se vacíen registros binarios durante la exportación. Para obtener más información, consulte Acceso a los registros binarios de MySQL.
8. Como medida adicional para asegurarse de que no se vacíen los registros binarios de la instancia de base de datos MySQL origen, cree una réplica de lectura en Amazon RDS de la

instancia de base de datos MySQL de origen. Para obtener más información, consulte Creación de una réplica de lectura.

9. Una vez creada la réplica de lectura de Amazon RDS, ejecute el procedimiento almacenado `mysql.rds_stop_replication` para detener el proceso de replicación. La instancia de base de datos MySQL de origen ya no vacía sus archivos de registro binarios, por lo que están disponibles para el proceso de replicación.
10. (Opcional) Configure los parámetros `max_allowed_packet` y `slave_max_allowed_packet` en el tamaño máximo para evitar errores de replicación. El tamaño máximo de ambos parámetros es 1 GB. Recomendamos esta configuración para ambos parámetros. Para obtener información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Copia de la base de datos

Realice los siguientes pasos para copiar la base de datos.

Para copiar la base de datos

1. Conéctese a la réplica de lectura de RDS de la instancia de base de datos MySQL de origen y ejecute la instrucción `SHOW REPLICA STATUS\G` de MySQL. Anote los valores siguientes:
   - `Master_Host`
   - `Master_Port`
   - `Master_Log_File`
   - `Exec_Master_Log_Pos`

   > **Note**
   >
   > Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

2. Use la utilidad mysqldump para crear una instantánea, que copia los datos de Amazon RDS a su equipo cliente local. Asegúrese de que el equipo cliente tenga suficiente espacio para albergar los archivos de `mysqldump` de las bases de datos que se van a replicar. Para las

bases de datos de gran tamaño, este proceso puede tardar varias horas. Siga las instrucciones de Creating a Data Snapshot Using mysqldump en la documentación de MySQL.

El siguiente ejemplo ejecuta `mysqldump` en un cliente y escribe el volcado en un archivo.

Para Linux, macOS o:Unix

```
mysqldump -h source_MySQL_DB_instance_endpoint \
    -u user \
    -ppassword \
    --port=3306 \
    --single-transaction \
    --routines \
    --triggers \
    --databases  database database2 > path/rds-dump.sql
```

En:Windows

```
mysqldump -h source_MySQL_DB_instance_endpoint ^
    -u user ^
    -ppassword ^
    --port=3306 ^
    --single-transaction ^
    --routines ^
    --triggers ^
    --databases  database database2 > path\rds-dump.sql
```

Puede cargar el archivo de copia de seguridad en la base de datos de MySQL externa. Para obtener más información, consulte Reloading SQL-Format Backups (Recargar las copias de seguridad con formato SQL) en la documentación de MySQL. Puede ejecutar otra utilidad para cargar los datos en la base de datos de MySQL externa.

Finalización de la exportación

Realice los siguientes pasos para completar la exportación.

Para finalizar la exportación

1. Utilice la instrucción `CHANGE MASTER` de MySQL para configurar la base de datos MySQL externa. Especifique el ID y la contraseña del usuario a los que se han concedido

permisos `REPLICATION SLAVE`. Especifique los valores `Master_Host`, `Master_Port`, `Relay_Master_Log_File` y `Exec_Master_Log_Pos` que obtuvo de la instrucción `SHOW REPLICA STATUS\G` de MySQL que ejecutó en la réplica de lectura de RDS. Para obtener más información, consulte CHANGE MASTER TO Statement en la documentación de MySQL.

> **Note**
>
> Versiones anteriores de MySQL utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

2. Utilice el comando `START REPLICA` de MySQL para iniciar la reproducción desde la instancia de base de datos MySQL de origen a la base de datos MySQL externa.

   Esto inicia la replicación desde la instancia de base de datos MySQL de origen y exporta todos los cambios de origen que se han producido después de detener la replicación desde la réplica de lectura de Amazon RDS.

   > **Note**
   >
   > Versiones anteriores de MySQL utilizaban `START SLAVE` en lugar de `START REPLICA`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `START SLAVE`.

3. Ejecute el comando `SHOW REPLICA STATUS\G` de MySQL en la base de datos MySQL externa para verificar que está funcionando como una réplica de lectura. Para obtener más información sobre la interpretación de los resultados, consulte SHOW SLAVE | REPLICA STATUS Statement en la documentación de MySQL.
4. Después de que la reproducción en la base de datos MySQL externa haya alcanzado la instancia de base de datos MySQL de origen, utilice el comando `STOP REPLICA` de MySQL para detener la reproducción desde la instancia de base de datos MySQL de origen.

   > **Note**
   >
   > Versiones anteriores de MySQL utilizaban `STOP SLAVE` en lugar de `STOP REPLICA`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `STOP SLAVE`.

5. En la réplica de lectura en Amazon RDS llame al procedimiento almacenado `mysql.rds_start_replication`. Ello permitirá a Amazon RDS comenzar a vaciar los archivos de registro binarios de la instancia de base de datos MySQL de origen.

Opciones para las instancias de bases de datos MySQL

A continuación, se incluye una descripción de las opciones, o características adicionales, que están disponibles para las instancias de Amazon RDS que ejecutan el motor de base de datos MySQL. Para activar estas opciones, puede añadirlas a un grupo de opciones personalizado y, a continuación, asociar el grupo de opciones a la instancia de base de datos. Para obtener más información acerca de cómo trabajar con grupos de opciones, consulte Trabajo con grupos de opciones.

Amazon RDS admite las siguientes opciones para MySQL:

Opción	ID de la opción	Versiones del motor
Compatibilidad con el complemento de auditoría de MariaDB para MySQL	`MARIADB_AUDIT_PLUGIN`	Todas las versiones MySQL 8.4 Versión de MySQL 8.0.28 y posteriores a la 8.0 Todas las versiones MySQL 5.7
Compatibilidad con memcached para MySQL	`MEMCACHED`	Todas las versiones de MySQL 5.7 y 8.0

Compatibilidad con el complemento de auditoría de MariaDB para MySQL

Amazon RDS ofrece un complemento de auditoría para instancias de bases de datos de MySQL basado en el complemento de auditoría de MariaDB de código abierto. Para obtener más información, consulte el repositorio GitHub del complemento de auditoría para el servidor MySQL.

> **Note**
>
> El complemento de auditoría para MySQL se basa en el complemento de auditoría de MariaDB. A lo largo de este artículo, lo denominaremos complemento de auditoría de MariaDB.

El complemento de auditoría de MariaDB registra la actividad de la base de datos, incluidos los usuarios que inician sesión en la base de datos y las consultas ejecutadas en la base de datos. El registro de la actividad de la base de datos se almacena en un archivo de registro.

Configuración de opciones del complemento de auditoría

Amazon RDS admite la siguiente configuración para la opción del complemento de auditoría de MariaDB.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
`SERVER_AUDIT_FILE_PATH`	`/rdsdbdata/log/audit/`	`/rdsdbdata/log/audit/`	La ubicación del archivo de registro. El archivo de registro contiene el registro de la actividad especificada en `SERVER_AUDIT_EVENTS`. Para obtener más información, consulte Visualización y descripción de archivos de registro de base de datos y Archivos de registro de base de datos de MySQL.
`SERVER_AUDIT_FILE_ROTATE_SIZE`	1–1 000 000 000	1000000	El tamaño en bytes que, al alcanzarse, hace que se rote el archivo. Para obtener más información, consulte Información general de

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
			los registros de bases de datos de RDS para MySQL.
SERVER_AUDIT_FILE_ROTATIONS	0–100	9	Es el número de rotaciones de registro que se debe guardar cuando `server_audit_output_type=file` . Si se establece en 0, el archivo de registro no gira nunca. Para obtener más información, consulte Información general de los registros de bases de datos de RDS para MySQL y Descarga de un archivo de registro de base de datos.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_EVENTS	CONNECT, QUERY, QUERY_DDL, QUERY_DML, QUERY_DML_NO_SELECT, QUERY_DCL	CONNECT, QUERY	Los tipos de actividad que se van a registrar en el registro. La instalación del complemento de auditoría de MariaDB también se registra. • CONNECT: registra las conexiones a la base de datos completadas y no completadas y también las desconexiones. • QUERY: registra el texto de todas las consultas que se ejecutan en la base de datos. • QUERY_DDL : similar al evento QUERY, pero solo devuelve consultas en lenguaje de definición de datos (DDL) (CREATE, ALTER, etc.). • QUERY_DML : similar al evento QUERY, pero solo devuelve consultas en lenguaje de manipulación de datos (DML) (INSERT, UPDATE, etc. y también SELECT). • QUERY_DML_NO_SELECT : similar al evento QUERY_DML , pero no registra consultas SELECT. • QUERY_DCL : similar al evento QUERY, pero solo devuelve consultas en lenguaje de control de datos (DCL) (GRANT, REVOKE, etc.). No se admite TABLE para MySQL.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_INCL_USERS	Varios valores separados por comas	Ninguno	Incluya solo la actividad de los usuarios especificados. De forma predeterminada, la actividad se registra para todos los usuarios. SERVER_AUDIT_INCL_USERS y SERVER_AUDIT_EXCL_USERS se excluyen mutuamente. Si agrega valores a SERVER_AUDIT_INCL_USERS, asegúrese de que no se agregan valores a SERVER_AUDIT_EXCL_USERS.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_EXCL_USERS	Varios valores separados por comas	Ninguno	Excluya la actividad de los usuarios especificados. De forma predeterminada, la actividad se registra para todos los usuarios. SERVER_AUDIT_INCL_USERS y SERVER_AUDIT_EXCL_USERS se excluyen mutuamente. Si agrega valores a SERVER_AUDIT_EXCL_USERS, asegúrese de que no se agregan valores a SERVER_AUDIT_INCL_USERS. El usuario rdsadmin consulta la base de datos cada segundo para comprobar su estado. Dependiendo de otros ajustes de configuración, esta actividad puede hacer que el tamaño del archivo de registro llegue a ser muy grande muy deprisa. Si no necesita registrar esta actividad, añada el usuario rdsadmin a la lista SERVER_AUDIT_EXCL_USERS. **Note** CONNECTLa actividad de siempre se registra para todos los usuarios, aunque se especifique el usuario de esta configuración de opciones.
SERVER_AUDIT_LOGGING	ON	ON	El registro está activo. El único valor válido es ON. Amazon RDS no permite desactivar el registro. Si desea desactivar el registro, elimine el complemento de auditoría de MariaDB. Para obtener más información, consulte Eliminación del complemento de auditoría de MariaDB.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
SERVER_AUDIT_QUERY_LOG_LIMIT	0–2147483647	1024	Límite de la longitud de la cadena de consulta en un registro.

Adición del complemento de auditoría de MariaDB

El proceso general para añadir el complemento de auditoría de MariaDB a una instancia de base de datos es el siguiente:

- Crear un grupo de opciones nuevo, o copiar o modificar un grupo de opciones existente
- Añadir la opción al grupo de opciones
- Asociar el grupo de opciones a la instancia de base de datos

Después de añadir el complemento de auditoría de MariaDB, no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, comenzará la auditoría.

> **Important**
>
> La adición del complemento de auditoría de MariaDB en una instancia de base de datos puede provocar una interrupción. Le recomendamos añadir el complemento de auditoría de MariaDB durante un periodo de mantenimiento o durante una carga de trabajo de base de datos baja.

Para añadir el complemento de auditoría de MariaDB

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado. Elija mysql para Motor y elija 5.7, 8.0 o 8.4 para Versión principal del motor. Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada la opción MARIADB_AUDIT_PLUGIN al grupo de opciones y configure los ajustes de las opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones. Para obtener más información acerca de cada opción, consulte Configuración de opciones del complemento de auditoría.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente.

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Formato de registro de auditoría

Los archivos de registro se representan como archivos de variables separadas por comas (CSV) en formato UTF-8.

> **Tip**
>
> Las entradas del archivo de registro no están en orden secuencial. Para ordenar las entradas, utilice el valor de marca temporal. Para ver los eventos más recientes, es posible que sea necesario revisar todos los archivos de registro. Para obtener más flexibilidad en la ordenación y búsqueda de los datos de registro, active la configuración para cargar los registros de auditoría en CloudWatch y verlos mediante la interfaz de CloudWatch.
> Para ver los datos de auditoría con más tipos de campos y con salida en formato JSON, también puede utilizar la característica Flujos de actividad de base de datos. Para obtener más información, consulte Supervisión de Amazon RDS con flujos de actividad de la base de datos.

Los archivos de registro de auditoría incluyen la siguiente información delimitada por comas en las filas en el orden especificado:

Campo	Descripción
marca de tiempo	YYYYMMDD seguido de HH:MI:SS (reloj de 24 horas) para el evento registrado.
serverhost	Nombre de la instancia para la que se ha registrado el evento.
username	Nombre de usuario conectado del usuario.
host	Host desde el que se ha conectado el usuario.
connectionid	Número de ID de conexión de la operación registrada.
queryid	Número de ID de la consulta que se puede usar para buscar los eventos de la tabla relacional y las consultas relacionadas. Para los eventos TABLE, se añaden varias líneas.
operación	Tipo de acción registrado. Los posibles valores son: CONNECT, QUERY, READ, WRITE, CREATE, ALTER, RENAME y DROP.
base de datos	Base de datos activa, definida por el comando USE.
objeto	Para los eventos de QUERY, este valor indica la consulta realizada por la base de datos. En los eventos TABLE, indica el nombre de la tabla.
retcode	Código devuelto de la operación registrada.
connection_type	Estado de seguridad de la conexión al servidor. Los valores posibles son los siguientes: • 0: sin definir • 1: TCP/IP • 2: conector • 3: canalización con nombre • 4: SSL/TLS • 5: memoria compartida

Visualización y descarga del registro del complemento de auditoría de MariaDB

Después de habilitar un complemento de auditoría de MariaDB, podrá obtener acceso a los resultados de los archivos de registro de la misma forma que a los de los demás archivos de registro basados en texto. Los archivos del registro de auditoría se encuentran en `/rdsdbdata/log/audit/`. Para obtener información acerca de la visualización del archivo de registro en la consola, consulte Visualización y descripción de archivos de registro de base de datos. Para obtener información acerca de la descarga del archivo de registro, consulte Descarga de un archivo de registro de base de datos.

Modificación de la configuración del complemento de auditoría de MariaDB

Después de activar el complemento de auditoría MariaDB, puede modificar la configuración. Para obtener más información acerca de cómo modificar la configuración de las opciones, consulte Modificación de una configuración de opciones. Para obtener más información acerca de cada opción, consulte Configuración de opciones del complemento de auditoría.

Eliminación del complemento de auditoría de MariaDB

Amazon RDS no permite desactivar el registro del complemento de auditoría de MariaDB. Sin embargo, puede eliminar el complemento de una instancia de base de datos. Cuando elimina el complemento de auditoría de MariaDB, la instancia de base de datos se reinicia automáticamente para detener la auditoría.

Para eliminar el complemento de auditoría de MariaDB de una instancia de base de datos, realice una de las siguientes operaciones:

- Elimine la opción del complemento de auditoría de MariaDB del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones
- Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya el complemento. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Compatibilidad con memcached para MySQL

Amazon RDS admite el uso de la interfaz memcached para las tablas de InnoDB que se introdujo en MySQL 5.6. La API de memcached permite a las aplicaciones utilizar las tablas de InnoDB de una manera similar a los almacenes de datos clave-valor de NoSQL.

> **Note**
>
> La interfaz memcached ya no está disponible en MySQL 8.4. Al actualizar las instancias de base de datos a MySQL 8.4, debe deshabilitar memcached en los grupos de opciones existentes.

La interfaz memcached es una caché sencilla y basada en claves. Las aplicaciones utilizan memcached para insertar, manipular y recuperar pares de datos de clave-valor de la memoria caché. MySQL 5.6 introdujo un complemento que implementa un servicio de daemon que expone los datos de las tablas de InnoDB a través del protocolo de memcached. Para obtener más información acerca del complemento memcached de MySQL, consulte InnoDB Integration with memcached.

A fin de habilitar el soporte de memcached para una instancia de base de datos RDS para MySQL

1. Determine el grupo de seguridad que se utilizará para controlar el acceso a la interfaz memcached. Si el conjunto de aplicaciones que utilizan la interfaz SQL es el mismo que tendrá acceso a la interfaz memcached, puede utilizar el grupo de seguridad de la VPC existente utilizado por la interfaz de SQL. Si otro conjunto de aplicaciones va a acceder a la interfaz memcached, defina un grupo de seguridad de base de datos nuevo o una VPC nueva. Para obtener más información acerca de la administración de grupos de seguridad, consulte Control de acceso con grupos de seguridad
2. Cree un grupo de opciones de base de datos personalizado, seleccionando MySQL como versión y tipo de motor. Para obtener más información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.
3. Añada la opción MEMCACHED al grupo de opciones. Especifique el puerto que utilizará la interfaz memcached y el grupo de seguridad que se utilizará para controlar el acceso a la interfaz. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

4. Modifique las opciones para configurar los parámetros de `memcached`, si es necesario. Para obtener más información acerca de cómo modificar la configuración de las opciones, consulte Modificación de una configuración de opciones.
5. Aplique el grupo de opciones a una instancia. Amazon RDS permite usar `memcached` para esa instancia cuando se aplica el grupo de opciones:
   - Para poder usar `memcached` para una instancia nueva, especifique el grupo de opciones personalizado al lanzar la instancia. Para obtener más información acerca de cómo lanzar una instancia de MySQL, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para poder usar `memcached` para una instancia existente, especifique el grupo de opciones personalizado al modificar la instancia. Para obtener más información acerca de la modificación de una instancia de base de datos de , consulte Modificación de una instancia de base de datos de Amazon RDS.
6. Especifique las columnas de las tablas de MySQL a las que se puede obtener acceso a través de la interfaz `memcached`. El complemento `memcached` crea una tabla de catálogo denominada `containers` en una base de datos dedicada denominada `innodb_memcache`. Inserte una fila en la tabla `containers` para asignar una tabla de InnoDB para el acceso a través de `memcached`. Especifique la columna de la tabla de InnoDB que se utiliza para almacenar los valores de clave de `memcached`, y una o varias columnas que se utilizan para almacenar los valores de datos asociados a la clave. También debe especificar el nombre que utiliza una aplicación de `memcached` para referirse a ese conjunto de columnas. Para obtener información detallada sobre cómo insertar filas en la tabla `containers`, consulte InnoDB memcached Plugin Internals. Para obtener un ejemplo de mapeo de una tabla InnoDB y acceso a ella a través de `memcached`, consulte Writing Applications for the InnoDB memcached Plugin.
7. Si las aplicaciones que acceden a la interfaz `memcached` se encuentran en equipos o instancias EC2 diferentes de los de las aplicaciones que utilizan la interfaz de SQL, añada la información de conexión para esos equipos al grupo de seguridad de la VPC asociado a la instancia de MySQL. Para obtener más información acerca de la administración de grupos de seguridad, consulte Control de acceso con grupos de seguridad.

Para desactivar la compatibilidad con `memcached` en una instancia, modifique la instancia y especifique el grupo de opciones predeterminado para la versión de MySQL. Para obtener más información acerca de la modificación de una instancia de base de datos de , consulte Modificación de una instancia de base de datos de Amazon RDS.

Consideraciones de seguridad de la interfaz memcached de MySQL

El protocolo de `memcached` no admite la autenticación de usuarios. Para obtener más información sobre las consideraciones de seguridad de `memcached` de MySQL, consulte Security Considerations for the InnoDB memcached Plugin (Consideraciones de seguridad del complemento Memcached de InnoDB) en la documentación de MySQL.

Puede realizar las siguientes acciones para aumentar la seguridad de la interfaz `memcached`:

- Al añadir la opción `MEMCACHED` al grupo de opciones, especifique un puerto distinto del predeterminado (11211).
- Asegúrese de asociar la interfaz `memcached` a un grupo de seguridad de VPC que limite el acceso a las direcciones de los clientes o las instancias EC2 que sean conocidas y de confianza. Para obtener más información acerca de la administración de grupos de seguridad, consulte Control de acceso con grupos de seguridad.

Información sobre la conexión de la interfaz memcached de MySQL

Para acceder a la interfaz `memcached`, una aplicación debe especificar tanto el nombre de DNS de la instancia de Amazon RDS como el número de puerto de `memcached`. Por ejemplo, si una instancia tiene el nombre de DNS `my-cache-instance.cg034hpkmmjt.region.rds.amazonaws.com` y la interfaz memcached utiliza el puerto 11212, la información de conexión especificada en PHP sería:

```
<?php

$cache = new Memcache;
$cache->connect('my-cache-instance.cg034hpkmmjt.region.rds.amazonaws.com',11212);
?>
```

Para encontrar el nombre DNS y el puerto de memcached de una instancia de base de datos de MySQL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la AWS Management Console, seleccione la región que contiene la instancia de base de datos.

3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Seleccione el nombre de la instancia de base de datos MySQL para mostrar sus detalles.
5. En la sección Connect, anote el valor del campo Endpoint. El nombre DNS será igual al punto de enlace. Asimismo, observe que el puerto de la sección Connect no se utiliza para obtener acceso a la interfaz de `memcached`.
6. En la sección Details, anote el nombre que aparece en el campo Option Group.
7. En el panel de navegación, elija Option groups (Grupos de opciones).
8. Seleccione el nombre del grupo de opciones utilizado por la instancia de base de datos MySQL para mostrar los detalles del grupo de opciones. En la sección Options, anote el valor de la configuración Port de la opción MEMCACHED.

Opciones de configuración de la interfaz memcached de MySQL

Amazon RDS expone los parámetros de la interfaz `memcached` de MySQL como opciones de configuración de la opción `MEMCACHED` de Amazon RDS.

Parámetros de la interfaz memcached de MySQL

- `DAEMON_MEMCACHED_R_BATCH_SIZE`: valor entero que especifica cuántas operaciones de lectura (get) de `memcached` se deben realizar antes de utilizar COMMIT para iniciar una transacción nueva. Los valores permitidos son de 1 a 4294967295, el valor predeterminado es 1. La opción no surtirá efecto hasta que no se reinicie la instancia.
- `DAEMON_MEMCACHED_W_BATCH_SIZE`: valor entero que especifica cuántas operaciones de escritura de `memcached`, como add, set o incr, se deben realizar antes de utilizar COMMIT para iniciar una transacción nueva. Los valores permitidos son de 1 a 4294967295, el valor predeterminado es 1. La opción no surtirá efecto hasta que no se reinicie la instancia.
- `INNODB_API_BK_COMMIT_INTERVAL`: valor entero que especifica la frecuencia con la que se confirmarán automáticamente las conexiones inactivas que utilizan la interfaz `memcached` de InnoDB. Los valores permitidos son de 1 a 1073741824, el valor predeterminado es 5. La opción entra en vigor inmediatamente, sin necesidad de reiniciar la instancia.
- `INNODB_API_DISABLE_ROWLOCK`: valor booleano que desactiva (1 (true)) o activa (0 (false)) el uso de los bloqueos de filas cuando se utiliza la interfaz `memcached` de InnoDB. El valor predeterminado es 0 (false). La opción no surtirá efecto hasta que no se reinicie la instancia.
- `INNODB_API_ENABLE_MDL`: valor booleano que, cuando se establece en 0 (false), bloquea la tabla utilizada por el complemento `memcached` de InnoDB, de modo que no pueda ser eliminado ni

alterado por DDL a través de la interfaz de SQL. El valor predeterminado es 0 (false). La opción no surtirá efecto hasta que no se reinicie la instancia.

- INNODB_API_TRX_LEVEL: valor entero que especifica el nivel de aislamiento de transacciones para las consultas procesadas por la interfaz memcached. Los valores permitidos son de 0 a 3. El valor predeterminado es 0. La opción no surtirá efecto hasta que no se reinicie la instancia.

Amazon RDS configura estos parámetros de memcached en MySQL y no es posible modificarlos: DAEMON_MEMCACHED_LIB_NAME, DAEMON_MEMCACHED_LIB_PATH e INNODB_API_ENABLE_BINLOG. Los parámetros que los administradores de MySQL establecen utilizando daemon_memcached_options están disponibles como opciones de configuración individuales de MEMCACHED en Amazon RDS.

Parámetros de daemon_memcached_options de MySQL

- BINDING_PROTOCOL: cadena que especifica el protocolo de enlace que se va a utilizar. Los valores permitidos son auto, ascii o binary. El valor predeterminado es auto, que significa que el servidor negocia automáticamente el protocolo con el cliente. La opción no surtirá efecto hasta que no se reinicie la instancia.
- BACKLOG_QUEUE_LIMIT – valor entero que especifica cuántas conexiones de red pueden estar esperando a que las procese memcached. Si se aumenta este límite, se pueden reducir los errores recibidos por un cliente que no puede conectarse a la instancia de memcached, pero no se mejora el desempeño del servidor. Los valores permitidos son de 1 a 2048, el valor predeterminado es 1024. La opción no surtirá efecto hasta que no se reinicie la instancia.
- CAS_DISABLED: valor booleano que activa (1 (verdadero)) o desactiva (0 (false)) el uso de la función de comparación e intercambio (CAS), lo que reduce el tamaño por cada elemento en 8 bytes. El valor predeterminado es 0 (false). La opción no surtirá efecto hasta que no se reinicie la instancia.
- CHUNK_SIZE: valor entero que especifica el tamaño mínimo del fragmento, en bytes, que se debe asignar para la clave, el valor y las marcas del elemento más pequeño. Los valores permitidos son de 1 a 48. El valor predeterminado es 48, y se puede mejorar significativamente la eficiencia de la memoria con un valor inferior. La opción no surtirá efecto hasta que no se reinicie la instancia.
- CHUNK_SIZE_GROWTH_FACTOR: valor de coma flotante que controla el tamaño de los fragmentos nuevos. El tamaño de un fragmento nuevo es el tamaño de fragmento anterior multiplicado por CHUNK_SIZE_GROWTH_FACTOR. Los valores permitidos son de 1 a 2, el valor predeterminado es 1.25. La opción no surtirá efecto hasta que no se reinicie la instancia.

- ERROR_ON_MEMORY_EXHAUSTED: valor booleano que, cuando se establece en 1 (true), especifica que memcached devolverá un error en lugar de desalojar elementos cuando no haya más memoria para almacenar elementos. Si se establece en 0 (false), memcached desalojará elementos cuando no haya más memoria. El valor predeterminado es 0 (false). La opción no surtirá efecto hasta que no se reinicie la instancia.
- MAX_SIMULTANEOUS_CONNECTIONS: valor entero que especifica el número máximo de conexiones simultáneas. Si este valor es menor que 10, MySQL no se iniciará. Los valores permitidos son de 10 a 1024, el valor predeterminado es 1024. La opción no surtirá efecto hasta que no se reinicie la instancia.
- VERBOSITY: cadena que especifica el nivel de información que el servicio memcached registra en el registro de errores de MySQL. La opción predeterminada es v. La opción no surtirá efecto hasta que no se reinicie la instancia. Los valores permitidos son:
  - v: registra los errores y las advertencias mientras de ejecuta el bucle del evento principal.
  - vv: además de la información registrada por v, también registra cada comando de cliente y la respuesta.
  - vvv: además de la información registrada por vv, también registra las transiciones entre los estados internos.

Amazon RDS configura estos parámetros de DAEMON_MEMCACHED_OPTIONS en MySQL; no es posible modificarlos: DAEMON_PROCESS, LARGE_MEMORY_PAGES, MAXIMUM_CORE_FILE_LIMIT, MAX_ITEM_SIZE, LOCK_DOWN_PAGE_MEMORY, MASK, IDFILE, REQUESTS_PER_EVENT, SOCKET y USER.

Parámetros de MySQL

De manera predeterminada, una instancia de base de datos de MySQL usa un grupo de parámetros de base de datos específico de una base de datos de MySQL. Este grupo de parámetros contiene parámetros para el motor de base de datos de MySQL. Para obtener información sobre cómo trabajar con grupos de parámetros y establecer parámetros, consulte Grupos de parámetros para Amazon RDS.

Los parámetros de RDS for MySQL se configuran en los valores predeterminados del motor de almacenamiento seleccionado. Para obtener más información sobre los parámetros de MySQL, consulte la documentación de MySQL. Para obtener más información sobre el almacenamiento de MySQL, consulte Motores de almacenamiento admitidos por RDS for MySQL.

Puede ver los parámetros disponibles para una versión específica de RDS for MySQL mediante la consola de RDS o la AWS CLI. Para obtener información acerca de cómo ver parámetros en un grupo de parámetros de MySQL en la consola RDS, consulte Visualización de los valores de parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Con la AWS CLI, puede ver los parámetros de una versión de RDS for MySQL ejecutando el comando `describe-engine-default-parameters`. Especifique uno de los siguientes valores para la opción `--db-parameter-group-family`:

- `mysql8.4`
- `mysql8.0`
- `mysql5.7`

Por ejemplo, para ver los parámetros de la versión 8.0 de RDS for MySQL, ejecute el siguiente comando.

```
aws rds describe-engine-default-parameters --db-parameter-group-family mysql8.0
```

El resultado tiene un aspecto similar al siguiente.

```
{
    "EngineDefaults": {
        "Parameters": [
            {
                "ParameterName": "activate_all_roles_on_login",
                "ParameterValue": "0",
```

```
                "Description": "Automatically set all granted roles as active after the
 user has authenticated successfully.",
                "Source": "engine-default",
                "ApplyType": "dynamic",
                "DataType": "boolean",
                "AllowedValues": "0,1",
                "IsModifiable": true
            },
            {
                "ParameterName": "allow-suspicious-udfs",
                "Description": "Controls whether user-defined functions that have only
 an xxx symbol for the main function can be loaded",
                "Source": "engine-default",
                "ApplyType": "static",
                "DataType": "boolean",
                "AllowedValues": "0,1",
                "IsModifiable": false
            },
            {
                "ParameterName": "auto_generate_certs",
                "Description": "Controls whether the server autogenerates SSL key and
 certificate files in the data directory, if they do not already exist.",
                "Source": "engine-default",
                "ApplyType": "static",
                "DataType": "boolean",
                "AllowedValues": "0,1",
                "IsModifiable": false
            },
        ...
```

Para enumerar solo los parámetros modificables de la versión 8.0 de RDS for MySQL, ejecute el siguiente comando.

Para Linux, macOS o Unix:

```
aws rds describe-engine-default-parameters --db-parameter-group-family mysql8.0 \
   --query 'EngineDefaults.Parameters[?IsModifiable==`true`]'
```

Para Windows:

```
aws rds describe-engine-default-parameters --db-parameter-group-family mysql8.0 ^
   --query "EngineDefaults.Parameters[?IsModifiable==`true`]"
```

Tareas comunes de administración de bases de datos para las instancias de bases de datos MySQL

en el siguiente contenido, puede encontrar descripciones de las implementaciones específicas de Amazon RDS de algunas tareas comunes de DBA para las instancias de bases de datos que ejecutan el motor de base de datos MySQL. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Para obtener información acerca de cómo trabajar con archivos de registro de MySQL en Amazon RDS, consulte Archivos de registro de base de datos de MySQL.

Usuarios predefinidos

Amazon RDS crea automáticamente varios usuarios predefinidos con nuevas instancias de base de datos de RDS para MySQL. Los usuarios predefinidos y sus privilegios no se pueden cambiar. No se pueden eliminar, cambiar de nombre ni modificar los privilegios de estos usuarios predefinidos. Intentar realizar una de estas operaciones producirá un error.

- rdsadmin: un usuario creado para administrar muchas de las tareas de administración que el administrador con privilegios de `superuser` realizaría en una base de datos PostgreSQL independiente. Este usuario lo utiliza internamente RDS para MySQL para muchas tareas de administración.
- rdsrepladmin: usuario que Amazon RDS utiliza internamente para respaldar las actividades de réplica en instancias y clústeres de bases de datos de RDS para MySQL.

Para obtener información sobre otras tareas comunes del administrador de bases de datos, consulte los siguientes temas.

Temas

- Modelo de privilegios basado en roles de RDS para MySQL
- Privilegios dinámicos de RDS para MySQL
- Finalización de una sesión o una consulta de RDS para MySQL
- Omisión del error de replicación actual de RDS para MySQL

- Uso de espacios de tablas de InnoDB para mejorar los tiempos de recuperación tras un bloqueo de RDS para MySQL
- Administración de Historial de estado global de RDS para MySQL
- Configuración del tamaño del grupo de búferes y la capacidad de registros redo en MySQL 8.4

Modelo de privilegios basado en roles de RDS para MySQL

A partir de RDS para MySQL versión 8.0.36, no se pueden modificar las tablas de base de datos de `mysql` directamente. En concreto, no puede crear usuarios de bases de datos realizando operaciones de lenguaje de manipulación de datos (DML) en las tablas `grant`. En su lugar, se utilizan instrucciones de administración de cuentas de MySQL como `CREATE USER`, `GRANT` y `REVOKE` para conceder privilegios basados en roles a los usuarios. Tampoco puede crear otros tipos de objetos, como procedimientos almacenados en la base de datos `mysql`. Aún puede consultar las tablas de `mysql`. Si utiliza la replicación de registros binarios, los cambios realizados directamente en las tablas `mysql` de la instancia de base de datos de origen no se replican en el clúster de destino.

En algunos casos, la aplicación puede utilizar accesos directos para crear usuarios u otros objetos insertándolos en las tablas de `mysql`. Si es así, cambie el código de la aplicación para utilizar las declaraciones correspondientes, como `CREATE USER`.

Para exportar metadatos para usuarios de bases de datos durante la migración desde una base de datos MySQL externa, utilice uno de los siguientes métodos:

- Utilice la utilidad de volcado de instancias del intérprete de comandos de MySQL con un filtro para excluir usuarios, roles y concesiones. En el siguiente ejemplo, se muestra la sintaxis de comandos que se utilizarán. Asegúrese de que `outputUrl` esté vacío.

  ```
  mysqlsh user@host -- util.dumpInstance(outputUrl,{excludeSchemas:['mysql'],users:
   true})
  ```

  Para obtener más información, consulte Instance Dump Utility, Schema Dump Utility, and Table Dump Utility en el Manual de referencia de MySQL.
- Utilice la utilidad de cliente de `mysqlpump`. Este ejemplo incluye todas las tablas, excepto las tablas de la base de datos del sistema `mysql`. También incluye las instrucciones `CREATE USER` y `GRANT` para reproducir todos los usuarios de MySQL de la base de datos migrada.

```
mysqlpump --exclude-databases=mysql --users
```

La utilidad de cliente `mysqlpump` ya no está disponible con MySQL 8.4. En su lugar, utilice `mysqldump`.

Para simplificar la administración de permisos para muchos usuarios o aplicaciones, puede utilizar la instrucción `CREATE ROLE` para crear un rol que tenga un conjunto de permisos. A continuación, puede utilizar las instrucciones `GRANT` y `SET ROLE` y la función `current_role` para asignar roles a usuarios o aplicaciones, cambiar el rol actual y verificar qué roles están en vigor. Para obtener más información sobre el sistema de permisos basado en roles de MySQL 8.0, consulte Uso de roles en el Manual de referencia de MySQL.

Important

Le recomendamos encarecidamente que no utilice el usuario maestro directamente en sus aplicaciones. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar un usuario de base de datos creado con los privilegios mínimos necesarios para su aplicación.

A partir de la versión 8.0.36, RDS para MySQ incluye un rol especial que tiene todos los siguientes privilegios. El rol se denomina `rds_superuser_role`. El usuario administrativo principal de cada instancia de base de datos ya tiene asignado este rol. El rol `rds_superuser_role` incluye los siguientes privilegios para todos los objetos de base de datos:

- `ALTER`
- `APPLICATION_PASSWORD_ADMIN`
- `ALTER ROUTINE`
- `CREATE`
- `CREATE ROLE`
- `CREATE ROUTINE`
- `CREATE TEMPORARY TABLES`
- `CREATE USER`
- `CREATE VIEW`
- `DELETE`

- DROP
- DROP ROLE
- EVENT
- EXECUTE
- INDEX
- INSERT
- LOCK TABLES
- PROCESS
- REFERENCES
- RELOAD
- REPLICATION CLIENT
- REPLICATION SLAVE
- ROLE_ADMIN
- SET_USER_ID
- SELECT
- SHOW DATABASES
- SHOW VIEW
- TRIGGER
- UPDATE
- XA_RECOVER_ADMIN

La definición de rol también incluye `WITH GRANT OPTION` para que un usuario administrativo pueda conceder ese rol a otros usuarios. En particular, el administrador debe conceder los privilegios necesarios para realizar la replicación de registros binarios con el clúster de MySQL como destino.

Tip

Para ver todos los detalles de los permisos, utilice la siguiente instrucción.

```
SHOW GRANTS FOR rds_superuser_role@'%';
```

Cuando concede acceso mediante roles en RDS para MySQL versión 8.0.36 y posteriores, también activa el rol mediante la instrucción `SET ROLE role_name` o `SET ROLE ALL`. El siguiente ejemplo muestra cómo. Sustituya el nombre de rol apropiado por `CUSTOM_ROLE`.

```
# Grant role to user
mysql> GRANT CUSTOM_ROLE TO 'user'@'domain-or-ip-address'

# Check the current roles for your user. In this case, the CUSTOM_ROLE role has not
 been activated.
# Only the rds_superuser_role is currently in effect.
mysql> SELECT CURRENT_ROLE();
+--------------------------+
| CURRENT_ROLE()           |
+--------------------------+
| `rds_superuser_role`@`%` |
+--------------------------+
1 row in set (0.00 sec)

# Activate all roles associated with this user using SET ROLE.
# You can activate specific roles or all roles.
# In this case, the user only has 2 roles, so we specify ALL.
mysql> SET ROLE ALL;
Query OK, 0 rows affected (0.00 sec)

# Verify role is now active
mysql> SELECT CURRENT_ROLE();
+-------------------------------------------------+
| CURRENT_ROLE()                                  |
+-------------------------------------------------+
| `CUSTOM_ROLE`@`%`,`rds_superuser_role`@`%` |
+-------------------------------------------------+
```

Privilegios dinámicos de RDS para MySQL

Los privilegios dinámicos son privilegios de MySQL que puede conceder de forma explícita mediante la instrucción `GRANT`. Según la versión de RDS para MySQL, RDS solo le permite conceder privilegios dinámicos específicos. RDS no permite algunos de estos privilegios porque pueden interferir con las operaciones específicas de la base de datos, como la replicación y la copia de seguridad.

La siguiente tabla muestra cuáles de estos privilegios se pueden conceder a las distintas versiones de MySQL. Si está actualizando desde una versión de MySQL anterior a 8.0.36 a una versión 8.0.36

o posterior, es posible que tenga que actualizar el código de la aplicación si ya no se permite conceder un privilegio concreto.

Privilegio	MySQL 8.0.35 y versiones anteriores	MySQL 8.0.36 y versiones secundarias posteriores	MySQL 8.4.3 y posteriores
ALLOW_NONEXISTENT_DEFINER	No disponible	No disponible	No permitido
APPLICATION_PASSWORD_ADMIN	Permitido	Permitida	Permitida
AUDIT_ABORT_EXEMPT	Permitido	No permitido	No permitidos
AUDIT_ADMIN	No permitidos	No permitidos	No permitidos
AUTHENTICATION_POLICY_ADMIN	Permitido	No permitido	No permitidos
BACKUP_ADMIN	Permitido	No permitido	No permitidos
BINLOG_ADMIN	Permitido	No permitido	No permitidos
BINLOG_ENCRYPTION_ADMIN	No permitidos	No permitidos	No permitidos
CLONE_ADMIN	No permitidos	No permitidos	No permitidos
CONNECTION_ADMIN	Permitido	No permitido	No permitidos
ENCRYPTION_KEY_ADMIN	No permitidos	No permitidos	No permitidos
FIREWALL_ADMIN	No permitidos	No permitidos	No permitidos

Privilegio	MySQL 8.0.35 y versiones anteriores	MySQL 8.0.36 y versiones secundarias posteriores	MySQL 8.4.3 y posteriores
FIREWALL_EXEMPT	Permitido	No permitido	No permitidos
FIREWALL_USER	No permitidos	No permitidos	No permitidos
FLUSH_OPTIMIZER_COSTS	Permitido	Permitida	Permitida
FLUSH_PRIVILEGES	No disponible	No disponible	Permitido
FLUSH_STATUS	Permitido	Permitida	Permitida
FLUSH_TABLES	Permitido	Permitida	Permitida
FLUSH_USER_RESOURCES	Permitido	Permitida	Permitida
GROUP_REPLICATION_ADMIN	No permitidos	No permitidos	No permitidos
GROUP_REPLICATION_STREAM	No permitidos	No permitidos	No permitidos
INNODB_REDO_LOG_ARCHIVE	No permitido	No permitidos	No permitidos
INNODB_REDO_LOG_ENABLE	No permitidos	No permitidos	No permitidos
MASKING_DICTIONARIES_ADMIN	No permitidos	No permitidos	No permitidos
NDB_STORED_USER	No permitidos	No permitidos	No permitidos

Privilegio	MySQL 8.0.35 y versiones anteriores	MySQL 8.0.36 y versiones secundarias posteriores	MySQL 8.4.3 y posteriores
OPTIMIZE_LOCAL_TABLE	No disponible	No disponible	No permitido
PASSWORDLESS_USER_ADMIN	No permitidos	No permitidos	No permitidos
PERSIST_RO_VARIABLES_ADMIN	No permitidos	No permitidos	No permitidos
REPLICATION_APPLIER	Permitido	No permitido	No permitidos
REPLICATION_SLAVE_ADMIN	No permitidos	No permitidos	No permitidos
RESOURCE_GROUP_ADMIN	Permitido	No permitido	No permitidos
RESOURCE_GROUP_USER	Permitido	No permitido	No permitidos
ROLE_ADMIN	Permitido	Permitida	Permitida
SENSITIVE_VARIABLES_OBSERVER	Permitido	Permitida	Permitida
SERVICE_CONNECTION_ADMIN	Permitido	No permitido	No permitidos
SESSION_VARIABLES_ADMIN	Permitido	Permitida	Permitida
SET_ANY_DEFINER	No disponible	No disponible	Permitido

Privilegio	MySQL 8.0.35 y versiones anteriores	MySQL 8.0.36 y versiones secundarias posteriores	MySQL 8.4.3 y posteriores
SET_USER_ID	Permitido	Permitida	No disponible
SHOW_ROUTINE	Permitido	Permitida	Permitida
SKIP_QUERY_REWRITE	No permitidos	No permitidos	No permitidos
SYSTEM_USER	No permitidos	No permitidos	No permitidos
SYSTEM_VARIABLES_ADMIN	No permitidos	No permitidos	No permitidos
TABLE_ENCRYPTION_ADMIN	No permitidos	No permitidos	No permitidos
TELEMETRY_LOG_ADMIN	Permitido	No permitido	No permitidos
TP_CONNECTION_ADMIN	No permitidos	No permitidos	No permitidos
TRANSACTION_GTID_TAG	No disponible	No disponible	No permitido
VERSION_TOKEN_ADMIN	No permitidos	No permitidos	No permitidos
XA_RECOVER_ADMIN	Permitido	Permitida	Permitida

Finalización de una sesión o una consulta de RDS para MySQL

Puede finalizar sesiones de usuario o consultas en instancias de bases de datos utilizando los comandos `rds_kill` y `rds_kill_query`. En primer lugar, conéctese a la instancia de la base de

datos MySQL y, a continuación, emita el comando adecuado como se muestra a continuación. Para obtener más información, consulte Conexión a la instancia de base de datos de MySQL.

```
CALL mysql.rds_kill(thread-ID)
CALL mysql.rds_kill_query(thread-ID)
```

Por ejemplo, para finalizar la sesión que se está ejecutando en el subproceso 99, debería escribir lo siguiente:

```
CALL mysql.rds_kill(99);
```

Para finalizar la consulta que se está ejecutando en el subproceso 99, debería escribir lo siguiente:

```
CALL mysql.rds_kill_query(99);
```

Omisión del error de replicación actual de RDS para MySQL

Puede omitir un error en la réplica de lectura si el error está haciendo que la réplica de lectura deje de responder y el error no afecta a la integridad de los datos.

> **Note**
>
> Primero verifique que el error en cuestión se puede omitir con seguridad. En una utilidad MySQL, conéctese a la réplica de lectura y ejecute el siguiente comando MySQL.
>
> ```
> SHOW REPLICA STATUS\G
> ```
>
> Para obtener información sobre los valores devueltos, consulte la documentación de MySQL. Las versiones anteriores de MySQL usaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MySQL anterior a la 8.0.23, utilice `SHOW SLAVE STATUS`.

Puede omitir un error en su réplica de lectura de las siguientes maneras.

Temas

- Llamar al procedimiento mysql.rds_skip_repl_error
- Configuración del parámetro slave_skip_errors

Llamar al procedimiento mysql.rds_skip_repl_error

Amazon RDS proporciona un procedimiento almacenado al que puede llamar para omitir un error en las réplicas de lectura. En primer lugar, conéctese a la réplica de lectura y, a continuación, emita los comandos correspondientes como se muestra a continuación. Para obtener más información, consulte Conexión a la instancia de base de datos de MySQL.

Para omitir el error, emita el siguiente comando.

```
CALL mysql.rds_skip_repl_error;
```

Este comando no tiene ningún efecto si lo ejecuta en la instancia de base de datos de origen o en una réplica de lectura en la que no se ha detectado un error de replicación.

Para obtener más información, como las versiones de MySQL que admiten `mysql.rds_skip_repl_error`, consulte mysql.rds_skip_repl_error.

> **Important**
>
> Si intenta llamar a `mysql.rds_skip_repl_error` y aparece el error `ERROR 1305 (42000): PROCEDURE mysql.rds_skip_repl_error does not exist`, actualice la instancia de la base de datos MySQL a la última versión secundaria o a una de las versiones secundarias mínimas que se indican en mysql.rds_skip_repl_error.

Configuración del parámetro slave_skip_errors

Para omitir uno o varios errores, puede configurar el parámetro estático `slave_skip_errors` en la réplica de lectura. Puede configurar este parámetro para omitir uno o varios códigos de error de replicación específicos. Actualmente, puede establecer este parámetro solo para instancias de bases de datos de RDS for MySQL 5.7. Después de cambiar la configuración de este parámetro, asegúrese de reiniciar su instancia de base de datos para que la nueva configuración surta efecto. Para obtener información sobre cómo funciona este parámetro, consulte la documentación de MySQL.

Recomendamos configurar este parámetro en un grupo de parámetros de base de datos independiente. Puede asociar este grupo de parámetros de base de datos solo a las réplicas de lectura que necesitan omitir errores. Seguir esta práctica recomendada reduce el impacto potencial en otras instancias de base de datos y réplicas de lectura.

> **Important**
>
> Establecer un valor no predeterminado para este parámetro puede provocar una incoherencia de la replicación. Establezca este parámetro solo en un valor no predeterminado si ha agotado otras opciones para resolver el problema y está seguro del posible impacto en los datos de la réplica de lectura.

Uso de espacios de tablas de InnoDB para mejorar los tiempos de recuperación tras un bloqueo de RDS para MySQL

Cada tabla de MySQL consta de una definición de tabla, datos e índices. El motor de almacenamiento InnoDB de MySQL almacena los datos y los índices de las tablas en un espacio de tabla. InnoDB crea un espacio de tablas global compartido que contiene un diccionario de datos y otros metadatos relevantes, y puede contener los datos e índices de las tablas. InnoDB también puede crear espacios de tabla independientes para cada tabla y partición. Estos espacios de tabla independientes se almacenan en archivos con la extensión .ibd y el encabezado de cada espacio de tabla contiene un número que lo identifica de forma inequívoca.

Amazon RDS proporciona un parámetro en un grupo de parámetros de MySQL denominado `innodb_file_per_table`. Este parámetro controla si InnoDB agrega los datos e índices de las tablas nuevas al espacio de tablas compartido (cuando se establece el valor del parámetro en 0) o a espacios de tabla individuales (cuando se establece el valor del parámetro en 1). Amazon RDS establece el valor predeterminado para el parámetro `innodb_file_per_table` en 1, que le permite eliminar tablas individuales de InnoDB y recuperar el almacenamiento utilizado por esas tablas para la instancia de base de datos. En la mayoría de los casos de uso, se recomienda establecer el parámetro `innodb_file_per_table` en 1.

Debe establecer el parámetro `innodb_file_per_table` en 0 si tiene un gran número de tablas, por ejemplo, más de 1 000 tablas si utiliza almacenamiento estándar (magnético) o SSD de uso general, o más de 10 000 tablas si utiliza almacenamiento de IOPS provisionadas. Cuando se establece este parámetro en 0, no se crean espacios de tabla individuales, y esto puede mejorar el tiempo que tarda la recuperación tras bloqueo de la base de datos.

MySQL procesa cada archivo de metadatos, lo que incluye los espacios de tabla, durante el ciclo de recuperación tras bloqueo. El tiempo que tarda MySQL en procesar la información de metadatos del espacio de tablas compartido es insignificante en comparación con el tiempo que tarda en procesar

miles de archivos de espacio de tabla si hay múltiples espacios de tabla. Debido a que el número del espacio de tabla se almacena en el encabezado de cada archivo, el tiempo global necesario para leer todos los archivos de espacios de tabla puede llegar a ser de varias horas. Por ejemplo, un millón de espacios de tabla de InnoDB en almacenamiento estándar pueden tardar entre cinco y ocho horas en procesarse durante un ciclo de recuperación tras bloqueo. En algunos casos, InnoDB puede determinar que necesita realizar una limpieza adicional después de un ciclo de recuperación tras bloqueo, por lo que iniciará otro ciclo que alargará el tiempo de recuperación. Tenga en cuenta que un ciclo de recuperación tras bloqueo, además del procesamiento de la información de los espacios de tabla, también conlleva la reversión de transacciones, la reparación de páginas dañadas y otras operaciones.

Dado que el parámetro `innodb_file_per_table` reside en un grupo de parámetros, puede cambiar el valor del parámetro editando el grupo de parámetros utilizado por la instancia de base de datos sin tener que reiniciarla. Después de cambiar la configuración, por ejemplo, de 1 (crear tablas individuales) a 0 (utilizar el espacio de tablas compartido), las tablas de InnoDB nuevas se añadirán al espacio de tablas compartido, mientras que las tablas existentes continuarán teniendo espacios de tabla individuales. Para mover una tabla InnoDB al espacio de tablas compartido, debe utilizar el comando `ALTER TABLE`.

Migración de varios espacios de tabla al espacio de tablas compartido

Puede mover los metadatos de una tabla de InnoDB desde su propio espacio de tabla al espacio de tablas compartido, lo que reconstruirá los metadatos de la tabla de acuerdo con el valor del parámetro `innodb_file_per_table`. En primer lugar, conéctese a la instancia de la base de datos MySQL y, a continuación, emita los comandos apropiados como se muestra a continuación. Para obtener más información, consulte Conexión a la instancia de base de datos de MySQL.

```
ALTER TABLE table_name ENGINE = InnoDB, ALGORITHM=COPY;
```

Por ejemplo, la siguiente consulta devuelve una instrucción `ALTER TABLE` para cada tabla de InnoDB que no está en el espacio de tablas compartido.

Para instancias de base de datos MySQL 5.7:

```
SELECT CONCAT('ALTER TABLE `',
REPLACE(LEFT(NAME , INSTR((NAME), '/') - 1), '`', '``'), '`.`',
REPLACE(SUBSTR(NAME FROM INSTR(NAME, '/') + 1), '`', '``'), '` ENGINE=InnoDB,
 ALGORITHM=COPY;') AS Query
FROM INFORMATION_SCHEMA.INNODB_SYS_TABLES
```

```
WHERE SPACE <> 0 AND LEFT(NAME, INSTR((NAME), '/') - 1) NOT IN ('mysql','');
```

Para instancias de base de datos MySQL 8.4 y 8.0:

```
SELECT CONCAT('ALTER TABLE `',
REPLACE(LEFT(NAME , INSTR((NAME), '/') - 1), '`', '``'), '`.`',
REPLACE(SUBSTR(NAME FROM INSTR(NAME, '/') + 1), '`', '``'), '` ENGINE=InnoDB,
 ALGORITHM=COPY;') AS Query
FROM INFORMATION_SCHEMA.INNODB_TABLES
WHERE SPACE <> 0 AND LEFT(NAME, INSTR((NAME), '/') - 1) NOT IN ('mysql','');
```

La reconstrucción de una tabla de MySQL para mover los metadatos de la tabla al espacio de tablas compartido requiere espacio de almacenamiento adicional temporalmente para reconstruir la tabla, por lo que la instancia de base de datos debe tener espacio de almacenamiento disponible. Durante la reconstrucción, la tabla está bloqueada e inaccesible para las consultas. Para las tablas pequeñas o las tablas a las que no se tiene acceso con frecuencia, esto puede no ser un problema. Para las tablas de gran tamaño o las tablas a las que se tiene acceso con frecuencia en un entorno con un gran número de accesos simultáneos, es posible reconstruir las tablas en una réplica de lectura.

Es posible crear una réplica de lectura y migrar los metadatos de las tablas al espacio de tablas compartido en la réplica de lectura. Aunque la instrucción ALTER TABLE bloquea el acceso en la réplica de lectura, la instancia de base de datos de origen no se ve afectada. La instancia de base de datos de origen continuará generando sus registros binarios, mientras que la réplica de lectura se retrasará con respecto a ella durante el proceso de reconstrucción de tablas. Dado que la reconstrucción requiere espacio de almacenamiento adicional y el archivo registro de reproducción puede ser muy grande, al crear una réplica de lectura, debe asignar una cantidad de almacenamiento mayor que la instancia de base de datos de origen.

Para crear una réplica de lectura y reconstruir las tablas de InnoDB para que utilicen el espacio de tablas compartido, siga estos pasos:

1. Asegúrese de que la retención de copias de seguridad esté habilitada en la instancia de base de datos de origen para que se active el registro binario.
2. Utilice la AWS Management Console o la AWS CLI para crear una réplica de lectura de la instancia de base de datos de origen. Dado que muchos de los procesos que conlleva la creación de una réplica de lectura coinciden con los de la recuperación tras bloqueo, el proceso de creación puede tardar cierto tiempo si hay un gran número de espacios de tabla de InnoDB. Asigne más espacio de almacenamiento en la réplica de lectura del que se utiliza actualmente en la instancia de base de datos de origen.

3. Cuando se haya creado la réplica de lectura, cree un grupo de parámetros con los valores `read_only = 0` y `innodb_file_per_table = 0`. A continuación, asocie el grupo de parámetros a la réplica de lectura.
4. Ejecute la siguiente instrucción SQL para todas las tablas que desea migrar en la réplica:

```
ALTER TABLE name ENGINE = InnoDB
```

5. Cuando hayan finalizado todas las instrucciones `ALTER TABLE` en la réplica de lectura, verifique que esta está conectada a la instancia de base de datos de origen y que las dos instancias están sincronizadas.
6. Utilice la consola o la CLI para convertir la réplica de lectura en la instancia. Asegúrese de que el grupo de parámetros utilizado para la nueva instancia de base de datos independiente tenga el parámetro `innodb_file_per_table` establecido en 0. Cambie el nombre de la nueva instancia de base de datos independiente y señale las aplicaciones a la nueva instancia de base de datos independiente.

Administración de Historial de estado global de RDS para MySQL

> **Tip**
>
> Para analizar el rendimiento de la base de datos, también puede utilizar Información de rendimiento en Amazon RDS. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.

MySQL mantiene muchas variables de estado que proporcionan información acerca de su funcionamiento. Su valor puede ayudarle a detectar problemas de bloqueo o de memoria en una instancia de base de datos. Los valores de estas variables de estado son acumulativos desde la última vez que se inició la instancia de base de datos. Puede restablecer la mayoría de las variables de estado a 0 utilizando el comando `FLUSH STATUS`.

Para permitir la monitorización de estos valores a lo largo del tiempo, Amazon RDS proporciona un conjunto de procedimientos que van creando snapshots de los valores de estas variables de estado y los escriben en una tabla, junto con cualquier cambio desde el último instantánea. Esta infraestructura, que se denomina Global Status History (GoSH), se instala en todas las instancias de bases de datos MySQL desde la versión 5.5.23. GoSH está deshabilitado de forma predeterminada.

Para habilitar GoSH, primero debe habilitar el programador de eventos desde un grupo de parámetros de base de datos estableciendo el parámetro `event_scheduler` en `ON`. Para las instancias de base de datos MySQL que ejecutan MySQL 5.7, configure también el parámetro `show_compatibility_56` en `1`. Para obtener información acerca de cómo crear y modificar un grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS. Para obtener información acerca de los efectos secundarios de la habilitación de este parámetro, consulte show_compatibility_56 en el Manual de referencia de MySQL 5.7.

A continuación, puede utilizar los procedimientos de la siguiente tabla para activar y configurar GoSH. En primer lugar, conéctese a la instancia de la base de datos MySQL y, a continuación, emita los comandos apropiados como se muestra a continuación. Para obtener más información, consulte Conexión a la instancia de base de datos de MySQL. Para cada procedimiento, ejecute el siguiente comando y sustituya *`procedure-name`*:

```
CALL procedure-name;
```

En la tabla siguiente se enumeran todos los procedimientos que puede utilizar para *`procedure-name`* en el comando anterior.

Procedimiento	Descripción
`mysql.rds_enable_gsh_collector`	Permite que GoSH tome los snapshots predeterminados con los intervalos especificados por `rds_set_gsh_collector` .
`mysql.rds_set_gsh_collector`	Especifica el intervalo, en minutos, entre snapshots. El valor predeterminado es 5.
`mysql.rds_disable_gsh_collector`	Desactiva los snapshots.
`mysql.rds_collect_global_status_history`	Toma una instantánea a petición.
`mysql.rds_enable_gsh_rotation`	Permite rotar el contenido de la tabla `mysql.rds_global_status_history` a `mysql.rds_global_status_history_old` con los intervalos especificados por `rds_set_gsh_rotation` .

Procedimiento	Descripción
`mysql.rds_set_gsh_rotation`	Especifica el intervalo, en días, entre rotaciones de la tabla. El valor predeterminado es 7.
`mysql.rds_disable_gsh_rotation`	Desactiva la rotación de la tabla.
`mysql.rds_rotate_global_status_history`	Rota el contenido de la tabla `mysql.rds_global_status_history` a `mysql.rds_global_status_history_old` a petición.

Cuando se ejecuta GoSH, es posible consultar las tablas en las que escribe. Por ejemplo, para consultar la tasa de aciertos del grupo del búfer Innodb, debería utilizar la siguiente consulta:

```
select a.collection_end, a.collection_start, (( a.variable_Delta-b.variable_delta)/
a.variable_delta)*100 as "HitRatio"
    from mysql.rds_global_status_history as a join mysql.rds_global_status_history as b
 on a.collection_end = b.collection_end
    where a. variable_name = 'Innodb_buffer_pool_read_requests' and b.variable_name =
 'Innodb_buffer_pool_reads'
```

Configuración del tamaño del grupo de búferes y la capacidad de registros redo en MySQL 8.4

En MySQL 8.4, Amazon RDS habilita el parámetro `innodb_dedicated_server` de forma predeterminada. Con el parámetro `innodb_dedicated_server`, el motor de base de datos calcula los parámetros `innodb_buffer_pool_size` y `innodb_redo_log_capacity`. Para obtener información sobre cómo se calculan estos parámetros, consulte Configuring InnoDB Buffer Pool Size y Redo Log en la documentación de MySQL.

Si `innodb_dedicated_server` está activado, el parámetro `innodb_buffer_pool_size` se calcula en función de la memoria de clases de la instancia de base de datos. En la siguiente tabla, se muestra la memoria de servidor detectada y el tamaño del grupo de búferes correspondiente.

Memoria de servidor detectada	Tamaño del grupo de búferes
<1 GB	El valor predeterminado es 128 MB
De 1 GB a 4 GB	*Memoria de servidor detectada* * 0,5
>4 GB	*Memoria de servidor detectada* * 0,75

El parámetro `innodb_redo_log_capacity` se escala automáticamente con la clase de instancia a (número de vCPU/2) GB hasta un máximo de 16 GB. Las clases de instancias más grandes tienen una mayor capacidad de rehacer registros, lo que puede mejorar el rendimiento y la resiliencia para las cargas de trabajo con un uso intensivo de escritura.

Antes de actualizar de MySQL 8.0 a MySQL 8.4, asegúrese de aumentar el espacio de almacenamiento para dar cabida a un posible aumento del tamaño de los registros redo que podría producirse una vez finalizada la actualización. Para obtener más información, consulte Aumento de la capacidad de almacenamiento de la instancia de base de datos.

Si no quiere que el parámetro `innodb_dedicated_server` calcule los valores de los parámetros `innodb_buffer_pool_size` y `innodb_redo_log_capacity`, puede anular estos valores configurando valores específicos para ellos en un grupo de parámetros personalizado. Como alternativa, puede deshabilitar el parámetro `innodb_dedicated_server` y establecer valores para los parámetros `innodb_buffer_pool_size` y `innodb_redo_log_capacity` en un grupo de parámetros personalizado. Para obtener más información, consulte Grupos de parámetros predeterminados y personalizados.

Si deshabilita el parámetro `innodb_dedicated_server` configurándolo como `0` y no establece valores para los parámetros `innodb_buffer_pool_size` y `innodb_redo_log_capacity`, Amazon RDS establece los dos últimos parámetros en 128 MB y 100 MB, respectivamente. Estos valores predeterminados se traducen en un rendimiento deficiente en clases de instancias más grandes.

Zona horaria local para las instancias de bases de datos MySQL

De manera predeterminada, la zona horaria para una instancia de base de datos de MySQL es el horario universal coordinado (UTC). En su lugar, puede definir la zona horaria de su instancia de base de datos en la zona horaria local de su aplicación.

Para definir la zona horaria local para una instancia de base de datos, configure el parámetro `time_zone` del grupo de parámetros de la instancia de base de datos en uno de los valores admitidos que se indican más adelante en esta sección. Al configurar el parámetro `time_zone` de un grupo de parámetros, todas las instancias de base de datos y réplicas de lectura que utilizan ese grupo de parámetros cambian para utilizar la nueva zona horaria local. Para obtener información acerca de cómo configurar los parámetros de un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.

Después de definir la zona horaria local, todas las conexiones nuevas con la base de datos reflejarán el cambio. Si tiene alguna conexión con la base de datos abierta al cambiar la zona horaria local, no verá la actualización de la zona horaria local hasta que cierre la conexión y abra una nueva conexión.

Puede definir una zona horaria local diferente para una instancia de base de datos y una o varias de sus réplicas de lectura. Para ello, utilice un grupo de parámetros diferente para la instancia de base de datos y para la réplica o las réplicas y establezca el parámetro `time_zone` de cada grupo de parámetros en una zona horaria local distinta.

Si se replica en las Regiones de AWS, la instancia de base de datos de origen y la réplica de lectura utilizan diferentes grupos de parámetros (los grupos de parámetros son exclusivos de una Región de AWS). Para usar la misma zona horaria local para cada instancia, debe configurar el parámetro `time_zone` en los grupos de parámetros de la instancia y de la réplica de lectura.

Cuando se restaura una instancia de base de datos desde una instantánea de base de datos, la zona horaria local se define como UTC. Podrá actualizar la zona horaria a su zona horaria local una vez que se haya completado la restauración. Si restaura una instancia de base de datos a un momento dado, la zona horaria local de la instancia de base de datos restaurada será el ajuste de zona horaria del grupo de parámetros de la instancia de base de datos restaurada.

Internet Assigned Numbers Authority (Autoridad de Números Asignados en Internet, IANA por sus siglas en inglés) publica nuevas zonas horarias en https://www.iana.org/time-zones varias veces al año. Cada vez que RDS publica una nueva versión secundaria de mantenimiento de MySQL,

incluye los datos de zona horaria más recientes en el momento de la publicación. Cuando utiliza las versiones más recientes de RDS para MySQL, dispone de datos de zona horaria recientes de RDS. Para garantizar que la instancia de base de datos tenga datos de zona horaria recientes, se recomienda actualizar a una versión posterior del motor de base de datos. Como alternativa, puede modificar las tablas de zonas horarias en las instancias de base de datos de MariaDB manualmente. Para ello, puede utilizar comandos SQL o ejecutar la herramienta mysql_tzinfo_to_sql en un cliente SQL. Tras actualizar los datos de la zona horaria de forma manual, reinicie la instancia de base de datos para que los cambios se apliquen. RDS no modifica ni restablece los datos de zona horaria de las instancias de base de datos en ejecución. Los nuevos datos de zona horaria solo se instalan cuando se actualiza la versión del motor de base de datos.

Puede definir su zona horaria local en uno de los valores siguientes.

Zona	Time zone (Zona horarioa)
África	África/El Cairo, África/Casablanca, África/Harare, África/Monrovia, África/Nairobi, África/Trípoli, África/Windhoek
América	América/Araguaína, América/Asunción, América/Bogotá, América/Buenos_Aires, América/Caracas, América/Chihuahua, América/Cuiabá, América/Denver, América/Fortaleza, América/Guatemala, América/Halifax, América/Manaos, América/Matamoros, América/Monterrey, América/Montevideo, América/Phoenix, América/Santiago, América/Tijuana
Asia	Asia/Amán, Asia/Asjabad, Asia/Bagdad, Asia/Bakú, Asia/Bangkok, Asia/Beirut, Asia/Calcuta, Asia/Daca, Asia/Damasco, Asia/Ereván, Asia/Irkutsk, Asia/Jerusalén, Asia/Kabul, Asia/Karachi, Asia/Katmandú, Asia/Krasnoyarsk, Asia/Magadán, Asia/Mascate, Asia/Novosibirsk, Asia/Riad, Asia/Seúl, Asia/Shanghái, Asia/Singapur, Asia/Taipéi, Asia/Teherán, Asia/Tokio, Asia/Ulán_Bator, Asia/Vladivostok, Asia/Yakutsk
Atlántico	Atlántico/Azores
Australia	Australia/Adelaida, Australia/Brisbane, Australia/Darwin, Australia/Hobart, Australia/Perth, Australia/Sídney
Brasil	Brasil/DeNoronha, Brasil/Este
Canadá	Canadá/Terranova, Canadá/Saskatchewan, Canadá/Yukón

Zona	Time zone (Zona horarioa)
Europa	Europa/Ámsterdam, Europa/Atenas, Europa/Dublín, Europa/Helsinki, Europa/Estambul, Europa/ Kaliningrado, Europa/Moscú, Europa/París, Europa/Praga, Europa/Sarajevo
Pacífico	Pacífico/Auckland, Pacífico/Fiyi, Pacífico/Guam, Pacífico/Honolulu, Pacífico/Samoa
EE. UU.	EE. UU./Alaska, EE. UU./Central, EE. UU./Indiana-Este, EE. UU./Este, EE. UU./Pacífico
UTC	UTC

Problemas conocidos y limitaciones para Amazon RDS para MySQL

Los siguientes son problemas conocidos y limitaciones para el uso en Amazon RDS para MySQL.

Temas

- Palabra reservada InnoDB
- Comportamiento completo del almacenamiento de información para Amazon RDS for MySQL
- Incoherencia en el tamaño del grupo de búfer de InnoDB
- La optimización de combinación de índice devuelve resultados incorrectos
- Excepciones en los parámetros de MySQL para las instancias de base de datos de Amazon RDS
- Límites de tamaño de archivo de MySQL en Amazon RDS
- Complemento de llavero de MySQL no compatible
- Puertos personalizados
- Limitaciones del procedimiento almacenado de MySQL
- Replicación basada en GTID con una instancia de origen externa
- Complemento de autenticación predeterminado de MySQL
- Anulación de innodb_buffer_pool_size
- Actualización de MySQL 5.7 a MySQL 8.4
- Compresión de página de InnoDB

Palabra reservada InnoDB

`InnoDB` es una palabra reservada para RDS para MySQL. No puede utilizar este nombre para una base de datos MySQL.

Comportamiento completo del almacenamiento de información para Amazon RDS for MySQL

Cuando el almacenamiento se llena para una instancia de base de datos MySQL, puede haber inconsistencias de metadatos, descoincidencias de diccionario y tablas huérfanas. Para evitar estos problemas, detiene Amazon RDS automáticamente una instancia de base de datos que alcanza el `storage-full` estado.

Una instancia de base de datos MySQL alcanza el `storage-full` estado en los siguientes casos:

- La instancia de base de datos tiene menos de 20.000 MiB de almacenamiento y el almacenamiento disponible alcanza 200 MiB o menos.
- La instancia de base de datos tiene más de 102.400 MiB de almacenamiento y el almacenamiento disponible alcanza 1024 MiB o menos.
- La instancia de base de datos tiene entre 20.000 MiB y 102.400 MiB de almacenamiento, y tiene menos del 1 % del almacenamiento disponible.

Después de Amazon RDS detener una instancia de base de datos automáticamente porque alcanzó el `storage-full` estado, aún puede modificarla. Para reiniciar la instancia de base de datos, complete al menos una de las siguientes opciones:

- Modifique la instancia de base de datos para habilitar el escalado automático del almacenamiento.

  Para obtener más información sobre el escalado automático del almacenamiento, consulte Administración automática de la capacidad con el escalado automático de almacenamiento de Amazon RDS.
- Modifique la instancia de base de datos para aumentar su capacidad de almacenamiento.

  Para obtener más información sobre el aumento de la capacidad de almacenamiento, consulte Aumento de la capacidad de almacenamiento de la instancia de base de datos.

Después de realizar uno de estos cambios, la instancia de base de datos se reinicia automáticamente. Para obtener más información acerca de la modificación de una instancia de base de datos , consulte Modificación de una instancia de base de datos de Amazon RDS.

Incoherencia en el tamaño del grupo de búfer de InnoDB

En MySQL 5.7, existe actualmente un error en el modo en que se administra el tamaño del grupo de búfer de InnoDB. MySQL 5.7 puede establecer en el parámetro `innodb_buffer_pool_size` un valor elevado que puede provocar que el grupo de búfer de InnoDB crezca demasiado y ocupe demasiada memoria. Este efecto puede hacer que el motor de base de datos MySQL deje de funcionar o impedir que se inicie. El problema es más común en las clases de instancia de base de datos que tienen poca memoria disponible.

Para resolverlo, defina como valor del parámetro `innodb_buffer_pool_size` un múltiplo del valor resultante de multiplicar `innodb_buffer_pool_instances` por

`innodb_buffer_pool_chunk_size`. Por ejemplo, puede definir como valor de `innodb_buffer_pool_size` ocho veces el producto de `innodb_buffer_pool_instances` por `innodb_buffer_pool_chunk_size`, como se indica en el ejemplo siguiente.

```
innodb_buffer_pool_chunk_size = 536870912
innodb_buffer_pool_instances = 4
innodb_buffer_pool_size = (536870912 * 4) * 8 = 17179869184
```

Para obtener más detalles sobre este error de MySQL 5.7, consulte https://bugs.mysql.com/bug.php?id=79379 en la documentación de MySQL.

La optimización de combinación de índice devuelve resultados incorrectos

Las consultas que utilizan la optimización de combinación de índice podrían devolver resultados incorrectos debido a un error en el optimizador de consultas de MySQL introducidos en MySQL 5.5.37. Cuando realiza una consulta en una tabla con múltiples índices, el optimizador examina rangos de filas según múltiples índices, pero no combina los resultados correctamente. Para obtener más información acerca del error del optimizador de consultas, consulte http://bugs.mysql.com/bug.php?id=72745 y http://bugs.mysql.com/bug.php?id=68194 en la base de datos de errores de MySQL.

Por ejemplo, imagine una consulta en una tabla con dos índices donde los argumentos de la búsqueda hacen referencia a las columnas indexadas.

```
SELECT * FROM table1
WHERE indexed_col1 = 'value1' AND indexed_col2 = 'value2';
```

En este caso, el motor de búsqueda buscará en los dos índices. Sin embargo, debido al error, los resultados combinados son incorrectos.

Para resolver este problema, puede seguir uno de estos pasos:

- Establezca en el parámetro `optimizer_switch` el valor `index_merge=off` en el grupo de parámetros de base de datos de la instancia MySQL. Para obtener información acerca de cómo configurar los parámetros de un grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.
- Actualice la instancia de base de datos MySQL a la versión de MySQL 5.7 u 8.0. Para obtener más información, consulte Actualizaciones del motor de base de datos de RDS para MySQL.

- Si no puede actualizar la instancia ni cambiar el parámetro `optimizer_switch`, puede evitar el error identificando explícitamente un índice para la consulta, por ejemplo:

```
SELECT * FROM table1
USE INDEX covering_index
WHERE indexed_col1 = 'value1' AND indexed_col2 = 'value2';
```

Para obtener más información, consulte Index merge optimization (Optimización de combinación de índice) en la documentación de MySQL.

Excepciones en los parámetros de MySQL para las instancias de base de datos de Amazon RDS

Algunos parámetros de MySQL requieren consideraciones especiales cuando se usan en una instancia de base de datos de Amazon RDS.

lower_case_table_names

Debido a que en el sistema de archivos de Amazon RDS se distingue entre mayúsculas y minúsculas, en el parámetro `lower_case_table_names` no se admite el valor 2 (los nombres se almacenan como se especifican pero se comparan en minúsculas). Los siguientes valores se admiten para instancias de base de datos de Amazon RDS para MySQL:

- 0 (nombres almacenados como se indican y las comparaciones distinguen de mayúsculas y minúsculas) se admite para todas las versiones de para MySQL.
- 1 (los nombres almacenados en minúsculas y las comparaciones no distinguen entre mayúsculas y minúsculas) es compatible con las versiones 5.7, 8.0.28 y posteriores de la versión 8.0 y versiones 8.4.

El parámetro `lower_case_table_names` debe definirse como parte de un grupo de parámetros de base de datos personalizado antes de crear una instancia de base de datos. Después, especifique el grupo de parámetros de base de datos personalizado al crear la instancia de base de datos.

Cuando un grupo de parámetros está asociado a una instancia de base de datos de MySQL con una versión inferior a 8.0, le recomendamos que evite cambiar el parámetro `lower_case_table_names` en el grupo de parámetros. Al cambiarlo, podría provocar

incoherencias con las copias de seguridad de restauración a un momento dado y con las instancias de base de datos de réplica de lectura.

Cuando un grupo de parámetros está asociado a una instancia de base de datos de MySQL con una versión 8.0 u 8.4, no puede cambiar el parámetro `lower_case_table_names` en el grupo de parámetros.

En las réplicas de lectura siempre debe usarse el mismo valor del parámetro `lower_case_table_names` que en la instancia de base de datos de origen.

long_query_time

En el parámetro `long_query_time` puede establecer un valor en coma flotante para poder registrar las consultas lentas en el registro de consultas lentas de MySQL con una resolución de microsegundos. Por ejemplo, el valor 0,1 corresponde a 100 milisegundos, lo que ayuda a depurar transacciones lentas que duran menos de un segundo.

Límites de tamaño de archivo de MySQL en Amazon RDS

Para las instancias de base de datos MySQL 8.0 y superiores, el tamaño máximo de archivo es de 16 TiB. Cuando se utilizan espacios de tablas archivo por tabla, el tamaño máximo de archivo limita el tamaño de una tabla de InnoDB a 16 TiB. Los espacios fila-por-tabla de InnoDB (en los que las tablas están cada una en el propio espacio de tabla) se habilitan de manera predeterminada para las instancias de base de datos MySQL. Para obtener más información, consulte InnoDB Limits en la documentación de MySQL.

> **Note**
>
> Algunas instancias de base de datos existentes tienen un límite inferior. Por ejemplo, las instancias de base de datos MySQL creadas antes de abril de 2014 tienen un límite de tamaño de tabla y de archivo de 2 TB. Este límite de tamaño de archivo de 2 TB también afecta a las instancias de base de datos o las réplicas de lectura creadas a partir de instantáneas de base de datos tomadas antes de abril de 2014, con independencia de cuándo se creó la instancia de base de datos.

El uso de los espacios de tabla file-per-table de InnoDB tiene pros y contras en función de la aplicación. Para determinar el mejor método para su aplicación, consulte File-Per-Table Tablespaces en la documentación de MySQL.

No es recomendable permitir que las tablas crezcan hasta el tamaño de archivo máximo. En general, es preferible dividir los datos en tablas más pequeñas, que pueden mejorar el desempeño y los tiempos de recuperación.

Una opción que se puede usar para dividir una tabla grande en tablas más pequeñas es la creación de particiones. Las particiones distribuyen las porciones de una tabla grande en archivos independientes en función de las reglas que se hayan especificado. Por ejemplo, si almacena las transacciones por fecha, puede crear reglas de partición que distribuyan las transacciones más antiguas entre distintos archivos por medio de la creación de particiones. Después, periódicamente, se pueden archivar los datos de transacciones históricos que no tengan que estar disponibles de forma inmediata para su aplicación. Para obtener información, consulte Partitioning en la documentación de MySQL.

Como no existe una sola tabla o vista del sistema que proporcione el tamaño de todas las tablas y del espacio de tablas del sistema InnoDB, debe consultar varias tablas para determinar el tamaño de los espacios de tablas.

Determinación del tamaño del espacio de tablas del sistema InnoDB y del espacio de tablas del diccionario de datos

- Utilice el comando SQL siguiente para determinar si algún espacio de tablas es demasiado grande y por lo tanto es candidato para particiones.

  > **Note**
  >
  > El espacio de tabla del diccionario de datos es específico de MySQL 8.0 y versiones posteriores.

```
select FILE_NAME,TABLESPACE_NAME, ROUND(((TOTAL_EXTENTS*EXTENT_SIZE)
/1024/1024/1024), 2)  as "File Size (GB)" from information_schema.FILES
where tablespace_name in ('mysql','innodb_system');
```

Para determinar el tamaño de las tablas de usuario de InnoDB fuera del espacio de tablas del sistema InnoDB (para las versiones de MySQL 5.7)

- Utilice el comando SQL siguiente para determinar si alguna de las tablas es demasiado grande y por lo tanto es candidata para particiones.

```
SELECT SPACE,NAME,ROUND((ALLOCATED_SIZE/1024/1024/1024), 2)
as "Tablespace Size (GB)"
FROM information_schema.INNODB_SYS_TABLESPACES ORDER BY 3 DESC;
```

Determinación del tamaño de las tablas de usuario de InnoDB fuera del espacio de tabla del sistema InnoDB (para las versiones de MySQL 8.0 y posteriores)

- Utilice el comando SQL siguiente para determinar si alguna de las tablas es demasiado grande y por lo tanto es candidata para particiones.

```
SELECT SPACE,NAME,ROUND((ALLOCATED_SIZE/1024/1024/1024), 2)
as "Tablespace Size (GB)"
FROM information_schema.INNODB_TABLESPACES ORDER BY 3 DESC;
```

Para determinar el tamaño de las tablas de usuario distintas de InnoDB

- Utilice el siguiente comando SQL para determinar si alguna de las tablas distintas de InnoDB es demasiado grande.

```
SELECT TABLE_SCHEMA, TABLE_NAME, round(((DATA_LENGTH + INDEX_LENGTH+DATA_FREE)
/ 1024 / 1024/ 1024), 2) As "Approximate size (GB)" FROM information_schema.TABLES
WHERE TABLE_SCHEMA NOT IN ('mysql', 'information_schema', 'performance_schema')
and ENGINE<>'InnoDB';
```

Para habilitar espacios de tablas file-per-table de InnoDB

- Establezca el parámetro innodb_file_per_table en 1 en el grupo de parámetros para la instancia de base de datos.

Para deshabilitar los espacios de tablas file-per-table de InnoDB

- Establezca el parámetro innodb_file_per_table en `0` en el grupo de parámetros para la instancia de base de datos.

Para obtener más información acerca de la actualización de un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.

Cuando haya habilitado o deshabilitado espacios de tablas file-per-table de InnoDB, puede ejecutar el comando `ALTER TABLE` para mover una tabla del espacio de tablas global a su propio espacio de tablas o viceversa, como se muestra en el ejemplo siguiente:

```
ALTER TABLE table_name TABLESPACE=innodb_file_per_table;
```

Complemento de llavero de MySQL no compatible

Actualmente, Amazon RDS para MySQL no admite el complemento de llavero de Amazon Web Services `keyring_aws` de MySQL.

Puertos personalizados

Amazon RDS bloquea las conexiones al puerto personalizado 33060 para el motor de MySQL. Elija un puerto diferente para su motor de MySQL.

Limitaciones del procedimiento almacenado de MySQL

Los procedimientos almacenados mysql.rds_kill y mysql.rds_kill_query no pueden finalizar las sesiones o consultas propiedad de usuarios de MySQL con nombres de usuario de más de 16 caracteres en las siguientes versiones de RDS para MySQL:

- Versión 8.0.32 y anteriores a la 8
- Versión 5.7.41 y anteriores a 5.7

Replicación basada en GTID con una instancia de origen externa

Amazon RDS admite la replicación basada en identificadores de transacciones globales (GTID) desde una instancia de MySQL externa en una instancia de base de datos de Amazon RDS para MySQL que requiere el ajuste de GTID_PURGED durante la configuración. Sin embargo, solo la versión 8.0.37 y versiones posteriores de RDS para MySQL admiten esta funcionalidad.

Complemento de autenticación predeterminado de MySQL

Las versiones 8.0.34 y las versiones 8.0 posteriores de RDS para MySQL utilizan el complemento `mysql_native_password`. No se puede cambiar la configuración de `default_authentication_plugin`.

La versión 8.4 y las versiones posteriores de RDS para MySQL utilizan el complemento `caching_sha2_password` como complemento de autenticación predeterminado. Puede cambiar el complemento de autenticación predeterminado de MySQL 8.4. El complemento `mysql_native_password` sigue funcionando con MySQL 8.4, pero el soporte de este complemento finaliza con MySQL 8.4. Para cambiar el complemento de autenticación predeterminado, cree un grupo de parámetros personalizado y modifique el valor del parámetro `authentication_policy`. Para obtener más información, consulte the section called “Grupos de parámetros predeterminados y personalizados”.

Anulación de innodb_buffer_pool_size

En el caso de las clases de microinstancias o instancias pequeñas de base de datos, el valor predeterminado del parámetro `innodb_buffer_pool_size` puede diferir del valor devuelto al ejecutar el siguiente comando:

```
mysql> SELECT @@innodb_buffer_pool_size;
```

Esta diferencia puede producirse cuando Amazon RDS necesita anular el valor predeterminado como parte de la administración de las clases de instancias de base de datos. Si es necesario, puede anular el valor predeterminado y establecerlo en un valor que admita la clase de instancia de base de datos. Para determinar un valor válido, añada el uso de memoria y la memoria total disponible en la instancia de base de datos. Para obtener más información, consulte Tipos de instancias de Amazon RDS.

Si su instancia de base de datos tiene solo 4 GB de memoria, no puede configurar `innodb_buffer_pool_size` en 8 GB, pero puede configurarla en 3 GB, en función de la cantidad de memoria que haya asignado a otros parámetros.

Si el valor que introduce es demasiado grande, Amazon RDS lo reduce a los siguientes límites:

- Clases de microinstancias de base de datos: 256 MB
- Clases de instancias de base de datos db.t4g.micro: 128 MB

Actualización de MySQL 5.7 a MySQL 8.4

No puede actualizar directamente de MySQL 5.7 a MySQL 8.4. Debe actualizar primero desde MySQL 5.7 a MySQL 8.0 y, a continuación, actualizar de MySQL 8.0 a MySQL 8.4. Para obtener más información, consulte Actualizaciones de versiones principales de RDS para MySQL.

Compresión de página de InnoDB

La compresión de páginas de InnoDB no funciona con las instancias de base de datos de Amazon RDS que tienen un tamaño de bloque del sistema de archivos de 16 000 porque el tamaño del bloque del sistema de archivos debe ser menor que el tamaño de la página de InnoDB. A partir de febrero de 2024, todas las instancias de bases de datos recién creadas tendrán un tamaño de bloque del sistema de archivos de 16 000, lo que aumenta el rendimiento y reduce el consumo de IOPS durante las descargas de páginas.

Referencia de procedimientos almacenados de RDS para MySQL

En estos temas, se describen los procedimientos almacenados del sistema que están disponibles para las instancias de Amazon RDS que ejecutan el motor de base de datos de MySQL. El usuario maestro debe ejecutar estos procedimientos.

Temas

- Recopilación y mantenimiento del historial de estado global
- Configuración, inicio y detención de la replicación del registro binario (binlog)
- Finalización de una sesión o una consulta
- Administración de clústeres activo-activo
- Administración de la replicación de varios orígenes
- Replicación de transacciones mediante GTID
- Rotación de los registros de consultas
- Establecimiento y muestra de la configuración del registro binario
- Calentamiento de caché de InnoDB

Recopilación y mantenimiento del historial de estado global

Amazon RDS proporciona un conjunto de procedimientos que crean instantáneas de los valores de las variables de estado a lo largo del tiempo y los escriben en una tabla, junto con cualquier cambio desde la última instantánea. Esta infraestructura se denomina Historial de estado global. Para obtener más información, consulte Administración de Historial de estado global de RDS para MySQL (Administrar el historial de estado global).

Los siguientes procedimientos almacenados administran la forma en que se recopila y mantiene el historial de estado global.

Temas

- mysql.rds_collect_global_status_history
- mysql.rds_disable_gsh_collector
- mysql.rds_disable_gsh_rotation
- mysql.rds_enable_gsh_collector
- mysql.rds_enable_gsh_rotation
- mysql.rds_rotate_global_status_history
- mysql.rds_set_gsh_collector
- mysql.rds_set_gsh_rotation

mysql.rds_collect_global_status_history

Toma una instantánea bajo demanda para el historial de estado global.

Sintaxis

```
CALL mysql.rds_collect_global_status_history;
```

mysql.rds_disable_gsh_collector

Desactiva las instantáneas tomadas por el historial de estado global.

Sintaxis

```
CALL mysql.rds_disable_gsh_collector;
```

mysql.rds_disable_gsh_rotation

Desactiva la rotación de la tabla `mysql.global_status_history`.

Sintaxis

```
CALL mysql.rds_disable_gsh_rotation;
```

mysql.rds_enable_gsh_collector

Activa el historial de estado global para tomar instantáneas predeterminadas a los intervalos especificados por `rds_set_gsh_collector`.

Sintaxis

```
CALL mysql.rds_enable_gsh_collector;
```

mysql.rds_enable_gsh_rotation

Activa la rotación del contenido de la tabla `mysql.global_status_history` a `mysql.global_status_history_old` a los intervalos especificados por `rds_set_gsh_rotation`.

Sintaxis

```
CALL mysql.rds_enable_gsh_rotation;
```

mysql.rds_rotate_global_status_history

Rota el contenido de la tabla `mysql.global_status_history` a `mysql.global_status_history_old` a petición.

Sintaxis

```
CALL mysql.rds_rotate_global_status_history;
```

mysql.rds_set_gsh_collector

Especifica el intervalo, en minutos, entre las instantáneas tomadas por el historial de estado global.

Sintaxis

```
CALL mysql.rds_set_gsh_collector(intervalPeriod);
```

Parámetros

intervalPeriod

El intervalo, en minutos, entre snapshots. El valor predeterminado es 5.

mysql.rds_set_gsh_rotation

Especifica el intervalo, en días, entre rotaciones de la tabla `mysql.global_status_history`.

Sintaxis

```
CALL mysql.rds_set_gsh_rotation(intervalPeriod);
```

Parámetros

intervalPeriod

El intervalo, en días, entre rotaciones de la tabla. El valor predeterminado es 7.

Configuración, inicio y detención de la replicación del registro binario (binlog)

Los siguientes procedimientos almacenados controlan la forma en la que se replican las transacciones desde una base de datos externa en RDS para MySQL o desde RDS para MySQL a una base de datos externa.

Cuando utilice estos procedimientos almacenados para administrar la replicación con un usuario de replicación configurado con `caching_sha2_password`, debe configurar TLS especificando `SOURCE_SSL=1`. `caching_sha2_password` es el complemento de autenticación predeterminado de RDS para MySQL 8.4. Para obtener más información, consulte Cifrado con SSL/TLS.

Para obtener más información acerca de la configuración, el uso y la administración de réplicas de lectura, consulte the section called “Réplicas de lectura de MySQL”.

Temas

- mysql.rds_next_master_log (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_next_source_log (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_external_master_with_auto_position (RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source_with_auto_position (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source_with_delay (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_external_source_gtid_purged

- mysql.rds_set_master_auto_position (RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_source_auto_position (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_source_delay
- mysql.rds_skip_repl_error
- mysql.rds_start_replication
- mysql.rds_start_replication_until
- mysql.rds_stop_replication

mysql.rds_next_master_log (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)

Cambia la posición del registro de instancia de base de datos de origen al inicio del siguiente registro binario en la instancia de base de datos de origen. Use este procedimiento únicamente si aparece el error de E/S de replicación 1236 en una réplica de lectura.

Sintaxis

```
CALL mysql.rds_next_master_log(
curr_master_log
);
```

Parámetros

curr_master_log

El índice del archivo de registro maestro actual. Por ejemplo, si el nombre del archivo actual es `mysql-bin-changelog.012345`, el índice es 12345. Para determinar el nombre del archivo de log maestro actual, ejecute el comando `SHOW REPLICA STATUS` y vea el campo `Master_Log_File`.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_next_master_log`.

> **Warning**
>
> Llame a `mysql.rds_next_master_log` solo si la replicación deja de funcionar tras una conmutación por error de una instancia de base de datos Multi-AZ que es el origen de la replicación y el campo `Last_IO_Errno` de `SHOW REPLICA STATUS` muestra el error de E/S 1236.
>
> La llamada a `mysql.rds_next_master_log` puede provocar una pérdida de datos en la réplica de lectura si las transacciones de la instancia de origen no se escribieron en el registro binario en el disco antes del evento de conmutación por error. Puede reducir el riesgo de que esto ocurra configurando los parámetros de la instancia de origen `sync_binlog` y `innodb_support_xa` en `1`, aunque esto podría reducir el rendimiento. Para obtener más información, consulte Solución de problemas de réplicas de lectura de MySQL.

Ejemplos

Supongamos que la replicación falla en una réplica de lectura de RDS para MySQL . La ejecución de `SHOW REPLICA STATUS\G` en la réplica de lectura devuelve el siguiente resultado:

```
*************************** 1. row ***************************
             Replica_IO_State:
                  Source_Host: myhost.XXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
                  Source_User: MasterUser
                  Source_Port: 3306
                Connect_Retry: 10
              Source_Log_File: mysql-bin-changelog.012345
          Read_Source_Log_Pos: 1219393
               Relay_Log_File: relaylog.012340
                Relay_Log_Pos: 30223388
        Relay_Source_Log_File: mysql-bin-changelog.012345
           Replica_IO_Running: No
          Replica_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
```

```
                  Skip_Counter: 0
           Exec_Source_Log_Pos: 30223232
               Relay_Log_Space: 5248928866
               Until_Condition: None
                Until_Log_File:
                 Until_Log_Pos: 0
            Source_SSL_Allowed: No
            Source_SSL_CA_File:
            Source_SSL_CA_Path:
               Source_SSL_Cert:
             Source_SSL_Cipher:
                Source_SSL_Key:
         Seconds_Behind_Master: NULL
Source_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 1236
                Last_IO_Error: Got fatal error 1236 from master when reading data from
 binary log: 'Client requested master to start replication from impossible position;
 the first event 'mysql-bin-changelog.013406' at 1219393, the last event read from
 '/rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4, the last byte read from '/
rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4.'
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Source_Server_Id: 67285976
```

El campo `Last_IO_Errno` muestra que la instancia ha recibido el error de E/S 1236. El campo `Master_Log_File` muestra que el nombre de archivo es `mysql-bin-changelog.012345`, lo que significa que el índice del archivo de registro es `12345`. Para resolver el error, puede llamar a `mysql.rds_next_master_log` con el siguiente parámetro:

```
CALL mysql.rds_next_master_log(12345);
```

mysql.rds_next_source_log (RDS para las versiones principales de MySQL 8.4 y superiores)

Cambia la posición del registro de instancia de base de datos de origen al inicio del siguiente registro binario en la instancia de base de datos de origen. Use este procedimiento únicamente si aparece el error de E/S de replicación 1236 en una réplica de lectura.

Sintaxis

```
CALL mysql.rds_next_source_log(
curr_source_log
);
```

Parámetros

curr_source_log

El índice del archivo de registro de origen actual. Por ejemplo, si el nombre del archivo actual es `mysql-bin-changelog.012345`, el índice es 12345. Para determinar el nombre del archivo de registro de origen actual, ejecute el comando `SHOW REPLICA STATUS` y vea el campo `Source_Log_File`.

Notas de uso

El usuario administrativo debe ejecutar el procedimiento `mysql.rds_next_source_log`.

> **Warning**
>
> Llame a `mysql.rds_next_source_log` solo si la replicación deja de funcionar tras una conmutación por error de una instancia de base de datos Multi-AZ que es el origen de la replicación y el campo `Last_IO_Errno` de `SHOW REPLICA STATUS` muestra el error de E/S 1236.
> La llamada a `mysql.rds_next_source_log` puede provocar una pérdida de datos en la réplica de lectura si las transacciones de la instancia de origen no se escribieron en el registro binario en el disco antes del evento de conmutación por error. Puede reducir el riesgo de que esto ocurra configurando los parámetros de la instancia de origen `sync_binlog` y `innodb_support_xa` en 1, aunque esto podría reducir el rendimiento. Para obtener más información, consulte Solución de problemas de réplicas de lectura de MySQL.

Ejemplos

Supongamos que la replicación falla en una réplica de lectura de RDS para MySQL . La ejecución de `SHOW REPLICA STATUS\G` en la réplica de lectura devuelve el siguiente resultado:

```
*************************** 1. row ***************************
             Replica_IO_State:
```

```
                  Source_Host: myhost.XXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
                  Source_User: MasterUser
                  Source_Port: 3306
                Connect_Retry: 10
              Source_Log_File: mysql-bin-changelog.012345
          Read_Source_Log_Pos: 1219393
               Relay_Log_File: relaylog.012340
                Relay_Log_Pos: 30223388
        Relay_Source_Log_File: mysql-bin-changelog.012345
           Replica_IO_Running: No
          Replica_SQL_Running: Yes
              Replicate_Do_DB:
          Replicate_Ignore_DB:
           Replicate_Do_Table:
       Replicate_Ignore_Table:
      Replicate_Wild_Do_Table:
  Replicate_Wild_Ignore_Table:
                   Last_Errno: 0
                   Last_Error:
                 Skip_Counter: 0
          Exec_Source_Log_Pos: 30223232
              Relay_Log_Space: 5248928866
              Until_Condition: None
               Until_Log_File:
                Until_Log_Pos: 0
           Source_SSL_Allowed: No
           Source_SSL_CA_File:
           Source_SSL_CA_Path:
              Source_SSL_Cert:
            Source_SSL_Cipher:
               Source_SSL_Key:
        Seconds_Behind_Source: NULL
Source_SSL_Verify_Server_Cert: No
                Last_IO_Errno: 1236
                Last_IO_Error: Got fatal error 1236 from source when reading data from
 binary log: 'Client requested source to start replication from impossible position;
 the first event 'mysql-bin-changelog.013406' at 1219393, the last event read from
 '/rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4, the last byte read from '/
rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4.'
               Last_SQL_Errno: 0
               Last_SQL_Error:
  Replicate_Ignore_Server_Ids:
             Source_Server_Id: 67285976
```

El campo `Last_IO_Errno` muestra que la instancia ha recibido el error de E/S 1236. El campo `Source_Log_File` muestra que el nombre de archivo es `mysql-bin-changelog.012345`, lo que significa que el índice del archivo de registro es `12345`. Para resolver el error, puede llamar a `mysql.rds_next_source_log` con el siguiente parámetro:

```
CALL mysql.rds_next_source_log(12345);
```

mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)

Vuelve a configurar una instancia de base de datos de RDS para MySQL para que deje de ser una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en `1`. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_reset_external_master;
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_reset_external_master`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a eliminar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados

principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Para obtener más información acerca del uso de la replicación para importar los datos desde una instancia de MySQL que se ejecuta fuera de Amazon RDS, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)

Vuelve a configurar una instancia de base de datos de RDS para MySQL para que deje de ser una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Important

Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en `1`. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_reset_external_source;
```

Notas de uso

El usuario administrativo debe ejecutar el procedimiento `mysql.rds_reset_external_source`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a eliminar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Note

Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga,

recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS.
Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos. Para obtener más información acerca del uso de la replicación para importar los datos desde una instancia de MySQL que se ejecuta fuera de Amazon RDS, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)

Configura una instancia de base de datos de RDS para MySQL para que sea una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Important

Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en `1`. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Note

Puede utilizar el procedimiento almacenado mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) para configurar una instancia de base de datos de origen externo y replicación retardada.

Sintaxis

```
CALL mysql.rds_set_external_master (
```

```
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de MySQL que se ejecuta fuera de Amazon RDS para convertirse en instancia de base de datos de origen.

host_port

El puerto usado por la instancia de MySQL que se ejecuta fuera de Amazon RDS que se configurará como instancia de base de datos de origen. Si la configuración de la red incluye la replicación de puertos SSH (Secure Shell) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El ID de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de MySQL que se ejecuta fuera de Amazon RDS. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia externa.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

mysql_binary_log_file_name

El nombre del registro binario de la instancia de base de datos de origen que contiene la información de replicación.

mysql_binary_log_file_location

La ubicación del registro binario `mysql_binary_log_file_name` en la que la replicación empieza a leer la información de la replicación.

Para determinar el nombre y la ubicación del archivo binlog, puede ejecutar `SHOW MASTER STATUS` en la instancia de base de datos de origen.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `MASTER_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_master`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a configurar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Antes de ejecutar `mysql.rds_set_external_master`, debe configurar la instancia de MySQL que se ejecuta fuera de Amazon RDS como instancia de base de datos de origen. Para conectarse a la instancia de MySQL que se ejecuta fuera de Amazon RDS, debe especificar los valores de `replication_user_name` y `replication_user_password` que indican un usuario de replicación que tiene los permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia externa de MySQL.

Para configurar una instancia externa de MySQL como instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia externa de MySQL y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   MySQL 5.7

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
   ```

   MySQL 8.0

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED WITH mysql_native_password BY
    'password';
   ```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

2. En la instancia externa de MySQL, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario “repl_user” de su dominio.

   MySQL 5.7

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
    IDENTIFIED BY 'password';
   ```

   MySQL 8.0

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
   ```

Para utilizar la replicación cifrada, configure la instancia de base de datos de origen para que utilice conexiones SSL.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Después de llamar a `mysql.rds_set_external_master` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura, puede llamar a mysql.rds_start_replication en la réplica de lectura para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_master`, Amazon RDS registra la hora, el usuario y una acción `set master` en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MySQL, el siguiente ejemplo configura la instancia de base de datos como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

```
call mysql.rds_set_external_master(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'password',
  'mysql-bin-changelog.0777',
  120,
  1);
```

mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores)

Configura una instancia de base de datos de RDS para MySQL para que sea una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_source (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de MySQL que se ejecuta fuera de Amazon RDS para convertirse en instancia de base de datos de origen.

host_port

El puerto usado por la instancia de MySQL que se ejecuta fuera de Amazon RDS que se configurará como instancia de base de datos de origen. Si la configuración de la red incluye la replicación de puertos SSH (Secure Shell) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El ID de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de MySQL que se ejecuta fuera de Amazon RDS. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia externa.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

mysql_binary_log_file_name

El nombre del registro binario de la instancia de base de datos de origen que contiene la información de replicación.

mysql_binary_log_file_location

La ubicación del registro binario `mysql_binary_log_file_name` en la que la replicación empieza a leer la información de la replicación.

Para determinar el nombre y la ubicación del archivo binlog, puede ejecutar `SHOW MASTER STATUS` en la instancia de base de datos de origen.

`ssl_encryption`

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `SOURCE_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

Notas de uso

El usuario administrativo debe ejecutar el procedimiento `mysql.rds_set_external_source`. Este procedimiento se debe ejecutar en la instancia de base de datos de RDS para MySQL que se va a configurar como réplica de lectura de una instancia de MySQL que se ejecute fuera de Amazon RDS.

Antes de ejecutar `mysql.rds_set_external_source`, debe configurar la instancia de MySQL que se ejecuta fuera de Amazon RDS como instancia de base de datos de origen. Para conectarse a la instancia de MySQL que se ejecuta fuera de Amazon RDS, debe especificar los valores de `replication_user_name` y `replication_user_password` que indican un usuario de replicación que tiene los permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia externa de MySQL.

Para configurar una instancia externa de MySQL como instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia externa de MySQL y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

```
CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'password';
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

2. En la instancia externa de MySQL, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario “repl_user” de su dominio.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com';
```

Para utilizar la replicación cifrada, configure la instancia de base de datos de origen para que utilice conexiones SSL. Asimismo, importe el certificado de la entidad de certificación, el certificado del cliente y la clave de cliente en la instancia de base de datos o clúster de base de datos mediante el procedimiento mysql.rds_import_binlog_ssl_material.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Después de llamar a `mysql.rds_set_external_source` para configurar una instancia de base de datos de RDS para MySQL como réplica de lectura, puede llamar a mysql.rds_start_replication en la réplica de lectura para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_source`, Amazon RDS registra la hora, el usuario y una acción `set master` en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de RDS para MySQL, el siguiente ejemplo configura la instancia de base de datos como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

```
call mysql.rds_set_external_source(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'password',
  'mysql-bin-changelog.0777',
  120,
  1);
```

mysql.rds_set_external_master_with_auto_position (RDS para las versiones principales de MySQL 8.0 e inferiores)

Configura una instancia de base de datos de RDS for MySQL para que sea una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS. Este procedimiento también configura la replicación retrasada y la replicación basada en identificadores de transacciones globales (GTID).

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_master_with_auto_position (
  host_name
```

```
  , host_port
  , replication_user_name
  , replication_user_password
  , ssl_encryption
  , delay
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de MySQL que se ejecuta fuera de Amazon RDS para convertirse en instancia de base de datos de origen.

host_port

El puerto usado por la instancia de MySQL que se ejecuta fuera de Amazon RDS que se configurará como instancia de base de datos de origen. Si la configuración de la red incluye la replicación de puertos SSH (Secure Shell) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El ID de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de MySQL que se ejecuta fuera de Amazon RDS. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia externa.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `MASTER_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

delay

El número mínimo de segundos para retrasar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_master_with_auto_position`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a configurar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Este procedimiento es compatible con todas las versiones de RDS para MySQL 5.7 y con las versiones de RDS para MySQL 8.0.26 y posteriores.

Antes de ejecutar `mysql.rds_set_external_master_with_auto_position`, debe configurar la instancia de MySQL que se ejecuta fuera de Amazon RDS como instancia de base de datos de origen. Para conectarse a la instancia de MySQL que se ejecuta fuera de Amazon RDS, debe especificar valores para `replication_user_name` y `replication_user_password`. Estos valores deben indicar a un usuario de replicación que tiene permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia externa de MySQL.

Para configurar una instancia externa de MySQL como instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia externa de MySQL y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
   ```

2. En la instancia externa de MySQL, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario `'repl_user'` de su dominio.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
   IDENTIFIED BY 'SomePassW0rd'
   ```

Para obtener más información, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Antes de llamar a `mysql.rds_set_external_master_with_auto_position`, asegúrese de llamar a the section called “mysql.rds_set_external_source_gtid_purged” para configurar la variable de sistema `gtid_purged` con un rango de GTID especificado desde un origen externo.

Después de llamar a `mysql.rds_set_external_master_with_auto_position` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura, puede llamar a mysql.rds_start_replication en la réplica de lectura para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_master_with_auto_position`, Amazon RDS registra la hora, el usuario y una acción `set master` en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Para la recuperación de desastres, puede utilizar este procedimiento con el procedimiento almacenado mysql.rds_start_replication_until o mysql.rds_start_replication_until_gtid. Puede ejecutar el procedimiento `mysql.rds_set_external_master_with_auto_position` para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Después de que el procedimiento `mysql.rds_start_replication_until_gtid` detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Para utiliza el procedimiento `mysql.rds_rds_start_replication_until_gtid`, debe habilitarse la replicación basada en GTID. Para omitir una transacción específica basada en GTID que se sabe que causa un desastre, puede usar el procedimiento almacenado mysql.rds_skip_transaction_with_gtid. Para obtener más información sobre el uso de la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MySQL, el siguiente ejemplo configura la instancia de base de datos como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS. Establece el retraso de replicación mínimo en una hora (3600 segundos) para la instancia de base de datos de MySQL. Un cambio en la instancia de base de datos de origen de MySQL que se ejecuta de forma externa a Amazon RDS no se aplica en la réplica de lectura de la instancia de base de datos de MySQL hasta que haya transcurrido al menos una hora.

```
call mysql.rds_set_external_master_with_auto_position(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'SomePassW0rd',
  1,
  3600);
```

mysql.rds_set_external_source_with_auto_position (RDS para las versiones principales de MySQL 8.4 y superiores)

Configura una instancia de base de datos de RDS for MySQL para que sea una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS. Este procedimiento también configura la replicación retrasada y la replicación basada en identificadores de transacciones globales (GTID).

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_source_with_auto_position (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , ssl_encryption
  , delay
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de MySQL que se ejecuta fuera de Amazon RDS para convertirse en instancia de base de datos de origen.

host_port

El puerto usado por la instancia de MySQL que se ejecuta fuera de Amazon RDS que se configurará como instancia de base de datos de origen. Si la configuración de la red incluye la replicación de puertos SSH (Secure Shell) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El ID de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de MySQL que se ejecuta fuera de Amazon RDS. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia externa.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción SOURCE_SSL_VERIFY_SERVER_CERT no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

delay

El número mínimo de segundos para retrasar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

Notas de uso

El usuario administrativo debe ejecutar el procedimiento `mysql.rds_set_external_source_with_auto_position`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a configurar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Antes de ejecutar `mysql.rds_set_external_source_with_auto_position`, debe configurar la instancia de MySQL que se ejecuta fuera de Amazon RDS como instancia de base de datos de origen. Para conectarse a la instancia de MySQL que se ejecuta fuera de Amazon RDS, debe especificar valores para `replication_user_name` y `replication_user_password`. Estos valores deben indicar a un usuario de replicación que tiene permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia externa de MySQL.

Para configurar una instancia externa de MySQL como instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia externa de MySQL y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
   ```

2. En la instancia externa de MySQL, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario `'repl_user'` de su dominio.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY 'SomePassW0rd'
```

Para obtener más información, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Antes de llamar a `mysql.rds_set_external_source_with_auto_position`, asegúrese de llamar a the section called “mysql.rds_set_external_source_gtid_purged” para configurar la variable de sistema `gtid_purged` con un rango de GTID especificado desde un origen externo.

Después de llamar a `mysql.rds_set_external_source_with_auto_position` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura, puede llamar a mysql.rds_start_replication en la réplica de lectura para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_source_with_auto_position`, Amazon RDS registra la hora, el usuario y una acción `set master` en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Para la recuperación de desastres, puede utilizar este procedimiento con el procedimiento almacenado mysql.rds_start_replication_until o mysql.rds_start_replication_until_gtid. Puede ejecutar el procedimiento `mysql.rds_set_external_source_with_auto_position` para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Después

de que el procedimiento `mysql.rds_start_replication_until_gtid` detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Para utiliza el procedimiento `mysql.rds_rds_start_replication_until_gtid`, debe habilitarse la replicación basada en GTID. Para omitir una transacción específica basada en GTID que se sabe que causa un desastre, puede usar el procedimiento almacenado mysql.rds_skip_transaction_with_gtid. Para obtener más información sobre el uso de la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MySQL, el siguiente ejemplo configura la instancia de base de datos como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS. Establece el retraso de replicación mínimo en una hora (3600 segundos) para la instancia de base de datos de MySQL. Un cambio en la instancia de base de datos de origen de MySQL que se ejecuta de forma externa a Amazon RDS no se aplica en la réplica de lectura de la instancia de base de datos de MySQL hasta que haya transcurrido al menos una hora.

```
call mysql.rds_set_external_source_with_auto_position(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'SomePassW0rd',
  1,
  3600);
```

mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)

Configura una instancia de base de datos de RDS for MySQL para que sea una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS y configura la reproducción retrasada.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo

modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_master_with_delay(
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
  , delay
);
```

Parámetros

host_name

El nombre del host o la dirección IP de la instancia de MySQL que se ejecuta fuera de Amazon RDS que se convertirá en instancia de base de datos de origen.

host_port

El puerto usado por la instancia de MySQL que se ejecuta fuera de Amazon RDS que se configurará como instancia de base de datos de origen. Si la configuración de la red incluye la replicación del puerto SSH que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El ID de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de MySQL que se ejecuta fuera de Amazon RDS. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia externa.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

mysql_binary_log_file_name

El nombre del registro binario de la instancia de base de datos de origen contiene la información de replicación.

mysql_binary_log_file_location

La ubicación del registro binario `mysql_binary_log_file_name` en la que la replicación comenzará a leer la información de la replicación.

Para determinar el nombre y la ubicación del archivo binlog, puede ejecutar `SHOW MASTER STATUS` en la instancia de base de datos de origen.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `MASTER_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

delay

El número mínimo de segundos para retrasar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_master_with_delay`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a configurar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Antes de ejecutar `mysql.rds_set_external_master_with_delay`, debe configurar la instancia de MySQL que se ejecuta fuera de Amazon RDS como instancia de base de datos de origen. Para

conectarse a la instancia de MySQL que se ejecuta fuera de Amazon RDS, debe especificar valores para `replication_user_name` y `replication_user_password`. Estos valores deben indicar a un usuario de replicación que tiene permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia externa de MySQL.

Para configurar una instancia externa de MySQL como instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia externa de MySQL y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
   ```

2. En la instancia externa de MySQL, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario `'repl_user'` de su dominio.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
   IDENTIFIED BY 'SomePassW0rd'
   ```

Para obtener más información, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Después de llamar a `mysql.rds_set_external_master_with_delay` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura, puede llamar a

mysql.rds_start_replication en la réplica de lectura para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_master_with_delay`, Amazon RDS registra la hora, el usuario y una acción `set master` en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Para la recuperación de desastres, puede utilizar este procedimiento con el procedimiento almacenado mysql.rds_start_replication_until o mysql.rds_start_replication_until_gtid. Puede ejecutar el procedimiento `mysql.rds_set_external_master_with_delay` para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Después de que el procedimiento `mysql.rds_start_replication_until` detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Para utiliza el procedimiento `mysql.rds_rds_start_replication_until_gtid`, debe habilitarse la replicación basada en GTID. Para omitir una transacción específica basada en GTID que se sabe que causa un desastre, puede usar el procedimiento almacenado mysql.rds_skip_transaction_with_gtid. Para obtener más información sobre el uso de la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

El procedimiento `mysql.rds_set_external_master_with_delay` está disponible en estas versiones de RDS para MySQL:

- Versión de MySQL 8.0.26 y versiones 8.0 posteriores
- Todas las versiones 5.7

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MySQL, el siguiente ejemplo configura la instancia de base de datos como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS. Establece el retraso de replicación mínimo en una hora (3600 segundos) para la instancia de base de datos de MySQL. Un cambio en la instancia de base de datos de origen de MySQL que se ejecuta de forma externa a Amazon RDS no se aplica en la réplica de lectura de la instancia de base de datos de MySQL hasta que haya transcurrido al menos una hora.

```
call mysql.rds_set_external_master_with_delay(
```

```
  'Externaldb.some.com',
  3306,
  'repl_user',
  'SomePassW0rd',
  'mysql-bin-changelog.000777',
  120,
  1,
  3600);
```

mysql.rds_set_external_source_with_delay (RDS para las versiones principales de MySQL 8.4 y superiores)

Configura una instancia de base de datos de RDS for MySQL para que sea una réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS y configura la reproducción retrasada.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_source_with_delay (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
  , delay
);
```

Parámetros

host_name

El nombre del host o la dirección IP de la instancia de MySQL que se ejecuta fuera de Amazon RDS que se convertirá en instancia de base de datos de origen.

host_port

El puerto usado por la instancia de MySQL que se ejecuta fuera de Amazon RDS que se configurará como instancia de base de datos de origen. Si la configuración de la red incluye la replicación del puerto SSH que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El ID de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de MySQL que se ejecuta fuera de Amazon RDS. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia externa.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

mysql_binary_log_file_name

El nombre del registro binario de la instancia de base de datos de origen contiene la información de replicación.

mysql_binary_log_file_location

La ubicación del registro binario `mysql_binary_log_file_name` en la que la replicación comenzará a leer la información de la replicación.

Para determinar el nombre y la ubicación del archivo binlog, puede ejecutar `SHOW MASTER STATUS` en la instancia de base de datos de origen.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción SOURCE_SSL_VERIFY_SERVER_CERT no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

delay

El número mínimo de segundos para retrasar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

Notas de uso

El usuario administrativo debe ejecutar el procedimiento `mysql.rds_set_external_source_with_delay`. Este procedimiento se debe ejecutar en la instancia de base de datos de MySQL que se va a configurar como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS.

Antes de ejecutar `mysql.rds_set_external_source_with_delay`, debe configurar la instancia de MySQL que se ejecuta fuera de Amazon RDS como instancia de base de datos de origen. Para conectarse a la instancia de MySQL que se ejecuta fuera de Amazon RDS, debe especificar valores para `replication_user_name` y `replication_user_password`. Estos valores deben indicar a un usuario de replicación que tiene permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia externa de MySQL.

Para configurar una instancia externa de MySQL como instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia externa de MySQL y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   ```
   CREATE USER 'repl_user'@'mydomain.com' IDENTIFIED BY 'SomePassW0rd'
   ```

2. En la instancia externa de MySQL, conceda a `REPLICATION CLIENT` y a `REPLICATION SLAVE` privilegios para el usuario de replicación. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario `'repl_user'` de su dominio.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'mydomain.com'
IDENTIFIED BY 'SomePassW0rd'
```

Para obtener más información, consulte Configuración de la replicación de posición de archivo de registro binario con una instancia de origen externa.

> **Note**
>
> Recomendamos que utilice réplicas de lectura para administrar la replicación entre dos instancias de base de datos de Amazon RDS cuando sea posible. Cuando lo haga, recomendamos que solo utilice este y otros procedimientos almacenados relacionados de replicación. Estas prácticas permiten topologías de replicación más complejas entre instancias de base de datos de Amazon RDS. Ofrecemos estos procedimientos almacenados principalmente para habilitar la replicación con las instancias de MySQL que se ejecutan fuera de Amazon RDS. Para obtener información sobre la administración de la replicación entre instancias de base de datos de Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Después de llamar a `mysql.rds_set_external_source_with_delay` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura, puede llamar a mysql.rds_start_replication en la réplica de lectura para iniciar el proceso de replicación. Puede llamar a mysql.rds_reset_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) para eliminar la configuración de la réplica de lectura.

Cuando se llama a `mysql.rds_set_external_source_with_delay`, Amazon RDS registra la hora, el usuario y una acción `set master` en las tablas `mysql.rds_history` y `mysql.rds_replication_status`.

Para la recuperación de desastres, puede utilizar este procedimiento con el procedimiento almacenado mysql.rds_start_replication_until o mysql.rds_start_replication_until_gtid. Puede ejecutar el procedimiento `mysql.rds_set_external_source_with_delay` para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Después de que el procedimiento `mysql.rds_start_replication_until` detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria

utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Para utiliza el procedimiento `mysql.rds_rds_start_replication_until_gtid`, debe habilitarse la replicación basada en GTID. Para omitir una transacción específica basada en GTID que se sabe que causa un desastre, puede usar el procedimiento almacenado mysql.rds_skip_transaction_with_gtid. Para obtener más información sobre el uso de la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MySQL, el siguiente ejemplo configura la instancia de base de datos como réplica de lectura de una instancia de MySQL que se ejecuta fuera de Amazon RDS. Establece el retraso de replicación mínimo en una hora (3600 segundos) para la instancia de base de datos de MySQL. Un cambio en la instancia de base de datos de origen de MySQL que se ejecuta de forma externa a Amazon RDS no se aplica en la réplica de lectura de la instancia de base de datos de MySQL hasta que haya transcurrido al menos una hora.

```
call mysql.rds_set_external_source_with_delay(
  'Externaldb.some.com',
  3306,
  'repl_user',
  'SomePassW0rd',
  'mysql-bin-changelog.000777',
  120,
  1,
  3600);
```

mysql.rds_set_external_source_gtid_purged

Establece la variable de sistema gtid_purged con un rango de GTID especificado de un origen externo. El valor `gtid_purged` es necesario para configurar la replicación basada en GTID y reanudar la replicación mediante el posicionamiento automático.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_source_gtid_purged(
  server_uuid
  , start_pos
  , end_pos
);
```

Parámetros

server_uuid

Es el identificador único universal (UUID) del servidor externo desde el que se importa el rango de GTID.

start_pos

La posición inicial del rango de GTID que se va a configurar.

end_pos

La posición inicial del rango de GTID que se va a configurar.

Notas de uso

El procedimiento `mysql.rds_set_external_source_gtid_purged` solo está disponible con las versiones 8.0.37 y otras versiones 8.0 posteriores de MySQL.

Llame a `mysql.rds_set_external_source_gtid_purged` antes de llamar a mysql.rds_set_external_master_with_auto_position (RDS para las versiones principales de MySQL 8.0 e inferiores), mysql.rds_set_external_source_with_auto_position (RDS para las versiones principales de MySQL 8.4 y superiores) o mysql.rds_set_external_source_with_auto_position_for_channel.

Antes de llamar a `mysql.rds_set_external_source_gtid_purged`, asegúrese de detener todos los canales de replicación activos de la base de datos. Para comprobar el estado de un canal, utilice la instrucción de MySQL `SHOW REPLICA STATUS`. Para detener la replicación en un canal, llame a the section called “mysql.rds_stop_replication_for_channel”.

El rango de GTID que especifique debe ser un superconjunto del valor existente de `GTID_PURGED`. Este procedimiento almacenado comprueba los siguientes valores antes de establecer el valor de `GTID_PURGED`:

- El `server_uuid` es válido.
- El valor de `start_pos` es mayor que `0` y menor que el valor de `end_pos`.
- El valor de `end_pos` es superior o igual al valor de `start_pos`.

Si el conjunto de GTID de su servidor externo contiene varios rangos de valores, valore la posibilidad de llamar al procedimiento varias veces con valores de conjunto de GTID diferentes.

Cuando llama a `mysql.rds_set_external_source_gtid_purged`, Amazon RDS registra la hora, el usuario y una acción `set gtid_purged` en la tabla `mysql.rds_history`.

Si no establece el valor de `gtid_purged` adecuado para la copia de seguridad que utiliza en la replicación, es posible que falten transacciones o que se dupliquen durante el proceso de replicación. Siga estos pasos para corregir el valor de `gtid_purged`.

Establecimiento del valor de gtid_purged en la réplica

1. Determine el momento o el archivo de copia de seguridad específico que se utilizará como punto de partida para la replicación. Puede ser una copia de seguridad lógica (un archivo mysqldump) o una copia de seguridad física (una instantánea de Amazon RDS).
2. Determine el valor de `gtid_executed`. Este valor representa el conjunto de todos los GTID que se confirmaron en el servidor. Para recuperar este valor, en la instancia de origen, realice una de las siguientes operaciones:
   - Ejecute la instrucción de SQL `SELECT @@GLOBAL.GTID_EXECUTED;` en el momento en que se realizó la copia de seguridad.
   - Si se incluye alguna opción relacionada en la utilidad de copia de seguridad correspondiente, extraiga el valor del archivo de copia de seguridad. Para obtener más información, consulte la opción set-gtid-purged en la documentación de MySQL.
3. Determine el valor de `gtid_purged` que se utilizará para la llamada a `mysql.rds_set_external_source_gtid_purged`. El valor de `gtid_purged` debe incluir todos los GTID que se ejecutaron en la instancia de origen y que ya no se necesitan para la replicación. Por lo tanto, el valor de `gtid_purged` debe ser un subconjunto del valor de `gtid_executed` que ha recuperado en el paso anterior.

   Para determinar el valor de `gtid_purged`, identifique los GTID que no están incluidos en la copia de seguridad y que ya no se necesitan para la replicación. Puede hacerlo analizando los

registros binarios o utilizando una herramienta como mysqlbinlog para buscar los GTID que se purgaron desde los registros binarios.

Si dispone de una copia de seguridad uniforme que incluya todos los registros binarios hasta el punto de copia de seguridad, también puede configurar el valor de `gtid_purged` para que sea el mismo que el de `gtid_executed` en el momento de la copia de seguridad.

4. Tras determinar el valor de `gtid_purged` adecuado que sea coherente con la copia de seguridad, llame al procedimiento almacenado `mysql.rds_set_external_source_gtid_purged` en la instancia de base de datos de RDS para MySQL a fin de establecer el valor.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de MySQL, el siguiente ejemplo establece el rango de GTID desde un servidor MySQL externo con el UUID `12345678-abcd-1234-efgh-123456789abc`, una posición inicial `1` y una posición final `100`. El valor de GTID resultante se establece en `+12345678-abcd-1234-efgh-123456789abc:1-100`.

```
CALL mysql.rds_set_external_source_gtid_purged('12345678-abcd-1234-efgh-123456789abc',
 1, 100);
```

mysql.rds_set_master_auto_position (RDS para las versiones principales de MySQL 8.0 e inferiores)

Establece el modo de replicación en el que se debe basar ya sea en posiciones de archivos de registros binarios o en identificadores de transacciones globales (GTID).

Sintaxis

```
CALL mysql.rds_set_master_auto_position (
auto_position_mode
);
```

Parámetros

`auto_position_mode`

Un valor que indicar si debe usarse la replicación de posición de los archivos de registro o la replicación basada en GTID:

- `0`: utilice el método de replicación basado en la posición del archivo de registro binario. El valor predeterminado es `0`.
- `1`: utilice el método de replicación basado en GTID.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_master_auto_position`.

Este procedimiento es compatible con todas las versiones de RDS para MySQL 5.7 y con las versiones de RDS para MySQL 8.0.26 y posteriores.

mysql.rds_set_source_auto_position (RDS para las versiones principales de MySQL 8.4 y superiores)

Establece el modo de replicación en el que se debe basar, ya sea en posiciones de archivos de registros binarios o en identificadores de transacciones globales (GTID).

Sintaxis

```
CALL mysql.rds_set_source_auto_position (auto_position_mode);
```

Parámetros

`auto_position_mode`

Un valor que indicar si debe usarse la replicación de posición de los archivos de registro o la replicación basada en GTID:

- `0`: utilice el método de replicación basado en la posición del archivo de registro binario. El valor predeterminado es `0`.
- `1`: utilice el método de replicación basado en GTID.

Notas de uso

El usuario administrativo debe ejecutar el procedimiento `mysql.rds_set_source_auto_position`.

mysql.rds_set_source_delay

Establece el número mínimo de segundos para retrasar la replicación desde la instancia de base de datos de origen a la réplica de lectura actual. Use este procedimiento cuando esté conectado a una réplica de lectura para retrasar la replicación desde su instancia de base de datos de origen.

Sintaxis

```
CALL mysql.rds_set_source_delay(
delay
);
```

Parámetros

delay

El número mínimo de segundos para retrasar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_source_delay`.

Para la recuperación de desastres, puede utilizar este procedimiento con el procedimiento almacenado mysql.rds_start_replication_until o el procedimiento almacenado mysql.rds_start_replication_until_gtid. Puede ejecutar el procedimiento `mysql.rds_set_source_delay` para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Después de que el procedimiento `mysql.rds_start_replication_until` o `mysql.rds_start_replication_until_gtid` detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Para utiliza el procedimiento `mysql.rds_rds_start_replication_until_gtid`, debe habilitarse la replicación basada en GTID. Para omitir una transacción específica basada en GTID que se sabe que causa un desastre, puede usar el procedimiento almacenado mysql.rds_skip_transaction_with_gtid. Para obtener más información acerca de la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

El procedimiento `mysql.rds_set_source_delay` está disponible en estas versiones de RDS for MySQL:

- Todas las versiones de RDS para MySQL 8.4
- Versión de MySQL 8.0.26 y versiones 8.0 posteriores
- Todas las versiones 5.7

Ejemplos

Para retrasar la replicación desde la instancia de base de datos de origen a la réplica de lectura actual durante al menos una hora (3600 segundos), puede llamar a `mysql.rds_set_source_delay` con el siguiente parámetro:

```
CALL mysql.rds_set_source_delay(3600);
```

mysql.rds_skip_repl_error

Omite y elimina un error de replicación en una réplica de lectura de base de datos de MySQL.

Sintaxis

```
CALL mysql.rds_skip_repl_error;
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_skip_repl_error` en una réplica de lectura. Para obtener más información sobre este procedimiento, consulte Llamar al procedimiento mysql.rds_skip_repl_error (Omitir el error de replicación actual).

Para determinar si hay errores, ejecute el comando `SHOW REPLICA STATUS\G` de MySQL. Si un error de replicación no es crítico, puede ejecutar `mysql.rds_skip_repl_error` para omitir el error. Si hay varios errores, `mysql.rds_skip_repl_error` elimina el primer error y advierte de que hay otros presentes. A continuación, puede usar `SHOW REPLICA STATUS\G` para determinar la acción correcta para el siguiente error. Para obtener información acerca de los valores devueltos, consulte la instrucción SHOW REPLICA STATUS en la documentación de MySQL.

Para obtener más información acerca de la resolución de problemas de replicación con Amazon RDS, consulte Solución de problemas de réplicas de lectura de MySQL.

Error de replicación detenida

Al llamar al procedimiento `mysql.rds_skip_repl_error`, es posible que reciba un mensaje de error en el que se indica que la réplica tiene un error o está deshabilitada.

Este mensaje de error aparece si ejecuta el procedimiento en la instancia principal en lugar de en la réplica de lectura. Debe ejecutar este procedimiento en la réplica de lectura para que funcione.

Este mensaje de error también puede aparecer si ejecuta el procedimiento en la réplica de lectura, pero la replicación no se puede reiniciar correctamente.

Si tiene que omitir un número de errores elevado, el retardo de réplica puede aumentar por encima del periodo de retención predeterminado para los archivos de log binarios (binlog). En este caso, puede producirse un error fatal porque los archivos binlog se están limpiando antes de reproducirse de nuevo en la réplica de lectura. Esta limpieza hace que la replicación se detenga y ya no se puede llamar al comando `mysql.rds_skip_repl_error` para omitir los errores de replicación.

Puede mitigar este problema incrementando el número de horas que los archivos binlog se retienen en la instancia de base de datos de origen. Después de incrementar el tiempo de retención de los archivos binlog, puede reiniciar la replicación y llamar al comando `mysql.rds_skip_repl_error` si es necesario.

Para definir el tiempo de retención de binlog, use el procedimiento mysql.rds_set_configuration y especifique un parámetro de configuración de `'binlog retention hours'` junto con el número de horas para retener los archivos binlog en el clúster de base de datos. El ejemplo siguiente define el período de retención de los archivos binlog en 48 horas.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

mysql.rds_start_replication

Inicia la replicación desde una instancia de base de datos de RDS para MySQL.

> **Note**
>
> Puede utilizar el procedimiento almacenado mysql.rds_start_replication_until o mysql.rds_start_replication_until_gtid para iniciar la replicación desde una instancia de base de datos de RDS para MySQL y detener la replicación en la ubicación del archivo de registro binario especificado.

Sintaxis

```
CALL mysql.rds_start_replication;
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_start_replication`.

Para importar datos desde una instancia de MySQL fuera de Amazon RDS, llame a `mysql.rds_start_replication` en la réplica de lectura para iniciar el proceso de replicación después de llamar a mysql.rds_set_external_master (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores) o mysql.rds_set_external_source (RDS para las versiones principales de MySQL 8.4 y superiores) para crear la configuración de replicación. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..

Para exportar datos a una instancia de MySQL externa a Amazon RDS, llame a `mysql.rds_start_replication` y a `mysql.rds_stop_replication` en la réplica de lectura para controlar algunas acciones de replicación, como la purga de registros binarios. Para obtener más información, consulte Exportación de datos desde una instancia de base de datos MySQL mediante replicación.

Puede llamar a `mysql.rds_start_replication` en la réplica de lectura para reiniciar cualquier proceso de replicación que haya detenido previamente llamando a `mysql.rds_stop_replication`. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.

mysql.rds_start_replication_until

Inicia la replicación desde una instancia de base de datos de RDS para MySQL y detiene la replicación en la ubicación del archivo de registro binario especificado.

Sintaxis

```
CALL mysql.rds_start_replication_until (
replication_log_file
  , replication_stop_point
```

```
);
```

Parámetros

replication_log_file

El nombre del registro binario de la instancia de base de datos de origen que contiene la información de replicación.

replication_stop_point

La ubicación del registro binario `replication_log_file` en la que la replicación se detendrá.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_start_replication_until`.

El procedimiento `mysql.rds_start_replication_until` está disponible en estas versiones de RDS for MySQL:

- Todas las versiones de RDS para MySQL 8.4
- Versión de MySQL 8.0.26 y versiones 8.0 posteriores
- Todas las versiones 5.7

Puede utilizar este procedimiento con la replicación retrasada para recuperación ante desastres. Si ha configurado la replicación retrasada, puede utilizar este procedimiento para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Después de que este procedimiento detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Puede configurar la replicación retrasada utilizando los procedimientos almacenados siguientes:

- mysql.rds_set_configuration
- mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source_with_delay (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_source_delay

El nombre de archivo especificado para el parámetro `replication_log_file` debe coincidir con el nombre del archivo binlog de instancia de base de datos de origen.

Cuando el parámetro `replication_stop_point` especifica una ubicación de parada correspondiente al pasado, la replicación se detiene de inmediato.

Ejemplos

En el ejemplo siguiente se inicia la replicación y se replican los cambios hasta que alcanza la ubicación `120` del archivo registro binario `mysql-bin-changelog.000777`.

```
call mysql.rds_start_replication_until(
  'mysql-bin-changelog.000777',
  120);
```

mysql.rds_stop_replication

Detiene la replicación desde una instancia de base de datos de MySQL.

Sintaxis

```
CALL mysql.rds_stop_replication;
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_stop_replication`.

Si desea configurar la replicación para importar datos desde una instancia de MySQL que se ejecuta fuera de Amazon RDS, llame a `mysql.rds_stop_replication` en la réplica de lectura para detener el proceso de replicación una vez completada la importación. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..

Si desea configurar la replicación para exportar datos a una instancia de MySQL externa a Amazon RDS, llame a `mysql.rds_start_replication` y a `mysql.rds_stop_replication` en la réplica de lectura para controlar algunas acciones de replicación, como la limpieza de registros binarios. Para obtener más información, consulte Exportación de datos desde una instancia de base de datos MySQL mediante replicación.

También puede usar `mysql.rds_stop_replication` para detener la replicación entre dos instancias de base de datos de Amazon RDS. Normalmente, se detiene la replicación para realizar

una operación con un tiempo de ejecución largo en la réplica de lectura, como crear un índice grande en la réplica de lectura. Puede reiniciar cualquier proceso de replicación que haya detenido llamando a mysql.rds_start_replication en la réplica de lectura. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Finalización de una sesión o una consulta

Los siguientes procedimientos almacenados finalizan una sesión o una consulta.

Temas

- mysql.rds_kill
- mysql.rds_kill_query

mysql.rds_kill

Finaliza una conexión al servidor de MySQL.

Sintaxis

```
CALL mysql.rds_kill(processID);
```

Parámetros

processID

La identidad del subproceso de conexión que se va a finalizar.

Notas de uso

Cada conexión al servidor de MySQL se ejecuta en un subproceso independiente. Para finalizar una conexión, use el procedimiento `mysql.rds_kill` y transfiera el ID de subproceso de esa conexión. Para obtener el ID del subproceso, use el comando SHOW PROCESSLIST de MySQL.

Para obtener información acerca de las limitaciones, consulte Limitaciones del procedimiento almacenado de MySQL.

Ejemplos

El siguiente ejemplo finaliza una conexión con el ID de subproceso 4243:

```
CALL mysql.rds_kill(4243);
```

mysql.rds_kill_query

Finaliza una consulta que se ejecuta en el servidor de MySQL.

Sintaxis

```
CALL mysql.rds_kill_query(processID);
```

Parámetros

processID

La identidad del proceso o subproceso que ejecuta la consulta que se va a finalizar.

Notas de uso

Para detener una consulta que se ejecuta en el servidor MySQL, utilice el procedimiento `mysql_rds_kill_query` y pase el ID de conexión del subproceso que está ejecutando la consulta. A continuación, el procedimiento finaliza la conexión.

Para obtener el ID, consulte la tabla INFORMATION_SCHEMA PROCESSLIST o utilice el comando MySQL SHOW PROCESSLIST. El valor de la columna ID de `SHOW PROCESSLIST` o `SELECT * FROM INFORMATION_SCHEMA.PROCESSLIST` es el *ID del proceso*.

Para obtener información acerca de las limitaciones, consulte Limitaciones del procedimiento almacenado de MySQL.

Ejemplos

El siguiente ejemplo detiene una consulta con el ID de subproceso 230040:

```
CALL mysql.rds_kill_query(230040);
```

Administración de clústeres activo-activo

Los siguientes procedimientos almacenados configuran y administran los clústeres activo-activo de RDS para MySQL. Para obtener más información, consulte the section called “Configuración de clústeres activo-activo”.

Estos procedimientos almacenados solo están disponibles con instancias de base de datos de RDS para MySQL que ejecuten las siguientes versiones:

- Todas las versiones MySQL 8.4
- MySQL 8.0.35 y versiones secundarias posteriores

Temas

- mysql.rds_group_replication_advance_gtid
- mysql.rds_group_replication_create_user
- mysql.rds_group_replication_set_recovery_channel
- mysql.rds_group_replication_start
- mysql.rds_group_replication_stop

mysql.rds_group_replication_advance_gtid

Crea GTID de marcador de posición en la instancia de base de datos actual.

Sintaxis

```
CALL mysql.rds_group_replication_advance_gtid(
begin_id
, end_id
, server_uuid
);
```

Parámetros

begin_id

El identificador de la transacción inicial que se va a crear.

end_id

El identificador de la transacción final que se va a crear.

begin_id

El `group_replication_group_name` de la transacción que se va a crear. El `group_replication_group_name` se especifica como un UUID en el grupo de parámetros de base de datos asociado a la instancia de base de datos.

Notas de uso

En un clúster activo-activo, para que una instancia de base de datos se una a un grupo, todas las transacciones GTID ejecutadas en la nueva instancia de base de datos deben existir en los demás miembros del clúster. En casos poco habituales, es posible que una nueva instancia de base de datos tenga más transacciones si las transacciones se ejecutan antes de unir la instancia al grupo. En este caso, no puede eliminar ninguna transacción existente, pero puede utilizar este procedimiento para crear los GTID de marcador de posición correspondientes en las demás instancias de base de datos del grupo. Antes de hacerlo, compruebe que las transacciones no afectan a los datos replicados.

Al llamar a este procedimiento, las transacciones GTID de `server_uuid:begin_id-end_id` se crean con contenido vacío. Para evitar problemas de replicación, no utilice este procedimiento en ninguna otra condición.

> **Important**
>
> Evite llamar a este procedimiento cuando el clúster activo-activo funcione normalmente. No llame a este procedimiento a menos que conozca las posibles consecuencias de las transacciones que va a crear. El uso de este procedimiento puede producir datos incoherentes.

Ejemplo

En el siguiente ejemplo, se crean GTID de marcador de posición en la instancia de base de datos actual:

```
CALL mysql.rds_group_replication_advance_gtid(5, 6,
 '11111111-2222-3333-4444-555555555555');
```

mysql.rds_group_replication_create_user

Crea el usuario de replicación `rdsgrprepladmin` para la replicación de grupo en la instancia de base de datos.

Sintaxis

```
CALL mysql.rds_group_replication_create_user(
replication_user_password
);
```

Parámetros

`replication_user_password`

La contraseña del usuario de replicación `rdsgrprepladmin`.

Notas de uso

- La contraseña del usuario de replicación `rdsgrprepladmin` debe ser la misma en todas las instancias de base de datos de un clúster activo-activo.
- El nombre de usuario `rdsgrprepladmin` está reservado para las conexiones de la replicación de grupo. Ningún otro usuario, incluido el usuario maestro, puede tener este nombre de usuario.

Ejemplo

En el siguiente ejemplo, se crea el usuario de replicación `rdsgrprepladmin` para la replicación de grupo en la instancia de base de datos:

```
CALL mysql.rds_group_replication_create_user('password');
```

mysql.rds_group_replication_set_recovery_channel

Establece el canal `group_replication_recovery` para un clúster activo-activo. El procedimiento utiliza el usuario reservado `rdsgrprepladmin` para configurar el canal.

Sintaxis

```
CALL mysql.rds_group_replication_set_recovery_channel(
```

```
replication_user_password);
```

Parámetros

replication_user_password

La contraseña del usuario de replicación `rdsgrprepladmin`.

Notas de uso

La contraseña del usuario de replicación `rdsgrprepladmin` debe ser la misma en todas las instancias de base de datos de un clúster activo-activo. Una llamada a `mysql.rds_group_replication_create_user` especifica la contraseña.

Ejemplo

En el siguiente ejemplo, se establece el canal `group_replication_recovery` para un clúster activo-activo.

```
CALL mysql.rds_group_replication_set_recovery_channel('password');
```

mysql.rds_group_replication_start

Inicia la replicación de grupo en la instancia de base de datos actual.

Sintaxis

```
CALL mysql.rds_group_replication_start(
bootstrap
);
```

Parámetros

bootstrap

Un valor que especifica si se debe inicializar un grupo nuevo o unirse a un grupo existente. `1`inicializa un grupo nuevo con la instancia de base de datos actual. `0` une la instancia de base de datos actual a un grupo existente conectándose a los puntos de conexión definidos en el parámetro `group_replication_group_seeds` del grupo de parámetros de base de datos asociado a la instancia de base de datos.

Ejemplo

En el siguiente ejemplo, se inicializa un grupo nuevo con la instancia de base de datos actual:

```
CALL mysql.rds_group_replication_start(1);
```

mysql.rds_group_replication_stop

Detiene la replicación de grupo en la instancia de base de datos actual.

Sintaxis

```
CALL mysql.rds_group_replication_stop();
```

Notas de uso

Cuando se detiene la replicación en una instancia de base de datos, esto no afecta a ninguna otra instancia de base de datos del clúster activo-activo.

Administración de la replicación de varios orígenes

Los siguientes procedimientos almacenados configuran y administran los canales de replicación en una réplica de varios orígenes de RDS para MySQL. Para obtener más información, consulte the section called “Configuración de la replicación de varios orígenes”.

Estos procedimientos almacenados solo están disponibles con instancias de base de datos de RDS para MySQL que ejecuten las siguientes versiones de motor:

- Todas las versiones 8.4
- 8.0.35 y versiones secundarias posteriores
- 5.7.44 y versiones secundarias posteriores

Cuando utilice procedimientos almacenados para administrar la replicación con un usuario de replicación configurado con `caching_sha2_passwword`, debe configurar TLS especificando `SOURCE_SSL=1`. `caching_sha2_password` es el complemento de autenticación predeterminado de RDS para MySQL 8.4.

> **Note**
>
> Si bien en esta documentación se hace referencia a las instancias de base de datos de origen como instancias de base de datos de RDS para MySQL, estos procedimientos también funcionan para las instancias de MySQL que se ejecutan de forma externa a Amazon RDS.

Temas

- mysql.rds_next_source_log_for_channel
- mysql.rds_reset_external_source_for_channel
- mysql.rds_set_external_source_for_channel
- mysql.rds_set_external_source_with_auto_position_for_channel
- mysql.rds_set_external_source_with_delay_for_channel
- mysql.rds_set_source_auto_position_for_channel
- mysql.rds_set_source_delay_for_channel
- mysql.rds_skip_repl_error_for_channel

- mysql.rds_start_replication_for_channel
- mysql.rds_start_replication_until_for_channel
- mysql.rds_start_replication_until_gtid_for_channel
- mysql.rds_stop_replication_for_channel

mysql.rds_next_source_log_for_channel

Cambia la posición del registro de instancia de base de datos de origen al inicio del siguiente registro binario en la instancia de base de datos de origen del canal. Use este procedimiento únicamente si aparece el error de E/S de replicación 1236 en una réplica de varios orígenes.

Sintaxis

```
CALL mysql.rds_next_source_log_for_channel(
curr_master_log,
channel_name
);
```

Parámetros

curr_master_log

El índice del archivo de registro de origen actual. Por ejemplo, si el nombre del archivo actual es `mysql-bin-changelog.012345`, el índice es 12345. Para determinar el nombre del archivo de registro de origen actual, ejecute el comando `SHOW REPLICA STATUS FOR CHANNEL 'channel_name'` y vea el campo `Source_Log_File`.

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_next_source_log_for_channel`. Si se produce un error IO_Thread, por ejemplo, puede utilizar este procedimiento para omitir todos los eventos del archivo de registro binario actual

y reanudar la replicación desde el siguiente archivo de registro binario para el canal especificado en `channel_name`.

Ejemplo

Suponga que la replicación falla en un canal de una réplica de varios orígenes. La ejecución de `SHOW REPLICA STATUS FOR CHANNEL 'channel_1'\G` en la réplica de varios orígenes devuelve el siguiente resultado:

```
mysql> SHOW REPLICA STATUS FOR CHANNEL 'channel_1'\G
*************************** 1. row ***************************
             Replica_IO_State: Waiting for source to send event
                  Source_Host: myhost.XXXXXXXXXXXXXX.rr-rrrr-1.rds.amazonaws.com
                  Source_User: ReplicationUser
                  Source_Port: 3306
                Connect_Retry: 60
              Source_Log_File: mysql-bin-changelog.012345
          Read_Source_Log_Pos: 1219393
               Relay_Log_File: replica-relay-bin.000003
                Relay_Log_Pos: 30223388
        Relay_Source_Log_File: mysql-bin-changelog.012345
           Replica_IO_Running: No
          Replica_SQL_Running: Yes
              Replicate_Do_DB:.
              .
              .
                Last_IO_Errno: 1236
                Last_IO_Error: Got fatal error 1236 from master when reading data from
 binary log: 'Client requested master to start replication from impossible position;
 the first event 'mysql-bin-changelog.013406' at 1219393, the last event read from
 '/rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4, the last byte read from '/
rdsdbdata/log/binlog/mysql-bin-changelog.012345' at 4.'
               Last_SQL_Errno: 0
               Last_SQL_Error:
               .
               .
                 Channel_name: channel_1
              .
              .
 -- Some fields are omitted in this example output
```

El campo `Last_IO_Errno` muestra que la instancia ha recibido el error de E/S 1236. El campo `Source_Log_File` muestra que el nombre de archivo es `mysql-bin-changelog.012345`, lo que significa que el índice del archivo de registro es `12345`. Para resolver el error, puede llamar a `mysql.rds_next_source_log_for_channel` con los siguientes parámetros:

```
CALL mysql.rds_next_source_log_for_channel(12345,'channel_1');
```

mysql.rds_reset_external_source_for_channel

Detiene el proceso de replicación en el canal especificado y elimina el canal y las configuraciones asociadas de la réplica de varios orígenes.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en `1`. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_reset_external_source_for_channel (channel_name);
```

Parámetros

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_reset_external_source_for_channel`. Este procedimiento elimina todos los registros de retransmisión que pertenecen al canal que se va a eliminar.

mysql.rds_set_external_source_for_channel

Puede configurar un canal de replicación en una instancia de base de datos de RDS para MySQL para replicar los datos de otra instancia de base de datos de RDS para MySQL.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

> **Note**
>
> Puede utilizar el procedimiento almacenado the section called "mysql.rds_set_external_source_with_delay_for_channel" en lugar de configurar este canal con replicación retardada.

Sintaxis

```
CALL mysql.rds_set_external_source_for_channel (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
  , channel_name
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de base de datos de origen de RDS para MySQL.

host_port

El puerto utilizado por la instancia de base de datos de origen de RDS para MySQL. Si la configuración de la red incluye la replicación de puertos Secure Shell (SSH) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El identificador de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de base de datos de origen de RDS para MySQL. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia de base de datos de origen.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

mysql_binary_log_file_name

El nombre del registro binario de la instancia de base de datos de origen que contiene la información de replicación.

mysql_binary_log_file_location

La ubicación del registro binario `mysql_binary_log_file_name` en la que la replicación empieza a leer la información de la replicación.

Para determinar el nombre y la ubicación del archivo binlog, puede ejecutar `SHOW BINARY LOG STATUS` en la instancia de base de datos de origen.

> **Note**
>
> Versiones anteriores de MySQL utilizaban `SHOW MASTER STATUS` en lugar de `SHOW BINARY LOG STATUS`. Si usa una versión de MySQL anterior a la 8.4, utilice `SHOW MASTER STATUS`.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `SOURCE_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

`nombre_canal`

El nombre del canal de replicación. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_source_for_channel`. Este procedimiento debe ejecutarse en la instancia de base de datos de RDS para MySQL de destino en la que va a crear el canal de replicación.

Antes de ejecutar `mysql.rds_set_external_source_for_channel`, configure un usuario de replicación en la instancia de base de datos de origen con los privilegios necesarios para la réplica de varios orígenes. Para conectar la réplica de varios orígenes a la instancia de base de datos de origen, debe especificar los valores de `replication_user_name` y `replication_user_password` de un usuario de la replicación que tenga permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de base de datos de origen.

Configuración de un usuario de replicación en la instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia de base de datos de origen y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   > **Important**
   >
   > Como práctica recomendada de seguridad, especifique una contraseña distinta del valor de marcador de posición que se muestra en los ejemplos siguientes.

```
CREATE USER 'repl_user'@'example.com' IDENTIFIED BY 'password';
```

2. En la instancia de base de datos de origen, conceda al usuario de replicación los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE`. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario “repl_user” de su dominio.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'example.com';
```

Para utilizar la replicación cifrada, configure la instancia de base de datos de origen para que utilice conexiones SSL.

Después de llamar a `mysql.rds_set_external_source_for_channel` para configurar este canal de replicación, puede llamar a mysql.rds_start_replication_for_channel en la réplica para iniciar el proceso de replicación en el canal. Puede llamar a the section called “mysql.rds_reset_external_source_for_channel” para detener la replicación en el canal y eliminar la configuración del canal de la réplica.

Cuando llama a `mysql.rds_set_external_source_for_channel`, Amazon RDS registra la hora, el usuario y una acción de `set channel source` en la tabla `mysql.rds_history` sin detalles específicos del canal y en la tabla `mysql.rds_replication_status` con el nombre del canal. Esta información se registra únicamente con fines de monitorización y uso interno. Para registrar toda la llamada al procedimiento con fines de auditoría, considere la posibilidad de habilitar los registros de auditoría o los registros generales, según los requisitos específicos de su aplicación.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de RDS para MySQL, el siguiente ejemplo permite configurar un canal de replicación denominado `channel_1` en esta instancia de base de datos para replicar los datos del origen especificado por el host `sourcedb.example.com` y el puerto `3306`.

```
call mysql.rds_set_external_source_for_channel(
  'sourcedb.example.com',
  3306,
  'repl_user',
  'password',
```

```
  'mysql-bin-changelog.0777',
  120,
  0,
  'channel_1');
```

mysql.rds_set_external_source_with_auto_position_for_channel

Configura un canal de replicación en una instancia de base de datos de RDS para MySQL con un retardo de replicación opcional. La replicación está basada en identificadores de transacciones globales (GTID).

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_source_with_auto_position_for_channel (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , ssl_encryption
  , delay
  , channel_name
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de base de datos de origen de RDS para MySQL.

host_port

El puerto utilizado por la instancia de base de datos de origen de RDS para MySQL. Si la configuración de la red incluye la replicación de puertos Secure Shell (SSH) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El identificador de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de base de datos de origen de RDS para MySQL. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia de base de datos de origen.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `SOURCE_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

delay

El número mínimo de segundos para retardar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

nombre_canal

El nombre del canal de replicación. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_source_with_auto_position_for_channel`. Este procedimiento debe ejecutarse en la instancia de base de datos de RDS para MySQL de destino en la que va a crear el canal de replicación.

Antes de ejecutar `rds_set_external_source_with_auto_position_for_channel`, configure un usuario de replicación en la instancia de base de datos de origen con los privilegios necesarios para la réplica de varios orígenes. Para conectar la réplica de varios orígenes a la instancia de base de datos de origen, debe especificar los valores de `replication_user_name` y `replication_user_password` de un usuario de la replicación que tenga permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de base de datos de origen.

Configuración de un usuario de replicación en la instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia de base de datos de origen y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   > **Important**
   >
   > Como práctica recomendada de seguridad, especifique una contraseña distinta del valor de marcador de posición que se muestra en los ejemplos siguientes.

   ```
   CREATE USER 'repl_user'@'example.com' IDENTIFIED BY 'password';
   ```

2. En la instancia de base de datos de origen, conceda al usuario de replicación los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE`. En el siguiente ejemplo se conceden los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario “repl_user” de su dominio.

   ```
   GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'example.com';
   ```

Para utilizar la replicación cifrada, configure la instancia de base de datos de origen para que utilice conexiones SSL.

Antes de llamar a `mysql.rds_set_external_source_with_auto_position_for_channel`, asegúrese de llamar a the section called “mysql.rds_set_external_source_gtid_purged” para configurar la variable de sistema `gtid_purged` con un rango de GTID especificado desde un origen externo.

Después de llamar a `mysql.rds_set_external_source_with_auto_position_for_channel` para configurar una instancia de base de datos de Amazon RDS como réplica de lectura en un canal específico, puede llamar a the section called “mysql.rds_start_replication_for_channel” en la réplica de lectura para iniciar el proceso de replicación en ese canal.

Después de llamar a `mysql.rds_set_external_source_with_auto_position_for_channel` para configurar este canal de replicación, puede llamar a mysql.rds_start_replication_for_channel en la réplica para iniciar el proceso de replicación en el canal. Puede llamar a the section called “mysql.rds_reset_external_source_for_channel” para detener la replicación en el canal y eliminar la configuración del canal de la réplica.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de RDS para MySQL, el siguiente ejemplo permite configurar un canal de replicación denominado `channel_1` en esta instancia de base de datos para replicar los datos del origen especificado por el host `sourcedb.example.com` y el puerto `3306`. Configura el retardo de replicación mínimo en una hora (3600 segundos). Esto significa que un cambio en la instancia de base de datos de RDS para MySQL de origen no se aplica en la réplica de varios orígenes hasta que haya transcurrido al menos una hora.

```
call mysql.rds_set_external_source_with_auto_position_for_channel(
  'sourcedb.example.com',
  3306,
  'repl_user',
  'password',
  1,
  3600,
  'channel_1');
```

mysql.rds_set_external_source_with_delay_for_channel

Configura un canal de replicación en una instancia de base de datos de RDS para MySQL con un retardo de replicación especificado.

> **Important**
>
> Para ejecutar este procedimiento, `autocommit` debe estar habilitado. Para habilitarlo, establezca el parámetro `autocommit` en 1. Para obtener información acerca de cómo modificar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Sintaxis

```
CALL mysql.rds_set_external_source_with_delay_for_channel (
  host_name
  , host_port
  , replication_user_name
  , replication_user_password
  , mysql_binary_log_file_name
  , mysql_binary_log_file_location
  , ssl_encryption
  , delay
  , channel_name
);
```

Parámetros

host_name

El nombre de host o la dirección IP de la instancia de base de datos de origen de RDS para MySQL.

host_port

El puerto utilizado por la instancia de base de datos de origen de RDS para MySQL. Si la configuración de la red incluye la replicación de puertos Secure Shell (SSH) que convierte el número de puerto, especifique el número de puerto expuesto por SSH.

replication_user_name

El identificador de un usuario con permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de base de datos de origen de RDS para MySQL. Es recomendable que proporcione una cuenta que se use solo para la replicación con la instancia de base de datos de origen.

replication_user_password

La contraseña del ID de usuario especificado en `replication_user_name`.

mysql_binary_log_file_name

El nombre del registro binario de la instancia de base de datos de origen que contiene la información de replicación.

mysql_binary_log_file_location

La ubicación del registro binario `mysql_binary_log_file_name` en la que la replicación comenzará a leer la información de la replicación.

Para determinar el nombre y la ubicación del archivo binlog, puede ejecutar `SHOW BINARY LOG STATUS` en la instancia de base de datos de origen.

> **Note**
>
> Versiones anteriores de MySQL utilizaban `SHOW MASTER STATUS` en lugar de `SHOW BINARY LOG STATUS`. Si usa una versión de MySQL anterior a la 8.4, utilice `SHOW MASTER STATUS`.

ssl_encryption

Valor que especifica si el cifrado de la capa de conexión segura (SSL) se usa en la conexión de reproducción. El 1 especifica que se usa el cifrado SSL; el 0 especifica que no se usa el cifrado. El valor predeterminado es 0.

> **Note**
>
> La opción `SOURCE_SSL_VERIFY_SERVER_CERT` no es compatible. Esta opción se establece en 0, lo que significa que la conexión está cifrada, pero los certificados no se verifican.

delay

El número mínimo de segundos para retardar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

nombre_canal

El nombre del canal de replicación. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_external_source_with_delay_for_channel`. Este procedimiento debe ejecutarse en la instancia de base de datos de RDS para MySQL de destino en la que va a crear el canal de replicación.

Antes de ejecutar `mysql.rds_set_external_source_with_delay_for_channel`, configure un usuario de replicación en la instancia de base de datos de origen con los privilegios necesarios para la réplica de varios orígenes. Para conectar la réplica de varios orígenes a la instancia de base de datos de origen, debe especificar los valores de `replication_user_name` y `replication_user_password` de un usuario de la replicación que tenga permisos `REPLICATION CLIENT` y `REPLICATION SLAVE` en la instancia de base de datos de origen.

Configuración de un usuario de replicación en la instancia de base de datos de origen

1. Con el cliente de MySQL que prefiera, conéctese a la instancia de base de datos de origen y cree una cuenta de usuario que se usará para la replicación. A continuación se muestra un ejemplo.

   > **Important**
   >
   > Como práctica recomendada de seguridad, especifique una contraseña distinta del valor de marcador de posición que se muestra en los ejemplos siguientes.

   ```
   CREATE USER 'repl_user'@'example.com' IDENTIFIED BY 'password';
   ```

2. En la instancia de base de datos de origen, conceda al usuario de replicación los privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE`. En el siguiente ejemplo se conceden los

privilegios `REPLICATION CLIENT` y `REPLICATION SLAVE` en todas las bases de datos al usuario “repl_user” de su dominio.

```
GRANT REPLICATION CLIENT, REPLICATION SLAVE ON *.* TO 'repl_user'@'example.com';
```

Para utilizar la replicación cifrada, configure la instancia de base de datos de origen para que utilice conexiones SSL.

Después de llamar a `mysql.rds_set_external_source_with_delay_for_channel` para configurar este canal de replicación, puede llamar a mysql.rds_start_replication_for_channel en la réplica para iniciar el proceso de replicación en el canal. Puede llamar a the section called “mysql.rds_reset_external_source_for_channel” para detener la replicación en el canal y eliminar la configuración del canal de la réplica.

Cuando llama a `mysql.rds_set_external_source_with_delay_for_channel`, Amazon RDS registra la hora, el usuario y una acción de `set channel source` en la tabla `mysql.rds_history` sin detalles específicos del canal y en la tabla `mysql.rds_replication_status` con el nombre del canal. Esta información se registra únicamente con fines de monitorización y uso interno. Para registrar toda la llamada al procedimiento con fines de auditoría, considere la posibilidad de habilitar los registros de auditoría o los registros generales, según los requisitos específicos de su aplicación.

Ejemplos

Cuando se ejecuta en una instancia de base de datos de RDS para MySQL, el siguiente ejemplo permite configurar un canal de replicación denominado `channel_1` en esta instancia de base de datos para replicar los datos del origen especificado por el host `sourcedb.example.com` y el puerto `3306`. Configura el retardo de replicación mínimo en una hora (3600 segundos). Esto significa que un cambio en la instancia de base de datos de RDS para MySQL de origen no se aplica en la réplica de varios orígenes hasta que haya transcurrido al menos una hora.

```
call mysql.rds_set_external_source_with_delay_for_channel(
  'sourcedb.example.com',
  3306,
  'repl_user',
  'password',
  'mysql-bin-changelog.000777',
  120,
  1,
```

```
  3600,
  'channel_1');
```

mysql.rds_set_source_auto_position_for_channel

Establece el modo de replicación para el canal especificado en el que se debe basar ya sea en posiciones de archivos de registros binarios o en identificadores de transacciones globales (GTID).

Sintaxis

```
CALL mysql.rds_set_source_auto_position_for_channel (
auto_position_mode
 , channel_name
);
```

Parámetros

auto_position_mode

Un valor que indicar si debe usarse la replicación de posición de los archivos de registro o la replicación basada en GTID:

- `0`: utilice el método de replicación basado en la posición del archivo de registro binario. El valor predeterminado es `0`.
- 1: utilice el método de replicación basado en GTID.

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_source_auto_position_for_channel`. Este procedimiento reinicia la replicación en el canal especificado para aplicar el modo de posición automática especificado.

Ejemplos

En el siguiente ejemplo, se establece el modo de posición automática para que channel_1 utilice el método de replicación basado en GTID.

```
call mysql.rds_set_source_auto_position_for_channel(1,'channel_1');
```

mysql.rds_set_source_delay_for_channel

Establece el número mínimo de segundos para retardar la replicación desde la instancia de base de datos de origen a la réplica de varios orígenes para el canal especificado.

Sintaxis

```
CALL mysql.rds_set_source_delay_for_channel(delay, channel_name);
```

Parámetros

delay

El número mínimo de segundos para retardar la replicación desde la instancia de base de datos de origen.

El límite de este parámetro es de un día (86400 segundos).

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_set_source_delay_for_channel`. Para utilizar este procedimiento, primero llame a `mysql.rds_stop_replication_for_channel` para detener la replicación. A continuación, llame a este procedimiento para establecer el valor del retardo de la replicación. Cuando el retardo esté establecido, llame a `mysql.rds_start_replication_for_channel` para reiniciar la replicación.

Ejemplos

En el ejemplo siguiente, se establece el retardo de replicación desde la instancia de base de datos de origen en `channel_1` de la réplica de varios orígenes en al menos una hora (3600 segundos).

```
CALL mysql.rds_set_source_delay_for_channel(3600,'channel_1');
```

mysql.rds_skip_repl_error_for_channel

Omite un evento de registro binario y elimina un error de replicación en una réplica de varios orígenes de base de datos MySQL para el canal especificado.

Sintaxis

```
CALL mysql.rds_skip_repl_error_for_channel(channel_name);
```

Parámetros

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_skip_repl_error_for_channel` en una réplica de lectura. Este procedimiento se puede utilizar de forma similar a como se utiliza `mysql.rds_skip_repl_error` para omitir un error en una réplica de lectura. Para obtener más información, consulte Llamar al procedimiento mysql.rds_skip_repl_error.

> **Note**
>
> Para omitir errores en la replicación basada en GTID, se recomienda utilizar este procedimiento en lugar de the section called “mysql.rds_skip_transaction_with_gtid”.

Para determinar si hay errores, ejecute el comando `SHOW REPLICA STATUS FOR CHANNEL '`*`channel_name`*`'\G` de MySQL. Si un error de replicación no es crítico, puede ejecutar

`mysql.rds_skip_repl_error_for_channel` para omitir el error. Si hay varios errores, `mysql.rds_skip_repl_error_for_channel` elimina el primer error en el canal de replicación especificado y advierte de que hay otros presentes. A continuación, puede usar `SHOW REPLICA STATUS FOR CHANNEL 'channel_name'\G` para determinar la acción correcta para el siguiente error. Para obtener información acerca de los valores devueltos, consulte la instrucción SHOW REPLICA STATUS en la documentación de MySQL.

mysql.rds_start_replication_for_channel

Inicia la replicación desde una instancia de base de datos de RDS para MySQL a una réplica de varios orígenes en el canal especificado.

> **Note**
>
> Puede utilizar el procedimiento almacenado mysql.rds_start_replication_until_for_channel o mysql.rds_start_replication_until_gtid_for_channel para iniciar la reproducción desde una instancia de base de datos de RDS for MySQL y detener la reproducción en la ubicación del archivo de registro binario especificado.

Sintaxis

```
CALL mysql.rds_start_replication_for_channel(channel_name);
```

Parámetros

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_start_replication_for_channel`. Tras importar los datos desde la instancia de base de datos de RDS para MySQL de origen, ejecute este comando en la réplica de varios orígenes para iniciar la replicación en el canal especificado.

Ejemplos

En el siguiente ejemplo, se inicia la replicación en `channel_1` de la réplica de varios orígenes.

```
CALL mysql.rds_start_replication_for_channel('channel_1');
```

mysql.rds_start_replication_until_for_channel

Inicia la replicación desde una instancia de base de datos de RDS para MySQL en el canal especificado y detiene la replicación en la ubicación del archivo de registro binario especificado.

Sintaxis

```
CALL mysql.rds_start_replication_until_for_channel (
replication_log_file
  , replication_stop_point
  , channel_name
);
```

Parámetros

`replication_log_file`

El nombre del registro binario de la instancia de base de datos de origen que contiene la información de replicación.

`replication_stop_point`

La ubicación del registro binario `replication_log_file` en la que la replicación se detendrá.

`nombre_canal`

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_start_replication_until_for_channel`. Con este procedimiento, la replicación

se inicia y, a continuación, se detiene cuando se alcanza la posición especificada del archivo binlog. Este procedimiento detiene tanto `SQL_THREAD` como `IO_THREAD`.

El nombre de archivo especificado para el parámetro `replication_log_file` debe coincidir con el nombre del archivo binlog de la instancia de base de datos de origen.

Cuando el parámetro `replication_stop_point` especifica una ubicación de parada correspondiente al pasado, la replicación se detiene de inmediato.

Ejemplos

En el ejemplo siguiente, se inicia la replicación en `channel_1` y se replican los cambios hasta que alcanza la ubicación `120` en el archivo de registro binario `mysql-bin-changelog.000777`.

```
call mysql.rds_start_replication_until_for_channel(
  'mysql-bin-changelog.000777',
  120,
  'channel_1'
  );
```

mysql.rds_start_replication_until_gtid_for_channel

Inicia la replicación en el canal especificado desde una instancia de base de datos de RDS para MySQL y detiene la replicación en el identificador de transacción global (GTID) especificado.

Sintaxis

```
CALL mysql.rds_start_replication_until_gtid_for_channel(gtid,channel_name);
```

Parámetros

`gtid`

El GTID después del cual debe detenerse la replicación.

`nombre_canal`

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_start_replication_until_gtid_for_channel`. El procedimiento inicia la replicación en el canal especificado y aplica todos los cambios hasta el valor de GTID especificado. A continuación, detiene la replicación en el canal.

Cuando el parámetro `gtid` especifica una transacción que ya ha ejecutado la réplica, la replicación se detiene de inmediato.

Antes de ejecutar este procedimiento, debe deshabilitar la réplica multiproceso estableciendo el valor de `replica_parallel_workers` o `slave_parallel_workers` en `0`.

Ejemplos

En el ejemplo siguiente, se inicia la replicación en `channel_1` y se replican los cambios hasta que alcanza la ubicación `3E11FA47-71CA-11E1-9E33-C80AA9429562:23` del GTI.

```
call mysql.rds_start_replication_until_gtid_for_channel('3E11FA47-71CA-11E1-9E33-
C80AA9429562:23','channel_1');
```

mysql.rds_stop_replication_for_channel

Detiene la replicación desde una instancia de base de datos de MySQL en el canal especificado.

Sintaxis

```
CALL mysql.rds_stop_replication_for_channel(channel_name);
```

Parámetros

nombre_canal

El nombre del canal de replicación de la réplica de varios orígenes. Cada canal de replicación recibe los eventos del registro binario de una sola instancia de base de datos de RDS para MySQL de origen que se ejecuta en un host y un puerto específicos.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_stop_replication_for_channel`.

Ejemplos

En el siguiente ejemplo, se detiene la replicación en `channel_1` de la réplica de varios orígenes.

```
CALL mysql.rds_stop_replication_for_channel('channel_1');
```

Replicación de transacciones mediante GTID

Los siguientes procedimientos almacenados controlan cómo se replican las transacciones mediante identificadores de transacciones globales (GTID) con RDS para MySQL. Para obtener más información sobre la replicación mediante GTID con RDS para MySQL, consulte Uso de la replicación basada en GTID.

Cuando utilice procedimientos almacenados para administrar la replicación con un usuario de replicación configurado con `caching_sha2_password`, debe configurar TLS especificando `SOURCE_SSL=1`. `caching_sha2_password` es el complemento de autenticación predeterminado de RDS para MySQL 8.4.

Temas

- mysql.rds_skip_transaction_with_gtid
- mysql.rds_start_replication_until_gtid

mysql.rds_skip_transaction_with_gtid

Omite la replicación de una transacción con el identificador de transacción global (GTID) especificado en una instancia de base de datos de MySQL.

Puede utilizar este procedimiento para la recuperación ante desastres cuando se sabe que una transacción de GTID específica causa un problema. Utilice este procedimiento almacenado para omitir la transacción problemática. Entre los ejemplos de transacciones problemáticas se incluyen transacciones que inhabilitan la replicación, eliminan datos importantes o provocan que la instancia de base de datos no esté disponible.

Sintaxis

```
CALL mysql.rds_skip_transaction_with_gtid (
gtid_to_skip
);
```

Parámetros

`gtid_to_skip`

El GTID de la transacción de replicación que se debe omitir.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_skip_transaction_with_gtid`.

Este procedimiento es compatible con todas las versiones de RDS para MySQL 5.7, con todas las versiones de RDS para MySQL 8.0 y con todas las versiones de RDS para MySQL 8.4.

Ejemplos

En el ejemplo siguiente se omite la replicación de la transacción con el GTID `3E11FA47-71CA-11E1-9E33-C80AA9429562:23`.

```
CALL mysql.rds_skip_transaction_with_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

mysql.rds_start_replication_until_gtid

Inicia la replicación desde una instancia de base de datos de RDS para MySQL y detiene la replicación inmediatamente después del identificador de transacción global (GTID) especificado.

Sintaxis

```
CALL mysql.rds_start_replication_until_gtid(gtid);
```

Parámetros

gtid

El GTID después del cual debe detenerse la replicación.

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_start_replication_until_gtid`.

Este procedimiento es compatible con todas las versiones de RDS para MySQL 5.7, con todas las versiones de RDS para MySQL 8.0 y con todas las versiones de RDS para MySQL 8.4.

Puede utilizar este procedimiento con la replicación retrasada para recuperación ante desastres. Si ha configurado la replicación retrasada, puede utilizar este procedimiento para restaurar los cambios

en una réplica de lectura retrasada al momento justo anterior de un desastre. Después de que este procedimiento detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Puede configurar la replicación retrasada utilizando los procedimientos almacenados siguientes:

- mysql.rds_set_configuration
- mysql.rds_set_external_master_with_delay (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores)
- mysql.rds_set_external_source_with_delay (RDS para las versiones principales de MySQL 8.4 y superiores)
- mysql.rds_set_source_delay

Cuando el parámetro `gtid` especifica una transacción que ya ha ejecutado la réplica, la replicación se detiene de inmediato.

Ejemplos

En el ejemplo siguiente se inicia la replicación y se replican los cambios hasta que alcanza el GTID `3E11FA47-71CA-11E1-9E33-C80AA9429562:23`.

```
call mysql.rds_start_replication_until_gtid('3E11FA47-71CA-11E1-9E33-C80AA9429562:23');
```

Rotación de los registros de consultas

Los siguientes procedimientos almacenados rotan los registros de MySQL en tablas de copia de seguridad. Para obtener más información, consulte Archivos de registro de base de datos de MySQL.

Temas

- mysql.rds_rotate_general_log
- mysql.rds_rotate_slow_log

mysql.rds_rotate_general_log

Rota la tabla `mysql.general_log` a una tabla de copia de seguridad.

Sintaxis

```
CALL mysql.rds_rotate_general_log;
```

Notas de uso

Para rotar la tabla `mysql.general_log` a una tabla de copia de seguridad, llame al procedimiento `mysql.rds_rotate_general_log`. Cuando se rotan las tablas de registro, la tabla de registro actual se copia en una tabla de registro de copia de seguridad y las entradas de la tabla de registro actual se eliminan. Si ya existe una tabla de registro de copia de seguridad, se elimina antes de copiar la tabla del registro actual en el copia de seguridad. Puede consultar la tabla de registro de copia de seguridad si es necesaria. La tabla de registro de copia de seguridad para la tabla `mysql.general_log` se llama `mysql.general_log_backup`.

Puede ejecutar este procedimiento solo cuando el parámetro `log_output` se establezca en`TABLE`.

mysql.rds_rotate_slow_log

Rota la tabla `mysql.slow_log` a una tabla de copia de seguridad.

Sintaxis

```
CALL mysql.rds_rotate_slow_log;
```

Notas de uso

Para rotar la tabla `mysql.slow_log` a una tabla de copia de seguridad, llame al procedimiento `mysql.rds_rotate_slow_log`. Cuando se rotan las tablas de registro, la tabla de registro actual se copia en una tabla de registro de copia de seguridad y las entradas de la tabla de registro actual se eliminan. Si ya existe una tabla de registro de copia de seguridad, se elimina antes de copiar la tabla del registro actual en el copia de seguridad.

Puede consultar la tabla de registro de copia de seguridad si es necesaria. La tabla de registro de copia de seguridad para la tabla `mysql.slow_log` se llama `mysql.slow_log_backup`.

Establecimiento y muestra de la configuración del registro binario

Los siguientes procedimientos almacenados establecen y muestran los parámetros de configuración, por ejemplo, para la retención de archivos de registro binario.

Temas

- mysql.rds_set_configuration
- mysql.rds_show_configuration

mysql.rds_set_configuration

Especifica el número de horas que se deben conservar los registros binarios o el número de segundos que se retrasará la replicación.

Sintaxis

```
CALL mysql.rds_set_configuration(name,value);
```

Parámetros

name

El nombre del parámetro de configuración que se va a definir.

value

El valor del parámetro de configuración.

Notas de uso

El procedimiento `mysql.rds_set_configuration` admite los parámetros de configuración siguientes:

- binlog retention hours
- Retardo del origen
- target delay

Los parámetros de configuración se almacenan de forma permanente y sobreviven a cualquier reinicio o conmutación por error de una instancia de base de datos.

binlog retention hours

El parámetro `binlog retention hours` se usa para especificar la cantidad de horas que se deben retener los archivos de registro binario. Por lo general, Amazon RDS limpia un registro binario lo antes posible, pero el registro binario podría seguir siendo necesario para la replicación con una base de datos MySQL externa a RDS.

El valor predeterminado de `binlog retention hours` es `NULL`. En RDS para MySQL, `NULL` significa que los registros binarios no se retienen (0 horas).

Para especificar el número de horas que se deben retener los registros binarios en una instancia de base de datos, utilice el procedimiento almacenado `mysql.rds_set_configuration` y especifique un periodo lo bastante largo como para realizar la replicación, como se muestra en el siguiente ejemplo.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

> **Note**
>
> No puede utilizar el valor `0` para `binlog retention hours`.

Para la mayoría de las instancias de base de datos de MySQL, el valor máximo de `binlog retention hours` es 168 (7 días).

Una vez que haya definido el periodo de retención, monitorice el uso del almacenamiento para la instancia de base de datos con el fin de asegurarse de que los logs binarios conservados no consuman demasiado almacenamiento.

Para las implementaciones de clústeres de base de datos multi-AZ, solo puede configurar la retención de registros binarios desde la instancia de base de datos del escritor y la configuración se propaga a todas las instancias de base de datos del lector de forma asíncrona. Si los registros binarios del clúster de base de datos superan la mitad del espacio total de almacenamiento local, Amazon RDS mueve automáticamente los registros obsoletos al volumen de EBS. Sin embargo, los registros más recientes permanecen en el almacenamiento local, por lo que podrían perderse si se produce un fallo que requiera la sustitución del host o si se escala la base de datos vertical u horizontalmente.

Retardo del origen

Utilice el parámetro `source delay` en una réplica de lectura para especificar el número de segundos que se debe retrasar la replicación desde la réplica de lectura a su instancia de base de datos de origen. Amazon RDS suele replicar los cambios lo antes posible, pero podría ser conveniente retrasar la replicación en algunos entornos. Por ejemplo, cuando la replicación se ha retrasado, puede restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Si una tabla se elimina por accidente, puede usar la replicación retardada para recuperarla rápidamente. El valor predeterminado de `target delay` es `0` (no retrasar la replicación).

Al utilizar este parámetro, se ejecuta mysql.rds_set_source_delay y aplica CHANGE primary TO MASTER_DELAY = valor de entrada. Si el procedimiento se realiza correctamente, guarda el parámetro `source delay` en la tabla `mysql.rds_configuration`.

Para especificar el número de segundos que Amazon RDS debe retrasar la replicación en una instancia de base de datos de origen, utilice el procedimiento almacenado `mysql.rds_set_configuration` y especifique el número de segundos que deberá retrasarse la replicación. En el ejemplo siguiente, se especifica que la replicación se retrasa al menos una hora (3600 segundos).

```
call mysql.rds_set_configuration('source delay', 3600);
```

A continuación, se ejecuta el procedimiento `mysql.rds_set_source_delay(3600)`.

El límite del parámetro `source delay` es de un día (86400 segundos).

target delay

Utilice el parámetro `target delay` para especificar el número de segundos que se retrasará la replicación entre una instancia de base de datos y cualquier réplica de lectura futura administrada por RDS creada a partir de esta instancia. Este parámetro se omite para las réplicas de lectura no administradas por RDS. Amazon RDS suele replicar los cambios lo antes posible, pero podría ser conveniente retrasar la replicación en algunos entornos. Por ejemplo, cuando la replicación se ha retrasado, puede restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre. Si una tabla se elimina por accidente, puede usar la replicación retrasada para recuperarla rápidamente. El valor predeterminado de `target delay` es `0` (no retrasar la replicación).

Para la recuperación de desastres, puede utilizar este parámetro de configuración con el procedimiento almacenado mysql.rds_start_replication_until o el procedimiento

almacenado mysql.rds_start_replication_until_gtid. Para restaurar los cambios en una réplica de lectura retrasada al momento justo anterior de un desastre puede ejecutar el procedimiento `mysql.rds_set_configuration` con este parámetro establecido. Después de que el procedimiento `mysql.rds_start_replication_until` o `mysql.rds_start_replication_until_gtid` detenga la replicación, puede promocionar la réplica de lectura para que sea la nueva instancia de base de datos primaria utilizando las instrucciones de Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Para utiliza el procedimiento `mysql.rds_rds_start_replication_until_gtid`, debe habilitarse la replicación basada en GTID. Para omitir una transacción específica basada en GTID que se sabe que causa un desastre, puede usar el procedimiento almacenado mysql.rds_skip_transaction_with_gtid. Para obtener más información sobre el uso de la replicación basada en GTID, consulte Uso de la replicación basada en GTID.

Para especificar el número de segundos que Amazon RDS debe retrasar la replicación en una réplica de lectura, utilice el procedimiento almacenado `mysql.rds_set_configuration` y especifique el número de segundos que deberá retrasarse la replicación. En el ejemplo siguiente se especifica que la replicación se retrasa al menos una hora (3600 segundos).

```
call mysql.rds_set_configuration('target delay', 3600);
```

El límite del parámetro `target delay` es de un día (86400 segundos).

mysql.rds_show_configuration

El número de horas que se conservan los registros binarios.

Sintaxis

```
CALL mysql.rds_show_configuration;
```

Notas de uso

Para verificar el número de horas que Amazon RDS conserva los registros binarios, use el procedimiento almacenado `mysql.rds_show_configuration`.

Ejemplos

El ejemplo siguiente muestra el periodo de retención:

```
call mysql.rds_show_configuration;
                name                          value     description
                binlog retention hours        24        binlog retention hours specifies
 the duration in hours before binary logs are automatically deleted.
```

Calentamiento de caché de InnoDB

Los siguientes procedimientos almacenados guardan, cargan o cancelan la carga del grupo de búferes de InnoDB en RDS para instancias de base de datos de RDS para MySQL. Para obtener más información, consulte Calentamiento de caché de InnoDB para MySQL en Amazon RDS.

Temas

- mysql.rds_innodb_buffer_pool_dump_now
- mysql.rds_innodb_buffer_pool_load_abort
- mysql.rds_innodb_buffer_pool_load_now

mysql.rds_innodb_buffer_pool_dump_now

Vuelca el estado actual del grupo del búfer en el disco.

Sintaxis

```
CALL mysql.rds_innodb_buffer_pool_dump_now();
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_innodb_buffer_pool_dump_now`.

mysql.rds_innodb_buffer_pool_load_abort

Cancela una carga del estado guardado del grupo del búfer mientras está en curso.

Sintaxis

```
CALL mysql.rds_innodb_buffer_pool_load_abort();
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_innodb_buffer_pool_load_abort`.

mysql.rds_innodb_buffer_pool_load_now

Carga el estado guardado del grupo del búfer desde el disco.

Sintaxis

```
CALL mysql.rds_innodb_buffer_pool_load_now();
```

Notas de uso

El usuario maestro debe ejecutar el procedimiento `mysql.rds_innodb_buffer_pool_load_now`.

Amazon RDS para Oracle

Amazon RDS admite instancias de base de datos que ejecutan las siguientes versiones y ediciones de Oracle Database:

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)

> **Note**
>
> Oracle Database 11g, Oracle Database 12c y Oracle Database 18c son versiones heredadas que ya no son compatibles con Amazon RDS.

Antes de crear una instancia de base de datos, complete los pasos que se describen en la sección Configuración del entorno para Amazon RDS de esta guía. Cuando crea una instancia de base de datos con su cuenta maestra, la cuenta obtiene privilegios de DBA, con algunas limitaciones. Utilice esta cuenta para tareas administrativas, como crear cuentas de base de datos adicionales. No puede utilizar SYS, SYSTEM u otras cuentas administrativas proporcionadas por Oracle.

Puede crear lo siguiente:

- Instancias de base de datos
- Instantáneas de base de datos
- Restauraciones a un momento dado
- Copias de seguridad automatizadas
- Copias de seguridad manuales

Puede utilizar instancias de base de datos que ejecuten la base de datos de Oracle dentro de una VPC. También puede agregar características a la instancia de base de datos mediante la habilitación de varias opciones, como Oracle Spatial u Oracle Statspack. Amazon RDS admite implementaciones multi-AZ para Oracle como una solución de conmutación por error de alta disponibilidad.

> **Important**
>
> Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Puede acceder a la base de datos con clientes estándar de SQL, como Oracle SQL*Plus. No obstante, no puede acceder al host directamente mediante Telnet o Secure Shell (SSH).

Temas

- Información general de Oracle en Amazon RDS
- Conexión a una instancia de base de datos de Oracle
- Protección de conexiones de instancias de base de datos de Oracle
- Uso de CDB con RDS para Oracle
- Administración de la instancia de base de datos de RDS para Oracle
- Configuración de características avanzadas de RDS para Oracle
- Importación de datos a Oracle en Amazon RDS
- Trabajo con las réplicas de lectura para Amazon RDS para Oracle
- Adición de opciones a instancias de base de datos de Oracle
- Actualización del motor de base de datos de RDS para Oracle
- Uso de software de terceros con la instancia de base de datos de RDS for Oracle
- Notas de la versión del motor de Oracle Database

Información general de Oracle en Amazon RDS

Puede leer las siguientes secciones para obtener una descripción general de RDS para Oracle.

Temas

- Características de RDS para Oracle
- Versiones de RDS para Oracle
- Opciones de licencias de RDS para Oracle
- Usuarios y privilegios de RDS para Oracle

- Clases de instancias de base de datos de RDS para Oracle
- Arquitectura de base de datos de RDS para Oracle
- Parámetros de inicialización de RDS para Oracle
- RDS para conjuntos de caracteres de Oracle
- Limitaciones de RDS para Oracle

Características de RDS para Oracle

Amazon RDS for Oracle admite la mayoría de las características y capacidades de Oracle Database. Algunas características pueden disponer de una compatibilidad limitada o de privilegios restringidos. Algunas características están solo disponibles en Enterprise Edition y otras requieren licencias adicionales. Para obtener información sobre las características de la Oracle Database para versiones específicas de Oracle Database, consulte el Oracle Database Licensing Information User Manual (Manual de usuario de información sobre concesión de licencias de Oracle Database) para la versión que esté utilizando.

Temas

- Características nuevas de RDS para Oracle
- Características admitidas de RDS para Oracle
- Características no admitidas de RDS para Oracle

Características nuevas de RDS para Oracle

Para ver las nuevas características en RDS para Oracle, busque Historial de revisión para la palabra clave **`Oracle`**.

Características admitidas de RDS para Oracle

Amazon RDS para Oracle admite las siguientes características de Oracle Database:

> **Note**
>
> Lo que sigue no es una lista completa.

- Advanced Compression

- Oracle Application Express

  Para obtener más información, consulte Oracle Application Express.
- Automatic Memory Management
- Automatic Undo Management
- Automatic Workload Repository (AWR)

  Para obtener más información, consulte Generación de informes de rendimiento con Automatic Workload Repository (AWR).
- Active Data Guard con el máximo rendimiento en la misma región de AWS o en todas las regiones de AWS

  Para obtener más información, consulte Trabajo con las réplicas de lectura para Amazon RDS para Oracle.
- Tablas de cadenas de bloques (Oracle Database 21c y posteriores)

  Para obtener más información, consulte el tema sobre administración de tablas de bloques en la documentación de Oracle Database.
- Notificación de consulta continua

  Para obtener más información, consulte Using Continuous Query Notification (CQN) en la documentación de Oracle.
- Data Redaction
- Notificación de consulta continua

  Para obtener más información, consulte Database Change Notification en la documentación de Oracle.
- Base de datos en memoria
- Distributed Queries and Transactions
- Edition-Based Redefinition

  Para obtener más información, consulte Configuración de la edición predeterminada para una instancia de base de datos.
- EM Express (12c y versiones posteriores)

  Para obtener más información, consulte Oracle Enterprise Manager.

- Fine-Grained Auditing
- Flashback Table, Flashback Query, Flashback Transaction Query
- Sustitución gradual de contraseñas para aplicaciones (Oracle Database 21c y versiones posteriores)

  Para obtener más información, consulte el tema sobre administración de la sustitución gradual de contraseñas de bases de datos para aplicaciones en la documentación de Oracle Database.
- HugePages

  Para obtener más información, consulte Activación de páginas de gran tamaño para una instancia de RDS para Oracle.
- Import/export (heredado y Data Pump) y SQL*Loader

  Para obtener más información, consulte Importación de datos a Oracle en Amazon RDS.
- Máquina virtual Java (JVM)

  Para obtener más información, consulte Máquina virtual Oracle Java.
- JavaScript (Oracle Database 21c y versiones posteriores)

  Para obtener más información, consulte DBMS_MLE en la documentación de Oracle Database.
- Label Security

  Para obtener más información, consulte Oracle Label Security.
- Locator

  Para obtener más información, consulte Oracle Locator.
- Vistas materializadas
- Multitenant

  La arquitectura multitenencia Oracle es compatible con todas las versiones de Oracle Database 19c y superiores. Para obtener más información, consulte Uso de CDB con RDS para Oracle.
- Network encryption

  Para obtener más información, consulte Oracle Native Network Encryption y Capa de conexión segura de Oracle.
- Particiones
- Real Application Testing

Para utilizar todas las funciones de captura y reproducción, debe utilizar Amazon Elastic File System (Amazon EFS) para acceder a los archivos generados por Oracle Real Application Testing. Para obtener más información, consulte Integración de Amazon EFS y la entrada del blog Use Oracle Real Application Testing features with Amazon RDS for Oracle.

- Partición en el nivel de aplicación (no incluye la característica de partición de Oracle)
- Spatial and Graph

  Para obtener más información, consulte Oracle Spatial.
- Star Query Optimization
- Streams and Advanced Queuing
- Summary Management – Materialized View Query Rewrite
- Text (los tipos de almacén de datos de URL y archivos no son compatibles)
- Total Recall
- Cifrado de datos transparente (TDE)

  Para obtener más información, consulte Cifrado de datos transparente de Oracle.
- Unified Auditing, Mixed Mode

  Para obtener más información, consulte Mixed Mode Auditing en la documentación de Oracle.
- XML DB (sin XML DB Protocol Server)

  Para obtener más información, consulte Oracle XML DB.
- Virtual Private Database

Características no admitidas de RDS para Oracle

Amazon RDS para Oracle no es compatible con las características de Oracle Database:

> **Note**
>
> Lo que sigue no es una lista completa.

- Automatic Storage Management (ASM)

- Database Vault
- Flashback Database

> **Note**
>
> Para obtener soluciones alternativas, consulte la entrada del blog de AWS sobre alternativas a la característica de base de datos flashback de Oracle en Amazon RDS para Oracle.

- FTP y SFTP
- Tablas particionadas híbridas
- Gateway de mensajería
- Oracle Enterprise Manager Cloud Control Management Repository
- Real Application Clusters (Oracle RAC)
- Real Application Security (RAS)
- Unified Auditing, Pure Mode
- Esquema de Workspace Manager (WMSYS)

> **Warning**
>
> En general, Amazon RDS no impide crear esquemas para características no admitidas. Sin embargo, si crea esquemas para características y componentes de Oracle que requieren privilegios SYSDBA, puede dañar el diccionario de datos y afectar a la disponibilidad de la instancia de base de datos. Utilice solo las características y esquemas compatibles que estén disponibles en Adición de opciones a instancias de base de datos de Oracle.

Versiones de RDS para Oracle

RDS para Oracle es compatible con múltiples versiones de Oracle Database.

> **Note**
>
> Para obtener información acerca de cómo actualizar sus versiones, consulte Actualización del motor de base de datos de RDS para Oracle.

Temas

- Oracle Database 21 con Amazon RDS
- Oracle Database 19c con Amazon RDS

Oracle Database 21 con Amazon RDS

Amazon RDS admite la versión Oracle Database 21c, que incluye Oracle Enterprise Edition y Oracle Standard Edition 2. Oracle Database 21c (21.0.0.0) incluye muchas características y actualizaciones nuevas con respecto a la versión anterior. Un cambio clave es que Oracle Database 21c solo admite la arquitectura multiinquilino: ya no se puede crear una base de datos como una base de datos tradicional no CDB. Para obtener más información sobre las diferencias entre bases de datos CDB y no CDB, consulte Limitaciones de las CDB de RDS para Oracle.

En esta sección encontrará características y cambios importantes para usar Oracle Database 21c (21.0.0.0) en Amazon RDS. Para obtener una lista completa de los cambios, consulte la documentación de Oracle Database 21c. Para ver una lista completa de las características compatibles de cada edición de Oracle Database 21c, consulte el tema sobre características admitidas, opciones y paquetes de administración de la oferta de productos de Oracle Database en la documentación de Oracle.

Amazon RDS cambios de parámetros para Oracle Database 21c (21.0.0.0)

Oracle Database 21c (21.0.0.0) incluye varios parámetros nuevos, así como parámetros con rangos y valores predeterminados nuevos.

Temas

- Parámetros nuevos
- Cambios en el parámetro compatible
- Parámetros eliminados

Parámetros nuevos

En la siguiente tabla se muestran los parámetros nuevos de Amazon RDS for Oracle Database 21c (21.0.0.0).

Nombre	Rango de valores	Valor predeterminado	Modificable	Descripción
blockchain_table_max_no_drop	NONE | 0	NONE	Y	Permite controlar la cantidad máxima de tiempo de inactividad que se puede especificar al crear una tabla de cadena de bloques.
dbnest_enable	NONE | CDB_RESOURCE_PDB_ALL	NONE	N	Permite habilitar o deshabilitar dbNest. dbNest permite aislar y administrar recursos del sistema operativo, aislar sistemas de archivos y computación segura para las PDB.
dbnest_pdb_fs_conf	NONE | *pathname*	NONE	N	Especifica el archivo de configuración del sistema de archivos dbNest para una PDB.
diagnostics_control	ERROR | WARNING | IGNORE	IGNORE	Y	Permite controlar y supervisar a los usuarios que realizan operaciones de diagnóstico de bases de datos potencialmente no seguras.
drcp_dedicated_opt	YES | NO	YES	Y	Habilita o deshabilita el uso de optimización dedicada con agrupación de conexiones residentes de bases de datos (DRCP).
enable_per_pdb_drcp	true | false	true	N	Controla si la agrupación de conexiones residentes de bases de datos (DRCP)

Nombre	Rango de valores	Valor predeterminado	Modificable	Descripción
				configura un grupo de conexiones para toda la CDB o un grupo de conexiones aislado para cada PDB.
inmemory_deep_vectorization	`true | false`	`true`	Y	Habilita o deshabilita el marco de vectorización profunda.
mandatory_user_profile	*`nombre_de_perfil`*	N/A	N	Especifica el perfil de usuario obligatorio para una CDB o una PDB.
optimizer_capture_sql_quarantine	`true | false`	`false`	Y	Habilita o deshabilita el marco de vectorización profunda.
optimizer_use_sql_quarantine	`true | false`	`false`	Y	Habilita o deshabilita la creación automática de configuraciones de cuarentena SQL.
result_cache_execution_threshold	De `0` a `68719476736`	`2`	Y	Especifica el número máximo de veces que se puede ejecutar una función PL/SQL antes de que su resultado se almacene en la caché de resultados.

Nombre	Rango de valores	Valor predeterminado	Modificable	Descripción
result_cache_max_temp_result	De 0 a 100	5	Y	Especifica el porcentaje de RESULT_CACHE_MAX_TEMP_SIZE que puede consumir un resultado de consulta almacenado en caché.
result_cache_max_temp_size	De 0 a 2199023255552	RESULT_CACHE_SIZE * 10	Y	Especifica la cantidad máxima de espacios de tabla temporal (en bytes) que puede consumir la caché de resultados.
sga_min_size	De 0 a 2199023255552 (el valor máximo es 50 % de sga_target)	0	Y	Indica un posible valor mínimo para el uso de SGA de una base de datos conectable (PDB).
tablespace_encryption_default_algorithm	GOST256 | SEED128 | ARIA256 | ARIA192 | ARIA128 | 3DES168 | AES256 | AES192 | AES128	AES128	Y	Especifica el algoritmo predeterminado que utiliza la base de datos al cifrar un espacio de tabla.

Cambios en el parámetro compatible

El parámetro `compatible` tiene un nuevo valor máximo para Oracle Database 21c (21.0.0.0) en Amazon RDS. En la siguiente tabla se muestra el valor predeterminado nuevo.

Nombre del parámetro	Valor máximo en Oracle Database 21c (21.0.0.0)
compatible	21.0.0

Parámetros eliminados

Los siguientes parámetros se han eliminado en Oracle 21c Database (21.0.0.0):

- `remote_os_authent`
- `sec_case_sensitive_logon`
- `unified_audit_sga_queue_size`

Oracle Database 19c con Amazon RDS

Amazon RDS admite Oracle Database 19c, que incluye Oracle Enterprise Edition y Oracle Standard Edition Two.

Oracle Database 19c (19.0.0.0) incluye muchas características y actualizaciones nuevas con respecto a la versión anterior. En esta sección, podrá encontrar las características y los cambios importantes para usar Oracle Database 19c (19.0.0.0) en Amazon RDS. Para obtener una lista completa de los cambios, consulte la documentación de Oracle Database 19c. Para obtener una lista completa de las características compatibles de cada edición de Oracle Database 19c, consulte Permitted Features, Options, and Management Packs by Oracle Database Offering en la documentación de Oracle.

Amazon RDS cambios de parámetros para Oracle Database 19c (19.0.0.0)

Oracle Database 19c (19.0.0.0) incluye varios parámetros nuevos, así como parámetros con rangos y valores predeterminados nuevos.

Temas

- Parámetros nuevos

- Cambios en el parámetro compatible
- Parámetros eliminados

Parámetros nuevos

En la siguiente tabla se muestran los parámetros nuevos de Amazon RDS for Oracle Database 19c (19.0.0.0).

Nombre	Valores	Modifi le	Descripción
lob_signature_enable	TRUE, FALSE (predeterminado)	S	Habilita o deshabilita la caracterí stica de firma del localizador de LOB.
max_datapump_parallel_per_job	1 a 1024 o AUTOMÁTICO	S	Especifica el número máximo de procesos paralelos permitidos para cada trabajo de Oracle Data Pump.

Cambios en el parámetro compatible

El parámetro `compatible` tiene un nuevo valor máximo para Oracle Database 19c (19.0.0.0) en Amazon RDS. En la siguiente tabla se muestra el valor predeterminado nuevo.

Nombre del parámetro	Valor máximo de Oracle Database 19c (19.0.0.0)
compatible	19.0.0

Parámetros eliminados

Los siguientes parámetros se eliminaron en Oracle 19c Database (19.0.0.0):

- `exafusion_enabled`
- `max_connections`
- `o7_dictionary_access`

Opciones de licencias de RDS para Oracle

Amazon RDS para Oracle tiene dos opciones de licencia: License Included (LI) y Bring Your Own License (BYOL). Después de crear una instancia de base de datos de Oracle en Amazon RDS, puede cambiar el modelo de licencia modificando la instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Important**
>
> Asegúrese de tener la licencia de Oracle Database adecuada, con Software Update License and Support, para su clase de instancia de base de datos y edición de Oracle Database. Asegúrese también de tener licencias para cualquier característica de Oracle Database con licencia independiente.

Temas

- Modelo con licencia incluida para SE2
- Traiga su propia licencia (BYOL) para EE y SE2
- Licencias en implementaciones Multi-AZ de Oracle

Modelo con licencia incluida para SE2

En el modelo de licencia incluida, no es necesario adquirir licencias de Oracle Database por separado; AWS tiene la licencia para el software de base de datos de Oracle. El modelo de licencia incluido solo es compatible con Amazon RDS para Oracle Database Standard Edition 2 (SE2).

En este modelo, si tiene una cuenta de AWS Support con soporte para incidencias, puede contactar a Soporte para las solicitudes de servicio relacionadas con Amazon RDS y Oracle Database. El uso de la opción LI de RDS para Oracle está sujeto a la sección 10.3.1 de los Términos de servicio de AWS.

Traiga su propia licencia (BYOL) para EE y SE2

En el modelo BYOL, puede utilizar sus licencias existentes de Oracle Database para desplegar bases de datos en Amazon RDS. Amazon RDS admite el modelo BYOL solo para Oracle Database Enterprise Edition (EE) y Oracle Database Standard Edition 2 (SE2).

Asegúrese de tener la licencia de Oracle Database adecuada (con Software Update License and Support) para la clase de instancia de base de datos y la edición de Oracle Database que desee ejecutar. También debe seguir las políticas de Oracle en cuanto a licencias de software de Oracle Database en el entorno de informática en la nube. Para obtener más información acerca de la política de licencias de Oracle para Amazon EC2, consulte Licensing Oracle Software in the Cloud Computing Environment.

En este modelo, continuará utilizando su cuenta de soporte de Oracle activa y se pondrá en contacto con Oracle directamente para las solicitudes de servicio relacionadas con Oracle Database. Si tiene una cuenta de AWS Support con soporte para incidencias, puede contactar a Soporte para solucionar problemas relacionados con Amazon RDS. Amazon Web Services y Oracle tienen un proceso de soporte multiproveedor para las incidencias que necesitan asistencia por parte de las dos organizaciones.

Integración con AWS License Manager

Para facilitar la supervisión del uso de licencias de Oracle en el modelo BYOL, AWS License Manager se integra con Amazon RDS para Oracle. License Manager admite el seguimiento de RDS para ediciones del motor de Oracle y paquetes de licencias basados en núcleos virtuales (vCPUs). También puede utilizar License Manager con AWS Organizations para administrar todas las cuentas de su organización de forma centralizada.

En la siguiente tabla se muestran los filtros de información del producto de RDS para Oracle.

Filtro	Nombre	Descripción
Edición del motor	`oracle-ee`	Oracle Database Enterprise Edition (EE)
	`oracle-se2`	Oracle Database Standard Edition 2 (SE2)
Paquete de licencias	`data guard`	Consulte Trabajo con las réplicas de lectura para Amazon RDS para Oracle (Oracle Active Data Guard)
	`olap`	Consulte Oracle OLAP
	`ols`	Consulte Oracle Label Security
	`diagnostic pack sqlt`	Consulte Oracle SQLT

Filtro	Nombre	Descripción
	`tuning pack sqlt`	Consulte Oracle SQLT.

Para hacer un seguimiento del uso de sus instancias de base de datos de Oracle, puede crear una licencia autoadministrada con AWS License Manager. En este caso, los recursos de RDS para Oracle que coinciden con el filtro de información del producto se asocian automáticamente a la configuración de la licencia autoadministrada. La detección de instancias de base de datos de Oracle puede tardar hasta 24 horas. También puede realizar un seguimiento de una licencia en todas las cuentas mediante AWS Resource Access Manager.

Consola

Creación de una licencia autoadministrada en AWS License Manager a fin de hacer un seguimiento del uso de licencias de sus instancias de base de datos de RDS para Oracle

1. Vaya a https://console.aws.amazon.com/license-manager/.
2. Seleccione Crear licencia autoadministrada.

   Para obtener instrucciones, consulte Create a self-managed license en la Guía del usuario de AWS License Manager.

   Agregue una regla para un RDS Product Information Filter (Filtro de información del producto de RSD) en el panel Product Information (Información del producto).

   Para obtener más información, consulte ProductInformation en la Referencia de la API de AWS License Manager.
3. (Solo para el seguimiento entre cuentas) Utilice AWS Resource Access Manager para compartir sus licencias autoadministradas con cualquier cuenta AWS o mediante AWS Organizations. Para obtener más información, consulte Uso compartido de los recursos de AWS.

AWS CLI

Para crear una licencia autoadministrada mediante la AWS CLI, llame al comando create-license-configuration. Use los parámetros `--cli-input-json` o `--cli-input-yaml` para transmitir los parámetros al comando.

Example

En el siguiente ejemplo, se crea una licencia autoadministrada para Oracle Enterprise Edition.

```
aws license-manager create-license-configuration --cli-input-json file://rds-oracle-
ee.json
```

Lo siguiente es el archivo `rds-oracle-ee.json` de muestra utilizado en el ejemplo.

```
{
    "Name": "rds-oracle-ee",
    "Description": "RDS Oracle Enterprise Edition",
    "LicenseCountingType": "vCPU",
    "LicenseCountHardLimit": false,
    "ProductInformationList": [
        {
            "ResourceType": "RDS",
            "ProductInformationFilterList": [
                {
                    "ProductInformationFilterName": "Engine Edition",
                    "ProductInformationFilterValue": ["oracle-ee"],
                    "ProductInformationFilterComparator": "EQUALS"
                }
            ]
        }
    ]
}
```

Para obtener más información acerca de la información del producto, consulte Detección automatizada del inventario de recursos en la Guía del usuario de AWS License Manager.

Para obtener más información sobre el parámetro `--cli-input`, consulte Generar AWS CLIel esqueleto y los parámetros de entrada a partir de un archivo de entrada JSON o YAML en la AWS CLIGuía del usuario de

Migración entre ediciones de Oracle Database

Si tiene una licencia BYOL Oracle Database sin utilizar adecuada para la edición y clase de instancia de base de datos que planea ejecutar, puede migrar de Standard Edition 2 (SE2) a Enterprise Edition (EE). No puede migrar de EE a otras ediciones.

Para cambiar de edición de Oracle Database y conservar los datos

1. Cree una instantánea de la instancia de la base de datos.

   Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
2. Restaure la instantánea a una instancia de base de datos nueva y seleccione la edición de la base de datos Oracle que desea utilizar.

   Para obtener más información, consulte Restauración a una instancia de base de datos.
3. (Opcional) Elimine la antigua instancia de base de datos, a menos que quiera que siga ejecutándose y disponga de las licencias para la base de datos Oracle necesarias.

   Para obtener más información, consulte Eliminación de una instancia de base de datos.

Licencias en implementaciones Multi-AZ de Oracle

Amazon RDS admite implementaciones Multi-AZ para Oracle como una solución de conmutación por error de alta disponibilidad. Recomendamos Multi-AZ para las cargas de trabajo de producción. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Si utiliza el modelo Bring-Your-Own-License, debe tener una licencia para la instancia de base de datos principal y para la instancia de base de datos en espera en una implementación Multi-AZ.

Usuarios y privilegios de RDS para Oracle

Al crear una instancia de base de datos de Amazon RDS para Oracle, el usuario maestro predeterminado tiene la mayoría de los permisos de usuario máximos de la instancia de base de datos. Utilice la cuenta del usuario maestro para las tareas administrativas, como la creación de cuentas de usuario adicionales en la base de datos. Dado que RDS es un servicio administrado, no se le permite iniciar sesión como `SYS` y `SYSTEM`, y por lo tanto no tiene privilegios `SYSDBA`.

Temas

- Limitaciones de los privilegios de Oracle DBA
- Administración de privilegios en los objetos SYS

Limitaciones de los privilegios de Oracle DBA

En la base de datos, un rol es una colección de privilegios que puede conceder o revocar a un usuario. Una base de datos de Oracle utiliza roles para proporcionar seguridad. Para obtener más información, consulte Configuring Privilege and Role Authorization en la documentación de Oracle Database.

El rol predefinido de DBA normalmente permite todos los privilegios administrativos en una base de datos de Oracle. Cuando crea una instancia de base de datos, su cuenta de usuario principal obtiene privilegios de DBA (con algunas limitaciones). Para ofrecer una experiencia administrada, una base de datos de RDS para Oracle no proporciona los siguientes privilegios para el rol de DBA:

- `ALTER DATABASE`
- `ALTER SYSTEM`
- `CREATE ANY DIRECTORY`
- `DROP ANY DIRECTORY`
- `GRANT ANY PRIVILEGE`
- `GRANT ANY ROLE`

Para obtener más información sobre los privilegios y funciones del sistema RDS para Oracle, consulte Privilegios de la cuenta de usuario maestro.

Administración de privilegios en los objetos SYS

Puede administrar los privilegios en objetos SYS mediante el paquete `rdsadmin.rdsadmin_util`. Por ejemplo, si crea el usuario de la base de datos `myuser`, puede utilizar el procedimiento `rdsadmin.rdsadmin_util.grant_sys_object` para conceder privilegios `SELECT` en `V_$SQLAREA` a `myuser`. Para obtener más información, consulte los temas siguientes:

- Concesión de privilegios SELECT o EXECUTE para objetos SYS
- Revocación de privilegios SELECT o EXECUTE para objetos SYS
- Concesión de privilegios a usuarios no maestros

Clases de instancias de base de datos de RDS para Oracle

La capacidad de cómputo y de memoria de la instancia de base de datos de RDS para Oracle se determina mediante su clase de instancia. La clase de instancia de base de datos que necesita depende de la potencia de procesamiento y de los requisitos de memoria.

Clases de instancias admitidas de RDS para Oracle

Las clases de instancia admitidas de RDS para Oracle son un subconjunto de las clases de instancia de base de datos de RDS. Para ver la lista completa de las clases de instancia de RDS, consulte Clases de instancia de base de datos de .

Clases de instancias de bases de datos preconfiguradas de RDS para Oracle

RDS para Oracle también ofrece clases de instancias preconfiguradas para cargas de trabajo que requieren memoria, almacenamiento y E/S adicionales por vCPU. Estas clases de instancia utilizan la siguiente convención de nomenclatura:

```
db.r5b.instance_size.tpcthreads_per_core.memratio
db.r5.instance_size.tpcthreads_per_core.memratio
```

A continuación, se muestra un ejemplo de una clase de instancia que está preconfigurada para memoria adicional:

```
db.r5b.4xlarge.tpc2.mem2x
```

Los componentes del nombre de clase de instancia anterior son los siguientes:

- `db.r5b.4xlarge`: el nombre de la clase de instancia.
- `tpc2`: los subprocesos por núcleo. Un valor de 2 significa que el multiproceso está activado. Un valor de 1 significa que el multiproceso está desactivado.
- `mem2x`: la relación entre la memoria adicional y la memoria estándar para la clase de instancia. En este ejemplo, la optimización proporciona el doble de memoria que una instancia de db.r5.4xlarge estándar.

Combinaciones de licencias, clase de instancia y ediciones compatibles en RDS para Oracle

Si utiliza la consola RDS, puede saber si una determinada edición, clase de instancia o combinación de licencia es compatible; para ello, seleccione Crear base de datos y especifique una opción diferente. En la AWS CLI, puede ejecutar el siguiente comando:

```
aws rds describe-orderable-db-instance-options --engine engine-type --license-
model license-type
```

En la siguiente tabla, se enumeran todas las ediciones, clases de instancias y tipos de licencia compatibles con RDS para Oracle. Para obtener información acerca de los atributos de memoria de cada tipo, consulte Tipos de instancia de RDS para Oracle. Para obtener más información acerca de los precios, consulte Modelos de precios de Amazon RDS para Oracle.

Edición de Oracle	Oracle Database 19c y versiones posteriores
Enterprise Edition (EE)	Clases de instancia estándar
Traiga su propia licencia (BYOL)	db.m7i.large–db.m7i.48xlarge db.m6id.large–db.m6id.32xlarge db.m6i.large–db.m6i.32xlarge db.m5d.large–db.m5d.24xlarge db.m5.large–db.m5.24xlarge
	Clases de instancia optimizadas para memoria
	db.r7i.large–db.r7i.48xlarge db.r6id.large–db.r6id.32xlarge db.r6i.large–db.r6i.32xlarge db.r5d.large–db.r5d.24xlarge db.r5b.large–db.r5b.24xlarge db.r5.large–db.r5.24xlarge

Edición de Oracle	Oracle Database 19c y versiones posteriores
	db.x2iedn.xlarge–db.x2iedn.32xlarge db.x2iezn.2xlarge–db.x2iezn.12xlarge db.x2idn.16xlarge–db.x2idn.32xlarge db.x1e.xlarge–db.x1e.32xlarge db.x1.16xlarge–db.x1.32xlarge[1] db.z1d.large–db.z1d.12xlarge
	Clases de instancias preconfiguradas y optimizadas para memoria

Edición de Oracle	Oracle Database 19c y versiones posteriores
	db.r6i.8xlarge.tpc2.mem4x
	db.r6i.8xlarge.tpc2.mem3x
	db.r6i.6xlarge.tpc2.mem4x
	db.r6i.4xlarge.tpc2.mem4x
	db.r6i.4xlarge.tpc2.mem3x
	db.r6i.4xlarge.tpc2.mem2x
	db.r6i.2xlarge.tpc2.mem8x
	db.r6i.2xlarge.tpc2.mem4x
	db.r6i.2xlarge.tpc1.mem2x
	db.r6i.xlarge.tpc2.mem4x
	db.r6i.xlarge.tpc2.mem2x
	db.r6i.large.tpc1.mem2x
	db.r5b.8xlarge.tpc2.mem3x
	db.r5b.6xlarge.tpc2.mem4x
	db.r5b.4xlarge.tpc2.mem4x
	db.r5b.4xlarge.tpc2.mem3x
	db.r5b.4xlarge.tpc2.mem2x
	db.r5b.2xlarge.tpc2.mem8x
	db.r5b.2xlarge.tpc2.mem4x
	db.r5b.2xlarge.tpc1.mem2x
	db.r5b.xlarge.tpc2.mem4x

Edición de Oracle	Oracle Database 19c y versiones posteriores
	db.r5b.xlarge.tpc2.mem2x
	db.r5b.large.tpc1.mem2x
	db.r5.12xlarge.tpc2.mem2x
	db.r5.8xlarge.tpc2.mem3x
	db.r5.6xlarge.tpc2.mem4x
	db.r5.4xlarge.tpc2.mem4x
	db.r5.4xlarge.tpc2.mem3x
	db.r5.4xlarge.tpc2.mem2x
	db.r5.2xlarge.tpc2.mem8x
	db.r5.2xlarge.tpc2.mem4x
	db.r5.2xlarge.tpc1.mem2x
	db.r5.xlarge.tpc2.mem4x
	db.r5.xlarge.tpc2.mem2x
	db.r5.large.tpc1.mem2x
	Clases de instancia de rendimiento con ráfagas
	db.t3.small–db.t3.2xlarge

Edición de Oracle	Oracle Database 19c y versiones posteriores
Standard Edition 2 (SE2)	Clases de instancia estándar
Traiga su propia licencia (BYOL)	db.m7i.large–db.m7i.4xlarge db.m6id.large–db.m6id.4xlarge db.m6i.large–db.m6i.4xlarge db.m5d.large–db.m5d.4xlarge db.m5.large–db.m5.4xlarge
	Clases de instancia optimizadas para memoria
	db.r7i.large–db.r7i.4xlarge db.r6id.large–db.r6id.4xlarge db.r6i.large–db.r6i.4xlarge db.r5d.large–db.r5d.4xlarge db.r5b.large–db.r5b.4xlarge db.r5.large–db.r5.4xlarge db.x2iedn.xlarge–db.x2iedn.4xlarge db.x2iezn.2xlarge–db.x2iezn.4xlarge db.z1d.large–db.z1d.3xlarge
	Clases de instancias preconfiguradas optimizadas para memoria

Edición de Oracle	Oracle Database 19c y versiones posteriores
	db.r6i.4xlarge.tpc2.mem4x
	db.r6i.4xlarge.tpc2.mem3x
	db.r6i.4xlarge.tpc2.mem2x
	db.r6i.2xlarge.tpc2.mem8x
	db.r6i.2xlarge.tpc2.mem4x
	db.r6i.2xlarge.tpc1.mem2x
	db.r6i.xlarge.tpc2.mem4x
	db.r6i.xlarge.tpc2.mem2x
	db.r6i.large.tpc1.mem2x
	db.r5b.4xlarge.tpc2.mem4x
	db.r5b.4xlarge.tpc2.mem3x
	db.r5b.4xlarge.tpc2.mem2x
	db.r5b.2xlarge.tpc2.mem8x
	db.r5b.2xlarge.tpc2.mem4x
	db.r5b.2xlarge.tpc1.mem2x
	db.r5b.xlarge.tpc2.mem4x
	db.r5b.xlarge.tpc2.mem2x
	db.r5b.large.tpc1.mem2x
	db.r5.4xlarge.tpc2.mem4x
	db.r5.4xlarge.tpc2.mem3x
	db.r5.4xlarge.tpc2.mem2x

Edición de Oracle	Oracle Database 19c y versiones posteriores
	db.r5.2xlarge.tpc2.mem8x
	db.r5.2xlarge.tpc2.mem4x
	db.r5.2xlarge.tpc1.mem2x
	db.r5.xlarge.tpc2.mem4x
	db.r5.xlarge.tpc2.mem2x
	db.r5.large.tpc1.mem2x
	Clases de instancia de rendimiento con ráfagas
	db.t3.small–db.t3.2xlarge
Standard Edition 2 (SE2)	Clases de instancia estándar
Licencia incluida	db.m5.large–db.m5.4xlarge
	Clases de instancia optimizadas para memoria
	db.r6i.large–db.r6i.4xlarge
	db.r5.large–db.r5.4xlarge
	Clases de instancia de rendimiento con ráfagas
	db.t3.small–db.t3.2xlarge

[1] Ya no puede crear instancias de base de datos de RDS para Oracle con la familia de clases de instancia X1.* (las clases de instancia X1e.* todavía se admiten). Si usa clases X1.* actualmente, cambie a una clase de instancia de nueva generación lo antes posible. A partir del 22 de enero de 2025, RDS iniciará las actualizaciones automatizadas dentro del periodo de mantenimiento definido. Durante la actualización, RDS elige el tipo de instancia X2iedn equivalente y lo actualiza. Para obtener más información, consulte el artículo de re:Post Amazon RDS for Oracle is ending support for X1 Database Instances on January 22, 2025.

> **Note**
>
> Animamos a todos los clientes con bring-your-own-license (traiga su propia licencia) a que consulten sus acuerdos de licencia para determinar el efecto de las obsolescencias de Amazon RDS for Oracle. Para obtener más información sobre la capacidad de computación de las clases de instancias de bases de datos admitidas por RDS para Oracle, consulte Clases de instancia de base de datos de y Configuración del procesador de una clase de instancias de base de datos en RDS para Oracle.

> **Note**
>
> Si tiene instantáneas de base de datos de instancias de bases de datos que usaban clases de instancia de base de datos obsoleta, puede elegir una instancia de base de datos que no esté obsoleta cuando restaure las instantáneas de base de datos. Para obtener más información, consulte Restauración a una instancia de base de datos.

Clases de instancias de bases de datos obsoletas para RDS para Oracle

A continuación, se presentan las clases de instancia de base de datos obsoletas para RDS para Oracle:

- db.m1, db.m2, db.m3, db.m4
- db.t1, db.t2
- db.r1, db.r2, db.r3, db.r4

Estas clases de instancia de base de datos se han sustituido por clases de instancia de base de datos con un mejor desempeño que están disponibles generalmente a un costo inferior. Si tiene instancias de base de datos que utilizan clases de instancias de bases de datos obsoletas, tiene las siguientes opciones:

- Permita que Amazon RDS modifique cada instancia de base de datos automáticamente para utilizar una clase de instancia de base de datos comparable no obsoleta. Para conocer los plazos de obsolescencia, consulte Tipos de clase de instancia de base de datos.

- Cambie la clase de instancia de la base de datos usted mismo modificando la instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Si tiene instantáneas de base de datos de instancias de bases de datos que usaban clases de instancia de base de datos obsoleta, puede elegir una instancia de base de datos que no esté obsoleta cuando restaure las instantáneas de base de datos. Para obtener más información, consulte Restauración a una instancia de base de datos.

Arquitectura de base de datos de RDS para Oracle

La arquitectura multitenencia de Oracle, también denominada arquitectura CDB, permite que una base de datos Oracle funcione como base de datos de tipo contenedor multitenencia (CDB). Una CDB puede incluir bases de datos conectables (PDB) creadas por el cliente. Una base de datos que no es CDB es una base de datos Oracle que utiliza la arquitectura tradicional y no puede contener PDB. Para obtener más información sobre la arquitectura de varios inquilinos, consulte Guía del administrador de Oracle de varios inquilinos.

Para Oracle Database 19c y superiores, puede crear una instancia de base de datos de RDS para Oracle que utilice la arquitectura de CDB. En RDS para Oracle, las PDB se denominan bases de datos de inquilinos. Las aplicaciones de cliente se conectan en el nivel de la base de datos de inquilinos (PDB) y no en el de la CDB. RDS para Oracle es compatible con las siguientes configuraciones de la arquitectura CDB:

Configuración de varios inquilinos

La plataforma RDS que se utilice para que una instancia de CDB de RDS para Oracle contenga entre 1 y 30 bases de datos de inquilinos, en función de la edición de la base de datos y de las licencias de opciones necesarias. Puede utilizar las API de RDS para agregar, modificar y eliminar bases de datos de inquilinos. La configuración de varios inquilinos en RDS para Oracle no admite las PDB de aplicación ni las PDB de proxy, que son tipos especiales de PDB. Para obtener más información sobre las PDB de aplicación y las PDB de proxy, consulte Tipos de PDB en la documentación de Oracle Database.

> **Note**
>
> La configuración de Amazon RDS se denomina “de varios inquilinos”, en lugar de “multitenencia”, ya que es una capacidad de la plataforma RDS, no solo del motor de

base de datos de Oracle. De manera similar, el término “inquilino” de RDS se refiere a cualquier inquilino en una configuración de RDS, no solo a las PDB de Oracle. En la documentación de RDS, el término “de varios inquilinos de Oracle” sin guion se refiere exclusivamente a la arquitectura CDB de la base de datos de Oracle, que es compatible tanto con las implementaciones en las instalaciones como con RDS.

Configuración de un solo inquilino

La característica de la plataforma RDS limita la instancia de CDB de RDS para Oracle a una base de datos de 1 inquilino (PDB). No puede añadir más PDB con las API de RDS. La configuración de un solo inquilino utiliza las mismas API de RDS que la arquitectura no CDB. Por lo tanto, la experiencia de trabajar con una CDB en la configuración de un solo inquilino es prácticamente la misma que la de trabajar con una no CDB.

Puede convertir una CDB con la configuración de un solo inquilino a la configuración de varios inquilinos, lo que le permite agregar PDB a su CDB. Este cambio de arquitectura es permanente e irreversible. Para obtener más información, consulte Convertir la configuración de un solo inquilino a una de varios inquilinos..

Note

No se puede acceder a la CDB en sí.

En Oracle Database 21c y versiones posteriores, todas las bases de datos son CDB. En cambio, puede crear una instancia de base de datos de Oracle Database 19c como CDB o no CDB. No puede actualizar una no CDB a CDB, pero puede convertir una Oracle Database 19c que no sea CDB en CDB y, a continuación, actualizarla. No se puede actualizar una CDB en no CDB.

Para obtener más información, consulte los siguientes recursos:

- Uso de CDB con RDS para Oracle
- Limitaciones de las CDB de RDS para Oracle
- Creación de una instancia de base de datos de Amazon RDS

Parámetros de inicialización de RDS para Oracle

En Amazon RDS, administre parámetros con un grupo de parámetros de base de datos. Con este grupo, puede personalizar los parámetros de inicialización. Por ejemplo, puede configurar el tamaño del área de ordenación con `sort_area_size`. Todas las instancias de base de datos de RDS para Oracle asociadas a un grupo de parámetros de base de datos específico utilizan la misma configuración de parámetros. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

Parámetros de inicialización admitidos en RDS para Oracle

Los parámetros admitidos para la instancia de base de datos dependen de la edición y versión de Oracle Database. Para ver los parámetros de inicialización compatibles con una edición y versión específicas de Oracle Database, ejecute el comando `describe-engine-default-parameters` de la AWS CLI. Por ejemplo, para ver los parámetros de inicialización admitidos para Enterprise Edition de Oracle Database 19c, ejecute el siguiente comando (ejemplo de salida incluido).

```
aws rds describe-engine-default-parameters \
    --db-parameter-group-family oracle-ee-19 \
    --output json | jq -r '.EngineDefaults.Parameters[].ParameterName'

_add_col_optim_enabled
_adg_parselock_timeout
_allow_insert_with_update_check
_allow_level_without_connect_by
_always_semi_join
_autotask_max_window
_awr_disabled_flush_tables
_awr_mmon_cpuusage
_awr_mmon_deep_purge_all_expired
_b_tree_bitmap_plans
_bct_bitmaps_per_file
_bloom_filter_enabled
_buffered_publisher_flow_control_threshold
_bug29394014_allow_triggers_on_vpd_table
_cleanup_rollback_entries
_client_enable_auto_unregister
_clusterwide_global_transactions
_complex_view_merging
_connect_by_use_union_all
_cost_equality_semi_join
```

```
_cursor_features_enabled
_cursor_obsolete_threshold
_datafile_write_errors_crash_instance
_db_block_buffers
...
```

Para describir un único parámetro de inicialización, utilice el siguiente comando, sustituyendo `sga_max_size` por el nombre del parámetro (se incluye un ejemplo de salida).

```
aws rds describe-engine-default-parameters \
    --db-parameter-group-family oracle-ee-19 \
    --query 'EngineDefaults.Parameters[?ParameterName==`sga_max_size`]' \
    --output json

[
    {
        "ParameterName": "sga_max_size",
        "Description": "max total SGA size",
        "Source": "engine-default",
        "ApplyType": "static",
        "DataType": "integer",
        "AllowedValues": "0-2199023255552",
        "IsModifiable": true
    }
]
```

Para encontrar documentación general de los parámetros de inicialización de la base de datos de Oracle, consulte Parámetros de inicialización en la documentación de Oracle Database. Tenga en cuenta que el parámetro `ARCHIVE_LAG_TARGET` tiene consideraciones especiales en RDS para Oracle. Este parámetro fuerza a que se cambie el registro de recuperación de cambios una vez transcurrido el tiempo especificado. En RDS para Oracle, `ARCHIVE_LAG_TARGET` se establece en `300` porque el objetivo de punto de recuperación (RPO) es de 5 minutos. Para cumplir este objetivo, RDS para Oracle cambia el registro redo en línea cada 5 minutos y lo almacena en un bucket de Amazon S3.

Si la frecuencia del cambio de registro de recuperación de cambios provoca un problema de rendimiento en la base de datos de RDS para Oracle, puede escalar la instancia de base de datos y el almacenamiento para usar un rendimiento y un IOPS más altos. Como alternativa, si utiliza RDS Custom para Oracle o implementa una base de datos de Oracle en Amazon EC2, puede ajustar la configuración del parámetro de inicialización `ARCHIVE_LAG_TARGET`.

Valores de parámetro válidos en RDS para Oracle

En RDS para Oracle, solo los siguientes caracteres son válidos para los valores de los parámetros:

- Letras (`A-Z` y `a-z`)
- Números (`0-9`)
- Espacios en blanco (espacios, tabulaciones y saltos de línea)
- Los siguientes caracteres especiales: `_ / . : + = ( ) ' * , % $ -` (guion)

RDS para conjuntos de caracteres de Oracle

RDS para Oracle admite dos tipos de juegos de caracteres: el juego de caracteres de base de datos y el juego de caracteres nacional.

Conjunto de caracteres de base de datos

El juego de caracteres de base de datos Oracle se utiliza en los tipos de datos `CHAR`, `VARCHAR2` y `CLOB`. La base de datos también utiliza este juego de caracteres para metadatos como nombres de tablas, nombres de columnas y sentencias SQL. Normalmente, el juego de caracteres de la base de datos Oracle se denomina juego de caracteres de base de datos.

Establezca el conjunto de caracteres al crear una instancia de base de datos. No puede cambiar el juego de caracteres de la base de datos después de crear la base de datos.

Conjuntos de caracteres de base de datos admitidos

En la siguiente tabla se enumeran los conjuntos de caracteres de Oracle Database admitidos en Amazon RDS. Puede usar un valor de esta tabla con el parámetro `--character-set-name` con el comando create-db-instance de la AWS CLI o con el parámetro `CharacterSetName` de la operación CreateDBInstance de la API de Amazon RDS.

> **Note**
>
> El conjunto de caracteres de una base de datos de contenedores (CDB) siempre es AL32UTF8. Puede establecer un conjunto de caracteres diferente solo para la base de datos conectable (PDB).

Valor	Descripción
AL32UTF8	Conjunto de caracteres universal UTF-8 Unicode 5.0 (predeterminado)
AR8ISO8859P6	ISO 8859-6: latinos/árabes
AR8MSWIN1256	Página de códigos 1256 de Microsoft Windows: latinos/árabes de 8 bits
BLT8ISO8859P13	ISO 8859-13: bálticos
BLT8MSWIN1257	Página de códigos 1257 de Microsoft Windows: bálticos de 8 bits
CL8ISO8859P5	ISO 88559-5: latinos/cirílicos
CL8MSWIN1251	Página de códigos 1251 de Microsoft Windows: latinos/cirílicos de 8 bits
EE8ISO8859P2	ISO 8859-2: Europa oriental
EL8ISO8859P7	ISO 8859-7: latinos/griegos
EE8MSWIN1250	Página de códigos 1250 de Microsoft Windows: Europa oriental (de 8 bits)
EL8MSWIN1253	Página de códigos 1253 de Microsoft Windows: latinos/griegos de 8 bits
IW8ISO8859P8	ISO 8859-8: latinos/hebreos
IW8MSWIN1255	Página de códigos 1255 de Microsoft Windows: latinos/hebreos de 8 bits
JA16EUC	EUC: japoneses de 24 bits
JA16EUCTILDE	Igual que JA16EUC, excepto para el mapeo de la raya ondulada y la tilde, desde y hacia Unicode

Valor	Descripción
JA16SJIS	Shift-JIS: japoneses de 16 bits
JA16SJISTILDE	Igual que JA16SJIS, excepto para el mapeo de la raya ondulada y la tilde, desde y hacia Unicode
KO16MSWIN949	Página de códigos 949 de Microsoft Windows: coreanos
NE8ISO8859P10	ISO 8859-10: Norte de Europa
NEE8ISO8859P4	ISO 8859-4: Norte y Noreste de Europa
TH8TISASCII	Estándar industrial tailandés 620-2533-ASCII de 8 bits
TR8MSWIN1254	Página de códigos 1254 de Microsoft Windows: turcos de 8 bits
US7ASCII	ASCII de 7 bits americano
UTF8	Conjunto de caracteres universal UTF-8 Unicode 3.0, conforme con CESU-8
VN8MSWIN1258	Página de códigos 1258 de Microsoft Windows: vietnamitas de 8 bits
WE8ISO8859P1	ISO 8859 parte 1: Europa occidental (de 8 bits)
WE8ISO8859P15	ISO 8859-15: Europa occidental
WE8ISO8859P9	ISO 8859-9: Europa occidental y turcos
WE8MSWIN1252	Página de códigos 1252 de Microsoft Windows: Europa occidental (de 8 bits)
ZHS16GBK	GBK: chino simplificado (de 16 bits)

Valor	Descripción
ZHT16HKSCS	Página de códigos 950 de Microsoft Windows con el conjunto de caracteres suplementarios HKSCS-2001 para Hong Kong. La conversión del conjunto de caracteres se basa en Unicode 3.0.
ZHT16MSWIN950	Página de códigos 950 de Microsoft Windows: chino tradicional
ZHT32EUC	EUC: chino tradicional (de 32 bits)

Variable de entorno NLS_LANG

Una configuración regional es un conjunto de información que aborda los requisitos lingüísticos y culturales que corresponde a un idioma y país determinados. La forma más sencilla de especificar el comportamiento de la configuración regional para Oracle consiste en establecer la variable de entorno NLS_LANG en el entorno del cliente. Esta variable establece el idioma y el territorio utilizados por la aplicación cliente y el servidor de bases de datos. También indica el conjunto de caracteres del cliente, que corresponde al conjunto de caracteres para los datos introducidos o mostrados por una aplicación cliente. Para obtener más información acerca de NLS_LANG y los conjuntos de caracteres, consulte What is a Character set or Code Page? en la documentación de Oracle.

Parámetros de inicialización de NLS

También puede especificar los siguientes parámetros de inicialización de National Language Support (NLS) en el nivel de la instancia para una instancia de base de datos de Oracle en Amazon RDS:

- NLS_DATE_FORMAT
- NLS_LENGTH_SEMANTICS
- NLS_NCHAR_CONV_EXCP
- NLS_TIME_FORMAT
- NLS_TIME_TZ_FORMAT
- NLS_TIMESTAMP_FORMAT
- NLS_TIMESTAMP_TZ_FORMAT

Para obtener información acerca de cómo modificar los parámetros de la instancia, consulte Grupos de parámetros para Amazon RDS.

También puede definir otros parámetros de inicialización de NLS en el cliente SQL. Por ejemplo, la siguiente instrucción especifica el parámetro de inicialización NLS_LANGUAGE en GERMAN para un cliente SQL conectado a una instancia de base de datos de Oracle:

```
ALTER SESSION SET NLS_LANGUAGE=GERMAN;
```

Para obtener información acerca de la conexión a su instancia de base de datos de Oracle con un cliente SQL, consulte Conexión a una instancia de base de datos de Oracle.

Conjunto de caracteres nacionales

El juego de caracteres nacional se utiliza en los tipos de datos `NCHAR`, `NVARCHAR2` y `NCLOB`. El conjunto de caracteres nacionales se conoce normalmente como el conjunto de caracteres NCHAR. A diferencia del conjunto de caracteres de base de datos, el conjunto de caracteres NCHAR no afecta a los metadatos de la base de datos.

El conjunto de caracteres NCHAR admite los siguientes conjuntos de caracteres:

- AL16UTF16 (predeterminado)
- UTF8

Puede especificar cualquiera de los valores con el parámetro `--nchar-character-set-name` del comando create-db-instance (AWS CLI solo versión 2). Si utiliza la API de Amazon RDS, especifique el parámetro `NcharCharacterSetName` de la operación CreateDBInstance. No se puede cambiar el juego de caracteres nacionales después de crear la base de datos.

Para obtener más información acerca de Unicode en bases de datos Oracle, consulte Compatibilidad con bases de datos multilingües con Unicode en la documentación de Oracle.

Limitaciones de RDS para Oracle

En las siguientes secciones, encontrará importantes limitaciones del uso de RDS para Oracle. Para conocer las limitaciones específicas de las CDB, consulte Limitaciones de las CDB de RDS para Oracle.

> **Note**
>
> Esta lista no es exhaustiva.

Temas

- Límites de tamaño de archivo Oracle en Amazon RDS
- Límites de tamaño de bloque en RDS para Oracle
- Sinónimos públicos de esquemas suministrados por Oracle
- Esquemas para características no admitidas de RDS para Oracle
- Limitaciones para los privilegios de DBA en RDS para Oracle
- Obsolescencia de Seguridad de la capa de transporte (TLS) 1.0 y 1.1 en RDS para Oracle

Límites de tamaño de archivo Oracle en Amazon RDS

El tamaño máximo de un archivo en las instancias de base de datos de RDS para Oracle es de 16 TiB. Este límite lo impone el sistema de archivos ext4 que utiliza la instancia. Por lo tanto, los archivos de datos Bigfile de Oracle están limitados a 16 TiB. Si intenta cambiar el tamaño de un archivo de datos de un espacio de tabla bigfile a un valor superior al límite, recibirá un error como el siguiente:

```
ORA-01237: cannot extend datafile 6
ORA-01110: data file 6: '/rdsdbdata/db/mydir/datafile/myfile.dbf'
ORA-27059: could not reduce file size
Linux-x86_64 Error: 27: File too large
Additional information: 2
```

Límites de tamaño de bloque en RDS para Oracle

El tamaño máximo de un bloque en las instancias de base de datos de RDS para Oracle es de 8 KB. No se admite el tamaño de bloque de 16 KB.

Sinónimos públicos de esquemas suministrados por Oracle

No cree o modifique los sinónimos públicos para los esquemas suministrados por Oracle, incluidos `SYS`, `SYSTEM` y `RDSADMIN`. Estas acciones pueden provocar la invalidación de los componentes principales de la base de datos y afectar a la disponibilidad de la instancia de base de datos.

Puede crear sinónimos públicos que hagan referencia a objetos en sus propios esquemas.

Esquemas para características no admitidas de RDS para Oracle

En general, Amazon RDS no impide crear esquemas para características no admitidas. Sin embargo, si crea esquemas para características y componentes de Oracle que requieren privilegios SYS, puede dañar el diccionario de datos y afectar a la disponibilidad de la instancia. Utilice solo las características y esquemas compatibles que estén disponibles en Adición de opciones a instancias de base de datos de Oracle.

Limitaciones para los privilegios de DBA en RDS para Oracle

En la base de datos, un rol es una colección de privilegios que puede conceder o revocar a un usuario. Una base de datos de Oracle utiliza roles para proporcionar seguridad.

El rol predefinido de `DBA` normalmente permite todos los privilegios administrativos en una base de datos de Oracle. Cuando crea una instancia de base de datos, su cuenta de usuario principal obtiene privilegios de DBA (con algunas limitaciones). Para ofrecer una experiencia administrada, una base de datos de RDS para Oracle no proporciona los siguientes privilegios para el rol de `DBA`:

- `ALTER DATABASE`
- `ALTER SYSTEM`
- `CREATE ANY DIRECTORY`
- `DROP ANY DIRECTORY`
- `GRANT ANY PRIVILEGE`
- `GRANT ANY ROLE`

Utilice la cuenta de usuario principal para tareas administrativas, como la creación de cuentas de usuario adicionales en la base de datos. No puede utilizar `SYS`, `SYSTEM` y otras cuentas administrativas proporcionadas por Oracle.

Obsolescencia de Seguridad de la capa de transporte (TLS) 1.0 y 1.1 en RDS para Oracle

Las versiones 1.0 y 1.1 del protocolo de Transport Layer Security (TLS 1.0 y TLS 1.1) están obsoletas. De acuerdo con las prácticas recomendadas de seguridad, Oracle ha dejado de usar TLS 1.0 y TLS 1.1. Para cumplir con los requisitos de seguridad, recomendamos encarecidamente que se utilice TLS 1.2 en su lugar.

Conexión a una instancia de base de datos de Oracle

Después de que Amazon RDS aprovisione su instancia de base de datos Oracle, puede usar cualquier aplicación cliente de SQL estándar para iniciar sesión en la instancia de base de datos. Como RDS es un servicio administrado, no puede iniciar sesión como SYS o SYSTEM. Para obtener más información, consulte Usuarios y privilegios de RDS para Oracle.

En este tema, aprenderá a usar Oracle SQL Developer o SQL*Plus para conectarse a una instancia de base de datos de RDS para Oracle. Para ver un ejemplo que le enseña los procesos para crear y conectarse a una instancia de base de datos de muestra, consulte Creación y conexión a una instancia de base de datos de Oracle.

Temas

- Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle
- Conexión a la instancia de base de datos mediante Oracle SQL Developer
- Conexión a la instancia de base de datos mediante SQL*Plus
- Consideraciones para grupos de seguridad
- Consideraciones para la arquitectura de procesos
- Solución de problemas de conexiones a la instancia de base de datos de Oracle
- Modificación de propiedades de conexión utilizando parámetros sqlnet.ora

Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle

Cada instancia de base de datos de Amazon RDS contiene un punto de enlace y cada punto de enlace contiene el nombre DNS y el número de puerto para la instancia de base de datos. Para conectarse a su instancia de base de datos mediante una aplicación cliente SQL, necesita el nombre DNS y el número de puerto para la instancia de base de datos.

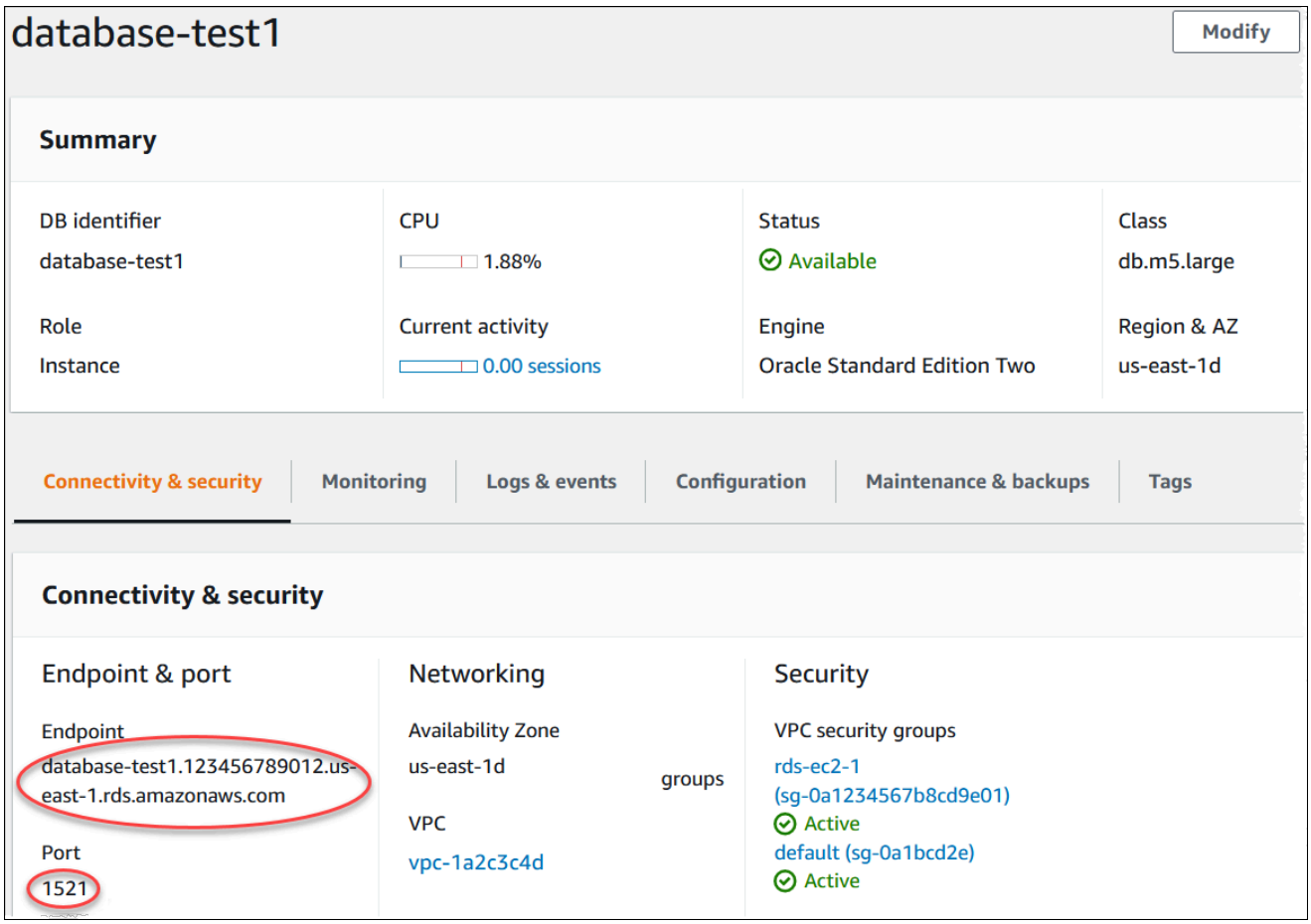
Puede encontrar los puntos de enlace para una instancia de base de datos mediante la consola de Amazon RDS o la AWS CLI.

> **Note**
>
> Si está utilizando autenticación Kerberos, consulte Conexión a Oracle con autenticación Kerberos.

Consola

Para buscar el punto de enlace mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola, elija la AWS región de la instancia de base de datos.
3. Busque el nombre DNS y el número de puerto para su instancia de base de datos.
   a. Elija Databases (Bases de datos) para ver una lista de las instancias de base de datos.
   b. Seleccione el nombre de la instancia de base de datos Oracle para mostrar los detalles de la instancia.
   c. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



AWS CLI

Para crear un punto de enlace para una instancia de base de datos de Oracle mediante la AWS CLI, llame al comando describe-db-instances.

Example Para buscar el punto de enlace mediante la AWS CLI

```
aws rds describe-db-instances
```

Busque `Endpoint` en la salida para encontrar el nombre DNS y el número de puerto para la instancia de base de datos. La línea `Address` en la salida contiene el nombre DNS. Véase a continuación un ejemplo de la salida del punto de enlace JSON.

```
"Endpoint": {
    "HostedZoneId": "Z1PVIF0B656C1W",
    "Port": 3306,
    "Address": "myinstance.123456789012.us-west-2.rds.amazonaws.com"
},
```

> **Note**
>
> La salida puede contener información acerca de varias instancias de base de datos.

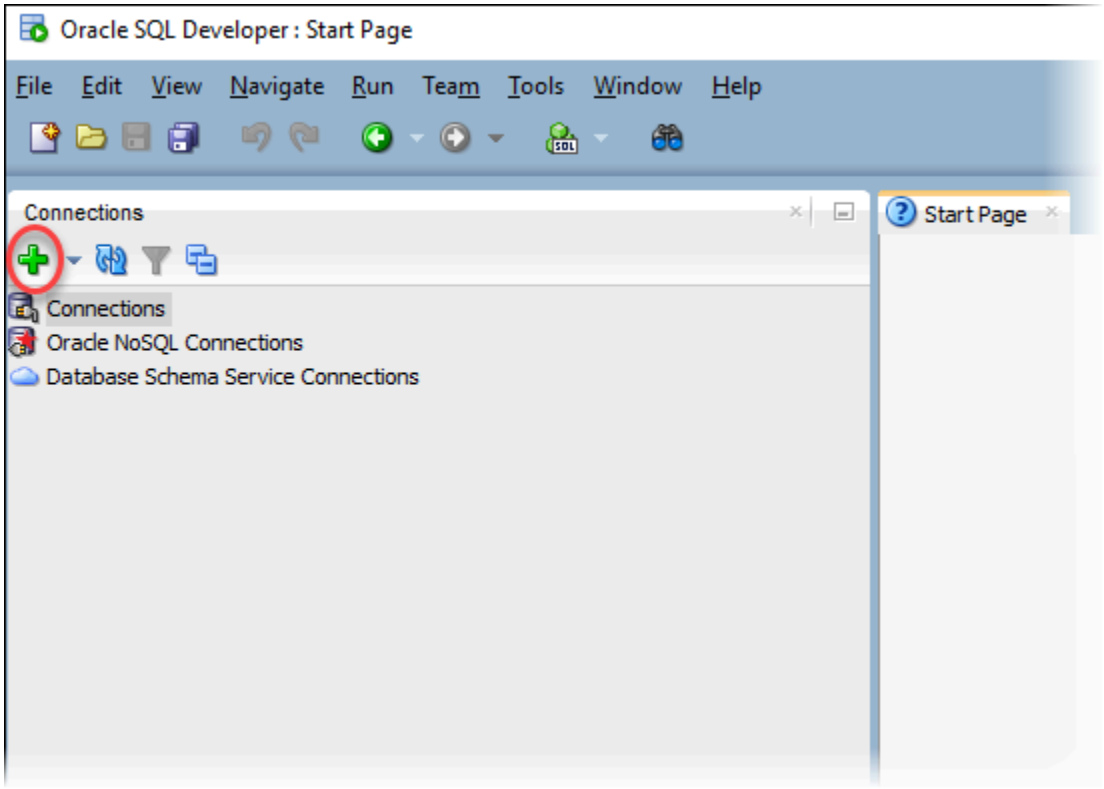
Conexión a la instancia de base de datos mediante Oracle SQL Developer

En este procedimiento, puede conectarse a la instancia de base de datos mediante Oracle SQL Developer. Para descargar una versión independiente de esta utilidad, consulte la página Oracle SQL Developer Downloads.

Para conectarse a una instancia de base de datos, necesita su nombre DNS y el número de puerto. Para obtener información sobre cómo buscar el nombre DNS y el número de puerto para una instancia de base de datos, consulte Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle.

Para conectarse a una instancia de base de datos mediante SQL Developer

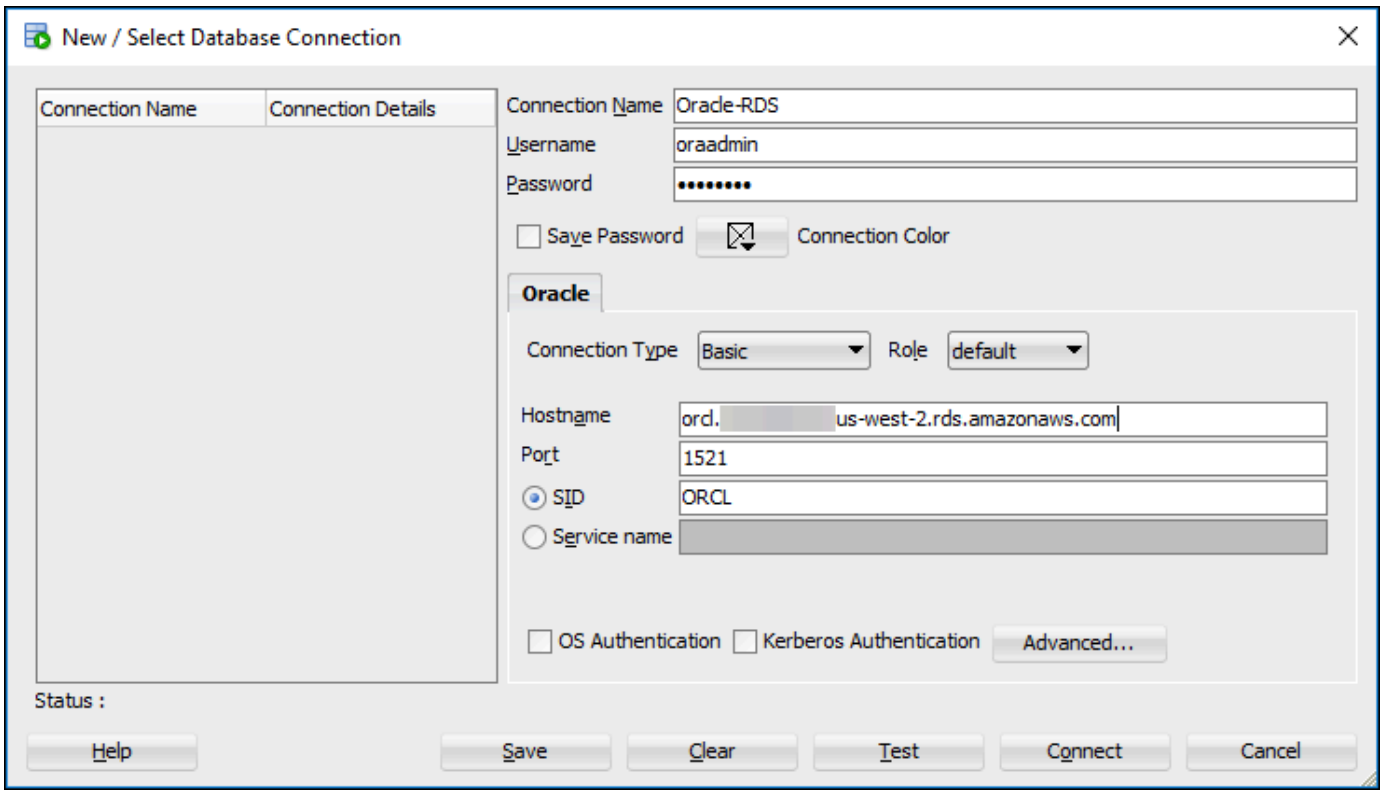
1. Inicie Oracle SQL Developer.
2. En la pestaña Connections, seleccione el icono add (+).



3. En el cuadro de diálogo New/Select Database Connection, proporcione la información de la instancia de base de datos:

   - En Connection Name (Nombre de la conexión), escriba un nombre que describa la conexión, como `Oracle-RDS`.
   - En Username (Nombre de usuario), escriba el nombre del administrador de base de datos para la instancia de base de datos.
   - En Password (Contraseña), escriba la contraseña del administrador de base de datos.
   - En Hostname (Nombre del host), escriba el nombre DNS de la instancia de base de datos.
   - En Port (Puerto), escriba el número de puerto.
   - Para SID, introduzca el nombre de la base de datos. Puede encontrar el nombre de la base de datos en la pestaña Configuration (Configuración) de la página de detalles de la base de datos.

   El cuadro de diálogo completo debería tener un aspecto similar al siguiente.

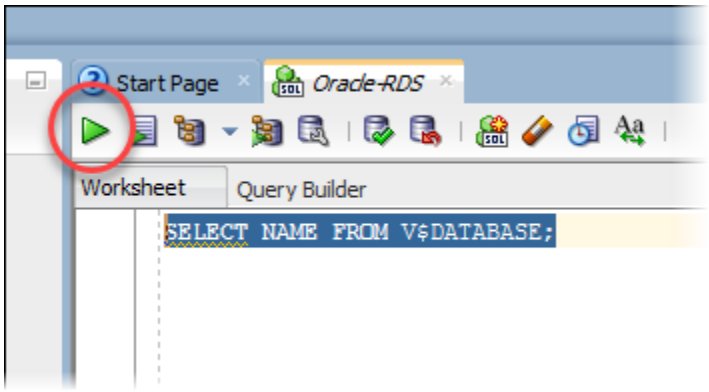


4. Elija Connect.
5. Ahora, puede comenzar a crear sus propias bases de datos y realizar consultas en la instancia de base de datos y bases de datos como siempre. Para ejecutar una consulta de prueba en la instancia de base de datos, haga lo siguiente:

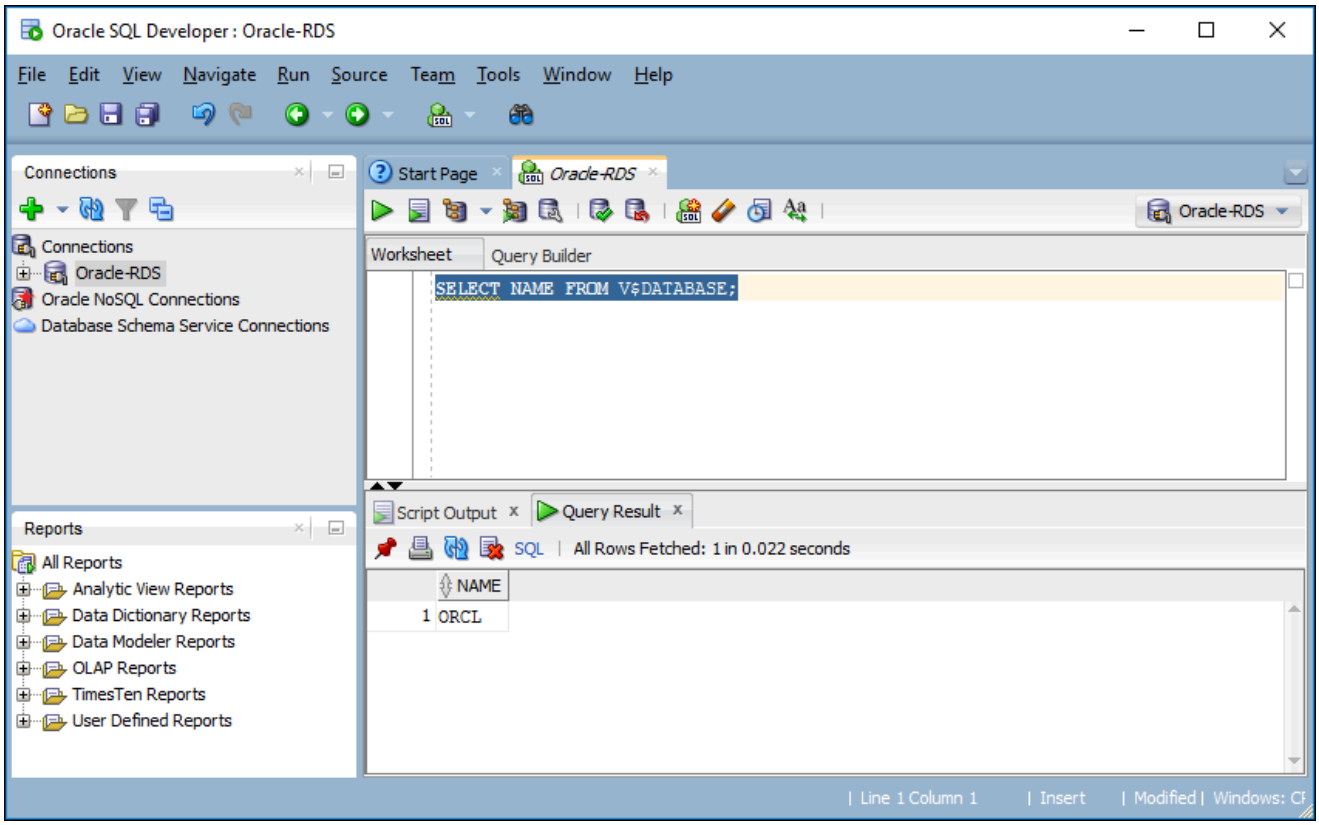
   a. En la pestaña Worksheet (Hoja de trabajo) de su conexión, escriba la siguiente consulta SQL.

   ```
   SELECT NAME FROM V$DATABASE;
   ```

   b. Seleccione el icono execute (ejecutar) para ejecutar la consulta.



SQL Developer devuelve el nombre de base de datos.



Conexión a la instancia de base de datos mediante SQL*Plus

Puede usar una utilidad como SQL*Plus para conectarse a una instancia de base de datos de Amazon RDS que ejecuta Oracle. Para descargar Oracle Instant Client, que incluye una versión independiente de SQL*Plus, consulte Oracle Instant Client Downloads.

Para conectarse a una instancia de base de datos, necesita su nombre DNS y el número de puerto. Para obtener información sobre cómo buscar el nombre DNS y el número de puerto para una instancia de base de datos, consulte Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle.

Example Para conectarse a una instancia de base de datos de Oracle mediante SQL*Plus

En los siguientes ejemplos, sustituya el nombre de usuario de su administrador de instancia de base de datos. Además, sustituya el nombre de DNS de su instancia de base de datos y, a continuación, incluya el número de puerto y el SID de Oracle. El valor del SID es el nombre de la base de datos de la instancia de base de datos que especificó cuándo creó la instancia de base de datos y no el nombre de la instancia de base de datos.

Para Linux, macOS o:Unix

```
sqlplus 'user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dns_name)(PORT=port))
(CONNECT_DATA=(SID=database_name)))'
```

En:Windows

```
sqlplus user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dns_name)(PORT=port))
(CONNECT_DATA=(SID=database_name)))
```

Debería ver un resultado similar a este.

```
SQL*Plus: Release 12.1.0.2.0 Production on Mon Aug 21 09:42:20 2017
```

Tras introducir la contraseña para el usuario, aparece la pregunta de SQL.

```
SQL>
```

> **Note**
>
> La cadena de conexión de formato más corto (EZ Connect), como `sqlplus USER/PASSWORD@longer-than-63-chars-rds-endpoint-here:1521/database-identifier`, podría tener un límite de máximo caracteres, así que le recomendamos que no la use para conectarse.

Consideraciones para grupos de seguridad

Para poder conectarse a la instancia de base de datos, esta debe estar asociada a un grupo de seguridad que contenga las direcciones IP y la configuración de red necesarias. La instancia de base de datos puede utilizar el grupo de seguridad predeterminado. Si se asignó un grupo de seguridad no configurado predeterminado cuando se creó la instancia de base de datos, el firewall evitará las conexiones. Para obtener información acerca de la creación de grupos de seguridad nuevos, consulte Control de acceso con grupos de seguridad.

Después de crear el nuevo grupo de seguridad, modifique la instancia de base de datos para asociarla al grupo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Puede mejorar la seguridad utilizando SSL para cifrar conexiones a su instancia de base de datos. Para obtener más información, consulte Capa de conexión segura de Oracle.

Consideraciones para la arquitectura de procesos

Los procesos del servidor se encargan de las conexiones del usuario a una instancia de base de datos de Oracle. De manera predeterminada, los procesos del servidor se encargan de las conexiones del usuario a una instancia de base de datos de Oracle. Con los procesos del servidor dedicados, cada proceso del servidor presta servicio a un solo proceso del usuario. Si lo prefiere, puede configurar procesos del servidor compartidos. Con los procesos del servidor compartidos, cada proceso del servidor presta servicio a varios procesos del usuario.

Puede considerar la posibilidad de usar los procesos del servidor compartidos cuando un número elevado de sesiones del usuario esté usando demasiada memoria en el servidor. También puede considerar dicha posibilidad, cuando las sesiones se conectan y desconectan con frecuencia dando como resultado problemas de desempeño. Asimismo, el uso de los procesos del servidor compartidos implica ciertos inconvenientes. Por ejemplo, puede agotar los recursos de CPU y resulta más complicado a la hora de configurarse y administrarse.

Para obtener más información acerca de los procesos del servidor dedicados y compartidos, consulte About Dedicated and Shared Server Processes en la documentación de Oracle. Para obtener más información acerca de la configuración de los procesos de servidor compartidos en una instancia de base de datos de RDS for Oracle, consulte ¿Cómo configuro Amazon RDS for Oracle Database para trabajar con servidores compartidos? en el Knowledge Center.

Solución de problemas de conexiones a la instancia de base de datos de Oracle

A continuación, aparecen problemas que pueden aparecer al tratar de conectarse a la instancia de base de datos de Oracle.

Problema	Sugerencias para la solución de problemas
No es posible conectarse a su instancia de base de datos.	En el caso de una instancia de base de datos recién creada, esta tendrá el estado creating hasta que esté lista para el uso. Cuando el estado cambie a available, podrá conectarse a la instancia de base de datos. Dependiendo de la clase de instancia de base de datos y de la cantidad de almacenamiento, es posible que la

Problema	Sugerencias para la solución de problemas
	nueva instancia de base de datos tarde hasta 20 minutos en estar disponible.
No es posible conectarse a su instancia de base de datos.	Si no puede enviar o recibir comunicaciones a través del puerto que especificó al crear la instancia de base de datos, no puede conectarse a ella. Consulte al administrador de red para comprobar que el puerto que especificó para su instancia de base de datos permite comunicación de entrada y salida.
No es posible conectarse a su instancia de base de datos.	Las reglas de acceso impuestas por el firewall local y las direccion es IP a las que autorizó el acceso a la instancia de base de datos en el grupo de seguridad para la instancia de base de datos podrían no coincidir. El problema muy probablemente se encuentra en las reglas entrantes o salientes de su firewall. Puede añadir o editar una regla de entrada en el grupo de seguridad. Para Source (Origen), elija My IP (Mi IP). Esto permite el acceso a la instancia de base de datos desde la dirección IP detectada en su navegador. Para obtener más información, consulte VPC de Amazon y Amazon RDS. Para obtener más información acerca de los grupos de seguridad, consulte Control de acceso con grupos de seguridad. Si desea conocer el proceso de configuración de reglas para su grupo de seguridad, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).
Error de la conexión porque el host o el objeto destino no existe: Oracle, Error: ORA-12545	Asegúrese de especificar correctamente el nombre del servidor y el número de puerto. En Server name (Nombre del servidor), escriba el nombre DNS desde la consola. Para obtener información sobre cómo buscar el nombre DNS y el número de puerto para una instancia de base de datos, consulte Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle.

Problema	Sugerencias para la solución de problemas
Nombre de usuario/contraseña no válidos; conexión denegada: Oracle, Error: ORA-01017	Ha podido alcanzar la instancia de base de datos, pero se rechazó la conexión. Esto suele deberse a que se ha proporcionado un nombre de usuario o contraseña incorrectos. Compruebe el nombre de usuario y la contraseña y, a continuación, vuelva a intentarlo.
TNS:listener does not currently know of SID given in connect descriptor - Oracle, ERROR: ORA-12505 (TNS:listener no conoce actualmente el SID indicado en el descriptor de conexión - Oracle, ERROR: ORA-12505)	Asegúrese de que se ha ingresado el SID correcto. El SID es el mismo que el nombre de su base de datos. Busque el nombre de la base de datos en la pestaña Configuration (Configuración) de la página Databases (Bases de datos) de la instancia. También puede encontrar el nombre de la base de datos utilizando la AWS CLI: `aws rds describe-db-instances --query 'DBInstances[*].[DBInstanceIdentifier,DBName]' --output text`

Para obtener más información sobre problemas de conexión, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Modificación de propiedades de conexión utilizando parámetros sqlnet.ora

El archivo sqlnet.ora incluye parámetros que configuran características de Oracle Net en servidores de base de datos y clientes de Oracle. Utilizando los parámetros en el archivo sqlnet.ora, puede modificar propiedades de conexiones dentro y fuera de la base de datos.

Para obtener más información acerca de porqué debería configurar los parámetros sqlnet.ora, consulte Configuring Profile Parameters en la documentación de Oracle.

Configuración de parámetros sqlnet.ora

Los grupos de parámetros de Amazon RDS for Oracle incluyen un subconjunto de parámetros sqlnet.ora. Los configura de la misma manera que configura otros parámetros de Oracle. El prefijo `sqlnetora.` identifica qué parámetros son parámetros sqlnet.ora. Por ejemplo, en un grupo de parámetros de Oracle en Amazon RDS, el parámetro `default_sdu_size` de sqlnet.ora es `sqlnetora.default_sdu_size`.

Para obtener información acerca de cómo administrar grupos de parámetros y configurar valores de parámetros, consulte Grupos de parámetros para Amazon RDS.

Parámetros sqlnet.ora admitidos

Amazon RDS admite los siguientes parámetros sqlnet.ora. Los cambios en parámetros sqlnet.ora dinámicos surten efecto de inmediato.

Parámetro	Valores válidos	Estático/ dinámico	Descripción
`sqlnetora.default_sdu_size`	`512` De a `20971`	Dinámico	El tamaño de la unidad de datos de sesión (SDU), en bytes. La SDU es la cantidad de datos que se coloca en un búfer y se envía a la red a la vez.
`sqlnetora.diag_adr_enabled`	`ON`, `OFF`	Dinámico	Un valor que habilita o inhabilita el rastreo de Repositorio de diagnóstico automático (ADR). `ON` especifica qué rastreo de archivo ADR se utiliza. `OFF` especifica que se utiliza el rastreo de archivo no ADR.
`sqlnetora.recv_buf_size`	`8192` De a `26843`	Dinámico	El límite de espacio de búfer para operaciones de recepción de sesiones, admitido por los protocolos TCP/IP, TCP/IP con SSL y SDP.

Parámetro	Valores válidos	Estático/ dinámico	Descripción
sqlnetora.send_buf_size	8192 De a 268435	Dinámico	El límite de espacio de búfer para operaciones de envío de sesiones, admitido por los protocolos TCP/IP, TCP/IP con SSL y SDP.
sqlnetora.sqlnet.allowed_logon_version_client	8, 10, 11, 12	Dinámico	Se permite la versión del protocolo de autenticación mínima para los clientes y los servidores que actúan como clientes, para establecer una conexión con instancias de base de datos de Oracle.
sqlnetora.sqlnet.allowed_logon_version_server	8, 9, 10, 11, 12, 12a	Dinámico	Se permite la versión del protocolo de autenticación mínima para establecer una conexión con instancias de base de datos de Oracle.
sqlnetora.sqlnet.expire_time	0 De a 1440	Dinámico	Intervalo de tiempo, en minutos, para enviar una comprobación de estado para verificar que las conexiones cliente-servidor están activas.
sqlnetora.sqlnet.inbound_connect_timeout	0 o 10 a 7200	Dinámico	Tiempo, en segundos, para que un cliente conecte con el servidor de base de datos y proporcione la información de autenticación necesaria.

Parámetro	Valores válidos	Estático/ dinámico	Descripción
sqlnetora.sqlnet.outbound_connect_timeout	0 o 10 a 7200	Dinámico	Tiempo, en segundos, para que un cliente establezca una conexión de Oracle Net con la instancia de base de datos.
sqlnetora.sqlnet.recv_timeout	0 o 10 a 7200	Dinámico	Tiempo, en segundos, que un servidor de base de datos espera los datos del cliente después de establecer una conexión.
sqlnetora.sqlnet.send_timeout	0 o 10 a 7200	Dinámico	Tiempo, en segundos, para que un servidor de base de datos complete una operación de envío a los clientes después de establecer una conexión.
sqlnetora.tcp.connect_timeout	0 o 10 a 7200	Dinámico	Tiempo, en segundos, para que un cliente establezca una conexión TCP al servidor de base de datos.
sqlnetora.trace_level_server	0, 4, 10, 16, OFF, USER, ADMIN, SUPPOF	Dinámico	Para un rastreo no ADR, activa el rastreo del servidor a un nivel especificado o lo desactiva.

El valor predeterminado para cada parámetro sqlnet.ora admitido es el valor predeterminado de Oracle Dabatase para la versión.

Ver parámetros sqlnet.ora

Puede ver parámetros sqlnet.ora y su configuración utilizando la AWS Management Console, la AWS CLI o un cliente SQL.

Ver parámetros sqlnet.ora utilizando la consola

Para obtener información acerca de cómo ver parámetros en un grupo de parámetros, consulte Grupos de parámetros para Amazon RDS.

En grupos de parámetros de Oracle, el prefijo `sqlnetora.` identifica qué parámetros son parámetros sqlnet.ora.

Ver parámetros sqlnet.ora utilizando la AWS CLI

Para ver los parámetros sqlnet.ora que se configuraron en un grupo de parámetros de Oracle, utilice el comando describe-db-parameters de la AWS CLI.

Para ver todos los parámetros sqlnet.ora para una instancia de base de datos de Oracle, llame al comando download-db-log-file-portion de la AWS CLI. Especifique el identificador de instancias de bases de datos, el nombre de archivo de registro y el tipo de salida.

Example

El código siguiente muestra todos los parámetros sqlnet.ora para `mydbinstance`.

Para Linux, macOS o:Unix

```
aws rds download-db-log-file-portion \
    --db-instance-identifier mydbinstance \
    --log-file-name trace/sqlnet-parameters \
    --output text
```

En:Windows

```
aws rds download-db-log-file-portion ^
    --db-instance-identifier mydbinstance ^
    --log-file-name trace/sqlnet-parameters ^
    --output text
```

Ver parámetros sqlnet.ora utilizando un cliente SQL

Después de conectar a la instancia de base de datos de Oracle en un cliente SQL, la siguiente consulta muestra los parámetros sqlnet.ora.

```
SELECT * FROM TABLE
   (rdsadmin.rds_file_util.read_text_file(
        p_directory => 'BDUMP',
        p_filename  => 'sqlnet-parameters'));
```

Para obtener información acerca de la conexión a su instancia de base de datos de Oracle en un cliente SQL, consulte Conexión a una instancia de base de datos de Oracle.

Protección de conexiones de instancias de base de datos de Oracle

Amazon RDS for Oracle admite conexiones cifradas SSL/TLS, así como la opción Oracle Native Network Encryption (NNE) para cifrar las conexiones entre la aplicación y la instancia de base de datos Oracle. Para obtener más información acerca de la opción Oracle Native Network Encryption, consulte Oracle Native Network Encryption.

Temas

- Uso de SSL con una instancia de base de datos de RDS para Oracle
- Actualización de aplicaciones para la conexión a las instancias de base de datos de Oracle con los nuevos certificados SSL/TLS
- Uso del cifrado de red nativo con una instancia de base de datos de RDS para Oracle
- Configuración de la autenticación Kerberos con Amazon RDS for Oracle
- Configuración del acceso UTL_HTTP mediante certificados y un wallet de Oracle.

Uso de SSL con una instancia de base de datos de RDS para Oracle

La capa de conexión segura (SSL) es un protocolo estándar del sector que se utiliza para proteger las conexiones de red entre el cliente y el servidor. Después de la versión 3.0 de SSL, el nombre se cambió a Transport Layer Security (TLS), pero a menudo nos referimos al protocolo como SSL. Amazon RDS admite el cifrado SSL para las instancias de Oracle Database. SSL permite cifrar una conexión entre el cliente de la aplicación y la instancia de base de datos Oracle. La compatibilidad con SSL está disponible en todas las regiones de AWS para Oracle.

A fin de habilitar el cifrado SSL para una instancia de base de datos de Oracle, agregue la opción Oracle SSL al grupo de opciones asociado a la instancia de base de datos. Amazon RDS utiliza un segundo puerto, según lo requiera Oracle, para las conexiones SSL. Esto permite que se produzca la comunicación cifrada de SSL y de texto sin cifrar al mismo tiempo entre una instancia de base de datos y un cliente de Oracle. Por ejemplo, es posible utilizar el puerto con la comunicación de texto sin cifrar para ponerse en contacto con otros recursos dentro de una VPC mientras se utiliza el puerto con comunicación cifrada SSL para ponerse en contacto con recursos situados fuera de la VPC.

Para obtener más información, consulte Capa de conexión segura de Oracle.

> **Note**
>
> No es posible utilizar SSL y Oracle Native Network Encryption (NNE) en la misma instancia de base de datos. Para poder utilizar el cifrado SSL, se debe desactivar cualquier otro cifrado de conexión.

Actualización de aplicaciones para la conexión a las instancias de base de datos de Oracle con los nuevos certificados SSL/TLS

El 13 de enero de 2023, Amazon RDS publicó nuevos certificados de entidades de certificación (CA) para la conexión a sus instancias de base de datos de RDS mediante la capa de sockets seguros o seguridad de la capa de transporte (SSL/TLS). Después, puede encontrar la información sobre la actualización de sus aplicaciones para utilizar los nuevos certificados.

Este tema puede ayudarle a determinar si las aplicaciones de cualquier cliente utilizan SSL/TLS para conectarse a sus instancias de base de datos.

> **Important**
>
> Cuando se cambia el certificado de una instancia de base de datos de Amazon RDS for Oracle, solo se reinicia el agente de escucha de la base de datos. La instancia de base de datos no se reinicia. Las conexiones de base de datos existentes no se ven afectadas, pero las conexiones nuevas tendrán errores durante el breve período en que se reinicia el agente de escucha.
> Le recomendamos que reinicie la base de datos de Oracle para evitar errores de conexión.

> **Note**
>
> Para las aplicaciones de clientes que utilizan SSL/TLS para conectarse a sus instancias de base de datos, debe actualizar los almacenes de confianza de la aplicación de su cliente para incluir los nuevos certificados de CA.

Después actualizar sus certificados de CA en los almacenes de confianza de la aplicación de su cliente, puede rotar los certificados en sus instancias de base de datos. Recomendamos

encarecidamente probar estos procedimientos en un entorno de desarrollo o ensayo antes de implementarlos en sus entornos de producción.

Para obtener más información acerca de la rotación de certificados, consulte Rotar certificados SSL/TLS. Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener información sobre el uso de SSL/TLS con las instancias de base de datos de Oracle, consulte Capa de conexión segura de Oracle.

Temas

- Averiguar si las aplicaciones se conectan mediante SSL
- Actualización del almacén de confianza de su aplicación
- Ejemplo de código Java para el establecimiento de conexiones SSL

Averiguar si las aplicaciones se conectan mediante SSL

Si su instancia de base de datos de Oracle utiliza una grupo de opciones con la opción `SSL` añadida, puede que utilice SSL. Compruébelo siguiendo las instrucciones en Descripción de opciones y configuración de opciones para un grupo de opciones. Para obtener información acerca de la opción `SSL`, consulte Capa de conexión segura de Oracle.

Compruebe el registro del agente de escucha para determinar si existen conexiones SSL. A continuación, se muestra un ejemplo del resultado en un registro del agente de escucha.

```
date time * (CONNECT_DATA=(CID=(PROGRAM=program)
(HOST=host)(USER=user))(SID=sid)) *
(ADDRESS=(PROTOCOL=tcps)(HOST=host)(PORT=port)) * establish * ORCL * 0
```

Cuando `PROTOCOL` tiene el valor `tcps` para cualquier entrada, muestra una conexión SSL. Sin embargo, cuando `HOST` es `127.0.0.1`, puede ignorar la entrada. Las conexiones de `127.0.0.1` son un agente de administración local en la instancia de base de datos. Estas conexiones no son conexiones SSL externas. Por lo tanto, tiene aplicaciones conectándose utilizando SSL si ve entradas del registro del agente de escucha en las que `PROTOCOL` es `tcps` y `HOST` no`127.0.0.1`.

Para comprobar el registro del agente de escucha, puede publicar el registro en Amazon CloudWatch Logs. Para obtener más información, consulte Publicación de registros de Oracle en Amazon CloudWatch Logs.

Actualización del almacén de confianza de su aplicación

Puede actualizar el almacén de confianza para las aplicaciones que utilizan SQL*Plus o JDBC para las conexiones SSL/TLS.

Actualización del almacén de confianza de su aplicación para SQL*Plus

Puede actualizar el almacén de confianza para las aplicaciones que utilizan SQL*Plus para las conexiones SSL/TLS.

> **Note**
>
> Cuando actualice el almacén de confianza, puede retener certificados antiguos además de añadir los nuevos certificados.

Para actualizar el almacén de confianza para las aplicaciones de SQL*Plus

1. Descargue el certificado raíz que funciona con todas las regiones de AWS y coloque el archivo en el directorio `ssl_wallet`.

   Para obtener información sobre la descarga del certificado raíz, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
2. Ejecute el siguiente comando para actualizar el wallet de Oracle.

   ```
   prompt>orapki wallet add -wallet $ORACLE_HOME/ssl_wallet -trusted_cert -cert
         $ORACLE_HOME/ssl_wallet/ssl-cert.pem -auto_login_only
   ```

   Reemplace el nombre de archivo por el que ha descargado.
3. Ejecute el comando siguiente para confirmar que el wallet se ha actualizado correctamente.

   ```
   prompt>orapki wallet display -wallet $ORACLE_HOME/ssl_wallet
   ```

   Su resultado debe contener lo siguiente.

   ```
   Trusted Certificates:
   Subject: CN=Amazon RDS Root 2019 CA,OU=Amazon RDS,O=Amazon Web Services\,
    Inc.,L=Seattle,ST=Washington,C=US
   ```

Actualización del almacén de confianza de su aplicación para JDBC

Puede actualizar el almacén de confianza para las aplicaciones que utilizan JDBC para las conexiones SSL/TLS.

Para obtener información sobre la descarga del certificado raíz, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Para obtener secuencias de comandos de ejemplo que importan certificados, consulte Script de muestra para la importación de certificados en su almacén de confianza.

Ejemplo de código Java para el establecimiento de conexiones SSL

El siguiente ejemplo de código muestra cómo configurar la conexión SSL mediante JDBC.

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;
import java.util.Properties;

public class OracleSslConnectionTest {
    private static final String DB_SERVER_NAME = "<dns-name-provided-by-amazon-rds>";
    private static final Integer SSL_PORT = "<ssl-option-port-configured-in-option-
group>";
    private static final String DB_SID = "<oracle-sid>";
    private static final String DB_USER = "<user name>";
    private static final String DB_PASSWORD = "<password>";
    // This key store has only the prod root ca.
    private static final String KEY_STORE_FILE_PATH = "<file-path-to-keystore>";
    private static final String KEY_STORE_PASS = "<keystore-password>";

    public static void main(String[] args) throws SQLException {
        final Properties properties = new Properties();
        final String connectionString = String.format(
                "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=%s)(PORT=
%d))(CONNECT_DATA=(SID=%s)))",
                DB_SERVER_NAME, SSL_PORT, DB_SID);
        properties.put("user", DB_USER);
        properties.put("password", DB_PASSWORD);
        properties.put("oracle.jdbc.J2EE13Compliant", "true");
        properties.put("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
        properties.put("javax.net.ssl.trustStoreType", "JKS");
        properties.put("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);
```

```
        final Connection connection = DriverManager.getConnection(connectionString,
 properties);
        // If no exception, that means handshake has passed, and an SSL connection can
 be opened
    }
}
```

> **Important**
>
> Después de que haya determinado que sus conexiones de base de datos utilizan SSL/TLS y haya actualizado el almacén de confianza de su aplicación, puede actualizar su base de datos para que utilice los certificados de rds-ca-rsa2048-g1. Para obtener instrucciones, consulte el paso 3 en Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos.

Uso del cifrado de red nativo con una instancia de base de datos de RDS para Oracle

Oracle Database ofrece dos formas de cifrar datos a través de la red: cifrado de red nativo (NNE, por sus siglas en inglés) y seguridad de la capa de transporte (TLS, por sus siglas en inglés). NNE es una característica de seguridad patentada de Oracle, mientras que TLS es un estándar del sector. RDS para Oracle es compatible con NNE en todas las ediciones de Oracle Database.

NNE tiene las siguientes ventajas con respecto a TLS:

- Puede controlar el NNE en el cliente y el servidor mediante la configuración de la opción NNE:
  - `SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS` y `SQLNET.ALLOW_WEAK_CRYPTO`
  - `SQLNET.CRYPTO_CHECKSUM_CLIENT` y `SQLNET.CRYPTO_CHECKSUM_SERVER`
  - `SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT` y `SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER`
  - `SQLNET.ENCRYPTION_CLIENT` y `SQLNET.ENCRYPTION_SERVER`
  - `SQLNET.ENCRYPTION_TYPES_CLIENT` y `SQLNET.ENCRYPTION_TYPES_SERVER`
- En la mayoría de los casos, no es necesario configurar el cliente o servidor. Por el contrario, TLS requiere que se configure tanto el cliente como el servidor.

- No se requieren certificados. En TLS, el servidor requiere un certificado (que eventualmente caduca) y el cliente requiere un certificado raíz de confianza para la autoridad certificadora que emitió el certificado del servidor.

A fin de habilitar el cifrado NNE para una instancia de base de datos de Oracle, agregue la opción Oracle NNE al grupo de opciones asociado a la instancia de base de datos. Para obtener más información, consulte Oracle Native Network Encryption.

> **Note**
>
> No se pueden utilizar NNE y TLS en la misma instancia de base de datos.

Configuración de la autenticación Kerberos con Amazon RDS for Oracle

Puede usar la autenticación Kerberos para autenticar a los usuarios cuando se conecten a su instancia de base de datos de Amazon RDS para Oracle. En esta configuración, su instancia de base de datos funciona con AWS Directory Service for Microsoft Active Directory, también llamado AWS Managed Microsoft AD. Cuando los usuarios se autentican con una instancia de base de datos de RDS para Oracle unida al dominio de confianza, las solicitudes de autenticación se reenvían al directorio que se ha creado con AWS Directory Service.

Mantener todas las credenciales en el mismo directorio puede ahorrarle tiempo y esfuerzo. Tiene un lugar centralizado para almacenar y administrar credenciales para varias instancias de bases de datos. Un directorio también puede mejorar su perfil de seguridad general.

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de RDS para Oracle con autenticación Kerberos, consulte Regiones y motores de base de datos admitidos para autenticación de Kerberos en Amazon RDS.

> **Note**
>
> La autenticación Kerberos no es compatible con las clases de instancia de base de datos que están en desuso para las instancias de base de datos de RDS para Oracle. Para obtener más información, consulte Clases de instancias de base de datos de RDS para Oracle.

Temas

- Configuración de autenticación Kerberos para instancias de base de datos de Oracle
- Administración de una instancia de base de datos en un dominio
- Conexión a Oracle con autenticación Kerberos

Configuración de autenticación Kerberos para instancias de base de datos de Oracle

Use AWS Directory Service for Microsoft Active Directory, también llamado AWS Managed Microsoft AD, para configurar la autenticación Kerberos para una instancia de base de datos de Oracle. Para configurar la autenticación Kerberos, complete los siguientes pasos:

- Paso 1: crear un directorio con AWS Managed Microsoft AD
- Paso 2: crear una relación de confianza
- Paso 3: Configure los permisos de IAM para Amazon RDS
- Paso 4: crear y configurar usuarios
- Paso 5: habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos
- Paso 6: crear o modificar una instancia de base de datos de Oracle
- Paso 7: crear inicios de sesión de Oracle de autenticación Kerberos
- Paso 8: configurar un cliente de Oracle

> **Note**
>
> Durante la configuración, RDS crea un usuario de base de datos de Oracle llamado *managed_service_user*@*ejemplo.com* con el privilegio `CREATE SESSION`, donde *ejemplo.com* es su nombre de dominio. Este usuario corresponde al usuario que crea Directory Service dentro de Active Directory administrado. Periódicamente, RDS utiliza las credenciales proporcionadas por Directory Service para iniciar sesión en la base de datos de Oracle. Después, RDS destruye inmediatamente la caché de tickets.

Paso 1: crear un directorio con AWS Managed Microsoft AD

AWS Directory Service crea un directorio de Active Directory completamente administrado en la nube de AWS. Cuando crea un directorio de AWS Managed Microsoft AD, AWS Directory Service crea dos

controladores de dominio y servidores del sistema de nombres de dominio (DNS) en su nombre. Los servidores de directorios se crean en diferentes subredes de una VPC. Esta redundancia ayuda a garantizar que su directorio permanezca accesible incluso si ocurre un error.

Cuando crea un directorio de AWS Managed Microsoft AD, AWS Directory Service realiza en su nombre las siguientes tareas:

- Configurar un Active Directory dentro de la VPC.
- Crea una cuenta de administrador para el directorio con el nombre de usuario Admin y la contraseña especificada. Esta cuenta le permite administrar el directorio.

> **Note**
>
> Asegúrese de guardar esta contraseña. AWS Directory Service no la almacena. Es posible restablecerla, pero no recuperarla.

- Crea un grupo de seguridad para los controladores del directorio.

Al lanzar AWS Managed Microsoft AD, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa tiene el nombre de NetBIOS que escribió al crear el directorio y se encuentra en la raíz del dominio. La raíz del dominio es propiedad de , que también se encarga de su administració AWS.

La cuenta de administrador que se creó con el directorio AWS Managed Microsoft AD dispone de permisos para realizar las actividades administrativas más habituales para la unidad organizativa:

- Crear, actualizar o eliminar usuarios
- Añadir recursos a su dominio, como servidores de archivos o de impresión y, a continuación, asignar permisos para esos recursos a usuarios dentro de la unidad organizativa
- Crear unidades organizativas y contenedores adicionales
- Delegar autoridad
- Restaurar objetos eliminados de la papelera de reciclaje de Active Directory
- Ejecutar módulos de AD y DNS de Windows PowerShell en el servicio web de Active Directory

La cuenta de administrador también tiene derechos para realizar las siguientes actividades en todo el dominio:

- Administrar configuraciones DNS (agregar, quitar o actualizar registros, zonas y programas de envío).
- Ver logs de eventos DNS
- Ver logs de eventos de seguridad

Para crear el directorio, use la API AWS Management Console, AWS CLI o AWS Directory Service. Asegúrese de abrir los puertos de salida relevantes en el grupo de seguridad del directorio para que el directorio pueda comunicarse con la instancia de base de datos de Oracle.

Para crear un directorio con AWS Managed Microsoft AD

1. Inicie sesión en AWS Management Console y abra la consola de AWS Directory Service en https://console.aws.amazon.com/directoryservicev2/.
2. En el panel de navegación, elija Directories (Directorios) y, a continuación, Set up Directory (Configurar directorio).
3. Elija AWS Managed Microsoft AD. AWS Managed Microsoft AD es la única opción que puede usar actualmente con Amazon RDS.
4. Introduzca la información siguiente:

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo **`corp.example.com`**.

   Nombre NetBIOS del directorio

   El nombre abreviado del directorio, como **`CORP`**.

   Descripción del directorio

   (Opcional) Descripción del directorio.

   Contraseña de administrador

   Contraseña del administrador del directorio. El proceso de creación de directorios crea una cuenta de administrador con el nombre de usuario Admin y esta contraseña.

   La contraseña del administrador del directorio no puede contener la palabra "admin".
   La contraseña distingue entre mayúsculas y minúsculas y debe tener un mínimo de 864 caracteres y un máximo de 64. También debe contener al menos un carácter de tres de las siguientes categorías:

- Letras minúsculas (a–z)
- Letras mayúsculas (A–Z)
- Números (0–9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password

Vuelva a escribir la contraseña de administrador.

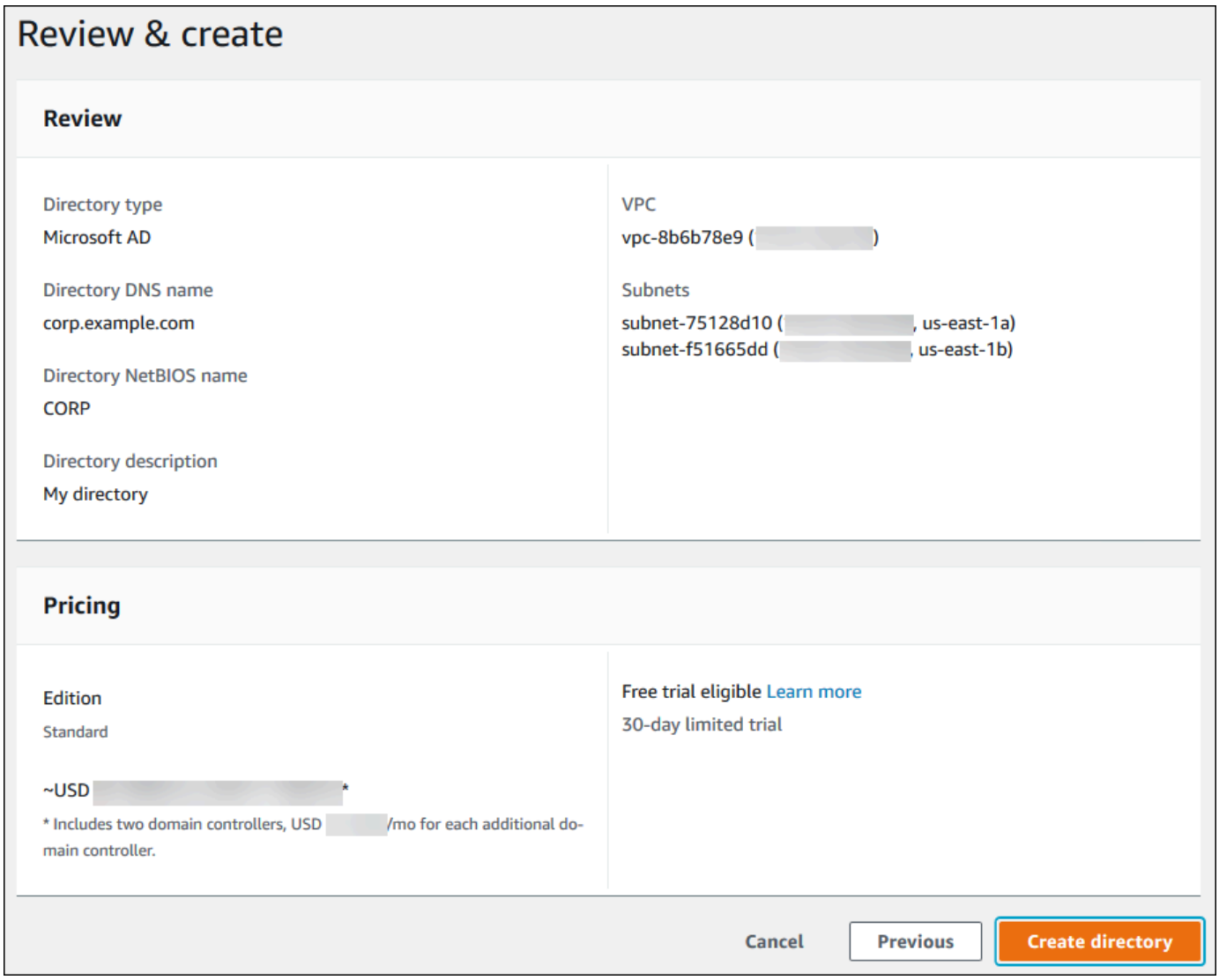
5. Elija Siguiente.
6. Escriba la siguiente información en la sección Networking (Redes) y luego seleccione Next (Siguiente):

   VPC

   VPC del directorio. Cree la instancia de base de datos de Oracle en esta misma VPC.

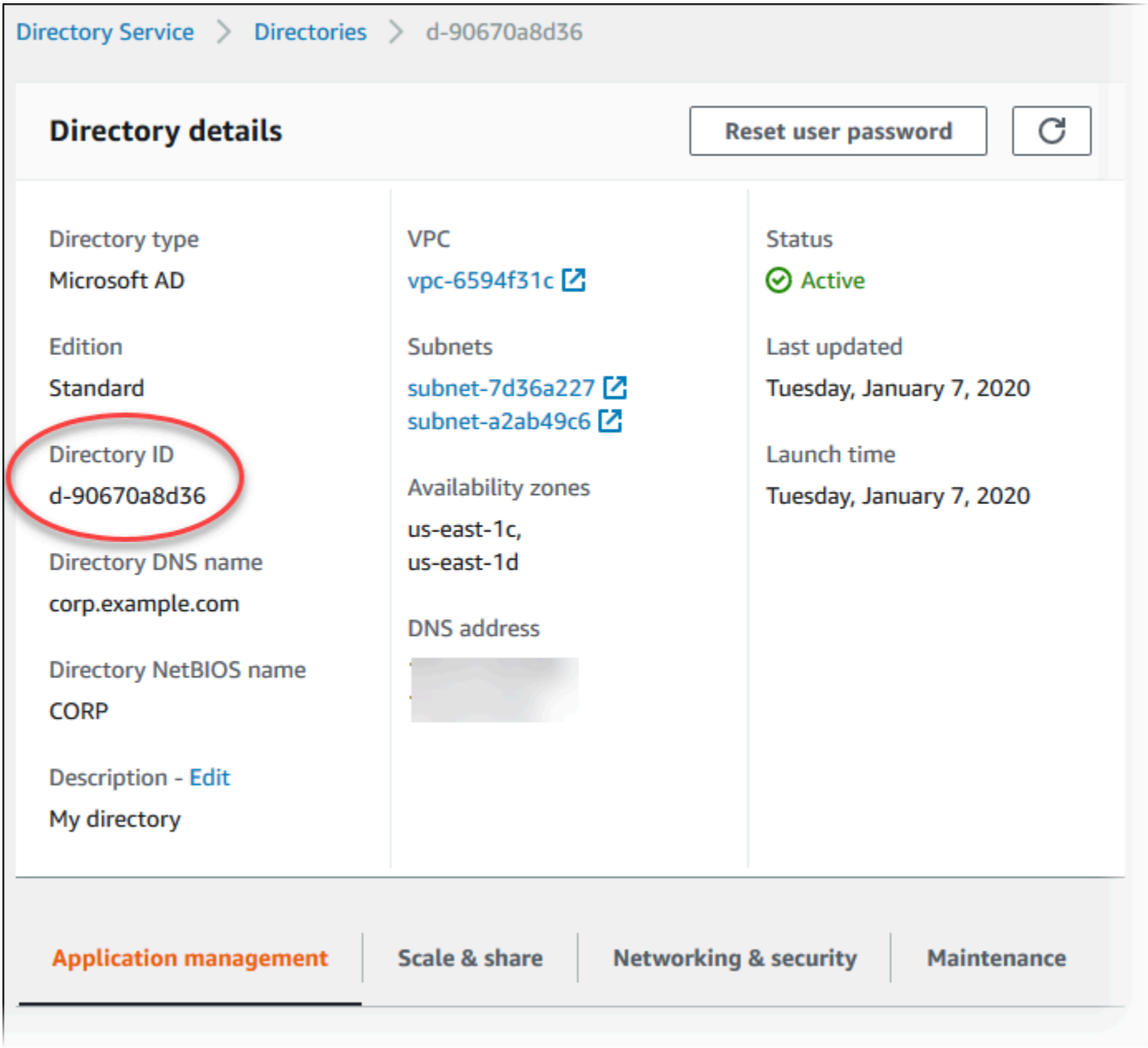
   Subredes

   Subredes de los servidores del directorio. Las dos subredes deben estar en diferentes zonas de disponibilidad.
7. Revise la información del directorio y haga los cambios necesarios. Cuando la información sea correcta, seleccione Create directory (Crear directorio).



La creación del directorio tarda varios minutos. Cuando se haya creado correctamente, el valor de Status (Estado) cambiará a Active (Activo).

Para consultar información de su directorio, seleccione el nombre del directorio en la descripción de directorios. Tenga en cuenta el valor de Directory ID (ID de directorio) porque necesitará este valor cuando cree o modifique su instancia de base de datos de Oracle.



Paso 2: crear una relación de confianza

Si planea utilizar AWS Managed Microsoft AD únicamente, pase a Paso 3: Configure los permisos de IAM para Amazon RDS.

Para habilitar la autenticación de Kerberos mediante Active Directory autoadministrado, debe crear una relación de confianza de bosque entre Active Directory autoadministrado y el AWS Managed Microsoft AD creado en el paso anterior. La confianza puede ser unidireccional, donde AWS Managed Microsoft AD confía en Active Directory autoadministrado. La confianza también puede ser bidireccional, donde ambos Active Directories confían entre sí. Para obtener más información acerca

de la configuración de relaciones de confianza entre bosques con AWS Directory Service, consulte Cuándo crear una relación de confianza en la Guía de administración de AWS Directory Service.

Paso 3: Configure los permisos de IAM para Amazon RDS

Para llamar a AWS Directory Service por usted, Amazon RDS requiere un rol de IAM que utilice la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. Este rol permite a Amazon RDS realizar llamadas a AWS Directory Service.

> **Note**
>
> Para que el rol permita el acceso, el punto de conexión AWS Security Token Service (AWS STS) debe activarse en la Región de AWS correcta para su Cuenta de AWS. Los puntos de conexión de AWS STS están activos de forma predeterminada en todas las Regiones de AWS y puede usarlos sin ninguna acción posterior. Para obtener más información, consulte Activación y desactivación de AWS STS en una región de Región de AWS en la Guía del usuario de IAM.

Creación de un rol de IAM

Cuando se crea una instancia de base de datos con la AWS Management Console y el usuario de la consola tiene el permiso `iam:CreateRole`, la consola crea `rds-directoryservice-kerberos-access-role` automáticamente. De no ser así, debe crear el rol de IAM manualmente. Cuando cree un rol de IAM automáticamente, elija `Directory Service` y asocie la política administrada de AWS `AmazonRDSDirectoryServiceAccess` a este.

A fin de obtener más información acerca de la creación de roles de IAM para un servicio, consulte Creación de un rol para delegar permisos a un servicio de AWS en la guía del usuario de IAM.

> **Note**
>
> El rol de IAM utilizado para la autenticación de Windows en RDS para Microsoft SQL Server no se puede usar en RDS para Oracle.

Creación manual de una política de confianza de IAM

Opcionalmente, puede crear políticas de recursos con los permisos requeridos en vez de utilizar la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. Especifique `directoryservice.rds.amazonaws.com` y `rds.amazonaws.com` como entidades principales.

A fin de limitar los permisos que Amazon RDS da a otro servicio para un recurso específico, le recomendamos utilizar las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos. La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo de un recurso de Amazon RDS. Para obtener más información, consulte Prevención de los problemas del suplente confuso entre servicios.

En el ejemplo siguiente, se muestra cómo se pueden utilizar las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en Amazon RDS para evitar el problema del suplente confuso.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:mydbinstance"
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

```
  ]
}
```

En el caso de las regiones que se suscriban voluntariamente, también debe incluir una entidad principal de servicio para esa región en forma de `directoryservice.rds.region_name.amazonaws.com`. Por ejemplo, en la región de África (Ciudad del Cabo), utilice la siguiente política de confianza:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "directoryservice.rds.af-south-1.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:rds:af-south-1:123456789012:db:mydbinstance"
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

El rol debe también tener la siguiente política de IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Paso 4: crear y configurar usuarios

Puede crear usuarios con la herramienta Usuarios y equipos de Active Directory, que es una de las herramientas Servicios de dominio de Active Directory y Active Directory Lightweight Directory Services. En este caso, los usuarios son las personas físicas o entidades que tienen acceso al directorio.

Para crear usuarios en un directorio de AWS Directory Service, debe estar conectado a una instancia de Amazon EC2 con Windows que sea miembro del directorio de AWS Directory Service. Al mismo tiempo, debe iniciar sesión como usuario con privilegios para crear usuarios. Para obtener más información sobre la creación de usuarios en su Microsoft Active Directory, consulte Administrar usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.

Paso 5: habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos

Si tiene previsto ubicar el directorio y la instancia de base de datos en la misma VPC, omita este paso y continúe con Paso 6: crear o modificar una instancia de base de datos de Oracle.

Si planea localizar el directorio y la instancia de base de datos en distintas cuentas de AWS o VPC, configure el tráfico entre VPC mediante interconexión de VPC o AWS Transit Gateway. El siguiente

procedimiento permite el tráfico entre VPC mediante la interconexión de VPC. Siga las instrucciones de ¿Qué es una interconexión de VPC? en la Guía de interconexión de Amazon Virtual Private Cloud.

Para habilitar el tráfico entre VPC mediante la interconexión de VPC

1. Configure las reglas de enrutamiento de VPC adecuadas para garantizar que el tráfico de red pueda fluir en ambos sentidos.
2. Asegúrese de que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico de entrada del grupo de seguridad del directorio. Para obtener más información, consulte Prácticas recomendadas para AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.
3. Asegúrese de que no haya una regla de lista de control de acceso (ACL) a la red para bloquear el tráfico.

Si una cuenta de AWS distinta es la propietaria del directorio, debe compartirlo.

Para compartir el directorio entre cuentas de AWS

1. Comience a compartir el directorio con la cuenta de AWS en la que se creará la instancia de base de datos mediante las instrucciones de Tutorial: Uso compartido del directorio de AWS Managed Microsoft AD para realizar la unión al dominio de EC2 sin problemas en la Guía de administración de AWS Directory Service.
2. Inicie sesión en la consola de AWS Directory Service utilizando la cuenta para la instancia de base de datos y asegúrese de que el dominio tiene el estado `SHARED` antes de continuar.
3. Una vez iniciada sesión en la consola de AWS Directory Service utilizando la cuenta de la instancia de base de datos, anote el valor de Directory ID (ID de directorio). Utilice este identificador de directorio para unir la instancia de base de datos al dominio.

Paso 6: crear o modificar una instancia de base de datos de Oracle

Cree o modifique una instancia de base de datos de Oracle para usarla con su directorio. Puede utilizar la consola, CLI, o la API de RDS para asociar una instancia de base de datos con un directorio. Puede hacerlo de una de las siguientes formas:

- Cree una nueva instancia de base de datos de Oracle utilizando la consola, el comando de CLI create-db-instance o la operación CreateDBInstance de la API de RDS.

Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.

- Modifique una instancia de base de datos de Oracle existente utilizando la consola, el comando de CLI modify-db-instance o la operación ModifyDBInstance de la API de RDS.

  Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.

- Restaure una instancia de base de datos de Oracle a partir de una instantánea de base de datos utilizando la consola, el comando de CLI restore-db-instance-from-db-snapshot o la operación RestoreDBInstanceFromDBSnapshot de la API de RDS.

  Para obtener instrucciones, consulte Restauración a una instancia de base de datos.

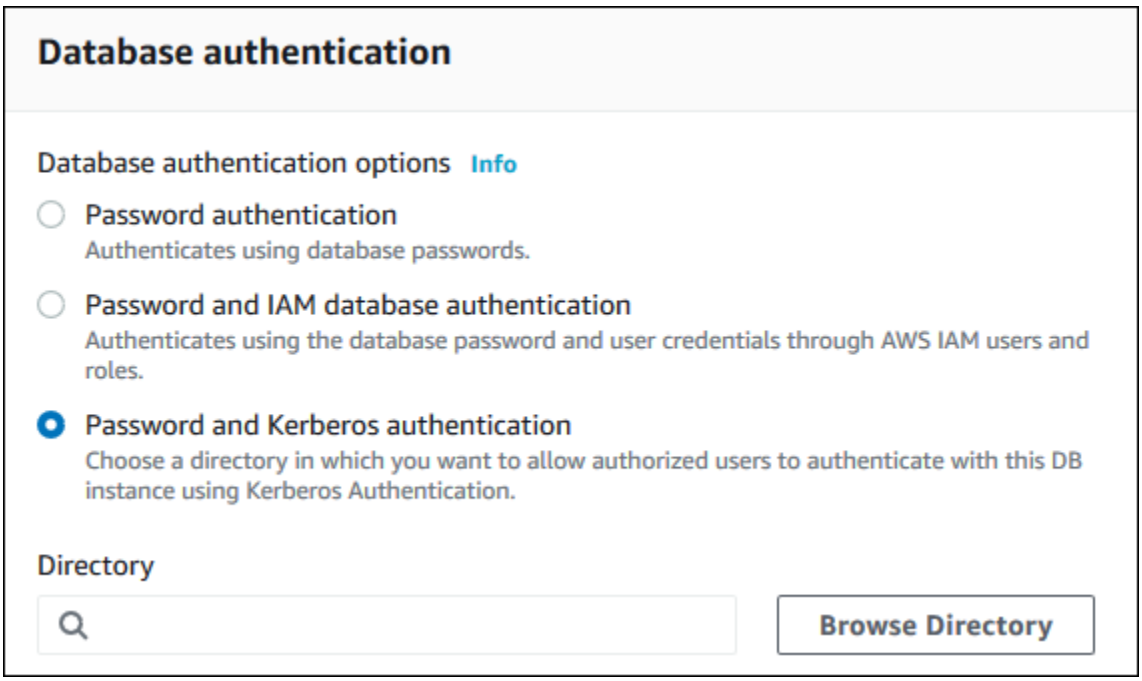
- Restaure una instancia de base de datos de Oracle a partir de un punto en el tiempo utilizando la consola, el comando de CLI restore-db-instance-to-point-in-time o la operación RestoreDBInstanceToPointInTime de la API de RDS.

  Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

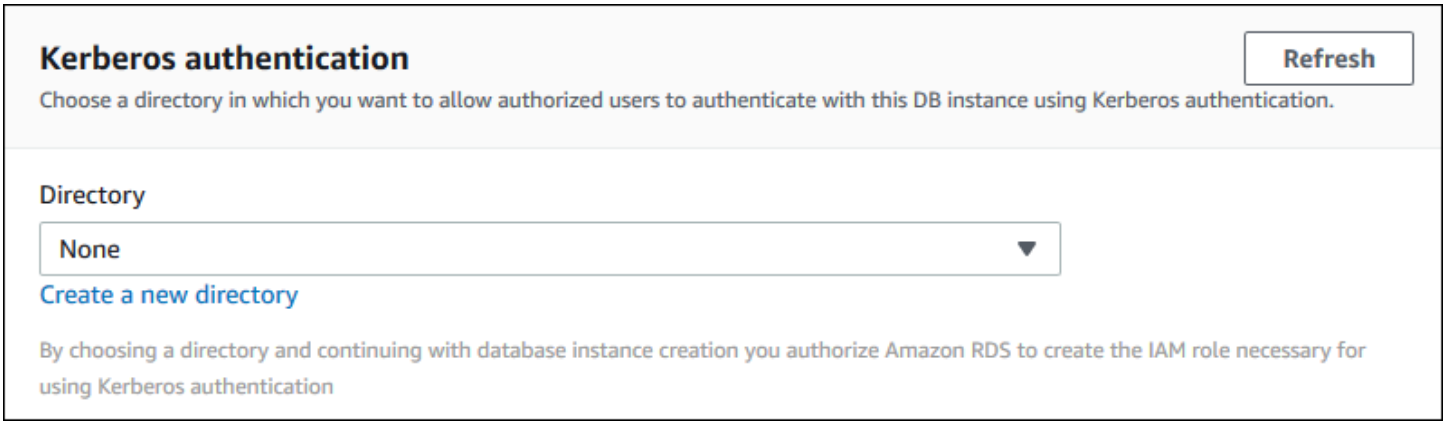
La autenticación Kerberos solo es compatible con instancias de base de datos de Oracle en una VPC. La instancia de DB puede estar en la misma VPC que el directorio o en una VPC diferente. Cuando cree o modifique la instancia de base de datos, haga lo siguiente:

- Proporcione el identificador de dominio (identificador `d-*`) que se generó cuando creó el directorio.
- Proporcione el nombre del rol de IAM que ha creado.
- Asegúrese de que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico entrante del grupo de seguridad del directorio y enviar tráfico saliente al directorio.

Si utiliza la consola para crear una instancia de base de datos, elija Password and Kerberos authentication (Contraseña y autenticación Kerberos) en la sección Database authentication (Autenticación de base de datos). Elija Browse Directory (Examinar directorio) y, a continuación, seleccione el directorio o elija Create a new directory (Crear un nuevo directorio).



Si utiliza la consola para modificar o restaurar una instancia de base de datos, elija el directorio en la sección Kerberos authentication (Autenticación Kerberos) o elija Create a new directory (Crear un nuevo directorio).



Cuando utilice la AWS CLI, se necesitan los siguientes parámetros para que la instancia de base de datos pueda usar el directorio que ha creado:

- Para el parámetro `--domain`, utilice el identificador de dominio (identificador "d-*") que se generó cuando creó el directorio.
- Para el parámetro `--domain-iam-role-name`, utilice el rol que creó que usa la política `AmazonRDSDirectoryServiceAccess` de IAM administrada.

Por ejemplo, el siguiente comando de CLI modifica una instancia de base de datos para usar un directorio.

Para Linux, macOS, o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --domain d-ID \
    --domain-iam-role-name role-name
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --domain d-ID ^
    --domain-iam-role-name role-name
```

Important

Si modifica una instancia de base de datos para habilitar la autenticación Kerberos, reinicie la instancia de base de datos después de realizar el cambio.

Note

MANAGED_SERVICE_USER es una cuenta de servicio cuyo nombre genera aleatoriamente Directory Service para RDS. Durante la configuración de la autenticación Kerberos, RDS para Oracle crea un usuario con el mismo nombre y le asigna el privilegio `CREATE SESSION`. El usuario de base de datos de Oracle se identifica externamente como *MANAGED_SERVICE_USER@EXAMPLE.COM*, donde *EXAMPLE.COM* es el nombre de su dominio. Periódicamente, RDS utiliza las credenciales proporcionadas por Directory Service para iniciar sesión en la base de datos de Oracle. Después, RDS destruye inmediatamente la caché de tickets.

Paso 7: crear inicios de sesión de Oracle de autenticación Kerberos

Use las credenciales del usuario maestro de Amazon RDS para conectarse a la instancia de base de datos de Oracle igaul que con cualquier otra instancia de base de datos. La instancia de base

de datos se une al dominio de AWS Managed Microsoft AD. Por lo tanto, puede aprovisionar inicios de sesión y usuarios de Oracle desde usuarios de Microsoft Active Directory en el dominio. Para administrar los permisos de la base de datos, otorgue y revoque los permisos estándar de Oracle para estos inicios de sesión.

Para permitir que un usuario de Microsoft Active Directory se autentique con Oracle

1. Conéctese a la instancia de base de datos de Oracle mediante sus credenciales de usuario maestro de Amazon RDS.
2. Cree un usuario autenticado externamente en la base de datos de Oracle.

   En el ejemplo siguiente, reemplace *KRBUSER@CORP.EXAMPLE.COM* por el nombre de usuario y el nombre de dominio.

   ```
   CREATE USER "KRBUSER@CORP.EXAMPLE.COM" IDENTIFIED EXTERNALLY;
   GRANT CREATE SESSION TO "KRBUSER@CORP.EXAMPLE.COM";
   ```

   Ahora, los usuarios (tanto humanos como aplicaciones) del dominio pueden conectarse a la instancia de base de datos de Oracle desde un equipo cliente unido al dominio mediante la autenticación Kerberos.

Paso 8: configurar un cliente de Oracle

Para configurar un cliente de Oracle, cumpla los requisitos siguientes:

- Cree un archivo de configuración denominado krb5.conf (Linux) o krb5.ini (Windows) para apuntar al dominio. Configure el cliente de Oracle para utilizar este archivo de configuración.
- Compruebe que el tráfico puede fluir entre el host cliente y AWS Directory Service sobre el puerto 53 de DNS y TCP/UDP, y los puertos de Kerberos (88 y 464 para AWS Directory Service administrado) sobre el puerto 389 de TCP y LDAP.
- Verifique que el tráfico puede fluir entre el host cliente y la instancia de base de datos sobre el puerto de base de datos.

A continuación, se encuentra el contenido de muestra para AWS Managed Microsoft AD.

```
[libdefaults]
 default_realm = EXAMPLE.COM
[realms]
```

```
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
[domain_realm]
 .example.com = CORP.EXAMPLE.COM
 example.com = CORP.EXAMPLE.COM
```

El siguiente es el contenido de muestra para Microsoft AD local. En el archivo krb5.conf o krb5.ini, sustituya*on-prem-ad-server-name* por el nombre del servidor AD local.

```
[libdefaults]
 default_realm = ONPREM.COM
[realms]
 AWSAD.COM = {
  kdc = awsad.com
  admin_server = awsad.com
 }
 ONPREM.COM = {
  kdc = on-prem-ad-server-name
  admin_server = on-prem-ad-server-name
 }
[domain_realm]
 .awsad.com = AWSAD.COM
 awsad.com= AWSAD.COM
 .onprem.com = ONPREM.COM
 onprem.com= ONPREM.COM
```

> **Note**
>
> Después de configurar el archivo krb5.ini o krb5.conf, le recomendamos que reinicie el servidor.

El siguiente es contenido sqlnet.ora de ejemplo para una configuración de SQL*Plus:

```
SQLNET.AUTHENTICATION_SERVICES=(KERBEROS5PRE,KERBEROS5)
SQLNET.KERBEROS5_CONF=path_to_krb5.conf_file
```

Para ver un ejemplo de una configuración de SQL Developer, consulte Document 1609359.1 de Oracle Support.

Administración de una instancia de base de datos en un dominio

Puede usar la consola, la CLI o la API de RDS para administrar su instancia de base de datos y su relación con su Microsoft Active Directory. Puede, por ejemplo, asociar un Microsoft Active Directory para habilitar la autenticación Kerberos. También puede disociar un Microsoft Active Directory para deshabilitar la autenticación Kerberos. También puede mover una instancia de base de datos para que sea autenticada externamente por un Microsoft Active Directory a otro.

Por ejemplo, con la CLI, puede hacer lo siguiente:

- Volver a intentar habilitar la autenticación Kerberos para una pertenencia fallida, use el comando de CLI modify-db-instance y especifique el ID de directorio de pertenencia actual para la opción `--domain`.
- Deshabilitar la autenticación Kerberos en una instancia de base de datos, utilice el comando de CLI modify-db-instance y especifique `none` para la opción `--domain`.
- Mover una instancia de base de datos de un dominio a otro, use el comando de CLI modify-db-instance y especifique el identificador de dominio del nuevo dominio para la opción `--domain`.

Visualización del estado de la suscripción al dominio

Una vez que haya creado o modificado una instancia de base de datos, esta se convierte en miembro del dominio. Puede ver el estado de la pertenencia del dominio para la instancia de base de datos en la consola o ejecutando el comando de CLI describe-db-instances. El estado de la instancia de base de datos puede ser uno de los siguientes:

- `kerberos-enabled`: la instancia de base de datos tiene habilitada la autenticación Kerberos.
- `enabling-kerberos` - AWS está en proceso de habilitar la autenticación Kerberos en esta instancia de base de datos.
- `pending-enable-kerberos`: la habilitación de la autenticación Kerberos está pendiente en esta instancia de base de datos.
- `pending-maintenance-enable-kerberos` - AWS intentará habilitar la autenticación Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `pending-disable-kerberos`: la deshabilitación de la autenticación Kerberos está pendiente en esta instancia de base de datos.
- `pending-maintenance-disable-kerberos` - AWS intentará desactivar la autenticación Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.

- `enable-kerberos-failed`: un problema de configuración ha impedido que AWS habilite la autenticación Kerberos en la instancia de base de datos. Corrija el problema de configuración antes de volver a ejecutar el comando para modificar la instancia de base de datos.
- `disabling-kerberos` - AWS está en proceso de desactivar la autenticación Kerberos en esta instancia de base de datos.

Una solicitud para habilitar la autenticación Kerberos puede generar un error a causa de un problema de conectividad de la red o de un rol de IAM incorrecto. Si el intento de habilitar la autenticación Kerberos falla al crear o modificar una instancia de base de datos, debe asegurarse de que está utilizando el rol de IAM correcto. A continuación, modifique la instancia de base de datos para unirse al dominio.

> **Note**
>
> Solo la autenticación Kerberos con Amazon RDS for Oracle envía tráfico a los servidores DNS del dominio. Las otras solicitudes de DNS se tratan como acceso de red saliente en las instancias de bases de datos que ejecutan Oracle. Para obtener más información acerca del acceso de red saliente con Amazon RDS para Oracle, consulte Configuración de un servidor DNS personalizado.

Rotación forzada de claves de Kerberos

Una clave secreta se comparte entre AWS Managed Microsoft AD y una instancia de base de datos de Amazon RDS for Oracle. Esta clave se rota automáticamente cada 45 días. Puede utilizar el siguiente procedimiento de Amazon RDS para forzar la rotación de esta clave.

```
SELECT rdsadmin.rdsadmin_kerberos_auth_tasks.rotate_kerberos_keytab AS TASK_ID FROM
 DUAL;
```

> **Note**
>
> En una configuración de réplica de lectura, este procedimiento solo está disponible en la instancia de base de datos de origen y no en la réplica de lectura.

La instrucción SELECT devuelve el identificador de la tarea en un tipo de datos VARCHAR2. Puede ver el estado de una tarea continua en un archivo bdump. Los archivos bdump están ubicados en el directorio /rdsdbdata/log/trace. El nombre del archivo bdump está en el siguiente formato.

```
dbtask-task-id.log
```

Para ver el resultado, visualice el archivo de salida de la tarea.

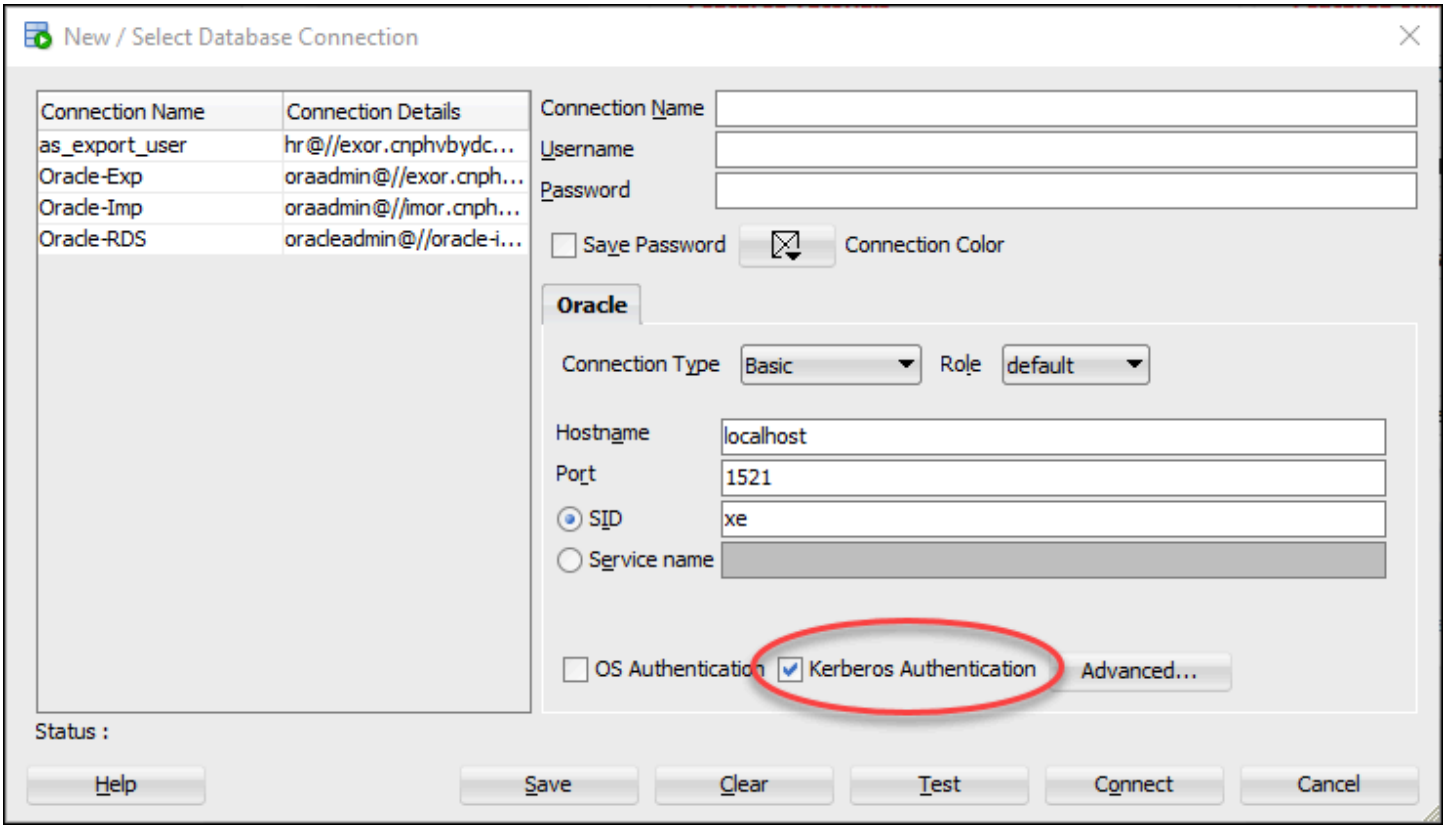
```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Reemplace *task-id* con el ID de tarea devuelto por el procedimiento.

> **Note**
>
> Las tareas se ejecutan de forma asíncrona.

Conexión a Oracle con autenticación Kerberos

En esta sección se supone que ha configurado el cliente de Oracle como se describe en Paso 8: configurar un cliente de Oracle. Para conectarse a la base de datos de Oracle con autenticación Kerberos, inicie sesión con el tipo de autenticación Kerberos. Por ejemplo, después de lanzar Oracle SQL Developer, elija Autenticación Kerberos como tipo de autenticación, como se puede ver a continuación.



Para conectarse a Oracle con autenticación Kerberos con SQL*Plus:

1. En el símbolo del sistema, ejecute el siguiente comando:

   ```
   kinit username
   ```

   Sustituya *username* por el nombre de usuario y, en el indicador, introduzca la contraseña almacenada en el Microsoft Active Directory para el usuario.

2. Abra SQL*Plus y conecte usando el nombre de DNS y el número de puerto para la instancia de base de datos de Oracle.

   Para obtener más información sobre la conexión a la instancia de base de datos de Oracle en SQL*Plus, consulte Conexión a la instancia de base de datos mediante SQL*Plus.

> **Tip**
>
> Si utiliza una caché nativa de Windows, también puede establecer el parámetro `SQLNET.KERBEROS5_CC_NAME` en `OSMSFT://` o `MSLSA` en el archivo sqlnet.ora para usar las credenciales almacenadas en Microsoft Active Directory.

Configuración del acceso UTL_HTTP mediante certificados y un wallet de Oracle.

Amazon RDS admite el acceso a la red saliente en las instancias de base de datos de RDS para Oracle. Para conectar la instancia de base de datos a la red, puede utilizar los siguientes paquetes PL/SQL:

`UTL_HTTP`

Este paquete realiza llamadas HTTP desde SQL y PL/SQL. Puede usarlo para acceder a los datos de Internet a través de HTTP. Para obtener más información, consulte UTL_HTTP en la documentación de Oracle.

`UTL_TCP`

Este paquete proporciona funcionalidad de acceso del lado del cliente TCP/IP en PL/SQL. Este paquete es útil para aplicaciones PL/SQL que utilizan protocolos de Internet y correo electrónico. Para obtener más información, consulte UTL_TCP en la documentación de Oracle.

`UTL_SMTP`

Este paquete proporciona interfaces a los comandos SMTP que permiten a un cliente enviar correos electrónicos a un servidor SMTP. Para obtener más información, consulte UTL_SMTP en la documentación de Oracle.

Al completar las siguientes tareas, puede configurar `UTL_HTTP.REQUEST` para trabajar con sitios web que requieren certificados de autenticación de cliente durante el protocolo de enlace SSL. También puede configurar la autenticación por contraseña para el acceso de `UTL_HTTP` a sitios web modificando los comandos de generación de wallets de Oracle y el procedimiento `DBMS_NETWORK_ACL_ADMIN.APPEND_WALLET_ACE`. Para más información, consulte DBMS_NETWORK_ACL_ADMIN en la documentación de Oracle Database.

> **Note**
>
> Puede adaptar las siguientes tareas para `UTL_SMTP`, que le permite enviar correos electrónicos a través de SSL/TLS (por ejemplo, Amazon Simple Email Service).

Temas

- Consideraciones al configurar el acceso UTL_HTTP
- Paso 1: obtener el certificado raíz de un sitio web
- Paso 2: crear un wallet de Oracle
- Paso 3: descargar el wallet de Oracle en su instancia de RDS for Oracle
- Paso 4: conceder permisos de usuario para el wallet de Oracle
- Paso 5: configurar el acceso a un sitio web desde la instancia de base de datos
- Paso 6: probar las conexiones desde la instancia de base de datos a un sitio web

Consideraciones al configurar el acceso UTL_HTTP

Tenga en cuenta lo siguiente antes de configurar el acceso:

- Puede utilizar SMTP con la opción UTL_MAIL. Para obtener más información, consulte Oracle UTL_MAIL.
- El nombre en el servidor de nombres de dominio (DNS) del host remoto puede ser cualquiera de los siguientes:
  - Uno que se pueda resolver públicamente.
  - El punto de enlace de una instancia de base de datos de Amazon RDS.
  - Uno que se pueda resolver a través de un servidor DNS personalizado. Para obtener más información, consulte Configuración de un servidor DNS personalizado.
  - El nombre de DNS privado de una instancia de Amazon EC2 de la misma VPC o de una VPC interconectada. En este caso, asegúrese de que el nombre se pueda resolver a través de un servidor DNS personalizado. Para utilizar el DNS proporcionado por Amazon, también puede activar el atributo `enableDnsSupport` en la configuración de la VPC y activar la compatibilidad con la resolución de DNS para la interconexión de VPC. Para obtener más información, consulte Compatibilidad de DNS en su VPC y Modificación de las opciones de conexión de interconexión de VPC.

- Para conectarse de forma segura a recursos remotos SSL/TLS, le recomendamos que cree y cargue Oracle Wallets personalizados. Utilice la integración de Simple Storage Service (Amazon S3) con la característica de Amazon RDS for Oracle para descargar un wallet de su Amazon S3 en instancias de base de datos de Oracle. Para obtener información sobre la integración de Amazon S3 para Oracle, consulte Integración de Amazon S3.
- Puede establecer enlaces de base de datos entre las instancias de base de datos de Oracle a través de un punto de enlace SSL/TLS si la opción de Oracle SSL está configurada para cada instancia. No se necesitan más configuraciones. Para obtener más información, consulte Capa de conexión segura de Oracle.

Paso 1: obtener el certificado raíz de un sitio web

Para que la instancia de base de datos de RDS para Oracle establezca conexiones seguras con un sitio web, agregue el certificado de entidad de certificación raíz. Amazon RDS utiliza el certificado raíz para firmar el certificado del sitio web en el wallet de Oracle.

Puede obtener el certificado raíz de varias formas. Por ejemplo, puede hacer lo siguiente:

1. Utilice un servidor web para visitar el sitio web protegido por el certificado.
2. Descargue el certificado raíz que se utilizó para la firma.

Para los servicios de AWS, los certificados raíz suelen residir en el repositorio de Amazon trust services.

Paso 2: crear un wallet de Oracle

Cree un wallet de Oracle que contenga tanto los certificados del servidor web como los certificados de autenticación del cliente. La instancia de RDS Oracle utiliza el certificado del servidor web para establecer una conexión segura con el sitio web. El sitio web necesita el certificado del cliente para autenticar al usuario de la base de datos Oracle.

Es posible que desee configurar conexiones seguras sin utilizar certificados de cliente para la autenticación. En este caso, puede omitir los pasos del almacén de claves de Java en el siguiente procedimiento.

Para crear un wallet de Oracle

1. Coloque los certificados raíz y de cliente en un único directorio y, a continuación, cambie a este directorio.
2. Convierta el certificado de cliente .p12 en el almacén de claves de Java.

   > **Note**
   >
   > Si no utiliza los certificados de cliente para la autenticación, puede omitir este paso.

   El siguiente ejemplo convierte el certificado de cliente denominado *client_certificate.p12* en el almacén de claves de Java denominado *client_keystore.jks*. El almacén de claves se incluye en el wallet de Oracle. La contraseña del almacén de claves es *P12PASSWORD*.

   ```
   orapki wallet pkcs12_to_jks -wallet ./client_certificate.p12 -
   jksKeyStoreLoc ./client_keystore.jks -jksKeyStorepwd P12PASSWORD
   ```
3. Cree un directorio para el wallet de Oracle que sea diferente del directorio del certificado.

   El siguiente ejemplo crea el directorio `/tmp/wallet`.

   ```
   mkdir -p /tmp/wallet
   ```
4. Cree un wallet de Oracle en su directorio de wallets.

   El siguiente ejemplo establece la contraseña del wallet de Oracle como *P12PASSWORD*, que es la misma contraseña utilizada por el almacén de claves de Java en un paso anterior. Es conveniente utilizar la misma contraseña, pero no es necesario. El parámetro `-auto_login` activa la característica de inicio de sesión automático, para que no sea necesario especificar una contraseña cada vez que se quiera acceder.

   > **Note**
   >
   > Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

```
orapki wallet create -wallet /tmp/wallet -pwd P12PASSWORD -auto_login
```

5. Agregue el almacén de claves de Java al wallet de Oracle.

> **Note**
>
> Si no utiliza los certificados de cliente para la autenticación, puede omitir este paso.

En el siguiente ejemplo se agrega el almacén de claves *cliente_keystore.jks* al wallet de Oracle denominado */tmp/wallet*. En este ejemplo, se especifica la misma contraseña para el almacén de claves de Java y el wallet de Oracle.

```
orapki wallet jks_to_pkcs12 -wallet /tmp/wallet -pwd P12PASSWORD -
keystore ./client_keystore.jks -jkspwd P12PASSWORD
```

6. Agregue el certificado raíz de su sitio web de destino al Oracle Wallet.

En el siguiente ejemplo se agrega un certificado denominado *Root_CA.cer*.

```
orapki wallet add -wallet /tmp/wallet -trusted_cert -cert ./Root_CA.cer -
pwd P12PASSWORD
```

7. Agregue los certificados intermedios.

El siguiente ejemplo agrega un certificado denominado *Intermediate.cer*. Repita este paso tantas veces como sea necesario para cargar todos los certificados intermedios.

```
orapki wallet add -wallet /tmp/wallet -trusted_cert -cert ./Intermediate.cer -
pwd P12PASSWORD
```

8. Confirme que el wallet de Oracle recién creado tenga los certificados necesarios.

```
orapki wallet display -wallet /tmp/wallet -pwd P12PASSWORD
```

Paso 3: descargar el wallet de Oracle en su instancia de RDS for Oracle

En este paso, cargue el wallet de Oracle en Simple Storage Service (Amazon S3) y, a continuación, descargue el wallet de Amazon S3 en su instancia de RDS para Oracle.

Para descargar el wallet de Oracle en su instancia de base de datos de RDS for Oracle.

1. Complete los requisitos previos para la integración de Amazon S3 con Oracle y añada la opción `S3_INTEGRATION` a su instancia de base de datos de Oracle. Asegúrese de que el rol de IAM para la opción disponga de acceso al bucket de Amazon S3 que está utilizando.

   Para obtener más información, consulte Integración de Amazon S3.
2. Inicie sesión en su instancia de base de datos como usuario principal y, a continuación, cree un directorio de Oracle para albergar el wallet de Oracle.

   El siguiente ejemplo crea un directorio de Oracle llamado *`WALLET_DIR`*.

   ```
   EXEC rdsadmin.rdsadmin_util.create_directory('WALLET_DIR');
   ```

   Para obtener más información, consulte Creación y eliminación de directorios en el espacio de almacenamiento de datos principal.
3. Cargue el Oracle Wallet en el bucket de Simple Storage Service (Amazon S3).

   Puede usar cualquier técnica de carga compatible.
4. Si va a volver a cargar un wallet de Oracle, elimine el wallet existente. De no ser así, vaya al siguiente paso.

   El siguiente ejemplo elimina el wallet existente, cuyo nombre es *`cwallet.sso`*.

   ```
   EXEC UTL_FILE.FREMOVE ('WALLET_DIR','cwallet.sso');
   ```
5. Descargue el Oracle Wallet desde su bucket de Simple Storage Service (Amazon S3) a la instancia de base de datos de Oracle.

   El siguiente ejemplo descarga el wallet llamado *`cwallet.sso`* desde el bucket de Simple Storage Service (Amazon S3) llamado *`my_s3_bucket`* al directorio de la instancia de base de datos llamado *`WALLET_DIR`*.

   ```
   SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
   ```

```
      p_bucket_name    =>  'my_s3_bucket',
      p_s3_prefix      =>  'cwallet.sso',
      p_directory_name =>  'WALLET_DIR')
   AS TASK_ID FROM DUAL;
```

6. (Opcional) Descargue un wallet de Oracle protegido por contraseña.

   Descargue este wallet solo si quiere requerir una contraseña para cada uso del wallet. El siguiente ejemplo descarga el wallet protegido por contraseña *ewallet.p12*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name    =>  'my_s3_bucket',
      p_s3_prefix      =>  'ewallet.p12',
      p_directory_name =>  'WALLET_DIR')
   AS TASK_ID FROM DUAL;
```

7. Verifique el estado de la tarea de la base de datos.

   Sustituya el ID de la tarea devuelto en los pasos anteriores por *dbtask-1234567890123-4567.log* en el siguiente ejemplo.

```
SELECT TEXT FROM
 TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1234567890123-4567.log'));
```

8. Verifique el contenido del directorio que se utiliza para almacenar el wallet de Oracle.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'WALLET_DIR'));
```

   Para obtener más información, consulte Descripción de los archivos de un directorio de instancia de base de datos.

Paso 4: conceder permisos de usuario para el wallet de Oracle

Puede crear un nuevo usuario de base de datos o configurar un usuario existente. En cualquiera de los dos casos, debe configurar el usuario para que acceda wallet de Oracle para las conexiones seguras y la autenticación del cliente mediante certificados.

Para conceder permisos de usuario para el wallet de Oracle

1. Inicie sesión en la instancia de base de datos de RDS for Oracle como usuario principal.

2. Si no desea configurar un usuario de base de datos existente, cree un nuevo usuario. De no ser así, vaya al siguiente paso.

   En el siguiente ejemplo, se crea un usuario de base de datos denominado *my-user*.

   ```
   CREATE USER my-user IDENTIFIED BY my-user-pwd;
   GRANT CONNECT TO my-user;
   ```

3. Conceda permiso a los usuarios de la base de datos en el directorio que contiene el wallet de Oracle.

   El siguiente ejemplo concede acceso de lectura al usuario *my-user* en el directorio *WALLET_DIR*.

   ```
   GRANT READ ON DIRECTORY WALLET_DIR TO my-user;
   ```

4. Conceda permiso al usuario de la base de datos para utilizar el paquete UTL_HTTP.

   El siguiente programa PL/SQL otorga acceso a UTL_HTTP al usuario *my-user*.

   ```
   BEGIN
     rdsadmin.rdsadmin_util.grant_sys_object('UTL_HTTP', UPPER('my-user'));
     END;
   /
   ```

5. Conceda permiso al usuario de la base de datos para utilizar el paquete UTL_FILE.

   El siguiente programa PL/SQL otorga acceso a UTL_FILE al usuario *my-user*.

   ```
   BEGIN
     rdsadmin.rdsadmin_util.grant_sys_object('UTL_FILE', UPPER('my-user'));
     END;
   /
   ```

Paso 5: configurar el acceso a un sitio web desde la instancia de base de datos

En este paso se configura el usuario de la base de datos Oracle para que pueda conectarse al sitio web de destino mediante UTL_HTTP, el wallet de Oracle cargado y el certificado del cliente. Para más información, consulte Configuring Access Control to an Oracle Wallet (Configuración del control de acceso a un wallet de Oracle) en la documentación de Oracle Database.

Para configurar el acceso a un sitio web desde la instancia de base de datos de RDS for Oracle

1. Inicie sesión en la instancia de base de datos de RDS for Oracle como usuario principal.
2. Cree una entrada de control de acceso al host (ACE) para el usuario y el sitio web de destino en un puerto seguro.

   El siguiente ejemplo configura *my-user* para acceder a *secret.encrypted-website.com* en el puerto seguro 443.

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(
    host       => 'secret.encrypted-website.com',
    lower_port => 443,
    upper_port => 443,
    ace        => xs$ace_type(privilege_list => xs$name_list('http'),
                              principal_name => 'my-user',
                              principal_type => xs_acl.ptype_db));
                           -- If the program unit results in PLS-00201, set
                           -- the principal_type parameter to 2 as follows:
                           -- principal_type => 2));
END;
/
```

> **Important**
>
> La unidad de programa anterior puede provocar el siguiente error: `PLS-00201: identifier 'XS_ACL' must be declared`. Si se devuelve este error, sustituya la línea que asigna un valor a `principal_type` por la línea siguiente y, a continuación, vuelva a ejecutar la unidad de programa:
>
> ```
> principal_type => 2));
> ```
>
> Para obtener más información acerca de las constantes del paquete PL/SQL `XS_ACL`, consulte la Real Application Security Administrator's and Developer's Guide en la documentación de Oracle Database.

Para más información, consulte Configuring Access Control for External Network Services (Configuración del control de acceso para servicios de red externos) en la documentación de Oracle Database.

3. (Opcional) Cree una ACE para el usuario y el sitio web de destino en el puerto estándar.

   Es posible que tenga que utilizar el puerto estándar si algunas páginas web reciben servicio desde el puerto estándar del servidor web (80) en lugar del puerto seguro (443).

```
BEGIN
  DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(
    host       => 'secret.encrypted-website.com',
    lower_port => 80,
    upper_port => 80,
    ace        => xs$ace_type(privilege_list => xs$name_list('http'),
                              principal_name => 'my-user',
                              principal_type => xs_acl.ptype_db));
                           -- If the program unit results in PLS-00201, set
                           -- the principal_type parameter to 2 as follows:
                           -- principal_type => 2));
END;
/
```

4. Confirme que las entradas de control de acceso existen.

```
SET LINESIZE 150
COLUMN HOST FORMAT A40
COLUMN ACL FORMAT A50

SELECT HOST, LOWER_PORT, UPPER_PORT, ACL
  FROM DBA_NETWORK_ACLS
ORDER BY HOST;
```

5. Conceda permiso al usuario de la base de datos para utilizar el paquete UTL_HTTP.

   El siguiente programa PL/SQL otorga acceso a UTL_HTTP al usuario *my-user*.

```
BEGIN
  rdsadmin.rdsadmin_util.grant_sys_object('UTL_HTTP', UPPER('my-user'));
  END;
/
```

6. Confirme que existen listas de control de acceso relacionadas.

```
SET LINESIZE 150
COLUMN ACL FORMAT A50
COLUMN PRINCIPAL FORMAT A20
COLUMN PRIVILEGE FORMAT A10

SELECT ACL, PRINCIPAL, PRIVILEGE, IS_GRANT,
       TO_CHAR(START_DATE, 'DD-MON-YYYY') AS START_DATE,
       TO_CHAR(END_DATE, 'DD-MON-YYYY') AS END_DATE
  FROM DBA_NETWORK_ACL_PRIVILEGES
ORDER BY ACL, PRINCIPAL, PRIVILEGE;
```

7. Conceda permiso al usuario de su base de datos de utilizar certificados para la autenticación del cliente y el wallet de Oracle para las conexiones.

> **Note**
>
> Si no utiliza los certificados de cliente para la autenticación, puede omitir este paso.

```
DECLARE
  l_wallet_path all_directories.directory_path%type;
BEGIN
  SELECT DIRECTORY_PATH
    INTO l_wallet_path
    FROM ALL_DIRECTORIES
   WHERE UPPER(DIRECTORY_NAME)='WALLET_DIR';
  DBMS_NETWORK_ACL_ADMIN.APPEND_WALLET_ACE(
    wallet_path => 'file:/' || l_wallet_path,
    ace         =>  xs$ace_type(privilege_list => xs
$name_list('use_client_certificates'),
                                principal_name => 'my-user',
                                principal_type => xs_acl.ptype_db));
END;
/
```

Paso 6: probar las conexiones desde la instancia de base de datos a un sitio web

En este paso, configurará al usuario de la base de datos para que pueda conectarse al sitio web mediante UTL_HTTP, el wallet de Oracle cargado y el certificado del cliente.

Para configurar el acceso a un sitio web desde la instancia de base de datos de RDS for Oracle

1. Inicie sesión en la instancia de base de datos de RDS for Oracle como usuario de base de datos con permisos UTL_HTTP.
2. Confirme que una conexión al sitio web de destino puede resolver la dirección del host.

   En el siguiente ejemplo, se obtiene la dirección de host de *secret.encrypted-website.com*.

   ```
   SELECT UTL_INADDR.GET_HOST_ADDRESS(host => 'secret.encrypted-website.com')
     FROM DUAL;
   ```
3. Pruebe una conexión fallida.

   La siguiente consulta falla porque UTL_HTTP requiere la ubicación del wallet de Oracle con los certificados.

   ```
   SELECT UTL_HTTP.REQUEST('secret.encrypted-website.com') FROM DUAL;
   ```
4. Pruebe el acceso al sitio web mediante UTL_HTTP.SET_WALLET y seleccione desde DUAL.

   ```
   DECLARE
     l_wallet_path all_directories.directory_path%type;
   BEGIN
     SELECT DIRECTORY_PATH
       INTO l_wallet_path
       FROM ALL_DIRECTORIES
      WHERE UPPER(DIRECTORY_NAME)='WALLET_DIR';
     UTL_HTTP.SET_WALLET('file:/' || l_wallet_path);
   END;
   /

   SELECT UTL_HTTP.REQUEST('secret.encrypted-website.com') FROM DUAL;
   ```

5. (Opcional) Pruebe el acceso al sitio web mediante el almacenamiento de la consulta en una variable y el uso de `EXECUTE IMMEDIATE`.

```
DECLARE
  l_wallet_path all_directories.directory_path%type;
  v_webpage_sql VARCHAR2(1000);
  v_results     VARCHAR2(32767);
BEGIN
  SELECT DIRECTORY_PATH
    INTO l_wallet_path
    FROM ALL_DIRECTORIES
   WHERE UPPER(DIRECTORY_NAME)='WALLET_DIR';
  v_webpage_sql := 'SELECT UTL_HTTP.REQUEST(''secret.encrypted-website.com'', '''',
 ''file:/' ||l_wallet_path||''') FROM DUAL';
  DBMS_OUTPUT.PUT_LINE(v_webpage_sql);
  EXECUTE IMMEDIATE v_webpage_sql INTO v_results;
  DBMS_OUTPUT.PUT_LINE(v_results);
END;
/
```

6. (Opcional) Busque la ubicación en el sistema de archivos de su directorio de wallets de Oracle.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'WALLET_DIR'));
```

Utilice el resultado del comando anterior para realizar una solicitud HTTP. Por ejemplo, si el directorio es *rdsdbdata/userdirs/01*, ejecute la siguiente consulta.

```
SELECT UTL_HTTP.REQUEST('https://secret.encrypted-website.com/', '',
 'file://rdsdbdata/userdirs/01')
FROM   DUAL;
```

Uso de CDB con RDS para Oracle

En la arquitectura multitenencia de Oracle, una base de datos de contenedores (CDB) puede incluir bases de datos conectables (PDB) creadas por el cliente. Para obtener más información sobre las CDB, consulte el tema de presentación de la arquitectura multitenencia en la documentación de Oracle Database.

Temas

- Descripción general de las CDB de RDS para Oracle
- Configuración de una CDB de RDS para Oracle
- Copia de seguridad y restauración de una CDB
- Conversión de una base de datos no CDB de RDS para Oracle en una CDB
- Convertir la configuración de un solo inquilino a una de varios inquilinos.
- Añadir una base de datos de inquilinos de RDS para Oracle a su instancia de CDB
- Modificación de una base de datos de inquilinos de RDS para Oracle
- Eliminar una base de datos de inquilinos de RDS para Oracle de su CDB
- Ver detalles de la base de datos de inquilinos
- Actualización de la CDB

Descripción general de las CDB de RDS para Oracle

Puede crear una instancia de base de datos de RDS para Oracle como base de datos de contenedores (CDB) al ejecutar Oracle Database 19c o una versión posterior. A partir de Oracle Database 21c, todas las bases de datos son CDB. La diferencia entre una CDB y una base de datos que no sea CDB es que la primera puede contener bases de datos conectables (PDB), llamadas bases de datos de inquilinos en RDS para Oracle. Una PDB es una colección portátil de esquemas y objetos que una aplicación ve como base de datos independiente.

Al crear la instancia de CDB, debe crear la base de datos de inquilinos (PDB) inicial. En RDS para Oracle, la aplicación cliente interactúa con la PDB en lugar de con la CDB. La experiencia con una PDB es, en general, idéntica a la de con una no CDB.

Temas

- Configuración de varios inquilinos de la arquitectura CDB
- Configuración de un solo inquilino de la arquitectura CDB

- Opciones de creación y conversión para CDB
- Cuentas de usuario y privilegios en una CDB
- Familias de grupos de parámetros en una CDB
- Limitaciones de las CDB de RDS para Oracle

Configuración de varios inquilinos de la arquitectura CDB

RDS para Oracle es compatible con la configuración de varios inquilinos de la arquitectura multitenencia de Oracle, también llamada arquitectura CDB. En esta configuración, la instancia de CDB de RDS para Oracle puede contener entre 1 y 30 bases de datos de inquilinos, en función de la edición de la base de datos y de las licencias de opciones que se requieran. En una base de datos de Oracle, una base de datos de inquilinos es una PDB. La instancia de base de datos debe usar la versión de base de datos Oracle 19.0.0.0.ru-2022-01.rur-2022.r1 o superior.

> **Note**
>
> La configuración de Amazon RDS se denomina “de varios inquilinos”, en lugar de “multitenencia”, ya que es una capacidad de la plataforma RDS, no solo del motor de base de datos de Oracle. De manera similar, el término “inquilino” de RDS se refiere a cualquier inquilino en una configuración de RDS, no solo a las PDB de Oracle. En la documentación de RDS, el término “de varios inquilinos de Oracle” sin guion se refiere exclusivamente a la arquitectura CDB de la base de datos de Oracle, que es compatible tanto con las implementaciones en las instalaciones como con RDS.

Puede configurar los siguientes ajustes:

- Nombre de la base de datos de inquilinos
- Nombre de usuario principal de la base de datos de inquilinos
- Contraseña principal de la base de datos de inquilinos (integrada opcionalmente con Secrets Manager)
- Conjunto de caracteres de la base de datos de inquilinos
- Conjunto de caracteres nacional de la base de datos de inquilinos

El conjunto de caracteres de la base de datos de inquilinos puede ser diferente del de la CDB. Lo mismo sucede con el conjunto de caracteres nacional. Tras crear la base de datos de inquilinos

inicial, puede crear, modificar o eliminar las bases de datos de inquilinos usando las API de RDS. El nombre predeterminado de la CDB es `RDSCDB` y no se puede cambiar. Para obtener más información, consulte Configuración de instancias de base de datos y Modificación de una base de datos de inquilinos de RDS para Oracle.

Configuración de un solo inquilino de la arquitectura CDB

RDS para Oracle es compatible con la antigua configuración de arquitectura multitenencia de Oracle, llamada configuración de un solo inquilino. En esta configuración, una instancia de CDB de RDS para Oracle solo puede contener un inquilino (PDB). No puede crear otras PDB más tarde.

Opciones de creación y conversión para CDB

Oracle Database 21c solo admite las CDB, mientras que Oracle Database 19c es compatible con bases de datos CDB y no CDB. Todas las instancias de CDB de RDS para Oracle son compatibles con configuraciones de varios inquilinos y de un solo inquilino.

Opciones de creación, conversión y actualización para la arquitectura de bases de datos de Oracle

La siguiente tabla muestra las diferentes opciones de arquitectura para crear y actualizar las bases de datos de RDS para Oracle.

Release	Opciones de creación de bases de datos	Opciones de conversión de arquitectura	Destinos de actualización de versión principal
Oracle Database 21c	Solo arquitectura CDB	N/A	N/A
Oracle Database 19c	Arquitectura para bases de datos CDB o no CDB	Arquitectura no CDB a CDB (RU de abril de 2021 o superior)	Oracle Database 21c CDB

Tal y como se muestra en la tabla anterior, no se puede actualizar directamente una base de datos que no sea CDB a una CDB en una nueva versión principal de base de datos. Sin embargo, puede convertir una Oracle Database 19c que no sea de CDB en una CDB de Oracle Database 19c y, a continuación, actualizar la CDB de Oracle Database 19c a una CDB de Oracle Database 21c. Para obtener más información, consulte Conversión de una base de datos no CDB de RDS para Oracle en una CDB.

Opciones de conversión para configuraciones de arquitectura CDB

La siguiente tabla muestra las diferentes opciones para convertir la configuración de arquitectura de una instancia de base de datos de RDS para Oracle.

Arquitectura y configuración actuales	Conversión de arquitectura CDB a la configuración de un solo inquilino	Conversión de arquitectura CDB a la configuración de varios inquilinos	Conversión a una arquitectura no CDB
No CDB	Compatible	Compatible*	N/A
CDB con configuración de un solo inquilino	N/A	Compatible	No compatible
CDB con configuración de varios inquilinos	No compatible	N/A	No compatible

* No se puede hacer la conversión de una base de datos no CDB a una configuración de varios inquilinos en una sola operación. Al convertir una base de datos no CDB a una CDB, la CDB está en la configuración de un solo inquilino. Luego, puede usar otra operación para convertir la configuración de un solo inquilino en una de varios inquilinos.

Cuentas de usuario y privilegios en una CDB

En la arquitectura multitenencia de Oracle, todas las cuentas de usuario son usuarios comunes o usuarios locales. Un usuario común de CDB es un usuario de base de datos cuya identidad y contraseña únicas se conocen en la raíz de CDB y en todas las PDB existentes y futuras. En cambio, un usuario local solo existe en una sola PDB.

El usuario maestro de RDS es una cuenta de usuario local de la PDB, a la que se asigna un nombre al crear la instancia de base de datos. Si crea nuevas cuentas de usuario, estos usuarios también serán usuarios locales que residen en la PDB. No puede usar ninguna cuenta de usuario para crear nuevas PDB ni modificar el estado de la PDB existente.

El usuario `rdsadmin` es una cuenta de usuario común. Puede ejecutar paquetes de RDS para Oracle que existen en esta cuenta, pero no puede iniciar sesión como `rdsadmin`. Para obtener más

información, consulte Acerca de los usuarios comunes y los usuarios locales en la documentación de Oracle.

Para los usuarios principales en las configuraciones de varios inquilinos y de un solo inquilino, puede usar credenciales autoadministradas o administradas por AWS Secrets Manager. En la configuración de un solo inquilino, se utilizan comandos CLI en el nivel de instancia, como `create-db-instance` para las contraseñas principales administradas. En la configuración de varios inquilinos, se utilizan los comandos de la base de datos de inquilinos, como `create-tenant-database` para las contraseñas principales administradas. Para obtener más información acerca de la integración de Secrets Manager, consulte Administración de la contraseña de usuario principal para una base de datos de inquilinos de RDS para Oracle con Secrets Manager.

Familias de grupos de parámetros en una CDB

Las CDB tienen sus propias familias de grupos de parámetros y valores de parámetros predeterminados. Las familias de grupos de parámetros de CDB son las siguientes:

- oracle-ee-cdb-21
- oracle-se2-cdb-21
- oracle-ee-cdb-19
- oracle-se2-cdb-19

Limitaciones de las CDB de RDS para Oracle

RDS para Oracle admite un subconjunto de características disponibles en una CDB en las instalaciones.

Limitaciones de la CDB

Las siguientes limitaciones se aplican a RDS para Oracle en el CDB:

- No puede conectarse a una CDB. Siempre se conecta a la base de datos de inquilinos (PDB), y no a la CDB. Especifique el punto de enlace de la PDB al igual que para una base de datos que no es CDB. La única diferencia es que especifica pdb_name para el nombre de base de datos, donde pdb_name es el nombre que eligió para la PDB.
- No se puede convertir una CDB con la configuración de varios inquilinos en una CDB con configuración de un solo inquilino. La conversión a la configuración de varios inquilinos solo se puede hacer en un sentido y es irreversible.

- No puede habilitar la configuración de varios inquilinos, ni hacer una conversión a esta, si la instancia de base de datos usa una versión de base de datos Oracle anterior a 19.0.0.0.ru-2022-01.rur-2022.r1.
- No puede utilizar una CDB de RDS para Oracle con ORDS 22 o una versión posterior. Como solución alternativa, puede utilizar una versión anterior de ORDS o utilizar Oracle Database 19c no CDB.
- No se puede utilizar Oracle Data Guard en la configuración de varios inquilinos, pero se puede utilizar en la configuración de un solo inquilino.
- No pueden utilizar los flujos de actividad de la base de datos en una CDB.
- No puede activar la auditoría desde dentro de `CDB$ROOT`. Debe habilitar la auditoría en cada PDB de forma individual.

Limitaciones de la base de datos de inquilinos (PDB)

Las bases de datos de inquilinos en la configuración de varios inquilinos de RDS para Oracle tienen las siguientes limitaciones:

- No puede aplazar las operaciones de la base de datos de inquilinos hasta el periodo de mantenimiento. Todos los cambios ocurren de forma inmediata.
- No puede agregar una base de datos de inquilinos a una CDB que utilice la configuración de un solo inquilino.
- No puede agregar ni modificar múltiples bases de datos de inquilinos en una sola operación. Solo puede agregarlas o modificarlas de una en una.
- No puede modificar una base de datos de inquilinos para que tenga el nombre `CDB$ROOT` o `PDB$SEED`.
- No puede eliminar una base de datos de inquilino si es la única inquilina en la CDB.
- No todos los tipos de clases de instancias de base de datos tienen recursos suficientes como para admitir varias PDB en una instancia de CDB de RDS para Oracle. Un mayor número de PDB afecta al rendimiento y la estabilidad de las clases de instancias más pequeñas y aumenta el tiempo de la mayoría de las operaciones en el nivel de instancia; por ejemplo, las actualizaciones de bases de datos.
- No puede usar varias Cuentas de AWS para crear PDB en la misma CDB. Las PDB deben pertenecer a la misma cuenta que la instancia de base de datos en la que se alojan las PDB.
- Todas las PDB de una CDB utilizan el mismo punto de conexión y oyente de base de datos.

- Las siguientes operaciones no son compatibles en el nivel de la PDB, pero sí lo son en el nivel de la CDB:
  - Copia de seguridad y recuperación
  - Actualizaciones de la base de datos
  - Acciones de mantenimiento
- Las siguientes características no son compatibles en el nivel de la PDB, pero sí lo son en el nivel de la CDB:
  - Grupos de opciones (las opciones están instaladas en todas las PDB de la instancia de CDB)
  - Grupos de parámetros (todos los parámetros se derivan del grupo de parámetros asociado a la instancia de CDB)
- Estas son algunas de las operaciones en el nivel de PDB compatibles en la arquitectura de CDB en las instalaciones, pero no en una CDB de RDS para Oracle:

  > **Note**
  >
  > Lo que sigue no es una lista completa.

  - PDB de aplicaciones
  - PDB proxy
  - Inicio y detención de una PDB
  - Conexión y desconexión de las PDB

    Para mover datos dentro o fuera de su CDB, debe utilizar las mismas técnicas que para una base de datos que no es CDB. Para obtener más información sobre cómo migrar datos, consulte Importación de datos a Oracle en Amazon RDS.
  - Opciones de configuración en el nivel de las PDB

    La PDB hereda la configuración del grupo de opciones de la CDB. Para obtener más información sobre la configuración de opciones, consulte Grupos de parámetros para Amazon RDS. Para ver las prácticas recomendadas, consulte Trabajo con los grupos de parámetros de base de datos.
  - Configuración de parámetros en una PDB

    La PDB hereda la configuración de parámetros de la CDB. Para obtener más información sobre la configuración, consulte Adición de opciones a instancias de base de datos de Oracle.

- Configuración de distintos oyentes para PDB en la misma CDB
- Características de Oracle Flashback

Configuración de una CDB de RDS para Oracle

Configurar una CDB es similar a configurar una no CDB.

Temas

- Creación de una instancia de CDB de RDS para Oracle
- Conexión a una PDB en la CDB de RDS para Oracle

Creación de una instancia de CDB de RDS para Oracle

En RDS para Oracle, crear una instancia de CDB es casi igual a crear una instancia que no sea de CDB. La diferencia es que debe elegir la arquitectura multitenencia de Oracle al crear la instancia de base de datos, además de elegir una configuración de arquitectura (un inquilino o varios inquilinos). Si crea etiquetas al crear una CDB en la configuración de varios inquilinos, RDS las propaga a la base de datos de inquilinos inicial. Para crear una CDB, utilice la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para crear una instancia de CDB

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la instancia de CDB.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija Create database (Crear base de datos).
5. En Choose a database creation method (Elegir un método de creación de base de datos), elija Standard Create (Creación estándar).
6. En Engine options (Opciones del motor), elija Oracle.
7. En Tipo de administración de base de datos, elija Amazon RDS Custom.
8. En Configuración de la arquitectura, elija Arquitectura multitenencia de Oracle.

9. En Configuración de la arquitectura, lleve a cabo una de las siguientes acciones:

   - Elija Configuración de varios inquilinos y vaya al siguiente paso.
   - Elija Configuración de un solo inquilino y vaya al paso 11.

10. (Configuración de varios inquilinos) En Configuración de la base de datos de inquilinos, haga los siguientes cambios:

    - En Nombre de la base de datos de inquilinos, escriba el nombre de la PDB inicial. El nombre de la PDB debe ser diferente del nombre de la CDB, que por defecto es `RDSCDB`.
    - En Nombre de usuario principal de la base de datos de inquilinos, escriba el nombre del usuario principal de la PDB. No puede usar el nombre de usuario principal de la base de datos de inquilinos para iniciar sesión en la propia CDB.
    - Para Administración de credenciales, elija cualquiera de las siguientes opciones de administración de credenciales:
      - Administrado en AWS Secrets Manager

        La contraseña administrada es para la base de datos de inquilinos inicial y no para la instancia. En Seleccionar la clave de cifrado, elija una clave de KMS que cree Secrets Manager o una clave que haya creado usted.

        > **Note**
        >
        > Recomendamos AWS Secrets Manager como la técnica más segura para administrar las credenciales. Se aplican cargos adicionales. Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.

      - Autoadministrado

        Para especificar una contraseña, desactive la casilla de verificación Generar una contraseña de forma automática si está seleccionada. Ingrese la misma contraseña en Contraseña principal y elija Confirmar contraseña principal.
    - En Conjunto de caracteres de base de datos de inquilinos, seleccione un conjunto de caracteres para la PDB. Puede elegir un conjunto de caracteres de base de datos de inquilinos distinto del de la CDB.

El conjunto de caracteres predeterminado de la PDB es AL32UTF8. Si elige un conjunto de caracteres PDB no predeterminado, es posible que la creación de la CDB sea más lenta.

> **Note**
>
> No puede especificar varias bases de datos de inquilinos en la operación de creación. La CDB tiene una PDB cuando se crea. Puede agregar PDB a una CDB existente en una operación independiente.

11. (Configuración de un solo inquilino) Elija la configuración que desee en función de las opciones que figuran en Configuración de instancias de base de datos:

    - En la sección Settings (Configuración), abra Credential Settings (Configuración de credenciales). A continuación, proceda del modo siguiente:

      i. En Nombre de usuario maestro, introduzca el nombre de un usuario local de su PDB. No puede usar el nombre de usuario maestro para iniciar sesión en la raíz de la CDB.

      ii. Para Administración de credenciales, elija cualquiera de las siguientes opciones de administración de credenciales:

      - Administrado en AWS Secrets Manager

        En Seleccionar la clave de cifrado, elija una clave de KMS que cree Secrets Manager o una clave que haya creado usted.

        > **Note**
        >
        > Recomendamos AWS Secrets Manager como la técnica más segura para administrar las credenciales. Se aplican cargos adicionales. Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.

      - Autoadministrado

        Para especificar una contraseña, desactive la casilla de verificación Generar una contraseña de forma automática si está seleccionada. Ingrese la misma contraseña en Contraseña principal y elija Confirmar contraseña principal.

12. En el resto de secciones, especifique los ajustes de configuración de la instancia de base de datos. Para obtener información acerca de cada configuración, consulte Configuración de instancias de base de datos.
13. Elija Creación de base de datos.

AWS CLI

Para crear una CDB en la configuración multitenencia, use el comando create-db-instance con los siguientes parámetros:

- `--db-instance-identifier`
- `--db-instance-class`
- `--engine { oracle-ee-cdb | oracle-se2-cdb }`
- `--master-username`
- `--master-user-password` o `--manage-master-user-password`
- `--multi-tenant` (para la configuración de un solo inquilino, no especifique `multi-tenant` o especifique `--no-multi-tenant`)
- `--allocated-storage`
- `--backup-retention-period`

Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

En el siguiente ejemplo, se crea una instancia de base de datos de RDS para Oracle denominada *`my-cdb-inst`* en la configuración de varios inquilinos. Si especifica `--no-multi-tenant` o no especifica `--multi-tenant`, la configuración de CDB predeterminada será de un solo inquilino. El motor es `oracle-ee-cdb`: un comando que especifica los fallos de `oracle-ee` y `--multi-tenant` con un error. La base de datos de inquilinos inicial se denomina *`mypdb`*.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --engine oracle-ee-cdb \
    --db-instance-identifier my-cdb-inst \
    --multi-tenant \
```

```
    --db-name mypdb \
    --allocated-storage 250 \
    --db-instance-class db.t3.large \
    --master-username pdb_admin \
    --manage-master-user-password \
    --backup-retention-period 3
```

Para Windows:

```
aws rds create-db-instance ^
    --engine oracle-ee-cdb ^
    --db-instance-identifier my-cdb-inst ^
    --multi-tenant ^
    --db-name mypdb ^
    --allocated-storage 250 ^
    --db-instance-class db.t3.large ^
    --master-username pdb_admin ^
    --manage-master-user-password \ ^
    --backup-retention-period 3
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

El resultado de este comando debería ser similar al siguiente. El nombre de la base de datos, el conjunto de caracteres, el conjunto de caracteres nacional, el usuario principal y el secreto del usuario principal no están incluidos en la salida. Puede ver esta información mediante el comando `describe-tenant-databases` de la CLI.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "my-cdb-inst",
        "DBInstanceClass": "db.t3.large",
        "MultiTenant": true,
        "Engine": "oracle-ee-cdb",
        "DBResourceId": "db-ABCDEFGJIJKLMNOPQRSTUVWXYZ",
        "DBInstanceStatus": "creating",
        "AllocatedStorage": 250,
        "PreferredBackupWindow": "04:59-05:29",
```

```
        "BackupRetentionPeriod": 3,
        "DBSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-0a1bcd2e",
                "Status": "active"
            }
        ],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.oracle-ee-cdb-19",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-1234567a",
            "SubnetGroupStatus": "Complete",
            ...
```

API de RDS

Para crear una instancia de base de datos con la API de Amazon RDS, llame a la operación CreateDBInstance.

Para obtener más información acerca de cada configuración, consulte Configuración de instancias de base de datos.

Conexión a una PDB en la CDB de RDS para Oracle

Puede usar una utilidad como SQL*Plus para conectarse a una PDB. Para descargar Oracle Instant Client, que incluye una versión independiente de SQL*Plus, consulte Oracle Instant Client Downloads.

Para conectarse a SQL*Plus en la PDB, necesitará la siguiente información:

- Nombre de PDB
- Nombre de usuario y contraseña de la base de datos
- Punto de conexión para la instancia de base de datos
- Número de puerto

Para obtener información sobre cómo buscar la información anterior, consulte Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle.

Example Para conectarse a la PDB mediante SQL*Plus

En los siguientes ejemplos, sustituya *master_user_name* por el usuario maestro. Además, sustituya el punto de conexión de su instancia de base de datos y, a continuación, incluya el número de puerto y el SID de Oracle. El valor SID es el nombre de la PDB que ha especificado al crear la instancia de base de datos y no el identificador de la instancia de base de datos.

Para Linux, macOS o Unix:

```
sqlplus 'master_user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=endpoint)
(PORT=port))(CONNECT_DATA=(SID=pdb_name)))'
```

Para Windows:

```
sqlplus master_user_name@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=endpoint)
(PORT=port))(CONNECT_DATA=(SID=pdb_name)))
```

Debería ver un resultado similar a este.

```
SQL*Plus: Release 19.0.0.0.0 Production on Mon Aug 21 09:42:20 2021
```

Tras introducir la contraseña para el usuario, aparece la pregunta de SQL.

```
SQL>
```

> **Note**
>
> La cadena de conexión de formato más corto (Easy connect o EZCONNECT), como `sqlplus username/password@LONGER-THAN-63-CHARS-RDS-ENDPOINT-HERE:1521/database-identifier`, puede encontrar un límite de máximo caracteres y no debería usarse para conexiones.

Copia de seguridad y restauración de una CDB

Puede hacer copias de seguridad y restaurar su CDB usando instantáneas de la base de datos de RDS o Recovery Manager (RMAN).

Copia de seguridad y restauración de una CDB mediante instantáneas de la base de datos

Las instantáneas de la base de datos funcionan de manera similar en las arquitecturas CDB y no CDB. Estas son las diferencias principales:

- Cuando restaura una instantánea de base de datos de una CDB, no puede cambiarle el nombre. La CDB recibe el nombre `RDSCDB` y no se puede cambiar.
- Cuando restaura una instantánea de base de datos de una CDB, no puede cambiarle el nombre a las PDB. Puede modificar el nombre de la PDB mediante el comando modify-tenant-database.
- Para buscar bases de datos de inquilino en una instantánea, utilice el comando describe-db-snapshot-tenant-databases de la CLI.
- No puede interactuar directamente con las bases de datos de inquilino en una instantánea de CDB que utiliza la configuración de arquitectura de varios inquilinos. Si restaura la instantánea de base de datos, restaurará todas las bases de datos de inquilino.
- De forma implícita, RDS para Oracle copia las etiquetas de una base de datos de inquilino en la base de datos de inquilino de una instantánea de base de datos. Al restaurar una base de datos de inquilino, las etiquetas aparecen en la base de datos restaurada.
- Si restaura una instantánea de base de datos y especifica nuevas etiquetas mediante el parámetro `--tags`, las nuevas etiquetas sobrescribirán todas las etiquetas existentes.
- Si toma una instantánea de base de datos de una instancia de CDB que tiene etiquetas y especifica `--copy-tags-to-snapshot`, RDS para Oracle copiará las etiquetas de las bases de datos de inquilino en las bases de datos de inquilino de la instantánea.

Para obtener más información, consulte Consideraciones sobre Oracle Database.

Copia de seguridad y restauración de una CDB mediante el RMAN

Para obtener información sobre las copias de seguridad y la restauración de una base de datos de inquilino individual o CDB mediante el RMAN, consulte Realización de tareas RMAN comunes para instancias de base de datos de Oracle.

Conversión de una base de datos no CDB de RDS para Oracle en una CDB

Puede cambiar la arquitectura de una base de datos Oracle de la arquitectura no CDB a la arquitectura multitenencia de Oracle, también conocida como arquitectura CDB, con el comando

`modify-db-instance`. En la mayoría de los casos, esta técnica es preferible a crear un nuevo CDB e importar datos. La operación de conversión provoca un tiempo de inactividad.

Al actualizar la versión del motor de base de datos, no puede cambiar la arquitectura de la base de datos en la misma operación. Por lo tanto, para actualizar una base de datos de Oracle Database 19c que no sea CDB a una CDB de Oracle Database 21c, primero debe convertir la no CDB a una CDB en un paso; luego, deberá actualizar la CDB de 19c a una CDB de 21c en otro paso distinto.

La operación de conversión de no CDB tiene los siguientes requisitos:

- Debe especificar `oracle-ee-cdb` o `oracle-se2-cdb` para el tipo de motor de base de datos. Estos son los únicos valores compatibles.
- Su motor de base de datos debe utilizar Oracle Database 19c con una actualización de la versión (RU) de abril de 2021 o posterior.

La operación tiene las siguientes limitaciones:

- No se puede convertir de una CDB a una no CDB. Solo se puede convertir de una no CDB a una CDB.
- No se puede hacer la conversión de una base de datos no CDB a una configuración de varios inquilinos en una sola llamada a `modify-db-instance`. Al convertir una base de datos no CDB a una CDB, la CDB estará en la configuración de un solo inquilino. Para convertir la configuración de un solo inquilino en una configuración de varios inquilinos, ejecute `modify-db-instance` de nuevo. Para obtener más información, consulte Convertir la configuración de un solo inquilino a una de varios inquilinos..
- No puede convertir una base de datos principal o de réplica que tenga activado Oracle Data Guard. Para convertir una no CDB con réplicas de lectura, elimine primero todas las réplicas de lectura.
- No puede actualizar la versión del motor de base de datos y convertir una no CDB en una CDB en la misma operación.

Antes de convertir una instancia que no sea CDB, tenga en cuenta lo siguiente:

- Las consideraciones para los grupos de opciones y parámetros son las mismas que para actualizar el motor de base de datos. Para obtener más información, consulte Consideraciones de las actualizaciones de base de datos de Oracle.

- Puede convertir las instancias existentes que no son de CDB y que utilizan contraseñas principales administradas en instancias de un solo inquilino en una sola operación. Las instancias de un solo inquilino heredan las contraseñas administradas.
- Si la instancia de base de datos tiene la opción `OEMAGENT` instalada, se recomienda eliminar esta opción antes de convertir la que no es CDB. Cuando la instancia que no es CDB se haya convertido a una CDB, vuelva a instalar la opción. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.
- Durante el proceso de conversión, RDS restablece el tamaño del registro de recuperación de cambios en línea a los 128 M predeterminados.

Consola

Para convertir una base de datos no CDB en una CDB

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS donde reside su instancia de base de datos.
3. En el panel de navegación, elija Bases de datos y, a continuación, seleccione la instancia no CDB que desee convertir en CDB.
4. Elija Modificar.
5. En Configuración de la arquitectura, elija Arquitectura multitenencia de Oracle. Tras la conversión, la CDB estará en la configuración de un solo inquilino.
6. (Opcional) En Grupo de parámetros de base de datos, elija un nuevo grupo de parámetros para la instancia de CDB. Se aplican las mismas consideraciones de grupo de parámetros al convertir una instancia de base de datos que al actualizar una instancia de base de datos. Para obtener más información, consulte Consideraciones relativas al grupo de parámetros.
7. (Opcional) En Grupo de opciones, elija un nuevo grupo de opciones para la instancia CDB. Se aplican las mismas consideraciones de grupo de parámetros de opciones al convertir una instancia de base de datos que al actualizar una instancia de base de datos. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.
8. (Opcional) Para Administración de credenciales, elija Administradas en AWS Secrets Manager o Autoadministradas. Para obtener más información, consulte Administración de la contraseña de usuario maestro de una instancia de base de datos con Secrets Manager.

9. Cuando haya realizado todos los cambios que desee, elija Continue y compruebe el resumen de las modificaciones.
10. (Opcional) Seleccione Apply immediately (Aplicar inmediatamente) para aplicar los cambios inmediatamente. Si se selecciona esta opción, puede producirse un tiempo de inactividad en algunos casos. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.
11. En la página de confirmación, revise los cambios. Si son correctos, elija Modificar la instancia de base de datos.

    O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para convertir la no CDB de la instancia de base de datos a una CDB en la configuración de un solo inquilino, establezca `--engine` en `oracle-ee-cdb` o `oracle-se2-cdb` en el comando modify-db-instance de la AWS CLI. Para obtener más información, consulte Configuración de instancias de base de datos.

El siguiente ejemplo convierte la instancia de base de datos denominada *my-non-cdb* y especifica un grupo de opciones y un grupo de parámetros personalizados. El comando también habilita la administración de contraseñas con Secrets Manager.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my-non-cdb \
    --engine oracle-ee-cdb \
    --option-group-name custom-option-group \
    --db-parameter-group-name custom-parameter-group \
    --manage-master-user-password
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my-non-cdb ^
    --engine oracle-ee-cdb ^
    --option-group-name custom-option-group ^
```

```
    --db-parameter-group-name custom-parameter-group ^
    --manage-master-user-password
```

API de RDS

Para convertir una no CDB en CDB, especifique `Engine` en la operación de la API de RDS ModifyDBInstance.

Convertir la configuración de un solo inquilino a una de varios inquilinos.

Puede modificar la arquitectura de una CDB de RDS para Oracle (de configuración de un solo inquilino a varios inquilinos). Antes y después de la conversión, la CDB contiene una base de datos de un solo inquilino (PDB). Las etiquetas de la instancia de base de datos se propagan a la base de datos de inquilinos inicial creada durante la conversión.

Antes de comenzar, asegúrese de que la política de IAM tiene permiso para crear una base de datos de inquilinos. Durante la conversión, RDS para Oracle migra los siguientes metadatos a la nueva base de datos de inquilinos:

- El nombre de usuario principal
- La contraseña principal administrada (si CDB de origen se integra con Secrets Manager)
- El nombre de la base de datos de
- El conjunto de caracteres
- El conjunto de caracteres nacional

Antes de la conversión, vea la información anterior mediante el comando `describe-db-instances`. Después de la conversión, puede ver la información mediante el comando `describe-tenant-database`.

La conversión de un solo inquilino a varios inquilinos tiene las siguientes limitaciones:

- No se puede volver a una configuración de un solo inquilino después de haber cambiado a configuración de varios inquilinos. La conversión es irreversible.
- No puede convertir una base de datos principal o de réplica que tenga activado Oracle Data Guard.
- No puede actualizar la versión del motor de base de datos y hacer la conversión a varios inquilinos en la misma operación.

- No puede habilitar ni desactivar las contraseñas de usuario principal durante la conversión.

Consola

Para convertir una CDB de un solo inquilino a una de varios inquilinos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS donde reside su instancia de base de datos.
3. En el panel de navegación, elija Bases de datos y, a continuación, seleccione la instancia no CDB que desee convertir en CDB.
4. Elija Modificar.
5. En Configuración de la arquitectura, elija Arquitectura multitenencia de Oracle.
6. En Configuración de la arquitectura, seleccione Configuración multitenencia.
7. (Opcional) En Grupo de parámetros de base de datos, elija un nuevo grupo de parámetros para la instancia de CDB. Se aplican las mismas consideraciones de grupo de parámetros al convertir una instancia de base de datos que al actualizar una instancia de base de datos.
8. (Opcional) En Grupo de opciones, elija un nuevo grupo de opciones para la instancia CDB. Se aplican las mismas consideraciones de grupo de parámetros de opciones al convertir una instancia de base de datos que al actualizar una instancia de base de datos.
9. Cuando haya realizado todos los cambios que desee, elija Continue y compruebe el resumen de las modificaciones.
10. Seleccione Apply immediately (Aplicar inmediatamente). Esta opción es necesaria cuando se cambia a una configuración de varios inquilinos. Tenga en cuenta que esta opción puede generar tiempo de inactividad en algunos casos.
11. En la página de confirmación, revise los cambios. Si son correctos, elija Modificar la instancia de base de datos.

    O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para convertir una CDB de un solo inquilino a una de varios inquilinos, especifique `--multi-tenant` en el comando modify-db-instance de la AWS CLI.

El siguiente ejemplo convierte la instancia de base de datos denominada `my-st-cdb` de la configuración de un solo inquilino a la de varios inquilinos. La opción `--apply-immediately` es obligatoria.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance --region us-east-1\
    --db-instance-identifier my-st-cdb \
    --multi-tenant \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance --region us-east-1 ^
    --db-instance-identifier my-st-cdb ^
    --multi-tenant ^
    --apply-immediately
```

El resultado es similar al siguiente.

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "my-st-cdb",
        "DBInstanceClass": "db.r5.large",
        "MultiTenant": false,
        "Engine": "oracle-ee-cdb",
        "DBResourceId": "db-AB1CDE2FGHIJK34LMNOPRLXTXU",
        "DBInstanceStatus": "modifying",
        "MasterUsername": "admin",
        "DBName": "ORCL",
        ...
        "EngineVersion": "19.0.0.0.ru-2022-01.rur-2022-01.r1",
        "AutoMinorVersionUpgrade": true,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "bring-your-own-license",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "default:oracle-ee-cdb-19",
                "Status": "in-sync"
            }
        ],
```

```
        ...
        "PendingModifiedValues": {
            "MultiTenant": "true"
        }
    }
}
```

Añadir una base de datos de inquilinos de RDS para Oracle a su instancia de CDB

En la configuración de varios inquilinos de RDS para Oracle, una base de datos de inquilinos es una PDB. Para agregar una base de datos de inquilinos, asegúrese de que cumple los siguientes requisitos previos:

- Su CDB tiene habilitada la configuración de varios inquilinos. Para obtener más información, consulte Configuración de varios inquilinos de la arquitectura CDB.
- Tiene los permisos de IAM necesarios para crear la base de datos de inquilinos.

Puede añadir una base de datos de inquilinos mediante la AWS Management Console, la AWS CLI o la API de RDS. No puede agregar varias bases de datos de inquilinos en una sola operación: debe agregarlas de una en una. Si la CDB tiene habilitada la retención de copias de seguridad, Amazon RDS realiza una copia de seguridad de la instancia de base de datos antes y después de añadir una nueva base de datos de inquilinos.

Consola

Para añadir una base de datos de inquilinos a su instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la base de datos de inquilinos.
3. En el panel de navegación, elija Databases (Bases de datos).
4. Elija la instancia de CDB a la que desea agregar una base de datos de inquilinos. La instancia de base de datos debe usar la configuración de varios inquilinos de la arquitectura CDB.
5. Elija Acciones y, a continuación, Agregar base de datos de inquilinos.
6. En Configuración de la base de datos de inquilinos, haga lo siguiente:

- En Nombre de la base de datos de inquilinos, escriba el nombre de la nueva PDB.
- En Nombre de usuario principal de la base de datos de inquilinos, escriba el nombre del usuario principal de la PDB.
- Elija cualquiera de las siguientes opciones de administración de credenciales:
  - Administrado en AWS Secrets Manager

    En Seleccionar la clave de cifrado, elija una clave de KMS que cree Secrets Manager o una clave que haya creado usted.

    > **Note**
    >
    > Recomendamos AWS Secrets Manager como la técnica más segura para administrar las credenciales. Se aplican cargos adicionales. Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.

  - Autoadministrado

    Para especificar una contraseña, desactive la casilla de verificación Generar una contraseña de forma automática si está seleccionada. Ingrese la misma contraseña en Contraseña principal y elija Confirmar contraseña principal.
  - En Configuración adicional, ingrese el nombre de la PDB para Nombre de base de datos inicial. No puede asignar un nombre a la CDB que tenga el nombre `RDSCDB` predeterminado.
- En Conjunto de caracteres de base de datos de inquilinos, seleccione un conjunto de caracteres para la PDB. El valor predeterminado es AL32UTF8. Puede elegir un conjunto de caracteres de PDB distinto del de la CDB.
- En Conjunto de caracteres nacional de la base de datos de inquilinos, seleccione un conjunto de caracteres para la PDB. El valor predeterminado es AL32UTF8. El conjunto de caracteres nacional especifica la codificación solo para las columnas que utilizan el tipo de datos `NCHAR` (`NCHAR`, `NVARCHAR2` y `NCLOB`), y no afecta a los metadatos de la base de datos.

Para obtener más información sobre estos ajustes, consulte Configuración de instancias de base de datos.

7. Seleccione Agregar inquilino.

AWS CLI

Para añadir una base de datos de inquilinos a su CDB con la AWS CLI, use el comando create-tenant-database con los siguientes parámetros obligatorios:

- `--db-instance-identifier`
- `--tenant-db-name`
- `--master-username`
- `--master-user-password`

En el siguiente ejemplo, se crea una base de datos de inquilinos denominada *mypdb2* en la instancia de CDB de RDS para Oracle denominada *my-cdb-inst*. El conjunto de caracteres de la PDB es `UTF-16`.

Example

Para Linux, macOS o Unix:

```
aws rds create-tenant-database --region us-east-1 \
    --db-instance-identifier my-cdb-inst \
    --tenant-db-name mypdb2 \
    --master-username mypdb2-admin \
    --master-user-password mypdb2-pwd \
    --character-set-name UTF-16
```

Para Windows:

```
aws rds create-tenant-database --region us-east-1 \
    --db-instance-identifier my-cdb-inst ^
    --tenant-db-name mypdb2 ^
    --master-username mypdb2-admin ^
    --master-user-password mypdb2-pwd ^
    --character-set-name UTF-16
```

El resultado tiene un aspecto similar al siguiente.

```
...}
    "TenantDatabase" :
         {
            "DbiResourceId" : "db-abc123",
```

```
            "TenantDatabaseResourceId" : "tdb-bac567",
            "TenantDatabaseArn" : "arn:aws:rds:us-east-1:123456789012:db:my-cdb-
inst:mypdb2",
            "DBInstanceIdentifier" : "my-cdb-inst",
            "TenantDBName" : "mypdb2",
            "Status" : "creating",
            "MasterUsername" : "mypdb2",
            "CharacterSetName" : "UTF-16",
            ...
        }
}...
```

Modificación de una base de datos de inquilinos de RDS para Oracle

Solo puede modificar el nombre de la PDB y la contraseña de usuario principal en una base de datos de inquilinos de su CDB. Tenga en cuenta los siguientes requisitos y limitaciones:

- Para modificar la configuración de una base de datos de inquilinos en su instancia de base de datos, debe haber una base de datos de inquilinos.
- No puede modificar múltiples bases de datos de inquilinos en una sola operación. Solo puede modificar una base de datos de inquilinos a la vez.
- No puede cambiar el nombre de una base de datos de inquilinos a `CDB$ROOT` o `PDB$SEED`.

Puede modificar PDB utilizando la AWS Management Console, la AWS CLI o la API de RDS.

Consola

Para modificar el nombre de la PDB o la contraseña principal de una base de datos de inquilinos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS en la que desea crear la base de datos de inquilinos.
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Elija la base de datos de inquilinos cuyo nombre de base de datos o contraseña de usuario principal desee modificar.
5. Elija Modificar.
6. En Configuración de la base de datos de inquilinos, lleve a cabo una de las siguientes acciones:

- En Nombre de la base de datos de inquilinos, escriba el nuevo nombre de la nueva PDB.
- En Contraseña principal de la base de datos de inquilinos, escriba una nueva contraseña.

7. Elija Modificar inquilino.

AWS CLI

Para modificar una base de datos de inquilinos con la AWS CLI, llame al comando modify-tenant-database con los siguientes parámetros:

- `--db-instance-identifier` *value*
- `--tenant-db-name` *value*
- `[--new-tenant-db-name` *value*`]`
- `[--master-user-password` *value*`]`

En el siguiente ejemplo, se cambia el nombre de la base de datos de inquilinos de `pdb1` a `pdb-hr` en una instancia de base de datos `my-cdb-inst`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-tenant-database --region us-east-1 \
    --db-instance-identifier my-cdb-inst \
    --tenant-db-name pdb1 \
    --new-tenant-db-name pdb-hr
```

En:Windows

```
aws rds modify-tenant-database --region us-east-1 ^
    --db-instance-identifier my-cdb-inst ^
    --tenant-db-name pdb1 ^
    --new-tenant-db-name pdb-hr
```

El resultado de este comando debería ser similar al siguiente.

```
{
    "TenantDatabase" : {
        "DbiResourceId" : "db-abc123",
```

```
        "TenantDatabaseResourceId" : "tdb-bac567",
        "TenantDatabaseArn" : "arn:aws:rds:us-east-1:123456789012:db:my-cdb-inst:pdb1",
        "DBInstanceIdentifier" : "my-cdb-inst",
        "TenantDBName" : "pdb1",
        "Status" : "modifying",
        "MasterUsername" : "tenant-admin-user"
        "Port" : "6555",
        "CharacterSetName" : "UTF-16",
        "MaxAllocatedStorage" : "1000",
        "ParameterGroups": [
            {
                "ParameterGroupName": "pdb1-params",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "pdb1-options",
                "Status": "in-sync"
            }
        ],
        "PendingModifiedValues": {
            "TenantDBName": "pdb-hr"
        }
    }
}
```

Eliminar una base de datos de inquilinos de RDS para Oracle de su CDB

Puede eliminar una base de datos de inquilinos (PDB) mediante la AWS Management Console, la AWS CLI o la API de RDS. Tenga en cuenta los siguientes requisitos previos y limitaciones:

- Debe haber una base de datos de inquilinos y una instancia de base de datos.
- Para que la eliminación ocurra correctamente, debe cumplirse una de las siguientes condiciones:
  - La base de datos de inquilinos y la instancia de base de datos están disponibles.

> **Note**
>
> Puede realizar una instantánea final, pero solo si la base de datos de inquilinos y la instancia de base de datos estaban disponibles antes de ejecutar el comando `delete-tenant-database`.

  - Se está creando la base de datos de inquilinos.
  - La instancia de base de datos está modificando la base de datos de inquilinos.
- No puede eliminar múltiples bases de datos de inquilinos en una sola operación.
- No puede eliminar una base de datos de inquilino si es la única inquilina en la CDB.

Consola

Para eliminar una base de datos de inquilinos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija la base de datos de inquilinos que desea eliminar.
3. En Actions (Acciones), elija Delete (Eliminar).
4. Para crear una instantánea de base de datos final para la instancia de base de datos, elija Create final snapshot? (¿Crear una instantánea final?).
5. Si elige crear una instantánea final, introduzca el nombre de instantánea final.
6. En el cuadro, escriba **`delete me`**.
7. Elija Eliminar (Delete).

AWS CLI

Para eliminar una base de datos de inquilinos con la AWS CLI, llame al comando delete-tenant-database con los siguientes parámetros:

- `--db-instance-identifier` *`value`*
- `--tenant-db-name` *`value`*
- `[--skip-final-snapshot | --no-skip-final-snapshot]`
- `[--final-snapshot-identifier` *`value`*`]`

En el siguiente ejemplo, se elimina la base de datos de inquilinos denominada *`pdb-test`* de la CDB denominada *`my-cdb-inst`*. De forma predeterminada, la operación crea una instantánea final.

Example

Para Linux, macOS o:Unix

```
aws rds delete-tenant-database --region us-east-1 \
    --db-instance-identifier my-cdb-inst \
    --tenant-db-name pdb-test \
    --final-snapshot-identifier final-snap-pdb-test
```

En:Windows

```
aws rds delete-tenant-database --region us-east-1 ^
    --db-instance-identifier my-cdb-inst ^
    --tenant-db-name pdb-test ^
    --final-snapshot-identifier final-snap-pdb-test
```

El resultado de este comando debería ser similar al siguiente.

```
{
    "TenantDatabase" : {
        "DbiResourceId" : "db-abc123",
        "TenantDatabaseResourceId" : "tdb-bac456",
        "TenantDatabaseArn" : "arn:aws:rds:us-east-1:123456789012:db:my-cdb-inst:pdb-
test",
        "DBInstanceIdentifier" : "my-cdb-inst",
        "TenantDBName" : "pdb-test",
        "Status" : "deleting",
        "MasterUsername" : "pdb-test-admin"
        "Port" : "6555",
        "CharacterSetName" : "UTF-16",
        "MaxAllocatedStorage" : "1000",
        "ParameterGroups": [
            {
                "ParameterGroupName": "tenant-1-params",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "tenant-1-options",
                "Status": "in-sync"
            }
```

```
        ]
    }
}
```

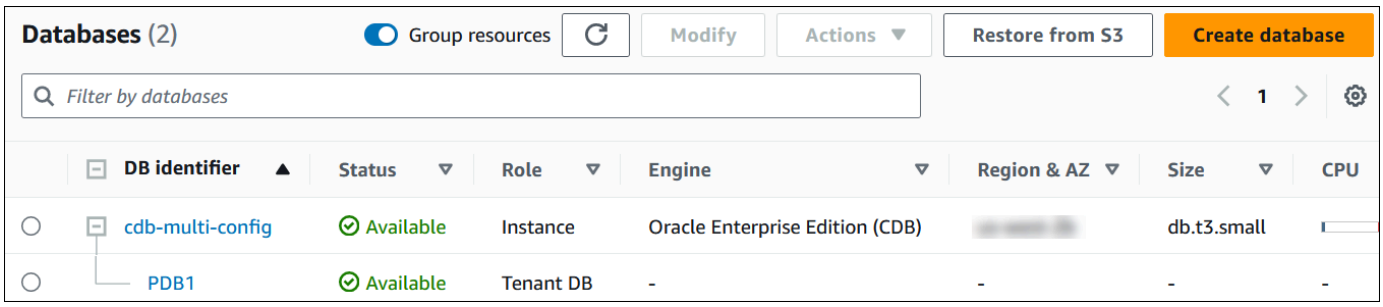
Ver detalles de la base de datos de inquilinos

Puede ver los detalles de una base de datos de inquilinos de la misma manera que puede ver los de una base de datos CDB o no CDB.

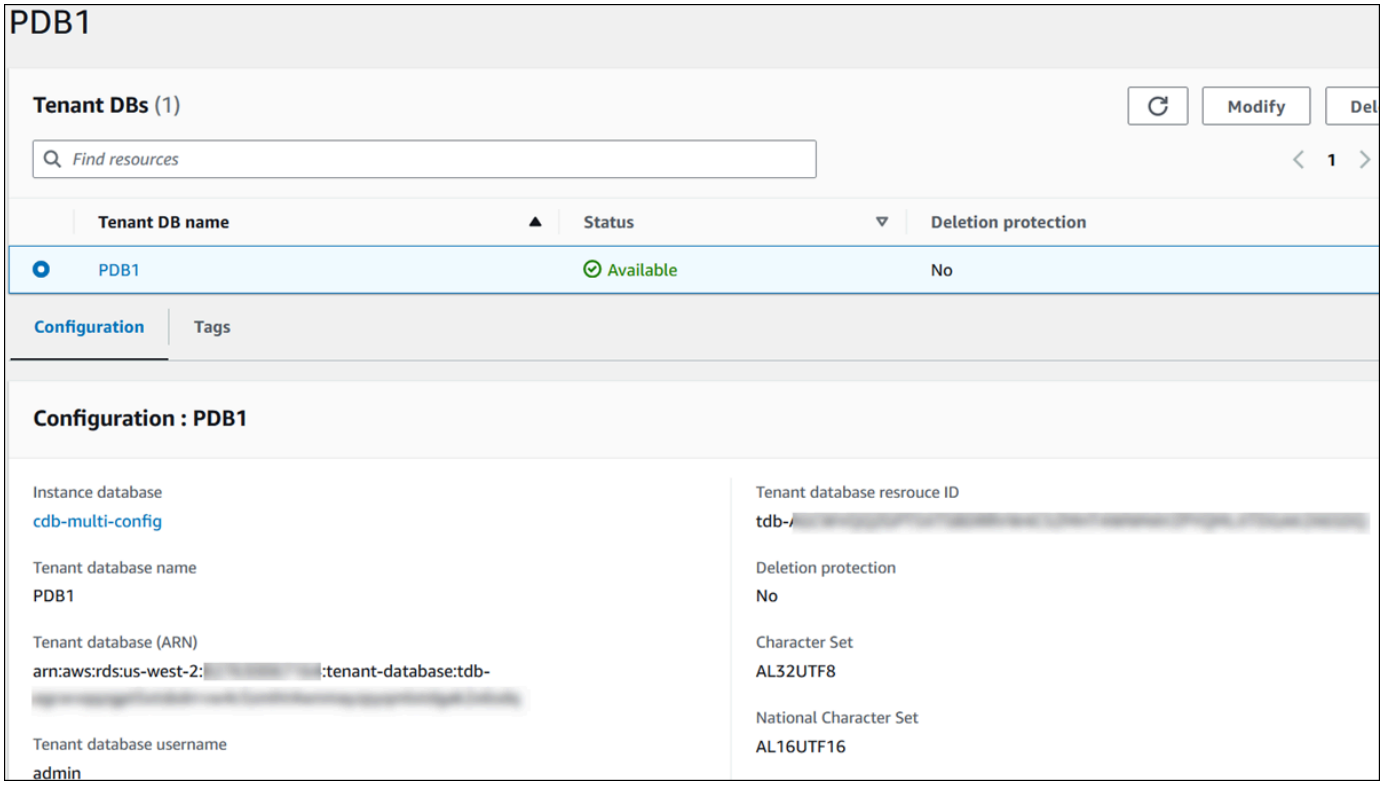
Consola

Para ver los detalles de una base de datos de inquilinos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola de Amazon RDS, elija la Región de AWS donde reside su instancia de base de datos.
3. En el panel de navegación, seleccione Databases (Bases de datos).



   En la imagen anterior, la base de datos de un solo inquilino (PDB) aparece como una base de datos secundaria de la instancia de base de datos.
4. Elija el nombre de una base de datos de inquilinos.



AWS CLI

Para ver los detalles de sus PDB, utilice el comando describe-tenant-databases de la AWS CLI.

En el siguiente ejemplo, se describen todas las bases de datos de inquilinos de la región especificada.

Example

Para Linux, macOS o:Unix

```
aws rds describe-tenant-databases --region us-east-1
```

En:Windows

```
aws rds describe-tenant-databases --region us-east-1
```

El resultado de este comando debería ser similar al siguiente.

```
    "TenantDatabases" : [
```

```
        {
           "DBInstanceIdentifier" : "my-cdb-inst",
           "TenantDBName" : "pdb-test",
           "Status" : "available",
           "MasterUsername" : "pdb-test-admin",
           "DbiResourceId" : "db-abc123",
           "TenantDatabaseResourceId" : "tdb-bac456",
           "TenantDatabaseArn" : "arn:aws:rds:us-east-1:123456789012:db:my-cdb-
inst:pdb-test",
           "CharacterSetName": "AL32UTF8",
           "NcharCharacterSetName": "AL16UTF16",
           "DeletionProtection": false,
           "PendingModifiedValues": {
                "MasterUserPassword": "****"
           },
           "TagList": []
        },
        {

           "DBInstanceIdentifier" : "my-cdb-inst2",
           "TenantDBName" : "pdb-dev",
           "Status" : "modifying",
           "MasterUsername" : "masterrdsuser"
           "DbiResourceId" : "db-xyz789",
           "TenantDatabaseResourceId" : "tdb-ghp890",
           "TenantDatabaseArn" : "arn:aws:rds:us-east-1:123456789012:db:my-cdb-
inst2:pdb-dev",
           "CharacterSetName": "AL32UTF8",
           "NcharCharacterSetName": "AL16UTF16",
           "DeletionProtection": false,
           "PendingModifiedValues": {
                "MasterUserPassword": "****"
           },
           "TagList": []
        },
        ... other truncated data
```

En el siguiente ejemplo, se describen todas las bases de datos de inquilinos en la instancia de base de datos `my-cdb-inst` de la región especificada.

Example

Para Linux, macOS o:Unix

```
aws rds describe-tenant-databases --region us-east-1 \
    --db-instance-identifier my-cdb-inst
```

En:Windows

```
aws rds describe-tenant-databases --region us-east-1 ^
    --db-instance-identifier my-cdb-inst
```

El resultado de este comando debería ser similar al siguiente.

```
{
    "TenantDatabase": {
        "TenantDatabaseCreateTime": "2023-10-19T23:55:30.046Z",
        "DBInstanceIdentifier": "my-cdb-inst",
        "TenantDBName": "pdb-hr",
        "Status": "creating",
        "MasterUsername": "tenant-admin-user",
        "DbiResourceId": "db-abc123",
        "TenantDatabaseResourceId": "tdb-bac567",
        "TenantDatabaseARN": "arn:aws:rds:us-west-2:579508833180:pdb-hr:tdb-
abcdefghi1jklmno2p3qrst4uvw5xy6zabc7defghi8jklmn90op",
        "CharacterSetName": "AL32UTF8",
        "NcharCharacterSetName": "AL16UTF16",
        "DeletionProtection": false,
        "PendingModifiedValues": {
            "MasterUserPassword": "****"
        },
        "TagList": [
            {
                "Key": "TEST",
                "Value": "testValue"
            }
        ]
    }
}
```

En el siguiente ejemplo, se describen las bases de datos de inquilinos `pdb1` en la instancia de base de datos `my-cdb-inst` de la región Este de EE. UU. (Norte de Virginia).

Example

Para Linux, macOS o:Unix

```
aws rds describe-tenant-databases --region us-east-1 \
--db-instance-identifier my-cdb-inst \
--tenant-db-name pdb1
```

En:Windows

```
aws rds describe-tenant-databases --region us-east-1 ^
--db-instance-identifier my-cdb-inst ^
--tenant-db-name pdb1
```

El resultado de este comando debería ser similar al siguiente.

```
{
    "TenantDatabases" : [
        {
            "DbiResourceId" : "db-abc123",
            "TenantDatabaseResourceId" : "tdb-bac567",
            "TenantDatabaseArn" : "arn:aws:rds:us-east-1:123456789012:db:my-cdb-
inst:pdb1"
            "DBInstanceIdentifier" : "my-cdb-inst",
            "TenantDBName" : "pdb1",
            "Status" : "ACTIVE",
            "MasterUsername" : "masterawsuser"
            "Port" : "1234",
            "CharacterSetName": "UTF-8",
            "ParameterGroups": [
                {
                    "ParameterGroupName": "tenant-custom-pg",
                    "ParameterApplyStatus": "in-sync"
                }
            ],
            {
            "OptionGroupMemberships": [
                {
                    "OptionGroupName": "tenant-custom-og",
                    "Status": "in-sync"
                }
            ]
         }
    ]
}
```

Actualización de la CDB

Puede actualizar una instancia CDB a otra versión de Oracle Database. Por ejemplo, puede actualizar una CDB de Oracle Database 19c a una CDB de Oracle Database 21c. No puede cambiar la arquitectura de la base de datos durante una actualización. Por lo tanto, no puede actualizar una no CDB a una CDB ni actualizar una CDB a una no CDB.

El procedimiento para actualizar una CDB a una CDB es el mismo que para actualizar una no CDB a una CDB. Para obtener más información, consulte Actualización del motor de base de datos de RDS para Oracle.

Administración de la instancia de base de datos de RDS para Oracle

A continuación, se presentan las tareas de administración comunes que se llevan a cabo con una instancia de base de datos de RDS para Oracle. Algunas tareas son las mismas para todas las instancias de base de datos de RDS. Otras tareas son específicas de RDS para Oracle.

Las siguientes tareas son comunes para todas las bases de datos de RDS, pero Oracle Database tiene algunos elementos particulares. Por ejemplo, se conecta a una base de datos de Oracle con los clientes de Oracle SQL*Plus y SQL Developer.

Área de la tarea	Documentación relacionada
Clases de instancias, almacenamiento y PIOPS Si está creando una instancia de producción, aprenda cómo funcionan las clases de instancia, los tipos de almacenamiento y las IOPS provisionadas en Amazon RDS.	Clases de instancias de base de datos de RDS para Oracle Tipos de almacenamiento de Amazon RDS
Implementaciones Multi-AZ Una instancia de base de datos de producción debe usar implementaciones Multi-AZ. Las implementaciones Multi-AZ proporcionan unos niveles superiores de disponibilidad, durabilidad de los datos y tolerancia a errores para las instancias de base de datos.	Configuración y administración de una implementación multi-AZ para Amazon RDS
Amazon VPC Si su cuenta de AWS tiene una nube privada virtual (VPC) predeterminada, la instancia de base de datos se creará automáticamente dentro de la VPC predeterminada. Si su cuenta no tiene una VPC predeterminada y desea que la instancia de base de datos esté en una VPC, cree los grupos de VPC y de subredes antes de crear la instancia.	Uso de una instancia de base de datos en una VPC
Grupos de seguridad	Control de acceso con grupos de seguridad

Área de la tarea	Documentación relacionada
De forma predeterminada, las instancias de base de datos utilizan un firewall que impide el acceso. Asegúrese de crear un grupo de seguridad con las direcciones IP y la configuración de red correctas para acceder a la instancia de base de datos.	
Grupos de parámetros Si su instancia de base de datos va a requerir unos parámetros de base de datos concretos, cree un grupo de parámetros antes de crear la instancia de base de datos.	Grupos de parámetros para Amazon RDS
Grupos de opciones Si la instancia de base de datos requiere opciones de base de datos concretas, cree un grupo de opciones antes de crear la instancia de base de datos.	Adición de opciones a instancias de base de datos de Oracle
Conexión a la instancia de base de datos Después de crear un grupo de seguridad y de asociarlo a una instancia de base de datos, puede conectarse a la instancia de base de datos usando cualquier aplicación cliente estándar de SQL, como Oracle SQL Plus.	Conexión a una instancia de base de datos de Oracle
Copia de seguridad y restauración Puede configurar su instancia de base de datos para que realice backups automatizados o tomar snapshots manuales y restaurar después las instancias a partir de los backups o los snapshots.	Copia de seguridad, restauración y exportación de datos
Supervisión Puede monitorizar una base de datos Oracle utilizando las métricas, los eventos y la monitorización avanzada de CloudWatch Amazon RDS.	Consulta de métricas en la consola de Amazon RDS Consulta de eventos de Amazon RDS

Área de la tarea	Documentación relacionada
Archivos de registro Puede obtener acceso a los archivos de log de la instancia de base de datos Oracle.	Supervisión de archivos de registro de Amazon RDS

A continuación, puede encontrar una descripción para implementaciones específicas de Amazon RDS de tareas comunes de DBA para RDS Oracle. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. Además, RDS restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. En muchas de las tareas, ejecute el paquete de `rdsadmin` , que es una herramienta específica de Amazon RDS que permite administrar la base de datos.

A continuación se indican las tareas comunes de DBA para las instancias de bases de datos que ejecutan Oracle:

- Tareas del sistema

Desconexión de una sesión	Método de Amazon RDS: `rdsadmin.rdsadmin_util.disconnect` Método de Oracle: `alter system disconnect session`
Terminación de una sesión	Método de Amazon RDS: `rdsadmin.rdsadmin_util.kill` Método de Oracle: `alter system kill session`
Cancelación de una instrucción SQL en una sesión	Método de Amazon RDS: `rdsadmin.rdsadmin_util.cancel` Método de Oracle: `alter system cancel sql`
Activación y desactivación de sesiones restringidas	Método de Amazon RDS: `rdsadmin.rdsadmin_util.restricted_session` Método de Oracle: `alter system enable restricted session`

Vaciado del grupo compartido	Método de Amazon RDS: `rdsadmin.rdsadmin_util.flush_shared_pool` Método de Oracle: `alter system flush shared_pool`
Vaciado de la caché de búfer	Método de Amazon RDS: `rdsadmin.rdsadmin_util.flush_buffer_cache` Método de Oracle: `alter system flush buffer_cache`
Concesión de privilegios SELECT o EXECUTE para objetos SYS	Método de Amazon RDS: `rdsadmin.rdsadmin_util.grant_sys_object` Método de Oracle: `grant`
Revocación de privilegios SELECT o EXECUTE para objetos SYS	Método de Amazon RDS: `rdsadmin.rdsadmin_util.revoke_sys_object` Método de Oracle: `revoke`
Administración de vistas RDS_X$ para instancias de bases de datos de Oracle	Método de Amazon RDS: `rdsadmin.rdsadmin_util.create_sys_x$_view` Método de Oracle: `CREATE VIEW`
Concesión de privilegios a usuarios no maestros	Método de Amazon RDS: `grant`
Creación de funciones personalizadas para comprobar contraseñas	Método de Amazon RDS: `rdsadmin.rdsadmin_password_verify.create_verify_function` Método de Amazon RDS: `rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn`
Configuración de un servidor DNS personalizado	—

Hacer una lista de los eventos de diagnóstico del sistema permitidos	Método de Amazon RDS: `rdsadmin.rdsadmin_util.list_allowed_system_events` Método de Oracle: —
Establecimiento de eventos de diagnóstico del sistema	Método de Amazon RDS: `rdsadmin.rdsadmin_util.set_allowed_system_events` Método de Oracle: `ALTER SYSTEM SET EVENTS 'set_event_clause'`
Hacer una lista de los eventos de diagnóstico del sistema establecidos	Método de Amazon RDS: `rdsadmin.rdsadmin_util.list_set_system_events` Método de Oracle: `ALTER SESSION SET EVENTS 'IMMEDIATE EVENTDUMP(SYSTEM)'`
Anular eventos de diagnóstico del sistema	Método de Amazon RDS: `rdsadmin.rdsadmin_util.unset_system_event` Método de Oracle: `ALTER SYSTEM SET EVENTS 'unset_event_clause'`

- Tareas de bases de datos

Cambio del nombre global de una base de datos	Método de Amazon RDS: `rdsadmin.rdsadmin_util.rename_global_name` Método de Oracle: `alter database rename`
Creación y especificación del tamaño de los espacios de tablas	Método de Amazon RDS: `create tablespace` Método de Oracle: `alter database`

Configuración del espacio de tabla predeterminado	Método de Amazon RDS: `rdsadmin.rdsadmin_util.alter_default_tablespace` Método de Oracle: `alter database default tablespace`
Configuración del espacio de tabla temporal predeterminado	Método de Amazon RDS: `rdsadmin.rdsadmin_util.alter_default_temp_tablespace` Método de Oracle: `alter database default temporary tablespace`
Creación de un espacio de tablas temporal en el almacén de instancias	Método de Amazon RDS: `rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace` Método de Oracle: `create temporary tablespace`
Creación de un punto de comprobación de una base de datos	Método de Amazon RDS: `rdsadmin.rdsadmin_util.checkpoint` Método de Oracle: `alter system checkpoint`
Configuración de la recuperación distribuida	Método de Amazon RDS: `rdsadmin.rdsadmin_util.enable_distr_recovery` Método de Oracle: `alter system enable distributed recovery`
Configuración de la zona horaria de la base de datos	Método de Amazon RDS: `rdsadmin.rdsadmin_util.alter_db_time_zone` Método de Oracle: `alter database set time_zone`
Uso de tablas externas de Oracle	—
Generación de informes de rendimiento con Automatic Workload Repository (AWR)	Método de Amazon RDS: procedimientos `rdsadmin.rdsadmin_diagnostic_util` Método de Oracle: paquete `dbms_workload_repository`

Ajuste de los enlaces de base de datos para usarlos con las instancias de bases de datos de una VPC	—
Configuración de la edición predeterminada para una instancia de base de datos	Método de Amazon RDS: `rdsadmin.rdsadmin_util.alter_default_edition` Método de Oracle: `alter database default edition`
Activación de la auditoría para la tabla SYS.AUD$	Método de Amazon RDS: `rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table` Método de Oracle: `audit`
Desactivación de la auditoría para la tabla SYS.AUD$	Método de Amazon RDS: `rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table` Método de Oracle: `noaudit`
Limpieza de construcciones interrumpidas de índices en línea	Método de Amazon RDS: `rdsadmin.rdsadmin_dbms_repair.online_index_clean` Método de Oracle: `dbms_repair.online_index_clean`
Omisión de bloques dañados	Método de Amazon RDS: varios procedimientos `rdsadmin.rdsadmin_dbms_repair` Método de Oracle: paquete `dbms_repair`

Redimensionamiento de espacios de tablas, archivos de datos y archivos temporales	Método de Amazon RDS: procedimientos `rdsadmin.rdsadmin_util.resize_temp_tablespace`, `rdsadmin.rdsadmin_util.resize_tempfile` o `rdsadmin.rdsadmin_util.autoextend_tempfile` Procedimiento `rdsadmin.rdsadmin_util.resize_datafile` o `rdsadmin.rdsadmin_util.autoextend_datafile` Método de Oracle: —
Depuración de la Papelera de reciclaje	Método de Amazon RDS: `EXEC rdsadmin.rdsadmin_util.purge_dba_recyclebin` Método de Oracle: `purge dba_recyclebin`
Configuración de los valores mostrados de forma predeterminada para la redacción completa	Método de Amazon RDS: `EXEC rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val` Método de Oracle: `exec dbms_redact.UPDATE_FULL_REDACTION_VALUES`

- Tareas relacionadas con los registros

Activación del modo force logging	Método de Amazon RDS: `rdsadmin.rdsadmin_util.force_logging` Método de Oracle: `alter database force logging`

Activación del modo supplemental logging	Método de Amazon RDS: `rdsadmin.rdsadmin_util.alter_supplemental_logging` Método de Oracle: `alter database add supplemental log`
Cambio de archivos de registro en línea	Método de Amazon RDS: `rdsadmin.rdsadmin_util.switch_logfile` Método de Oracle: `alter system switch logfile`
Adición de registros REDO en línea	Método de Amazon RDS: `rdsadmin.rdsadmin_util.add_logfile`
Eliminación de registros REDO en línea	Método de Amazon RDS: `rdsadmin.rdsadmin_util.drop_logfile`
Cambio de tamaño de los registros REDO en línea	—
Retención de los registros REDO archivados	Método de Amazon RDS: `rdsadmin.rdsadmin_util.set_configuration`

Descargue registros de rehacer archivados de Amazon S3	Método de Amazon RDS: `rdsadmin.rdsadmin_archive_log_download.download_log_with_seqnum` Método de Amazon RDS: `rdsadmin.rdsadmin_archive_log_download.download_logs_in_seqnum_range`
Acceso a los registros de rehacer en línea y archivados	Método de Amazon RDS: `rdsadmin.rdsadmin_master_util.create_archivelog_dir` Método de Amazon RDS: `rdsadmin.rdsadmin_master_util.create_onlinelog_dir`

- Tareas de RMAN

Validación de archivos de base de datos en RDS para Oracle	Método de Amazon RDS: `rdsadmin_rman_util. procedure` Método de Oracle: `RMAN VALIDATE`

Activación y desactivación del seguimiento de cambio de bloques	Método de Amazon RDS: `rdsadmin_rman_util . procedure` Método de Oracle: `ALTER DATABASE`
Comprobación cruzada de los registros REDO archivados	Método de Amazon RDS: `rdsadmin_rman_util .crosscheck_archivelog` Método de Oracle: `RMAN BACKUP`
Copia de seguridad de archivos de registro REDO	Método de Amazon RDS: `rdsadmin_rman_util . procedure` Método de Oracle: `RMAN BACKUP`
Realización de una copia de seguridad completa de una base de datos	Método de Amazon RDS: `rdsadmin_rman_util .backup_database_full` Método de Oracle: `RMAN BACKUP`
Realización de una copia de seguridad incremental de una base de datos	Método de Amazon RDS: `rdsadmin_rman_util .backup_database_incremental` Método de Oracle: `RMAN BACKUP`

Copia de seguridad de un espacio de tablas	Método de Amazon RDS: `rdsadmin_rman_util.backup_database_tablespace` Método de Oracle: `RMAN BACKUP`

- Tareas del programador de Oracle

Modificación de trabajos DBMS_SCHEDULER	Método de Amazon RDS: `dbms_scheduler.set_attribute` Método de Oracle: `dbms_scheduler.set_attribute`
Modificar las ventanas de mantenimiento de AutoTask	Método de Amazon RDS: `dbms_scheduler.set_attribute` Método de Oracle: `dbms_scheduler.set_attribute`
Configuración de zona horaria para trabajos de Oracle Scheduler	Método de Amazon RDS: `dbms_scheduler.set_scheduler_attribute` Método de Oracle: `dbms_scheduler.set_scheduler_attribute`

Desactivación de los trabajos del programador de Oracle propiedad de SYS	Método de Amazon RDS: `rdsadmin.rdsadmin_dbms_scheduler.disable` Método de Oracle: `dbms_scheduler.disable`
Activación de los trabajos del programador de Oracle propiedad de SYS	Método de Amazon RDS: `rdsadmin.rdsadmin_dbms_scheduler.enable` Método de Oracle: `dbms_scheduler.enable`
Modificación del intervalo de repetición del programador de Oracle para los trabajos del tipo CALENDAR	Método de Amazon RDS: `rdsadmin.rdsadmin_dbms_scheduler.set_attribute` Método de Oracle: `dbms_scheduler.set_attribute`
Modificación del intervalo de repetición del programador de Oracle para los trabajos del tipo NAMED	Método de Amazon RDS: `rdsadmin.rdsadmin_dbms_scheduler.set_attribute` Método de Oracle: `dbms_scheduler.set_attribute`

Desactivación de la confirmación automática para la creación de trabajos del programador de Oracle	Método de Amazon RDS: `rdsadmin.rdsadmin_dbms_scheduler.set_no_commit_flag` Método de Oracle: `dbms_isched.set_no_commit_flag`

- Diagnóstico de problemas

Descripción de incidentes	Método de Amazon RDS: `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents` Método Oracle: comando ADRCI `show incident`
Descripción de problemas	Método de Amazon RDS: `rdsadmin.rdsadmin_adrci_util.list_adrci_problem` Método Oracle: comando ADRCI `show problem`
Creación de paquetes de incidentes	Método de Amazon RDS: `rdsadmin.rdsadmin_adrci_util.create_adrci_package` Método Oracle: comando ADRCI `ips create package`

Mostrar archivos de seguimiento	Método de Amazon RDS: `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile` Método Oracle: comando ADRCI `show tracefile`

- Otras tareas

Creación y eliminación de directorios en el espacio de almacenamiento de datos principal	Método de Amazon RDS: `rdsadmin.rdsadmin_util.create_directory` Método de Oracle: `CREATE DIRECTORY` Método de Amazon RDS: `rdsadmin.rdsadmin_util.drop_directory` Método de Oracle: `DROP DIRECTORY`
Descripción de los archivos de un directorio de instancia de base de datos	Método de Amazon RDS: `rdsadmin.rds_file_util.listdir` Método de Oracle: —
Lectura de archivos de un directorio de instancia de base de datos	Método de Amazon RDS: `rdsadmin.rds_file_util.read_text_file` Método de Oracle: —

Acceso a los archivos de Opatch	Método de Amazon RDS: `rdsadmin.rds_file_util.read_text_file` o `rdsadmin.tracefile_listing` Método de Oracle: `opatch`
Configuración de parámetros para tareas del asesor	Método de Amazon RDS: `rdsadmin.rdsadmin_util.advisor_task_set_parameter` Método de Oracle: varios procedimientos de paquetes almacenados
Desactivación de AUTO_STATS_ADVISOR_TASK	Método de Amazon RDS: `rdsadmin.rdsadmin_util.advisor_task_drop` Método de Oracle: —
Volver a habilitar AUTO_STATS_ADVISOR_TASK	Método de Amazon RDS: `rdsadmin.rdsadmin_util.dbms_stats_init` Método de Oracle: —

También puede utilizar procedimientos de Amazon RDS para integración de Amazon S3 con Oracle y para ejecutar tareas de base de datos de OEM Management Agent. Para obtener más información, consulte Integración de Amazon S3 y Realización de tareas de base de datos con Management Agent.

Realización de tareas comunes del sistema para instancias de base de datos de Oracle

A continuación, puede encontrar cómo realizar ciertas tareas comunes de DBA relacionadas con el sistema en las instancias de base de datos de Amazon RDS que ejecutan Oracle. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de bases de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Temas

- Desconexión de una sesión
- Terminación de una sesión
- Cancelación de una instrucción SQL en una sesión
- Activación y desactivación de sesiones restringidas
- Vaciado del grupo compartido
- Concesión de privilegios SELECT o EXECUTE para objetos SYS
- Revocación de privilegios SELECT o EXECUTE para objetos SYS
- Administración de vistas RDS_X$ para instancias de bases de datos de Oracle
- Concesión de privilegios a usuarios no maestros
- Creación de funciones personalizadas para comprobar contraseñas
- Configuración de un servidor DNS personalizado
- Establecer y anular eventos de diagnóstico del sistema

Desconexión de una sesión

Utilice el procedimiento de Amazon RDS para desconectar la sesión actual mediante la finalización del proceso del servidor dedicad `rdsadmin.rdsadmin_util.disconnect`. El procedimiento `disconnect` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`sid`	número	—	Sí	El identificador de sesión.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`serial`	número	—	Sí	El número de serie de la sesión.
`method`	varchar	'IMMEDIATE'	No	Los valores válidos son `'IMMEDIATE'` o `'POST_TRANSACTION'`.

En el siguiente ejemplo se desconecta una sesión.

```
begin
    rdsadmin.rdsadmin_util.disconnect(
        sid    => sid,
        serial => serial_number);
end;
/
```

Para obtener el identificador de la sesión y el número serie de la sesión, consulte la vista `V$SESSION`. En el siguiente ejemplo se obtienen todas las sesiones del usuario `AWSUSER`.

```
SELECT SID, SERIAL#, STATUS FROM V$SESSION WHERE USERNAME = 'AWSUSER';
```

La base de datos debe estar abierta para utilizar este método. Para obtener más información acerca de cómo desconectar una sesión, consulte ALTER SYSTEM en la documentación de Oracle.

Terminación de una sesión

Para terminar una sesión, utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_util.kill`. El procedimiento `kill` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`sid`	número	—	Sí	El identificador de sesión.
`serial`	número	—	Sí	El número de serie de la sesión.
`method`	varchar	null	No	Los valores válidos son `'IMMEDIATE'` o `'PROCESS'` . Si especifica `IMMEDIATE` , tiene el mismo efecto que ejecutar la siguiente instrucción: `ALTER SYSTEM KILL SESSION 'sid,serial#' IMMEDIATE` Si especifica `PROCESS`, termina los procesos asociados a una sesión. Solo debe especificar `PROCESS` si no consigue terminar la sesión mediante el uso de `IMMEDIATE` .

Para obtener el identificador de la sesión y el número serie de la sesión, consulte la vista `V$SESSION`. En el siguiente ejemplo se obtienen todas las sesiones del usuario *`AWSUSER`*..

```
SELECT SID, SERIAL#, STATUS FROM V$SESSION WHERE USERNAME = 'AWSUSER';
```

En el ejemplo siguiente se termina una sesión.

```
BEGIN
    rdsadmin.rdsadmin_util.kill(
        sid    => sid,
        serial => serial_number,
        method => 'IMMEDIATE');
END;
/
```

En el siguiente ejemplo, se terminan los procesos asociados a una sesión.

```
BEGIN
    rdsadmin.rdsadmin_util.kill(
        sid    => sid,
        serial => serial_number,
        method => 'PROCESS');
END;
/
```

Cancelación de una instrucción SQL en una sesión

Utilice el procedimiento de Amazon RDS para cancelar una instrucción SQL en una sesió `rdsadmin.rdsadmin_util.cancel`.

> **Note**
>
> Este procedimiento se admite para Oracle Database 19c (19.0.0) y todas las versiones principales y secundarias posteriores de RDS for Oracle.

El procedimiento `cancel` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`sid`	número	—	Sí	El identificador de sesión.
`serial`	número	—	Sí	El número de serie de la sesión.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
sql_id	varchar2	null	No	El identificador SQL de la instrucción SQL.

En el siguiente ejemplo se cancela una instrucción SQL en una sesión.

```
begin
    rdsadmin.rdsadmin_util.cancel(
        sid    => sid,
        serial => serial_number,
        sql_id => sql_id);
end;
/
```

Para obtener el identificador de la sesión, el número de serie de la sesión y el identificador SQL de una instrucción SQL, consulte la vista V$SESSION. En el siguiente ejemplo se obtienen todas las sesiones e identificadores SQL del usuario AWSUSER.

```
select SID, SERIAL#, SQL_ID, STATUS from V$SESSION where USERNAME = 'AWSUSER';
```

Activación y desactivación de sesiones restringidas

Utilice el procedimiento de Amazon RDS para activar y desactivar las sesiones restringida rdsadmin.rdsadmin_util.restricted_session. El procedimiento restricted_session tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Sí	Descripción
p_enable	booleano	true	No	Establézcalo en true para activar las sesiones restringidas y en false para desactivarlas.

En el siguiente ejemplo se muestra cómo activar y desactivar las sesiones restringidas.

```
/* Verify that the database is currently unrestricted. */

SELECT LOGINS FROM V$INSTANCE;

LOGINS
-------
ALLOWED

/* Enable restricted sessions */

EXEC rdsadmin.rdsadmin_util.restricted_session(p_enable => true);


/* Verify that the database is now restricted. */

SELECT LOGINS FROM V$INSTANCE;

LOGINS
----------
RESTRICTED


/* Disable restricted sessions */

EXEC rdsadmin.rdsadmin_util.restricted_session(p_enable => false);


/* Verify that the database is now unrestricted again. */

SELECT LOGINS FROM V$INSTANCE;

LOGINS
-------
ALLOWED
```

Vaciado del grupo compartido

Utilice el procedimiento de Amazon RDS para vaciar el grupo compartid `rdsadmin.rdsadmin_util.flush_shared_pool`. El procedimiento `flush_shared_pool` no tiene ningún parámetro.

En el siguiente ejemplo se vacía el grupo compartido.

```
EXEC rdsadmin.rdsadmin_util.flush_shared_pool;
```

Vaciado de la caché de búfer

Utilice el procedimiento de Amazon RDS para vaciar la caché del búfe `rdsadmin.rdsadmin_util.flush_buffer_cache`. El procedimiento `flush_buffer_cache` no tiene ningún parámetro.

En el siguiente ejemplo se vacía la caché de búfer.

```
EXEC rdsadmin.rdsadmin_util.flush_buffer_cache;
```

Vaciado de la caché flash inteligente de la base de datos

Para vaciar la caché flash inteligente de la base de datos, utilice el procedimiento `rdsadmin.rdsadmin_util.flush_flash_cache` de Amazon RDS. El procedimiento `flush_flash_cache` no tiene ningún parámetro. En el siguiente ejemplo se vacía la caché flash inteligente de la base de datos.

```
EXEC rdsadmin.rdsadmin_util.flush_flash_cache;
```

Para obtener más información acerca del uso de la caché flash inteligente de la base de datos con RDS para Oracle, consulte Almacenamiento de datos temporales en un almacén de instancias de RDS para Oracle.

Concesión de privilegios SELECT o EXECUTE para objetos SYS

Por lo general, para transferir privilegios se utilizan los roles, que pueden contener muchos objetos. Utilice el procedimiento de Amazon RDS para conceder privilegios a un solo objet `rdsadmin.rdsadmin_util.grant_sys_object`. El procedimiento solo concede los privilegios que ya haya obtenido el usuario maestro mediante un rol o una concesión directa.

El procedimiento `grant_sys_object` tiene los siguientes parámetros.

> **Important**
>
> Para todos los valores de parámetros, utilice mayúsculas a no ser que haya creado el usuario con un identificador que distingue entre mayúsculas y minúsculas. Por ejemplo, si

ejecuta `CREATE USER myuser` o `CREATE USER MYUSER`, el diccionario de datos almacena `MYUSER`. Sin embargo, si utiliza comillas dobles en `CREATE USER "MyUser"`, el diccionario de datos almacena `MyUser`.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_obj_name`	varchar2	—	Sí	El nombre del objeto para el que se van a conceder privilegios. El objeto puede ser un directorio, una función, un paquete, un procedimiento, una secuencia, una tabla o una vista. Los nombres de los objetos deben escribirse exactamente como aparecen en `DBA_OBJECTS`. La mayoría de los objetos del sistema están definidos en mayúsculas, por lo que recomendamos que lo intente como primera opción.
`p_grantee`	varchar2	—	Sí	El nombre del objeto al que se van a conceder privilegios. El objeto puede ser un esquema o un rol.
`p_privilege`	varchar2	null	Sí	—

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_grant_option	booleano	false	No	Establézcalo en true para usar la opción de concesión (WITH GRANT OPTION).

En el siguiente ejemplo se le concede el privilegio SELECT sobre el objeto V_$SESSION al usuario USER1.

```
begin
    rdsadmin.rdsadmin_util.grant_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_grantee   => 'USER1',
        p_privilege => 'SELECT');
end;
/
```

En el siguiente ejemplo se le concede el privilegio SELECT sobre el objeto V_$SESSION al usuario USER1 con la opción de concesión.

```
begin
    rdsadmin.rdsadmin_util.grant_sys_object(
        p_obj_name     => 'V_$SESSION',
        p_grantee      => 'USER1',
        p_privilege    => 'SELECT',
        p_grant_option => true);
end;
/
```

Para poder conceder privilegios sobre un objeto, una cuenta debe haber obtenido los privilegios directamente con la opción de concesión o a través de un rol concedido utilizando `with admin option`. En el caso más común, es posible que desee conceder SELECT para una vista de administración de bases de datos que se haya concedido al rol SELECT_CATALOG_ROLE. Si a su usuario no se le ha concedido ese rol directamente utilizando `with admin option`, no podrá transferir el privilegio. Si tiene el privilegio de DBA, puede conceder el rol directamente a otro usuario.

En el siguiente ejemplo se conceden SELECT_CATALOG_ROLE y EXECUTE_CATALOG_ROLE a USER1. Dado que se utiliza with admin option, USER1 ahora puede conceder acceso a los objetos SYS que se hayan concedido a SELECT_CATALOG_ROLE.

```
GRANT SELECT_CATALOG_ROLE TO USER1 WITH ADMIN OPTION;
GRANT EXECUTE_CATALOG_ROLE to USER1 WITH ADMIN OPTION;
```

No es necesario volver a conceder los objetos que ya se han concedido a PUBLIC. Si utiliza el procedimiento grant_sys_object para volver a conceder acceso, la llamada al procedimiento se realiza correctamente.

Revocación de privilegios SELECT o EXECUTE para objetos SYS

Utilice el procedimiento de Amazon RDS para revocar privilegios a un solo objet rdsadmin.rdsadmin_util.revoke_sys_object. El procedimiento solo revoca los privilegios que ya haya obtenido la cuenta maestra mediante un rol o una concesión directa.

El procedimiento revoke_sys_object tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_obj_name	varchar2	—	Sí	El nombre del objeto para el que se van a revocar privilegios. El objeto puede ser un directorio, una función, un paquete, un procedimiento, una secuencia, una tabla o una vista. Los nombres de los objetos deben escribirse exactamente como aparecen en DBA_OBJECTS . La mayoría de los objetos del sistema están definidos en mayúscula

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				s, por lo que recomendamos que pruebe así primero.
p_revokee	varchar2	—	Sí	El nombre del objeto para el que se van a revocar privilegios. El objeto puede ser un esquema o un rol.
p_privilege	varchar2	null	Sí	—

En el siguiente ejemplo se le revoca el privilegio SELECT sobre el objeto V_$SESSION desde un usuario USER1.

```
begin
    rdsadmin.rdsadmin_util.revoke_sys_object(
        p_obj_name  => 'V_$SESSION',
        p_revokee   => 'USER1',
        p_privilege => 'SELECT');
end;
/
```

Administración de vistas RDS_X$ para instancias de bases de datos de Oracle

Puede que necesite acceder a las tablas fijas SYS.X$, a las que solo se puede acceder mediante SYS. Para crear vistas SYS.RDS_X$ en las tablas X$ aptas, utilice los procedimientos del paquete rdsadmin.rdsadmin_util. A su usuario maestro se le concede automáticamente el privilegio SELECT … WITH GRANT OPTION sobre las vistas RDS_X$.

Los procedimientos rdsadmin.rdsadmin_util están disponibles en las siguientes versiones del motor de base de datos:

- 21.0.0.0.ru-2023-10.rur-2023-10.r1 y versiones de Oracle Database 21c posteriores
- 19.0.0.0.ru-2023-10.rur-2023-10.r1 y versiones de Oracle Database 19c posteriores

> **Important**
>
> Internamente, el paquete `rdsadmin.rdsadmin_util` crea vistas en las tablas X$. Las tablas X$ son objetos internos del sistema que no se describen en la documentación de Oracle Database. Se recomienda probar vistas específicas en la base de datos que utilice fuera de producción y que solo cree vistas en la base de datos de producción sirviéndose de la orientación de Oracle Support.

Enumeración de tablas fijas X$ aptas para su uso en las vistas RDS_X$

Para enumerar tablas X$ aptas para su uso en vistas RDS_X$, utilice el procedimiento de RDS `rdsadmin.rdsadmin_util.list_allowed_sys_x$_views`. Este procedimiento no acepta parámetros. En las siguientes instrucciones se enumeran todas las tablas X$ aptas (se incluye un ejemplo de resultados).

```
SQL> SET SERVEROUTPUT ON
SQL> SELECT * FROM TABLE(rdsadmin.rdsadmin_util.list_allowed_sys_x$_views);

'X$BH'
'X$K2GTE'
'X$KCBWBPD'
'X$KCBWDS'
'X$KGLLK'
'X$KGLOB'
'X$KGLPN'
'X$KSLHOT'
'X$KSMSP'
'X$KSPPCV'
'X$KSPPI'
'X$KSPPSV'
'X$KSQEQ'
'X$KSQRS'
'X$KTUXE'
'X$KQRFP'
```

La lista de tablas X$ aptas puede cambiar con el tiempo. Para asegurarse de que su lista de tablas fijas X$ aptas esté actualizada, vuelva a ejecutar `list_allowed_sys_x$_views` periódicamente.

Creación de vistas SYS.RDS_X$

Para crear una vista RDS_X$ en una tabla X$ apta, utilice el procedimiento de RDS `rdsadmin.rdsadmin_util.create_sys_x$_view`. Solo puede crear vistas para las tablas que figuren en la salida de `rdsadmin.rdsadmin_util.list_allowed_sys_x$_views`. El procedimiento `create_sys_x$_view` acepta los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_x$_tbl`	varchar2	Nulo	Sí	Un nombre de tabla X$ válido. El valor debe ser una de las tablas X$ notificadas por `list_allowed_sys_x$_views` .
`p_force_creation`	Booleano	`FALSE`	No	Un valor que indica si se debe forzar la creación de una vista RDS_X$ que ya exista para una tabla X$. De forma predeterminada, RDS no creará una vista si ya existe. Para forzar la creación, defina este parámetro como `TRUE`.

En el siguiente ejemplo se crea una vista `SYS.RDS_X$KGLOB` de la tabla `X$KGLOB`. El formato del nombre de la vista es RDS_*X$tablename*.

```
SQL> SET SERVEROUTPUT ON
SQL> EXEC rdsadmin.rdsadmin_util.create_sys_x$_view('X$KGLOB');

PL/SQL procedure successfully completed.
```

La siguiente consulta del diccionario de datos muestra la vista SYS.RDS_X$KGLOB y su estado. A su usuario maestro se le concede automáticamente el privilegio SELECT ... WITH GRANT OPTION sobre esta vista.

```
SQL> SET SERVEROUTPUT ON
SQL> COL OWNER FORMAT A30
SQL> COL OBJECT_NAME FORMAT A30
SQL> COL STATUS FORMAT A30
SQL> SET LINESIZE 200
SQL> SELECT OWNER, OBJECT_NAME, STATUS
FROM DBA_OBJECTS
WHERE OWNER = 'SYS' AND OBJECT_NAME = 'RDS_X$KGLOB';

OWNER                          OBJECT_NAME                    STATUS
------------------------------ ------------------------------
 -------------------------------
SYS                            RDS_X$KGLOB                    VALID
```

Important

No se garantiza que las tablas X$ permanezcan iguales antes y después de una actualización. RDS para Oracle elimina y vuelve a crear las vistas RDS_X$ de las tablas X$ durante una actualización del motor. A continuación, concede el privilegio SELECT ... WITH GRANT OPTION al usuario maestro. Tras una actualización, conceda los privilegios necesarios a los usuarios de la base de datos en las vistas RDS_X$ correspondientes.

Enumeración de vistas SYS.RDS_X$

Para enumerar las vistas RDS_X$ existentes, utilice el procedimiento de RDS rdsadmin.rdsadmin_util.list_created_sys_x$_views. El procedimiento muestra solo las vistas que se crearon mediante el procedimiento create_sys_x$_view. En el siguiente ejemplo, se enumeran las tablas X$ que tienen las vistas RDS_X$ correspondientes (se incluye un ejemplo de salida).

```
SQL> SET SERVEROUTPUT ON
SQL> COL XD_TBL_NAME FORMAT A30
SQL> COL STATUS FORMAT A30
SQL> SET LINESIZE 200
SQL> SELECT * FROM TABLE(rdsadmin.rdsadmin_util.list_created_sys_x$_views);
```

```
XD_TBL_NAME                    STATUS
------------------------------ ------------------------------
X$BH                           VALID
X$K2GTE                        VALID
X$KCBWBPD                      VALID

3 rows selected.
```

Eliminación de vistas RDS_X$

Para eliminar una vista SYS.RDS_X$, utilice el procedimiento de RDS `rdsadmin.rdsadmin_util.drop_sys_x$_view`. Solo puede eliminar vistas que figuren en la salida de `rdsadmin.rdsadmin_util.list_allowed_sys_x$_views`. El procedimiento `drop_sys_x$_view` acepta el siguiente parámetro.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_x$_tbl	varchar2	Nulo	Sí	Un nombre de tabla fija X$ válido. El valor debe ser una de las tablas fijas X$ notificadas por `list_created_sys_x$_views` .

En el siguiente ejemplo se elimina una vista RDS_X$KGLOB, que se creó en la tabla X$KGLOB.

```
SQL> SET SERVEROUTPUT ON
SQL> EXEC rdsadmin.rdsadmin_util.drop_sys_x$_view('X$KGLOB');

PL/SQL procedure successfully completed.
```

El siguiente ejemplo muestra que la vista SYS.RDS_X$KGLOB se ha eliminado (se incluye un ejemplo de salida).

```
SQL> SET SERVEROUTPUT ON
SQL> COL OWNER FORMAT A30
```

```
SQL> COL OBJECT_NAME FORMAT A30
SQL> COL STATUS FORMAT A30
SQL> SET LINESIZE 200
SQL> SELECT OWNER, OBJECT_NAME, STATUS
FROM DBA_OBJECTS
WHERE OWNER = 'SYS' AND OBJECT_NAME = 'RDS_X$KGLOB';

no rows selected
```

Concesión de privilegios a usuarios no maestros

Puede conceder privilegios SELECT para muchos objetos del esquema SYS utilizando el rol SELECT_CATALOG_ROLE. El rol SELECT_CATALOG_ROLE concede a los usuarios privilegios SELECT para las vistas del diccionario de datos. En el siguiente ejemplo se concede el rol SELECT_CATALOG_ROLE a un usuario denominado user1.

```
GRANT SELECT_CATALOG_ROLE TO user1;
```

Puede conceder privilegios EXECUTE para muchos objetos del esquema SYS utilizando el rol EXECUTE_CATALOG_ROLE. El rol EXECUTE_CATALOG_ROLE concede a los usuarios privilegios EXECUTE para los paquetes y los procedimientos del diccionario de datos. En el siguiente ejemplo se concede el rol EXECUTE_CATALOG_ROLE a un usuario denominado user1.

```
GRANT EXECUTE_CATALOG_ROLE TO user1;
```

En el siguiente ejemplo se obtienen los permisos que conceden los roles SELECT_CATALOG_ROLE y EXECUTE_CATALOG_ROLE.

```
  SELECT *
    FROM ROLE_TAB_PRIVS
   WHERE ROLE IN ('SELECT_CATALOG_ROLE','EXECUTE_CATALOG_ROLE')
ORDER BY ROLE, TABLE_NAME ASC;
```

En el siguiente ejemplo se crea un usuario no maestro denominado user1, se le concede el privilegio CREATE SESSION y el privilegio SELECT para una base de datos denominada sh.sales.

```
CREATE USER user1 IDENTIFIED BY PASSWORD;
GRANT CREATE SESSION TO user1;
GRANT SELECT ON sh.sales TO user1;
```

Creación de funciones personalizadas para comprobar contraseñas

Puede crear una función personalizada de verificación de contraseñas de las siguientes maneras.

- Para usar la lógica de verificación estándar y guardar la función en el esquema SYS, utilice el procedimiento `create_verify_function`.
- Para usar la lógica de verificación personalizada y evitar guardar la función en el esquema SYS, utilice el procedimiento `create_passthrough_verify_fcn`.

El procedimiento create_verify_function

Puede crear una función personalizada para comprobar las contraseñas mediante el procedimiento de Amazon RDS `rdsadmin.rdsadmin_password_verify.create_verify_function`. El procedimiento `create_verify_function` admite todas las versiones de RDS para Oracle.

El procedimiento `create_verify_function` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_verify_function_name`	varchar2	—	Sí	El nombre de la función personalizada. Esta función se crea automáticamente en el esquema SYS. Esta función se asigna a los perfiles de usuario.
`p_min_length`	número	8	No	El número mínimo necesario de caracteres.
`p_max_length`	número	256	No	El número máximo de caracteres permitido.
`p_min_letters`	número	1	No	El número mínimo necesario de letras.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_min_uppercase	número	0	No	El número mínimo necesario de letras mayúsculas.
p_min_lowercase	número	0	No	El número mínimo necesario de letras minúsculas.
p_min_digits	número	1	No	El número mínimo necesario de dígitos.
p_min_special	número	0	No	El número mínimo necesario de caracteres especiales.
p_min_different_chars	número	3	No	El número mínimo de caracteres diferentes necesarios entre la contraseña antigua y la nueva.
p_disallow_username	booleano	true	No	Establezca esta opción en true para no permitir el nombre de usuario en la contraseña.
p_disallow_reverse	booleano	true	No	Establézcalo en true para impedir que se use el nombre de usuario a la inversa en la contraseña.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_disallow_db_name	booleano	true	No	Establézcalo en true para impedir que se use el nombre de la base de datos o del servidor en la contraseña.
p_disallow_simple_strings	booleano	true	No	Establézcalo en true para impedir que se usen cadenas sencillas en la contraseña.
p_disallow_whitespace	booleano	false	No	Establézcalo en true para impedir que se usen caracteres de espacio en blanco en la contraseña.
p_disallow_at_sign	booleano	false	No	Establézcalo en true para impedir que se use el carácter @ en la contraseña.

Puede crear distintas funciones de verificación de contraseñas.

El nombre de la función personalizada está sujeto a ciertas restricciones. Su función personalizada no puede tener el mismo nombre que un objeto de sistema existente. El nombre no puede tener más de 30 caracteres de longitud. Asimismo, el nombre debe incluir una de las siguientes cadenas: PASSWORD, VERIFY, COMPLEXITY, ENFORCE o STRENGTH.

El siguiente ejemplo crea una función con el nombre CUSTOM_PASSWORD_FUNCTION. La función requiere que una contraseña tenga al menos 12 caracteres, 2 caracteres en mayúsculas, 1 dígito y 1 carácter especial, y que la contraseña no incluya el carácter @.

```
begin
    rdsadmin.rdsadmin_password_verify.create_verify_function(
```

```
        p_verify_function_name => 'CUSTOM_PASSWORD_FUNCTION',
        p_min_length           => 12,
        p_min_uppercase        => 2,
        p_min_digits           => 1,
        p_min_special          => 1,
        p_disallow_at_sign     => true);
end;
/
```

Para ver el texto de la función de verificación, realice una consulta de DBA_SOURCE. En el siguiente ejemplo se obtiene el texto de una función de contraseña personalizada llamada CUSTOM_PASSWORD_FUNCTION.

```
COL TEXT FORMAT a150

  SELECT TEXT
    FROM DBA_SOURCE
   WHERE OWNER = 'SYS'
     AND NAME = 'CUSTOM_PASSWORD_FUNCTION'
ORDER BY LINE;
```

Para asociar la función de verificación a un perfil de usuario, utilice `alter profile`. En el siguiente ejemplo se asocia una función de verificación al perfil de usuario DEFAULT.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION CUSTOM_PASSWORD_FUNCTION;
```

Para ver qué perfiles de usuario están asociados a cada función de verificación, consulte DBA_PROFILES. En el siguiente ejemplo se obtienen los perfiles asociados a la función de verificación personalizada llamada CUSTOM_PASSWORD_FUNCTION.

```
SELECT * FROM DBA_PROFILES WHERE RESOURCE_NAME = 'PASSWORD' AND LIMIT =
 'CUSTOM_PASSWORD_FUNCTION';


PROFILE                    RESOURCE_NAME                    RESOURCE  LIMIT
-------------------------  -------------------------------  --------
 ------------------------
DEFAULT                    PASSWORD_VERIFY_FUNCTION         PASSWORD
 CUSTOM_PASSWORD_FUNCTION
```

En el siguiente ejemplo se obtienen todos los perfiles y las funciones de verificación de contraseñas a las que están asociados.

```
SELECT * FROM DBA_PROFILES WHERE RESOURCE_NAME = 'PASSWORD_VERIFY_FUNCTION';

PROFILE                    RESOURCE_NAME                    RESOURCE  LIMIT
------------------------  --------------------------------  --------
 ------------------------
DEFAULT                    PASSWORD_VERIFY_FUNCTION         PASSWORD
 CUSTOM_PASSWORD_FUNCTION
RDSADMIN                   PASSWORD_VERIFY_FUNCTION         PASSWORD  NULL
```

El procedimiento create_passthrough_verify_fcn

El procedimiento `create_passthrough_verify_fcn` admite todas las versiones de RDS para Oracle.

Puede crear una función personalizada para comprobar las contraseñas mediante el procedimiento de Amazon RDS `rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn`. El procedimiento `create_passthrough_verify_fcn` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_verify_function_name`	varchar2	—	Sí	El nombre de la función de verificación personalizada. Es una función contenedora que se crea automáticamente en el esquema SYS y no contiene ninguna lógica de verificación. Esta función se asigna a los perfiles de usuario.
`p_target_owner`	varchar2	—	Sí	El propietario del esquema de la función

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				de verificación personalizada.
`p_target_function_name`	varchar2	—	Sí	El nombre de la función personalizada existente que contiene la lógica de verificación. La función personalizada debe devolver un valor booleano. La función debe devolver `true` si la contraseña es válida y `false` si la contraseña no es válida.

En el siguiente ejemplo se crea una función de verificación de contraseñas que utiliza la lógica de la función `PASSWORD_LOGIC_EXTRA_STRONG`.

```
begin
    rdsadmin.rdsadmin_password_verify.create_passthrough_verify_fcn(
        p_verify_function_name => 'CUSTOM_PASSWORD_FUNCTION',
        p_target_owner         => 'TEST_USER',
        p_target_function_name => 'PASSWORD_LOGIC_EXTRA_STRONG');
end;
/
```

Para asociar la función de verificación a un perfil de usuario, utilice `alter profile`. En el siguiente ejemplo se asocia la función de verificación al perfil de usuario `DEFAULT`.

```
ALTER PROFILE DEFAULT LIMIT PASSWORD_VERIFY_FUNCTION CUSTOM_PASSWORD_FUNCTION;
```

Configuración de un servidor DNS personalizado

Amazon RDS admite el acceso de red saliente en las instancias de bases de datos que ejecutan Oracle. Para obtener más información acerca del acceso de red saliente, incluidos los requisitos previos, consulte Configuración del acceso UTL_HTTP mediante certificados y un wallet de Oracle..

Amazon RDS Oracle permite realizar la resolución del servicio de nombres de dominio (DNS) desde un servidor DNS personalizado propiedad del cliente. Solo es posible resolver nombres de dominio completos desde una instancia de base de datos de Amazon RDS a través de un servidor DNS personalizado.

Después de configurar un servidor de nombres DNS personalizado, se tardan hasta 30 minutos en propagar los cambios a la instancia de base de datos. Una vez que se propaguen los cambios a la instancia de base de datos, todo el tráfico de red saliente que requiera una búsqueda de DNS consultará el servidor DNS personalizado a través del puerto 53.

Para configurar un servidor DNS personalizado para su instancia de base de datos de Amazon RDS for Oracle, haga lo siguiente:

- Desde el conjunto de opciones de DHCP asociado a la nube virtual privada (VPC), establezca la opción `domain-name-servers` en la dirección IP del servidor de nombres DNS. Para obtener más información, consulte Conjuntos de opciones de DHCP.

  > **Note**
  >
  > La opción `domain-name-servers` acepta hasta cuatro valores, pero la instancia de base de datos de Amazon RDS solo utiliza el primer valor.

- Asegúrese de que el servidor DNS puede resolver todas las consultas de búsqueda, incluidos los nombres de DNS públicos, los nombres de DNS privados de Amazon EC2 y los nombres de DNS específicos del cliente. Si el tráfico de red saliente contiene búsquedas de DNS que el servidor DNS no puede resolver, este debe tener configurados los proveedores de DNS correspondientes.
- Configure el servidor DNS para que genere respuestas de protocolo de datagramas de usuario (UDP) de 512 bytes como máximo.
- Configure el servidor DNS para que genere respuestas de protocolo de control de transmisión (TCP) de 1024 bytes como máximo.
- Configure el servidor DNS para que permita el tráfico entrante desde las instancias de bases de datos de Amazon RDS a través del puerto 53. Si el servidor DNS está en una Amazon VPC, la

VPC debe tener un grupo de seguridad que contenga reglas entrantes que permitan el tráfico UDP y TCP en el puerto 53. Si el servidor DNS no está en una Amazon VPC, debe tener lista de permitidos de firewall apropiada para permitir el tráfico entrante UDP y TCP en el puerto 53.

Para obtener más información, consulte Grupos de seguridad de su VPC y Adición, eliminación y actualización de reglas.

- Configure la VPC de la instancia de base de datos de Amazon RDS para que permita el tráfico saliente a través del puerto 53. La VPC debe tener un grupo de seguridad que contenga reglas salientes que permitan el tráfico UDP y TCP en el puerto 53.

  Para obtener más información, consulte Grupos de seguridad de su VPC y Adición, eliminación y actualización de reglas.
- La ruta de direccionamiento entre la instancia de base de datos de Amazon RDS y el servidor DNS debe configurarse correctamente para permitir el tráfico de DNS.
  - Si la instancia de base de datos de Amazon RDS y el servidor DNS no están en la misma VPC, debe establecerse una interconexión entre ellos. Para obtener más información, consulte ¿Qué es un emparejamiento de VPC?

Establecer y anular eventos de diagnóstico del sistema

Para establecer y anular eventos de diagnóstico a nivel de sesión, puede utilizar la instrucción de Oracle SQL `ALTER SESSION SET EVENTS`. Sin embargo, para establecer eventos a nivel del sistema no puede utilizar Oracle SQL. En vez de eso, utilice los procedimientos de evento de sistema que hay en el paquete `rdsadmin.rdsadmin_util`. Los procedimientos de evento de sistema están disponibles en las siguientes versiones del motor:

- Todas las versiones de Oracle Database 21c
- 19.0.0.0.ru-2020-10.rur-2020-10.r1 Oracle Database 19c y versiones posteriores

Para obtener más información, consulte la sección sobre la versión 19.0.0.0.ru-2020-10.rur-2020-10.r1 en las notas de la versión de Amazon RDS para Oracle.

> **Important**
>
> Internamente, con el paquete `rdsadmin.rdsadmin_util` se establecen eventos mediante el uso de la instrucción `ALTER SYSTEM SET EVENTS`. Esta instrucción `ALTER SYSTEM` no

figura en la Documentación de la base de datos de Oracle. Algunos eventos de diagnóstico del sistema pueden generar grandes cantidades de información de seguimiento, provocar contención o afectar la disponibilidad de la base de datos. Se recomienda probar eventos de diagnóstico concretos en la base de datos que no utilice para producir y que solo establezca eventos en la base de datos de producción sirviéndose de la orientación de Oracle Support.

Hacer una lista de los eventos de diagnóstico del sistema permitidos

Para hacer una lista de los eventos de sistema que puede establecer, utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_util.list_allowed_system_events`. Este procedimiento no acepta parámetros.

En el ejemplo siguiente se hace una lista de todos los eventos de sistema que puede establecer.

```
SET SERVEROUTPUT ON
EXEC rdsadmin.rdsadmin_util.list_allowed_system_events;
```

En la siguiente salida de ejemplo se muestran los números de eventos y sus descripciones. Utilice el procedimiento `set_system_event` de Amazon RDS para establecer estos eventos y el procedimiento `unset_system_event` de Amazon RDS para anularlos.

```
604   - error occurred at recursive SQL level
942   - table or view does not exist
1401  - inserted value too large for column
1403  - no data found
1410  - invalid ROWID
1422  - exact fetch returns more than requested number of rows
1426  - numeric overflow
1427  - single-row subquery returns more than one row
1476  - divisor is equal to zero
1483  - invalid length for DATE or NUMBER bind variable
1489  - result of string concatenation is too long
1652  - unable to extend temp segment by  in tablespace
1858  - a non-numeric character was found where a numeric was expected
4031  - unable to allocate  bytes of shared memory ("","","","")
6502  - PL/SQL: numeric or value error
10027 - Specify Deadlock Trace Information to be Dumped
10046 - enable SQL statement timing
10053 - CBO Enable optimizer trace
```

```
10173 - Dynamic Sampling time-out error
10442 - enable trace of kst for ORA-01555 diagnostics
12008 - error in materialized view refresh path
12012 - error on auto execute of job
12504 - TNS:listener was not given the SERVICE_NAME in CONNECT_DATA
14400 - inserted partition key does not map to any partition
31693 - Table data object  failed to load/unload and is being skipped due to error:
```

> **Note**
>
> La lista de eventos de sistema permitidos puede cambiar con el tiempo. Para confirmar que tiene la lista más reciente de eventos aptos, use `rdsadmin.rdsadmin_util.list_allowed_system_events`.

Establecimiento de eventos de diagnóstico del sistema

Para establecer un evento de sistema, utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_util.set_system_event`. Solo puede establecer eventos que figuren en la salida de `rdsadmin.rdsadmin_util.list_allowed_system_events`. El procedimiento `set_system_event` acepta los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_event`	número	—	Sí	El número de evento de sistema. El valor debe ser uno de los números de evento que se informaron mediante `list_allowed_system_events` .
`p_level`	número	—	Sí	El nivel del evento. Consulte la Documentación de la base de datos de Oracle u

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				Oracle Support para obtener las descripciones de diferentes valores de niveles.

Con el procedimiento `set_system_event` se construyen y se ejecutan las instrucciones `ALTER SYSTEM SET EVENTS` requeridas de acuerdo con los siguientes principios:

- El tipo de evento (`context` o `errorstack`) se determina automáticamente.
- Con una instrucción `ALTER SYSTEM SET EVENTS 'event LEVEL event_level'` se establecen los eventos de contexto. Esta notación es equivalente a `ALTER SYSTEM SET EVENTS 'event TRACE NAME CONTEXT FOREVER, LEVEL event_level'`.
- Con una instrucción `ALTER SYSTEM SET EVENTS 'event ERRORSTACK (event_level)'` se establecen los eventos de pila de errores. Esta notación es equivalente a `ALTER SYSTEM SET EVENTS 'event TRACE NAME ERRORSTACK LEVEL event_level'`.

En el ejemplo siguiente se establece el evento 942 a nivel 3 y el evento 10442 a nivel 10. Se incluye la salida de muestra.

```
SQL> SET SERVEROUTPUT ON
SQL> EXEC rdsadmin.rdsadmin_util.set_system_event(942,3);
Setting system event 942 with: alter system set events '942 errorstack (3)'

PL/SQL procedure successfully completed.

SQL> EXEC rdsadmin.rdsadmin_util.set_system_event(10442,10);
Setting system event 10442 with: alter system set events '10442 level 10'

PL/SQL procedure successfully completed.
```

Hacer una lista de los eventos de diagnóstico del sistema establecidos

Para hacer una lista de los eventos del sistema establecidos, utilice el procedimiento `rdsadmin.rdsadmin_util.list_set_system_events` de Amazon RDS. Con

este procedimiento se informan solo los eventos establecidos a nivel del sistema por `set_system_event`.

En el ejemplo siguiente se hace una lista de los eventos de sistema activos.

```
SET SERVEROUTPUT ON
EXEC rdsadmin.rdsadmin_util.list_set_system_events;
```

En la siguiente salida de ejemplo se muestran la lista de eventos, el tipo de evento, el nivel a que los eventos están configurados actualmente y la hora a que se estableció el evento.

```
942 errorstack (3) - set at 2020-11-03 11:42:27
10442 level 10 - set at 2020-11-03 11:42:41

PL/SQL procedure successfully completed.
```

Anular eventos de diagnóstico del sistema

Para anular un evento de sistema, utilice el procedimiento `rdsadmin.rdsadmin_util.unset_system_event` de Amazon RDS. Solo puede anular eventos que figuren en la salida de `rdsadmin.rdsadmin_util.list_allowed_system_events`. El procedimiento `unset_system_event` acepta el siguiente parámetro.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_event`	número	—	Sí	El número de evento de sistema. El valor debe ser uno de los números de evento que se informaron mediante `list_allowed_system_events` .

En el ejemplo siguiente se anulan los eventos 942 y 10442. Se incluye la salida de muestra.

```
SQL> SET SERVEROUTPUT ON
```

```
SQL> EXEC rdsadmin.rdsadmin_util.unset_system_event(942);
Unsetting system event 942 with: alter system set events '942 off'

PL/SQL procedure successfully completed.

SQL> EXEC rdsadmin.rdsadmin_util.unset_system_event(10442);
Unsetting system event 10442 with: alter system set events '10442 off'

PL/SQL procedure successfully completed.
```

Ejecución de tareas comunes de base de datos para instancias de base de datos

A continuación, puede encontrar cómo realizar ciertas tareas comunes de DBA relacionadas con las bases de datos en las instancias de base de datos de Amazon RDS que ejecutan Oracle. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. Amazon RDS también restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Temas

- Cambio del nombre global de una base de datos
- Uso de espacios de tabla
- Uso de archivos temporales
- Creación de un punto de comprobación de una base de datos
- Configuración de la recuperación distribuida
- Configuración de la zona horaria de la base de datos
- Uso de tablas externas de Oracle
- Generación de informes de rendimiento con Automatic Workload Repository (AWR)
- Ajuste de los enlaces de base de datos para usarlos con las instancias de bases de datos de una VPC
- Configuración de la edición predeterminada para una instancia de base de datos
- Activación de la auditoría para la tabla SYS.AUD$
- Desactivación de la auditoría para la tabla SYS.AUD$
- Limpieza de construcciones interrumpidas de índices en línea
- Omisión de bloques dañados

- Redimensionamiento de espacios de tablas, archivos de datos y archivos temporales
- Depuración de la Papelera de reciclaje
- Configuración de los valores mostrados de forma predeterminada para la redacción completa

Cambio del nombre global de una base de datos

Utilice el procedimiento de Amazon RDS para cambiar el nombre global de una base de dato `rdsadmin.rdsadmin_util.rename_global_name`. El procedimiento `rename_global_name` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_new_global_name`	varchar2	—	Sí	El nuevo nombre global de la base de datos.

La base de datos debe estar abierta para que se produzca el cambio de nombre. Para obtener más información acerca de cómo cambiar el nombre global de una base de datos, consulte ALTER DATABASE en la documentación de Oracle.

En el siguiente ejemplo se cambia el nombre global de una base de datos a `new_global_name`.

```
EXEC rdsadmin.rdsadmin_util.rename_global_name(p_new_global_name => 'new_global_name');
```

Uso de espacios de tabla

Puede utilizar los espacios de tabla con RDS para Oracle, que es una unidad de almacenamiento lógico y almacena los datos de la base de datos.

Temas

- Creación y especificación del tamaño de los espacios de tablas
- Configuración del espacio de tabla predeterminado
- Configuración del espacio de tabla temporal predeterminado
- Creación de un espacio de tablas temporal en el almacén de instancias

Creación y especificación del tamaño de los espacios de tablas

Amazon RDS solo admite los archivos administrados de Oracle (OMF) para los archivos de datos, los archivos de registro y los archivos de control. Cuando se crean archivos de datos y archivos de registro, no se pueden especificar los nombres de los archivos físicos.

De forma predeterminada, si no especifica el tamaño de archivo de datos, los espacios de tabla se crean con el tamaño predeterminado de `AUTOEXTEND ON` y sin tamaño máximo. En el siguiente ejemplo, el espacio de tablas *`users1`* es ampliable automáticamente.

```
CREATE TABLESPACE users1;
```

Debido a estos valores predeterminados, los espacios de tabla pueden llegar a consumir todo el almacenamiento asignado. Recomendamos que especifique un tamaño máximo adecuado para los espacios de tabla permanentes y temporales, y que monitorice cuidadosamente el uso del espacio.

En el siguiente ejemplo, se crea un espacio de tabla denominado *`users2`* con un tamaño inicial de 1 gigabyte. Dado que se especifica el tamaño de un archivo de datos, pero no se especifica `AUTOEXTEND ON`, el espacio de tablas no se puede ampliar automáticamente.

```
CREATE TABLESPACE users2 DATAFILE SIZE 1G;
```

En el siguiente ejemplo, se crea un espacio de tabla denominado *`users3`* con un tamaño inicial de 1 gigabyte, con la ampliación automática activada y un tamaño máximo de 10 gigabytes.

```
CREATE TABLESPACE users3 DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE 10G;
```

En el siguiente ejemplo, se crea un espacio de tabla temporal denominado *`temp01`*.

```
CREATE TEMPORARY TABLESPACE temp01;
```

Puede cambiar el tamaño de un espacio de tabla bigfile utilizando `ALTER TABLESPACE`. Puede especificar el tamaño en kilobytes (K), megabytes (M), gigabytes (G) o terabytes (T). En el siguiente ejemplo, se cambia el tamaño de un espacio de tabla bigfile denominado *`users_bf`* a 200 MB.

```
ALTER TABLESPACE users_bf RESIZE 200M;
```

En el siguiente ejemplo, se añade un archivo de datos adicional a un espacio de tabla smallfile denominado *`users_sf`*.

```
ALTER TABLESPACE users_sf ADD DATAFILE SIZE 100000M AUTOEXTEND ON NEXT 250m
 MAXSIZE UNLIMITED;
```

Configuración del espacio de tabla predeterminado

Utilice el procedimiento de Amazon RDS para configurar el espacio de tabla predeterminad `rdsadmin.rdsadmin_util.alter_default_tablespace`. El procedimiento `alter_default_tablespace` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`tablespace_name`	varchar	—	Sí	El nombre del espacio de tabla predeterminado.

En el siguiente ejemplo se establece el espacio de tabla predeterminado en *`users2`*:

```
EXEC rdsadmin.rdsadmin_util.alter_default_tablespace(tablespace_name => 'users2');
```

Configuración del espacio de tabla temporal predeterminado

Utilice el procedimiento de Amazon RDS para configurar el espacio de tabla temporal predeterminad `rdsadmin.rdsadmin_util.alter_default_temp_tablespace`. El procedimiento `alter_default_temp_tablespace` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`tablespace_name`	varchar	—	Sí	El nombre del espacio de tabla temporal predeterminado.

En el siguiente ejemplo se establece el espacio de tabla temporal predeterminado en *`temp01`*.

```
EXEC rdsadmin.rdsadmin_util.alter_default_temp_tablespace(tablespace_name => 'temp01');
```

Creación de un espacio de tablas temporal en el almacén de instancias

Utilice el procedimiento `rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace` de Amazon RDS para crear un espacio de tabla temporal en el almacén de instancias. El procedimiento `create_inst_store_tmp_tblspace` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_tablespace_name`	varchar	—	Sí	El nombre del espacio de tabla temporal.

En el siguiente ejemplo, se crea el espacio de tablas temporal *`temp01`* en el almacén de instancias.

```
EXEC rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace(p_tablespace_name =>
 'temp01');
```

> **Important**
>
> Cuando se ejecuta `rdsadmin_util.create_inst_store_tmp_tblspace`, el espacio de tabla temporal recién creado no se establece automáticamente como el espacio de tabla temporal predeterminado. Para configurarlo como predeterminado, consulte Configuración del espacio de tabla temporal predeterminado.

Para obtener más información, consulte Almacenamiento de datos temporales en un almacén de instancias de RDS para Oracle.

Uso de archivos temporales

Adición de un archivo temporal al almacén de instancias en una réplica de lectura

Cuando crea un espacio de tabla temporal en una instancia de base de datos principal, la réplica de lectura no crea archivos temporales. Supongamos que existe un espacio de tablas temporal vacío en la réplica de lectura por cualquiera de los siguientes motivos:

- Eliminó un archivo temporal del espacio de tablas de su réplica de lectura. Para obtener más información, consulte Eliminación de archivos temporales en una réplica de lectura.
- Creó un nuevo espacio de tablas temporal en la instancia de base de datos principal. En este caso, RDS para Oracle sincroniza los metadatos con la réplica de lectura.

Puedes añadir un archivo temporal al espacio de tablas temporal vacío y almacenar el archivo temporal en el almacén de instancias. Utilice el procedimiento `rdsadmin.rdsadmin_util.add_inst_store_tempfile` de Amazon RDS para crear un archivo temporal en el almacén de instancias. Este procedimiento solo se puede utilizar en una réplica de lectura. El procedimiento tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_tablespace_name`	varchar	—	Sí	El nombre del espacio de tabla temporal de la réplica de lectura.

En el siguiente ejemplo, el espacio de tabla temporal vacío *`temp01`* existe en la réplica de lectura. Ejecute el siguiente comando para crear un archivo temporal para este espacio de tabla y almacénelo en el almacén de instancias.

```
EXEC rdsadmin.rdsadmin_util.add_inst_store_tempfile(p_tablespace_name => 'temp01');
```

Para obtener más información, consulte Almacenamiento de datos temporales en un almacén de instancias de RDS para Oracle.

Eliminación de archivos temporales en una réplica de lectura

No puede eliminar un espacio de tabla temporal existente en una réplica de lectura. Puede cambiar el almacenamiento del archivo temporal en una réplica de lectura de Amazon EBS al almacén de instancias o del almacén de instancias a Amazon EBS. Para lograr estos objetivos, haga lo siguiente:

1. Elimine los archivos temporales actuales en el espacio de tablas temporal de la réplica de lectura.
2. Cree nuevos archivos temporales en un almacenamiento diferente.

Utilice el procedimiento `rdsadmin.rdsadmin_util. drop_replica_tempfiles` de Amazon RDS para eliminar archivos temporales. Este procedimiento solo se puede utilizar en réplicas de lectura. El procedimiento `drop_replica_tempfiles` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_tablespace_name`	varchar	—	Sí	El nombre del espacio de tabla temporal de la réplica de lectura.

Suponga que un espacio de tablas temporal denominado *`temp01`* reside en el almacén de instancias de su réplica de lectura. Elimine todos los archivos temporales de este espacio de tabla ejecutando el siguiente comando.

```
EXEC rdsadmin.rdsadmin_util.drop_replica_tempfiles(p_tablespace_name => 'temp01');
```

Para obtener más información, consulte Almacenamiento de datos temporales en un almacén de instancias de RDS para Oracle.

Creación de un punto de comprobación de una base de datos

Utilice el procedimiento de Amazon RDS para crear un punto de comprobación de la base dato `rdsadmin.rdsadmin_util.checkpoint`. El procedimiento `checkpoint` no tiene ningún parámetro.

En el siguiente ejemplo, se crea un punto de comprobación de la base de datos.

```
EXEC rdsadmin.rdsadmin_util.checkpoint;
```

Configuración de la recuperación distribuida

Utilice los procedimientos `rdsadmin.rdsadmin_util.enable_distr_recovery` y `disable_distr_recovery` de Amazon RDS para configurar la recuperación distribuida. Los procedimientos no tienen ningún parámetro.

En el siguiente ejemplo se activa la recuperación distribuida.

```
EXEC rdsadmin.rdsadmin_util.enable_distr_recovery;
```

En el siguiente ejemplo se desactiva la recuperación distribuida.

```
EXEC rdsadmin.rdsadmin_util.disable_distr_recovery;
```

Configuración de la zona horaria de la base de datos

Puede definir la zona horaria de la base de datos de Amazon RDS for Oracle de las siguientes maneras:

- La opción `Timezone`

  La opción `Timezone` cambia la zona horaria en el nivel del host y afecta a todos los valores y columnas de fecha, como `SYSDATE`. Para obtener más información, consulte Zona horaria Oracle.
- El procedimiento de Amazon RDS `rdsadmin.rdsadmin_util.alter_db_time_zone`

  El procedimiento `alter_db_time_zone` solo cambia la zona horaria de determinados tipos de datos y no cambia `SYSDATE`. En la documentación de Oracle se especifican otras restricciones para configurar la zona horaria.

> **Note**
>
> También puede establecer la zona horaria predeterminada para Oracle Scheduler. Para obtener más información, consulte Configuración de zona horaria para trabajos de Oracle Scheduler.

El procedimiento `alter_db_time_zone` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_new_tz`	varchar2	—	Sí	La nueva zona horaria expresada como una región con nombre o

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				un desfase absoluto con relación a la hora universal coordinada (UTC). Los desfases válidos oscilan entre -12:00 y +14:00.

En el siguiente ejemplo se cambia la zona horaria a UTC más tres horas.

```
EXEC rdsadmin.rdsadmin_util.alter_db_time_zone(p_new_tz => '+3:00');
```

En el siguiente ejemplo, se cambia la zona horaria a la de la región África/Argel.

```
EXEC rdsadmin.rdsadmin_util.alter_db_time_zone(p_new_tz => 'Africa/Algiers');
```

Después de cambiar la zona horaria utilizando el procedimiento `alter_db_time_zone`, reinicie su instancia de base de datos para que el cambio surta efecto. Para obtener más información, consulte Reinicio de una instancia de base de datos. Para obtener información acerca de cómo actualizar las zonas horarias, consulte Consideraciones sobre la zona horaria.

Uso de tablas externas de Oracle

Las tablas externas de Oracle son tablas con datos no incluidos en la base de datos. Los datos se encuentran en archivos externos a los que la base de datos puede acceder. Las tablas externas le permiten acceder a datos sin cargarlos en la base de datos. Para obtener más información sobre las tablas externas, consulte la sección Managing External Tables en la documentación de Oracle.

Amazon RDS le permite almacenar archivos de tablas externas en objetos de directorio. Puede crear un objeto de directorio o utilizar uno predefinido en la base de datos Oracle como, por ejemplo, el directorio DATA_PUMP_DIR. Para obtener información sobre la creación de objetos de directorio, consulte Creación y eliminación de directorios en el espacio de almacenamiento de datos principal. Puede consultar la vista ALL_DIRECTORIES para elaborar una lista de los objetos de directorio de la instancia de base de datos de Oracle en Amazon RDS.

> **Note**
>
> Los objetos de directorio apuntan hacia el espacio de almacenamiento de datos principal (volumen de Amazon EBS) utilizado por la instancia. El espacio utilizado, junto con los archivos de datos, registros REDO, archivos de auditoría, de seguimiento y de otro tipo, cuenta a la hora de calcular el almacenamiento asignado.

Puede desplazar un archivo de datos externos de una base de datos Oracle a otra base de datos utilizando el paquete DBMS_FILE_TRANSFER o el paquete UTL_FILE. El archivo de datos externos se traslada de un directorio en la base de datos de origen al directorio especificado en la base de datos de destino. Para obtener más información acerca del uso de DBMS_FILE_TRANSFER, consulte Importación mediante Oracle Data Pump.

Después de trasladar el archivo de datos externos, este le permite crear una tabla externa. En el siguiente ejemplo se crea una tabla externa que usa el archivo `emp_xt_file1.txt` en el directorio USER_DIR1.

```
CREATE TABLE emp_xt (
  emp_id      NUMBER,
  first_name  VARCHAR2(50),
  last_name   VARCHAR2(50),
  user_name   VARCHAR2(20)
)
ORGANIZATION EXTERNAL (
  TYPE ORACLE_LOADER
  DEFAULT DIRECTORY USER_DIR1
  ACCESS PARAMETERS (
    RECORDS DELIMITED BY NEWLINE
    FIELDS TERMINATED BY ','
    MISSING FIELD VALUES ARE NULL
    (emp_id,first_name,last_name,user_name)
  )
  LOCATION ('emp_xt_file1.txt')
)
PARALLEL
REJECT LIMIT UNLIMITED;
```

Suponga que quiere trasladar datos de una instancia de base de datos de Oracle en Amazon RDS a un archivo de datos externos. En ese caso, puede rellenar el archivo de datos externos creando

una tabla externa y seleccionando los datos de la tabla en la base de datos. Por ejemplo, la siguiente instrucción SQL crea la tabla externa `orders_xt` mediante la consulta a la tabla `orders` de la base de datos.

```
CREATE TABLE orders_xt
  ORGANIZATION EXTERNAL
   (
     TYPE ORACLE_DATAPUMP
     DEFAULT DIRECTORY DATA_PUMP_DIR
     LOCATION ('orders_xt.dmp')
   )
   AS SELECT * FROM orders;
```

En este ejemplo, los datos se rellenan en el archivo `orders_xt.dmp` del directorio DATA_PUMP_DIR.

Generación de informes de rendimiento con Automatic Workload Repository (AWR)

Para recopilar datos de rendimiento y generar informes, Oracle recomienda Automatic Workload Repository (AWR). AWR requiere Oracle Database Enterprise Edition y una licencia para los paquetes Diagnostics and Tuning. Para habilitar AWR, establezca el parámetro de inicialización `CONTROL_MANAGEMENT_PACK_ACCESS` en `DIAGNOSTIC` o `DIAGNOSTIC+TUNING`.

Trabajar con informes de AWR en RDS

Para generar informes de AWR, puede ejecutar scripts como `awrrpt.sql`. Estos scripts se instalan en el servidor host de la base de datos. En Amazon RDS, no tiene acceso directo al host. Sin embargo, puede obtener copias de scripts SQL desde otra instalación de Oracle Database.

También puede utilizar AWR ejecutando procedimientos en el paquete `SYS.DBMS_WORKLOAD_REPOSITORY` PL/SQL. Puede utilizar este paquete para administrar bases de referencia e instantáneas, así como para mostrar informes ASH y AWR. Por ejemplo, para generar un informe AWR en formato de texto, ejecute el procedimiento `DBMS_WORKLOAD_REPOSITORY.AWR_REPORT_TEXT`. Sin embargo, no puede acceder a estos informes de AWR desde la AWS Management Console.

Cuando se trabaja con AWR, se recomienda utilizar los procedimientos `rdsadmin.rdsadmin_diagnostic_util`. Puede utilizar estos procedimientos para generar lo siguiente:

- Informes AWR

- Informes de Historial de Sesiones Activas (ASH)
- Informes del Monitor de diagnóstico automático de bases de datos (ADDM)
- Archivos de volcado de datos AWR de Oracle Data Pump Export

Los procedimientos `rdsadmin_diagnostic_util` guardan los informes en el sistema de archivos de instancia de base de datos. Puede acceder a estos informes desde la consola. También puede acceder a los informes mediante los procedimientos `rdsadmin.rds_file_util` y puede acceder a los informes que se copian en Amazon S3 mediante la opción Integración de S3. Para obtener más información, consulte Lectura de archivos de un directorio de instancia de base de datos y Integración de Amazon S3.

Puede utilizar los procedimientos `rdsadmin_diagnostic_util` en las siguientes versiones del motor para bases de datos de Amazon RDS for Oracle:

- Todas las versiones de Oracle Database 21c
- 19.0.0.0.ru-2020-04.rur-2020-04.r1 Oracle Database 19c y versiones posteriores

Para ver un blog que explica cómo trabajar con los informes de diagnóstico en un escenario de replicación, consulte Generate AWR reports for Amazon RDS for Oracle read replicas.

Parámetros comunes para el paquete de utilidad de diagnóstico

Normalmente se utilizan los siguientes parámetros al administrar AWR y ADDM con el paquete `rdsadmin_diagnostic_util`.

Parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`begin_snap_id`	`NUMBER`	—	Sí	El ID de la instantánea inicial.
`end_snap_id`	`NUMBER`	—	Sí	El ID de la instantánea final.
`dump_directory`	`VARCHAR`	`BDUMP`	No	El directorio en el que se escribe el informe o el archivo de exportación. Si especifica un directorio no predeterminado, el usuario que ejecuta los procedimientos

Parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				`rdsadmin_diagnostic_util` debe tener permisos de escritura para el directorio.
`p_tag`	VARCHA	—	No	Una cadena que se puede usar para distinguir entre las copias de seguridad para indicar el propósito o el uso de las copias de seguridad, como `incremental` o `daily`. Puede especificar hasta 30 caracteres. Los caracteres válidos son `a-z`, `A-Z`, `0-9`, un guión bajo (_), un guión (-) y un punto (.). La etiqueta no distingue entre mayúsculas y minúsculas. RMAN siempre almacena las etiquetas en mayúsculas, independientemente del caso que se haya usado al ingresarlas. Las etiquetas no tienen que ser únicas, por lo que varias copias de seguridad pueden tener la misma etiqueta. Si no se especifica una etiqueta, RMAN asigna de forma automática una etiqueta predeterminada con el formato `TAG`*`YYYYMMDDTHHMMSS`*, donde *`YYYY`* es el año, *`MM`* es el mes, *`DD`* es el día, *`HH`* es la hora (en formato de 24 horas), *`MM`* son los minutos y *`SS`* son los segundos La fecha y la hora indican cuándo RMAN inició la copia de seguridad. Por ejemplo, una copia de seguridad con la etiqueta predeterminada `TAG20190927T214517` indica una copia de seguridad que se inició el 2019-09-27 a las 21:45:17. El parámetro `p_tag` es compatible con las siguientes versiones del motor para bases de datos de RDS for Oracle: • Oracle Database 21c (21.0.0) • Base de datos Oracle 19c (19.0.0), que usa 19.0.0.0.ru-2021-10.rur-2021-10.r1 y versiones posteriores

Parámetro	Tipo de datos	Valor predet inado	Obliga io	Descripción
report_ty pe	VARCHA	HTML	No	El formato del informe. Los valores válidos son TEXT y HTML.
dbid	NUMBEF	—	No	Un identificador de base de datos válido (DBID) que se muestra en la vista DBA_HIST_DATABASE_INSTANCE de Oracle. Si no se especifica este parámetro, RDS utiliza el DBID actual, que se muestra en la vista V $DATABASE.DBID .

Normalmente, se utilizan los siguientes parámetros al administrar ASH con el paquete rdsadmin_diagnostic_util.

Parámetro	Tipo de datos	Valor predete inado	Obligat io	Descripción
begin_tim e	DATE	—	Sí	La hora de inicio del análisis ASH.
end_time	DATE	—	Sí	La hora de finalización del análisis ASH.
slot_widt h	NUMBER	0	No	Duración de las ranuras (en segundos) utilizadas en la sección «Actividad principal» del informe ASH. Si no se especifica este parámetro, el intervalo de tiempo entre begin_time y end_time utiliza no más de 10 ranuras.
sid	NUMBER	Null	No	El ID de sesión.
sql_id	VARCHAR2	Null	No	El ID de SQL.
wait_clas s	VARCHAR2	Null	No	El nombre de la clase de espera.

Parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
service_hash	NUMBER	Null	No	El hash del nombre del servicio.
module_name	VARCHAR2	Null	No	El nombre del módulo.
action_name	VARCHAR2	Null	No	El nombre de la acción.
client_id	VARCHAR2	Null	No	El ID específico de la aplicación de la sesión de base de datos.
plsql_entry	VARCHAR2	Null	No	El punto de entrada PL/SQL.

Generación de un informe AWR

Para generar un informe AWR, utilice el procedimiento `rdsadmin.rdsadmin_diagnostic_util.awr_report`.

En el ejemplo siguiente se genera un informe AWR para el rango de instantáneas 101–106. El archivo de texto de salida se denomina `awrrpt_101_106.txt`. Puede obtener acceso a este informe desde la AWS Management Console.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_report(101,106,'TEXT');
```

En el ejemplo siguiente se genera un informe HTML para el rango de instantáneas 63–65. El archivo HTML de salida se denomina `awrrpt_63_65.html`. El procedimiento escribe el informe en el directorio de base de datos no predeterminado denominado `AWR_RPT_DUMP`.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_report(63,65,'HTML','AWR_RPT_DUMP');
```

Extracción de datos de AWR en un archivo de volcado

Para extraer datos de AWR en un archivo de volcado, utilice el procedimiento `rdsadmin.rdsadmin_diagnostic_util.awr_extract`.

En el siguiente ejemplo se extrae el rango de instantáneas 101–106. El archivo de volcado de salida se denomina `awrextract_101_106.dmp`. Puede acceder a este archivo a través de la consola.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_extract(101,106);
```

En el siguiente ejemplo se extrae el rango de instantáneas 63–65. El archivo de volcado de salida se denomina `awrextract_63_65.dmp`. El archivo se almacena en el directorio de base de datos no predeterminado denominado `AWR_RPT_DUMP`.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.awr_extract(63,65,'AWR_RPT_DUMP');
```

Generación de un informe ADDM

Para generar un informe ADDM, utilice el procedimiento `rdsadmin.rdsadmin_diagnostic_util.addm_report`.

En el ejemplo siguiente se genera un informe ADDM para el rango de instantáneas 101–106. El archivo de texto de salida se denomina `addmrpt_101_106.txt`. Puede acceder al informe a través de la consola.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.addm_report(101,106);
```

En el ejemplo siguiente se genera un informe ADDM para el rango de instantáneas 63–65. El archivo de texto de salida se denomina `addmrpt_63_65.txt`. El archivo se almacena en el directorio de base de datos no predeterminado denominado `ADDM_RPT_DUMP`.

```
EXEC rdsadmin.rdsadmin_diagnostic_util.addm_report(63,65,'ADDM_RPT_DUMP');
```

Generación de un informe ASH

Para generar un informe ASH, utilice el procedimiento `rdsadmin.rdsadmin_diagnostic_util.ash_report`.

En el ejemplo siguiente se genera un informe ASH que incluye los datos desde hace 14 minutos hasta la hora actual. El nombre del archivo de salida utiliza el formato

`ashrpt`*`begin_time`*`end_time`.`txt`, donde *`begin_time`* y *`end_time`* utilizan el formato `YYYYMMDDHH24MISS`. Puede acceder al archivo a través de la consola.

```
BEGIN
    rdsadmin.rdsadmin_diagnostic_util.ash_report(
        begin_time     =>     SYSDATE-14/1440,
        end_time       =>     SYSDATE,
        report_type    =>     'TEXT');
END;
/
```

En el siguiente ejemplo se genera un informe ASH que incluye los datos del 18 de noviembre de 2019, a las 6:07 PM hasta el 18 de noviembre de 2019, a las 6:15 PM. El nombre del informe HTML de salida es `ashrpt_20190918180700_20190918181500.html`. El informe se almacena en el directorio de base de datos no predeterminado denominado `AWR_RPT_DUMP`.

```
BEGIN
    rdsadmin.rdsadmin_diagnostic_util.ash_report(
        begin_time     =>    TO_DATE('2019-09-18 18:07:00', 'YYYY-MM-DD HH24:MI:SS'),
        end_time       =>    TO_DATE('2019-09-18 18:15:00', 'YYYY-MM-DD HH24:MI:SS'),
        report_type    =>    'html',
        dump_directory =>    'AWR_RPT_DUMP');
END;
/
```

Acceso a los informes de AWR desde la consola o la CLI

Para acceder a informes de AWR o exportar archivos de volcado, puede utilizar la AWS Management Console o la AWS CLI. Para obtener más información, consulte Descarga de un archivo de registro de base de datos.

Ajuste de los enlaces de base de datos para usarlos con las instancias de bases de datos de una VPC

Para utilizar enlaces de base de datos Oracle con instancias de bases de datos de Amazon RDS dentro de la misma nube virtual privada (VPC) o VPC interconectadas, debe existir una ruta válida entre las dos instancias de bases de datos. Compruebe que existe una ruta válida entre las instancias de bases de datos utilizando las tablas de enrutamiento de VPC y la lista de control de acceso (ACL) de red.

El grupo de seguridad de cada instancia de base de datos debe permitir la entrada y la salida desde la otra instancia de base de datos. Las reglas de entrada y salida pueden referirse a grupos de seguridad de la misma VPC o de una VPC interconectada. Para obtener más información, consulte Actualización de los grupos de seguridad para que hagan referencia a grupos de la VPC del mismo nivel.

Si ha configurado un servidor DNS personalizado mediante los conjuntos de opciones de DHCP en la VPC, el servidor DNS personalizado debe ser capaz de resolver el nombre del destino del enlace de base de datos. Para obtener más información, consulte Configuración de un servidor DNS personalizado.

Para obtener más información acerca del uso de los enlaces de base de datos con Oracle Data Pump, consulte Importación mediante Oracle Data Pump.

Configuración de la edición predeterminada para una instancia de base de datos

Puede redefinir objetos de la base de datos en un entorno privado llamado edición. Puede utilizar la redefinición basada en la edición para actualizar los objetos de la base de datos de una aplicación con un tiempo de inactividad mínimo.

Puede definir la edición predeterminada de una instancia de base de datos de Oracle en Amazon RDS mediante el uso del procedimiento `rdsadmin.rdsadmin_util.alter_default_edition` de Amazon RDS.

En el siguiente ejemplo se define la edición predeterminada de la instancia de base de datos de Oracle en Amazon RDS en `RELEASE_V1`.

```
EXEC rdsadmin.rdsadmin_util.alter_default_edition('RELEASE_V1');
```

En el siguiente ejemplo se vuelve a definir la edición predeterminada de la instancia de base de datos de Oracle en Amazon RDS como la edición predeterminada de Oracle.

```
EXEC rdsadmin.rdsadmin_util.alter_default_edition('ORA$BASE');
```

Para obtener más información sobre la redefinición basada en la edición de Oracle, consulte About Editions and Edition-Based Redefinition en la documentación de Oracle.

Activación de la auditoría para la tabla SYS.AUD$

Utilice el procedimiento `SYS.AUD$` de Amazon RDS para activar la auditoría en la tabla de prueba de auditoría de base datos `rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table`. La única propiedad de auditoría admitida es `ALL`. No puede auditar o no auditar declaraciones u operaciones individuales.

La activación de la auditoría se admite en instancias de base de datos Oracle que ejecutan las siguientes versiones:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

El procedimiento `audit_all_sys_aud_table` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_by_access`	booleano	true	No	Establézcalo en `true` para auditar `BY ACCESS`. Establézcalo en `false` para auditar `BY SESSION`.

La siguiente consulta devuelve la configuración de auditoría actual de `SYS.AUD$` para una base de datos.

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OWNER='SYS' AND OBJECT_NAME='AUD$';
```

Los siguientes comandos activan la auditoría de `ALL` en `SYS.AUD$ BY ACCESS`.

```
EXEC rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table;

EXEC rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table(p_by_access => true);
```

Los siguientes comandos activan la auditoría de `ALL` en `SYS.AUD$ BY SESSION`.

```
EXEC rdsadmin.rdsadmin_master_util.audit_all_sys_aud_table(p_by_access => false);
```

Para más información, consulte AUDIT (Traditional Auditing) en la documentación de Oracle.

Desactivación de la auditoría para la tabla SYS.AUD$

Utilice el procedimiento `SYS.AUD$` de Amazon RDS para desactivar la auditoría en la tabla de prueba de auditoría de base de datos `rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table`. Este procedimiento no acepta parámetros.

La siguiente consulta devuelve la configuración de auditoría actual de `SYS.AUD$` para una base de datos:

```
SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OWNER='SYS' AND OBJECT_NAME='AUD$';
```

El siguiente comando desactiva la auditoría de `ALL` en `SYS.AUD$`.

```
EXEC rdsadmin.rdsadmin_master_util.noaudit_all_sys_aud_table;
```

Para más información, consulte NO AUDIT (Traditional Auditing) en la documentación de Oracle.

Limpieza de construcciones interrumpidas de índices en línea

Para limpiar construcciones de índices online fallidas, utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_dbms_repair.online_index_clean`.

El procedimiento `online_index_clean` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`object_id`	entero_binario	`ALL_INDEX_ID`	No	El ID de objeto del índice. Por lo general, puede usar el ID de objeto del texto de error ORA-08104.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`wait_for_lock`	entero_binario	`rdsadmin.rdsadmin_dbms_repair.lock_wait`	No	Especifique `rdsadmin.rdsadmin_dbms_repair.lock_wait` , el valor predeterminado, para intentar obtener un bloqueo en el objeto subyacente y volver a intentarlo hasta que se alcance un límite interno si el bloqueo falla. Especifique `rdsadmin.rdsadmin_dbms_repair.lock_nowait` para intentar obtener un bloqueo en el objeto subyacente, pero sin volver a intentarlo si falla el bloqueo.

El siguiente ejemplo limpia una construcción de índice online fallida:

```
declare
  is_clean boolean;
begin
  is_clean := rdsadmin.rdsadmin_dbms_repair.online_index_clean(
    object_id     => 1234567890,
    wait_for_lock => rdsadmin.rdsadmin_dbms_repair.lock_nowait
  );
end;
/
```

Para obtener más información, consulte ONLINE_INDEX_CLEAN Function en la documentación de Oracle.

Omisión de bloques dañados

Para omitir bloques dañados durante análisis de índice y tablas, utilice el paquete `rdsadmin.rdsadmin_dbms_repair`.

Los siguientes procedimientos encapsulan la funcionalidad del procedimiento `sys.dbms_repair.admin_table` y no toman parámetros:

- `rdsadmin.rdsadmin_dbms_repair.create_repair_table`
- `rdsadmin.rdsadmin_dbms_repair.create_orphan_keys_table`
- `rdsadmin.rdsadmin_dbms_repair.drop_repair_table`
- `rdsadmin.rdsadmin_dbms_repair.drop_orphan_keys_table`
- `rdsadmin.rdsadmin_dbms_repair.purge_repair_table`
- `rdsadmin.rdsadmin_dbms_repair.purge_orphan_keys_table`

Los siguientes procedimientos toman los mismos parámetros que sus contrapartes en el paquete `DBMS_REPAIR` para bases de datos de Oracle:

- `rdsadmin.rdsadmin_dbms_repair.check_object`
- `rdsadmin.rdsadmin_dbms_repair.dump_orphan_keys`
- `rdsadmin.rdsadmin_dbms_repair.fix_corrupt_blocks`
- `rdsadmin.rdsadmin_dbms_repair.rebuild_freelists`
- `rdsadmin.rdsadmin_dbms_repair.segment_fix_status`
- `rdsadmin.rdsadmin_dbms_repair.skip_corrupt_blocks`

Para obtener más información sobre la gestión de daños en la base de datos, consulte DBMS_REPAIR en la documentación de Oracle.

Example Respuesta a bloques dañados

En este ejemplo se muestra el flujo de trabajo básico para responder a bloques dañados. Sus pasos dependerán de la ubicación y la naturaleza del daño de sus bloques.

> **Important**
>
> Antes de intentar reparar bloques dañados, revise detenidamente la documentación de DBMS_REPAIR.

Para omitir bloques dañados durante análisis de índices y tablas

1. Ejecute los siguientes procedimientos para crear tablas de reparación si aún no existen.

```
EXEC rdsadmin.rdsadmin_dbms_repair.create_repair_table;
EXEC rdsadmin.rdsadmin_dbms_repair.create_orphan_keys_table;
```

2. Ejecute los siguientes procedimientos para verificar los registros existentes y purgarlos, si corresponde.

```
SELECT COUNT(*) FROM SYS.REPAIR_TABLE;
SELECT COUNT(*) FROM SYS.ORPHAN_KEY_TABLE;
SELECT COUNT(*) FROM SYS.DBA_REPAIR_TABLE;
SELECT COUNT(*) FROM SYS.DBA_ORPHAN_KEY_TABLE;

EXEC rdsadmin.rdsadmin_dbms_repair.purge_repair_table;
EXEC rdsadmin.rdsadmin_dbms_repair.purge_orphan_keys_table;
```

3. Ejecute el siguiente procedimiento para verificar si hay bloques dañados.

```
SET SERVEROUTPUT ON
DECLARE v_num_corrupt INT;
BEGIN
  v_num_corrupt := 0;
  rdsadmin.rdsadmin_dbms_repair.check_object (
    schema_name => '&corruptionOwner',
    object_name => '&corruptionTable',
    corrupt_count =>  v_num_corrupt
  );
  dbms_output.put_line('number corrupt: '||to_char(v_num_corrupt));
END;
/

COL CORRUPT_DESCRIPTION FORMAT a30
COL REPAIR_DESCRIPTION FORMAT a30
```

```
SELECT OBJECT_NAME, BLOCK_ID, CORRUPT_TYPE, MARKED_CORRUPT,
       CORRUPT_DESCRIPTION, REPAIR_DESCRIPTION
FROM   SYS.REPAIR_TABLE;

SELECT SKIP_CORRUPT
FROM   DBA_TABLES
WHERE  OWNER = '&corruptionOwner'
AND    TABLE_NAME = '&corruptionTable';
```

4. Utilice el procedimiento `skip_corrupt_blocks` para habilitar o desactivar la omisión de daños de las tablas afectadas. En función de la situación, es posible que también necesite extraer datos en una tabla nueva y, a continuación, soltar la tabla que contiene el bloque dañado.

   Ejecute el siguiente procedimiento para habilitar la omisión de daños en tablas afectadas.

   ```
   begin
     rdsadmin.rdsadmin_dbms_repair.skip_corrupt_blocks (
       schema_name => '&corruptionOwner',
       object_name => '&corruptionTable',
       object_type => rdsadmin.rdsadmin_dbms_repair.table_object,
       flags => rdsadmin.rdsadmin_dbms_repair.skip_flag);
   end;
   /
   select skip_corrupt from dba_tables where owner = '&corruptionOwner' and table_name
    = '&corruptionTable';
   ```

   Ejecute el siguiente procedimiento para desactivar la omisión de daños.

   ```
   begin
     rdsadmin.rdsadmin_dbms_repair.skip_corrupt_blocks (
       schema_name => '&corruptionOwner',
       object_name => '&corruptionTable',
       object_type => rdsadmin.rdsadmin_dbms_repair.table_object,
       flags => rdsadmin.rdsadmin_dbms_repair.noskip_flag);
   end;
   /

   select skip_corrupt from dba_tables where owner = '&corruptionOwner' and table_name
    = '&corruptionTable';
   ```

5. Cuando haya completado todo el trabajo de reparación, ejecute los siguientes procedimientos para eliminar las tablas de reparación.

```
EXEC rdsadmin.rdsadmin_dbms_repair.drop_repair_table;
EXEC rdsadmin.rdsadmin_dbms_repair.drop_orphan_keys_table;
```

Redimensionamiento de espacios de tablas, archivos de datos y archivos temporales

De forma predeterminada, los espacios de tabla de Oracle se crean con la ampliación automática activada y sin tamaño máximo. Debido a estos valores predeterminados, los espacios de tabla pueden llegar a ser demasiado grandes en algunos casos. Recomendamos que especifique un tamaño máximo adecuado para los espacios de tabla permanentes y temporales, y que monitorice cuidadosamente el uso del espacio.

Redimensionamiento de espacios de tabla permanentes

Para cambiar el tamaño de un espacio de tabla permanente en una instancia de base de datos de RDS para Oracle, utilice cualquiera de los siguientes procedimientos de Amazon RDS:

- `rdsadmin.rdsadmin_util.resize_datafile`
- `rdsadmin.rdsadmin_util.autoextend_datafile`

El procedimiento `resize_datafile` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_data_file_id`	número	—	Sí	El identificador del archivo de datos que se va a cambiar de tamaño.
`p_size`	varchar2	—	Sí	El tamaño del archivo de datos. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G).

El procedimiento `autoextend_datafile` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_data_file_id`	número	—	Sí	El identificador del archivo de datos que se va a cambiar de tamaño.
`p_autoextend_state`	varchar2	—	Sí	El estado de la característica de ampliación automática. Especifique `ON` para ampliar el archivo de datos automáticamente y `OFF` para desactivar la ampliación automática.
`p_next`	varchar2	—	No	El tamaño del incremento del siguiente archivo de datos. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G).
`p_maxsize`	varchar2	—	No	El espacio máximo en disco permitido para la ampliación automática. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G). Puede especificar `UNLIMITED` para

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				eliminar el límite de tamaño del archivo.

En el ejemplo siguiente, se cambia el tamaño del archivo de datos de 4 a 500 MB.

```
EXEC rdsadmin.rdsadmin_util.resize_datafile(4,'500M');
```

En el siguiente ejemplo, se desactiva la ampliación automática del archivo de datos 4. También se activa la ampliación automática para el archivo de datos 5, con un incremento de 128 MB y sin tamaño máximo.

```
EXEC rdsadmin.rdsadmin_util.autoextend_datafile(4,'OFF');
EXEC rdsadmin.rdsadmin_util.autoextend_datafile(5,'ON','128M','UNLIMITED');
```

Redimensionamiento de espacios de tabla temporales

Para redimensionar un espacio de tabla temporal en una instancia de base de datos de RDS para Oracle, incluida una réplica de lectura, utilice cualquiera de los siguientes procedimientos de Amazon RDS:

- `rdsadmin.rdsadmin_util.resize_temp_tablespace`
- `rdsadmin.rdsadmin_util.resize_tempfile`
- `rdsadmin.rdsadmin_util.autoextend_tempfile`

El procedimiento `resize_temp_tablespace` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_temp_tablespace_name`	varchar2	—	Sí	El nombre del espacio de tabla temporal al que se va a cambiar el tamaño.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_size	varchar2	—	Sí	El tamaño del espacio de tabla. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G).

El procedimiento resize_tempfile tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_temp_file_id	número	—	Sí	El identificador del archivo temporal al que se va a cambiar el tamaño.
p_size	varchar2	—	Sí	El tamaño del archivo temporal. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G).

El procedimiento autoextend_tempfile tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_temp_file_id	número	—	Sí	El identificador del archivo temporal al que se va a cambiar el tamaño.
p_autoextend_state	varchar2	—	Sí	El estado de la característica de ampliación automática. Especifique ON para ampliar el archivo temporal automáticamente y OFF para desactivar la ampliación automática.
p_next	varchar2	—	No	El tamaño del incremento del siguiente archivo temporal. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G).
p_maxsize	varchar2	—	No	El espacio máximo en disco permitido para la ampliación automática. Puede especificar el tamaño en bytes (la opción predeterminada), kilobytes (K), megabytes (M) o gigabytes (G). Puede especificar UNLIMITED para

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				eliminar el límite de tamaño del archivo.

Los siguientes ejemplos cambian el tamaño de un espacio de tabla temporal llamado `TEMP` hasta 4 GB.

```
EXEC rdsadmin.rdsadmin_util.resize_temp_tablespace('TEMP','4G');
```

```
EXEC rdsadmin.rdsadmin_util.resize_temp_tablespace('TEMP','4096000000');
```

El siguiente ejemplo cambia el tamaño de un espacio de tabla temporal en función del archivo temporal con el identificador de archivo 1 hasta los 2 MB.

```
EXEC rdsadmin.rdsadmin_util.resize_tempfile(1,'2M');
```

En el siguiente ejemplo, se desactiva la ampliación automática del archivo temporal 1. También se establece el tamaño máximo de ampliación automática del archivo temporal de 2 a 10 GB, con un incremento de 100 MB.

```
EXEC rdsadmin.rdsadmin_util.autoextend_tempfile(1,'OFF');
EXEC rdsadmin.rdsadmin_util.autoextend_tempfile(2,'ON','100M','10G');
```

Para obtener más información acerca de las réplicas de lectura para las instancias de base de datos de Oracle, consulte Trabajo con las réplicas de lectura para Amazon RDS para Oracle.

Depuración de la Papelera de reciclaje

Cuando se elimina una tabla, la base de datos Oracle no elimina inmediatamente su espacio de almacenamiento. La base de datos cambia el nombre de la tabla y la coloca junto con los objetos asociados en una papelera de reciclaje. Al eliminar la papelera de reciclaje, se eliminan estos elementos y se libera su espacio de almacenamiento.

Para eliminar toda la papelera de reciclaje, utilice el procedimiento `rdsadmin.rdsadmin_util.purge_dba_recyclebin` de Amazon RDS. Sin embargo, este

procedimiento no puede eliminar la papelera de reciclaje de objetos SYS y RDSADMIN. Si necesita eliminar estos objetos, contáctese con AWS Support.

En el ejemplo siguiente se elimina toda la papelera de reciclaje.

```
EXEC rdsadmin.rdsadmin_util.purge_dba_recyclebin;
```

Configuración de los valores mostrados de forma predeterminada para la redacción completa

Para cambiar los valores mostrados de forma predeterminada para la redacción completa en la instancia de Oracle de Amazon RDS, use el procedimiento de Amazon RDS rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val. Tenga en cuenta que crea una política de redacción con el paquete PL/SQL DBMS_REDACT, tal y como se explica en la documentación de Oracle Database. El procedimiento dbms_redact_upd_full_rdct_val especifica los caracteres que se mostrarán para los diferentes tipos de datos afectados por una política actual.

El procedimiento dbms_redact_upd_full_rdct_val tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_number_val	number	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos NUMBER.
p_binfloat_val	binary_float	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos BINARY_FLOAT .
p_bindouble_val	binary_double	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos BINARY_DOUBLE .

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_char_val	char	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos CHAR.
p_varchar_val	varchar2	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos VARCHAR2.
p_nchar_val	nchar	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos NCHAR.
p_nvarchar_val	nvarchar2	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos NVARCHAR2 .
p_date_val	date	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos DATE.
p_ts_val	Marca de tiempo	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos TIMESTAMP .

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_tswtz_val	timestamp with time zone	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos TIMESTAMP WITH TIME ZONE.
p_blob_val	blob	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos BLOB.
p_clob_val	clob	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos CLOB.
p_nclob_val	nclob	Nulo	No	Modifica el valor predeterminado de las columnas del tipo de datos NCLOB.

El siguiente ejemplo cambia el valor redactado predeterminado a * para el tipo de datos CHAR:

```
EXEC rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val(p_char_val => '*');
```

El siguiente ejemplo cambia los valores redactados predeterminados para los tipos de datos NUMBER, DATE y CHAR:

```
BEGIN
rdsadmin.rdsadmin_util.dbms_redact_upd_full_rdct_val(
    p_number_val=>1,
    p_date_val=>to_date('1900-01-01','YYYY-MM-DD'),
    p_varchar_val=>'X');
END;
```

```
/
```

Después de modificar los valores predeterminados para la redacción completa con el procedimiento `dbms_redact_upd_full_rdct_val`, reinicie la instancia de base de datos para que el cambio surta efecto. Para obtener más información, consulte Reinicio de una instancia de base de datos.

Realización de tareas comunes relacionadas con el registro para instancias de base de datos Oracle

A continuación, puede encontrar cómo realizar ciertas tareas comunes de DBA relacionadas con el registro en las instancias de base de datos de Amazon RDS que ejecutan Oracle. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de bases de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Para obtener más información, consulte Archivos de registro de base de datos de Amazon RDS para Oracle.

Temas

- Activación del modo force logging
- Activación del modo supplemental logging
- Cambio de archivos de registro en línea
- Adición de registros REDO en línea
- Eliminación de registros REDO en línea
- Cambio de tamaño de los registros REDO en línea
- Retención de los registros REDO archivados
- Acceso a los registros de rehacer en línea y archivados
- Descargue registros de rehacer archivados de Amazon S3

Activación del modo force logging

En el modo force logging, Oracle registra todos los cambios realizados en la base de datos, excepto los cambios efectuados en los espacios de tabla temporales y los segmentos temporales (las

cláusulas NOLOGGING se omiten). Para obtener más información, consulte Specifying FORCE LOGGING Mode en la documentación de Oracle.

Utilice el procedimiento de Amazon RDS para configurar el modo force loggin `rdsadmin.rdsadmin_util.force_logging`. El procedimiento `force_logging` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Sí	Descripción
`p_enable`	booleano	true	No	Establezca este parámetro en `true` para poner la base de datos en modo force logging, y en `false` para quitar la base de datos del modo force logging.

En el siguiente ejemplo se pone la base de datos en el modo force logging.

```
EXEC rdsadmin.rdsadmin_util.force_logging(p_enable => true);
```

Activación del modo supplemental logging

Si habilita el registro complementario, LogMiner tiene la información necesaria para admitir filas encadenadas y tablas agrupadas. Para obtener más información, consulte Supplemental Logging en la documentación de Oracle.

Oracle Database no tiene activado el modo supplemental logging de forma predeterminada. Utilice el procedimiento de Amazon RDS para activar y desactivar el modo supplemental loggin `rdsadmin.rdsadmin_util.alter_supplemental_logging`. Para obtener más información acerca de cómo gestiona Amazon RDS la conservación de los registros REDO archivados para las instancias de bases de datos Oracle, consulte Retención de los registros REDO archivados.

El procedimiento `alter_supplemental_logging` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_action	varchar2	—	Sí	'ADD' para activar el modo supplemental logging, 'DROP' para desactivarlo.
p_type	varchar2	null	No	El tipo de supplemental logging. Los valores válidos son: 'ALL', 'FOREIGN KEY', 'PRIMARY KEY', 'UNIQUE' o PROCEDURAL .

En el siguiente ejemplo se activa el modo supplemental logging.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD');
end;
/
```

En el siguiente ejemplo se activa el modo supplemental logging para todas las columnas de tamaño máximo y de longitud fija.

```
begin
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD',
        p_type   => 'ALL');
end;
/
```

En el siguiente ejemplo se activa el modo supplemental logging para las columnas de clave principal.

```
begin
```

```
    rdsadmin.rdsadmin_util.alter_supplemental_logging(
        p_action => 'ADD',
        p_type   => 'PRIMARY KEY');
end;
/
```

Cambio de archivos de registro en línea

Utilice el procedimiento de Amazon RDS para cambiar los archivos de registr `rdsadmin.rdsadmin_util.switch_logfile`. El procedimiento `switch_logfile` no tiene ningún parámetro.

En el siguiente ejemplo se cambian los archivos de registro.

```
EXEC rdsadmin.rdsadmin_util.switch_logfile;
```

Adición de registros REDO en línea

Una instancia de base de datos de Amazon RDS que ejecuta Oracle comienza con cuatro registros REDO online de 128 MB cada uno. Utilice el procedimiento de Amazon RDS para añadir registros REDO adicionale `rdsadmin.rdsadmin_util.add_logfile`.

El procedimiento `add_logfile` tiene los siguientes parámetros.

> **Note**
>
> Los parámetros son mutuamente excluyentes.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`bytes`	positivo	null	No	El tamaño del archivo de registro en bytes. Utilice este parámetro solo si el tamaño del registro es inferior a 2 147 483 648 bytes

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				(2 GiB). De lo contrario, RDS emite un error. Para tamaños de registro superiores a este valor en bytes, utilice el parámetro `p_size` en su lugar.
`p_size`	varchar2	—	Sí	El tamaño del archivo de registro en kilobytes (K), megabytes (M) o gigabytes (G).

El comando siguiente añade un archivo de registro de 100 MB.

```
EXEC rdsadmin.rdsadmin_util.add_logfile(p_size => '100M');
```

Eliminación de registros REDO en línea

Utilice el procedimiento de Amazon RDS para eliminar registros RED `rdsadmin.rdsadmin_util.drop_logfile`. El procedimiento `drop_logfile` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`grp`	positivo	—	Sí	El número de grupo del registro.

En el siguiente ejemplo se elimina el registro cuyo grupo es el número 3.

```
EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 3);
```

Solo puede eliminar los registros cuyo estado sea no utilizado o inactivo. En el siguiente ejemplo se obtienen los estados de los registros.

```
SELECT GROUP#, STATUS FROM V$LOG;

GROUP#     STATUS
---------- ----------------
1          CURRENT
2          INACTIVE
3          INACTIVE
4          UNUSED
```

Cambio de tamaño de los registros REDO en línea

Una instancia de base de datos de Amazon RDS que ejecuta Oracle comienza con cuatro registros REDO online de 128 MB cada uno. En el siguiente ejemplo se muestra cómo puede utilizar los procedimientos de Amazon RDS para cambiar el tamaño de cada uno de los registros de 128 MB a 512 MB.

```
/* Query V$LOG to see the logs.          */
/* You start with 4 logs of 128 MB each. */

SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#     BYTES      STATUS
---------- ---------- ----------------
1          134217728  INACTIVE
2          134217728  CURRENT
3          134217728  INACTIVE
4          134217728  INACTIVE


/* Add four new logs that are each 512 MB */

EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);
EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);
EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);
EXEC rdsadmin.rdsadmin_util.add_logfile(bytes => 536870912);


/* Query V$LOG to see the logs. */
/* Now there are 8 logs.        */
```

```
SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#     BYTES      STATUS
---------- ---------- ----------------
1          134217728  INACTIVE
2          134217728  CURRENT
3          134217728  INACTIVE
4          134217728  INACTIVE
5          536870912  UNUSED
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED


/* Drop each inactive log using the group number. */

EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 1);
EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 3);
EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 4);


/* Query V$LOG to see the logs. */
/* Now there are 5 logs.        */

select GROUP#, BYTES, STATUS from V$LOG;

GROUP#     BYTES      STATUS
---------- ---------- ----------------
2          134217728  CURRENT
5          536870912  UNUSED
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED


/* Switch logs so that group 2 is no longer current. */

EXEC rdsadmin.rdsadmin_util.switch_logfile;


/* Query V$LOG to see the logs.        */
/* Now one of the new logs is current. */
```

```
SQL>SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#     BYTES      STATUS
---------- ---------- ----------------
2          134217728  ACTIVE
5          536870912  CURRENT
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED


/* If the status of log 2 is still "ACTIVE", issue a checkpoint to clear it to
 "INACTIVE".  */

EXEC rdsadmin.rdsadmin_util.checkpoint;


/* Query V$LOG to see the logs.            */
/* Now the final original log is inactive. */

select GROUP#, BYTES, STATUS from V$LOG;

GROUP#     BYTES      STATUS
---------- ---------- ----------------
2          134217728  INACTIVE
5          536870912  CURRENT
6          536870912  UNUSED
7          536870912  UNUSED
8          536870912  UNUSED


# Drop the final inactive log.

EXEC rdsadmin.rdsadmin_util.drop_logfile(grp => 2);


/* Query V$LOG to see the logs.    */
/* Now there are four 512 MB logs. */

SELECT GROUP#, BYTES, STATUS FROM V$LOG;

GROUP#     BYTES      STATUS
---------- ---------- ----------------
5          536870912  CURRENT
```

```
6           536870912  UNUSED
7           536870912  UNUSED
8           536870912  UNUSED
```

Retención de los registros REDO archivados

Puede retener los registros de rehacer archivados localmente en una instancia de base de datos para su uso con productos como Oracle LogMiner (`DBMS_LOGMNR`). Después de conservar los registros REDO, puede utilizar LogMiner para analizarlos. Para obtener más información, consulte Using LogMiner to Analyze Redo Log Files en la documentación de Oracle.

Utilice el procedimiento de Amazon RDS para conservar los registros REDO archivado `rdsadmin.rdsadmin_util.set_configuration`. Si utiliza este procedimiento en una instancia principal de Oracle Data Guard, RDS cambia la configuración de retención del registro de archivado en la instancia principal y abre las réplicas de lectura, pero no en las réplicas montadas. RDS retiene los registros REDO del archivo más recientes en las réplicas montadas durante un breve periodo de tiempo. RDS elimina automáticamente los registros más antiguos descargados en las réplicas montadas.

El procedimiento `set_configuration` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`name`	varchar	—	Sí	El nombre de la configuración que se debe actualizar. Para cambiar las horas de retención de los registros REDO archivados, defina el nombre en `archivelog retention hours` .
`value`	varchar	—	Sí	El valor de la configuración. Defina el valor del número de horas que se

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				van a retener los registros .

En el siguiente ejemplo se conservan 24 horas de registros REDO.

```
begin
    rdsadmin.rdsadmin_util.set_configuration(
        name  => 'archivelog retention hours',
        value => '24');
end;
/
commit;
```

> **Note**
>
> La confirmación es necesaria para que los cambios surtan efecto.

Utilice el procedimiento de Amazon RDS para ver durante cuánto tiempo se conservan los registros REDO archivados para la instancia de base de dato `rdsadmin.rdsadmin_util.show_configuration`.

El siguiente ejemplo muestra el tiempo de retención del registro.

```
set serveroutput on
EXEC rdsadmin.rdsadmin_util.show_configuration;
```

La salida muestra el valor actual de `archivelog retention hours`. La siguiente salida muestra que los registros REDO archivados se conservan durante 48 horas.

```
NAME:archivelog retention hours
VALUE:48
DESCRIPTION:ArchiveLog expiration specifies the duration in hours before archive/redo
 log files are automatically deleted.
```

Dado que los registros REDO archivados se conservan en la instancia de base de datos, asegúrese de que esta tenga suficiente almacenamiento asignado para los registros que se van a conservar. Para determinar cuánto espacio ha utilizado la instancia de base de datos en las últimas X horas, puede ejecutar la consulta siguiente, sustituyendo X por el número de horas.

```
SELECT SUM(BLOCKS * BLOCK_SIZE) bytes
  FROM V$ARCHIVED_LOG
 WHERE FIRST_TIME >= SYSDATE-(X/24) AND DEST_ID=1;
```

RDS for Oracle solo se genera registros de rehacer si el periodo de retención de copia de seguridad de la instancia de base de datos es mayor que cero. De forma predeterminada, el periodo de retención de copia de seguridad es mayor que cero.

Cuando expira el periodo de retención de registros archivados, RDS for Oracle elimina los registros de rehacer archivados de la instancia de base de datos. Para admitir la restauración de la instancia de base de datos en un momento determinado, Amazon RDS retiene los registros de rehacer archivados fuera de la instancia de base de datos en función del periodo de retención de copia de seguridad. Para modificar el periodo de retención de copia de seguridad, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Note**
>
> En algunos casos, podría utilizar JDBC en Linux para descargar registros REDO archivados y experimentar tiempos de latencia largos y restablecimientos de conexión. En tales casos, los problemas pueden estar causados por el ajuste predeterminado del generador de números aleatorios en su cliente Java. Recomendamos configurar los controladores JDBC para usar un generador de números aleatorio sin bloqueos.

Acceso a los registros de rehacer en línea y archivados

Es posible que desee obtener acceso a los archivos de registros REDO online y archivados para realizar tareas de minería de datos con herramientas externas como GoldenGate, Attunity, Informatica y otras. Para acceder a estos archivos, haga lo siguiente:

1. Cree objetos de directorio que proporcionen acceso de solo lectura a las rutas de acceso de los archivos físicos.

Utilice `rdsadmin.rdsadmin_master_util.create_archivelog_dir` y `rdsadmin.rdsadmin_master_util.create_onlinelog_dir`.

2. Lea los archivos mediante PL/SQL.

   Puede leer los archivos mediante PL/SQL. Para obtener más información acerca de cómo leer archivos de los objetos de directorio, consulte Descripción de los archivos de un directorio de instancia de base de datos y Lectura de archivos de un directorio de instancia de base de datos.

El acceso a los registros de transacciones es compatible con las siguientes versiones:

- Oracle Database 21c
- Oracle Database 19c

El siguiente código crea directorios que proporcionan acceso de solo lectura a los archivos de registros REDO online y archivados:

> **Important**
>
> Este código también revoca el privilegio `DROP ANY DIRECTORY`.

```
EXEC rdsadmin.rdsadmin_master_util.create_archivelog_dir;
EXEC rdsadmin.rdsadmin_master_util.create_onlinelog_dir;
```

El siguiente código elimina los directorios de los archivos de registros REDO online y archivados.

```
EXEC rdsadmin.rdsadmin_master_util.drop_archivelog_dir;
EXEC rdsadmin.rdsadmin_master_util.drop_onlinelog_dir;
```

El código siguiente concede y revoca el privilegio `DROP ANY DIRECTORY`.

```
EXEC rdsadmin.rdsadmin_master_util.revoke_drop_any_directory;
EXEC rdsadmin.rdsadmin_master_util.grant_drop_any_directory;
```

Descargue registros de rehacer archivados de Amazon S3

Puede descargar registros de rehacer archivados en su instancia de base de datos con el paquete `rdsadmin.rdsadmin_archive_log_download`. Si los registros de rehacer archivados ya no están en su instancia de base de datos, es posible que desee descargarlos de nuevo desde Amazon S3. Después, puede extraer los registros o usarlos para recuperar o reproducir su base de datos.

> **Note**
>
> No se pueden descargar registros de recuperación de cambios archivados en instancias de réplica de lectura.

Descargue registros de rehacer archivados: pasos básicos

La disponibilidad de los registros de rehacer archivados depende de las siguientes políticas de retención:

- Política de retención de copias de seguridad: los registros dentro de esta política están disponibles en Amazon S3. Los registros fuera de esta política se eliminan.
- Política de retención de registros archivados: los registros dentro de esta política están disponibles en su instancia de base de datos. Los registros fuera de esta política se eliminan.

Si los registros no se encuentran en su instancia, pero están protegidos por el periodo de retención de copia de seguridad, puede usar `rdsadmin.rdsadmin_archive_log_download` para descargarlos nuevamente. RDS for Oracle guarda los registros en el directorio de `/rdsdbdata/log/arch` en la instancia de base de datos.

Para descargar registros de rehacer archivados de Amazon S3

1. Configure el período de retención para garantizar que los registros REDO archivados descargados se retengan durante el tiempo que los necesite. Asegúrese de `COMMIT` su cambio.

   RDS retiene los registros descargados de acuerdo con la política de retención de registros archivados, a partir del momento en que se descargaron los registros. Si quiere obtener información para configurar la política de retención, consulte Retención de los registros REDO archivados.

2. Espere hasta 5 minutos para que el cambio de la política de retención de registros archivados surta efecto.
3. Puede descargar registros de rehacer archivados de Amazon S3 mediante `rdsadmin.rdsadmin_archive_log_download`.

   Para obtener más información, consulte Descarga de un único registro de rehacer archivado y Descargue una serie de registros de rehacer archivados.

   > **Note**
   >
   > RDS comprueba automáticamente el almacenamiento disponible antes de descargar. Si los registros solicitados consumen un alto porcentaje de espacio, recibirá una alerta.

4. Confirme que los registros se descargaron correctamente de Amazon S3.

   Puede ver el estado de una tarea de descarga en un archivo bdump. Los archivos bdump tienen el nombre de ruta `/rdsdbdata/log/trace/dbtask-`*`task-id`*`.log`. En el paso de descarga anterior, ejecute una sentencia `SELECT` que devuelva el ID de tarea en un tipo de datos `VARCHAR2`. Para obtener más información, vea ejemplos similares en Monitoreo del estado de una transferencia de archivos.

Descarga de un único registro de rehacer archivado

Para descargar un único registro de rehacer archivado en el directorio de `/rdsdbdata/log/arch`, utilice `rdsadmin.rdsadmin_archive_log_download.download_log_with_seqnum`. Este procedimiento tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`seqnum`	número	—	Sí	El número secuencial del registro de rehacer archivado.

En el siguiente ejemplo, se descarga el registro con el número de secuencia 20.

```
SELECT rdsadmin.rdsadmin_archive_log_download.download_log_with_seqnum(seqnum => 20)
       AS TASK_ID
FROM   DUAL;
```

Descargue una serie de registros de rehacer archivados

Para descargar una serie de registros de rehacer archivados en el directorio de `/rdsdbdata/log/arch`, utilice `download_logs_in_seqnum_range`. La descarga está limitada a 300 registros por solicitud. El procedimiento `download_logs_in_seqnum_range` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`start_seq`	número	—	Sí	El número secuencial inicial para la serie.
`end_seq`	número	—	Sí	El número secuencial final para la serie.

En el siguiente ejemplo, se descargan los registros de la secuencia 50 a 100.

```
SELECT rdsadmin.rdsadmin_archive_log_download.download_logs_in_seqnum_range(start_seq
 => 50, end_seq => 100)
       AS TASK_ID
FROM   DUAL;
```

Realización de tareas RMAN comunes para instancias de base de datos de Oracle

En la siguiente sección, puede buscar cómo puede realizar tareas de DBA Oracle Recovery Manager (RMAN) en sus instancias de base de datos de Amazon RDS que ejecutan Oracle. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Puede utilizar el paquete de Amazon RDS `rdsadmin.rdsadmin_rman_util` para hacer copias de seguridad de RMAN de su base de datos de Amazon RDS para Oracle en disco. El paquete

`rdsadmin.rdsadmin_rman_util` admite copias de seguridad de archivos de bases de datos completas e incrementales, copias de seguridad de espacios de tabla y copias de seguridad de registros REDO.

Una vez finalizada la copia de seguridad de RMAN, puede copiar los archivos de copia de seguridad fuera del host de instancias de bases de datos de Amazon RDS for Oracle. Podría hacer esto con la finalidad de restaurar en un host que no sea de RDS host o para almacenamiento a largo plazo de almacenamiento. Por ejemplo, puede copiar los archivos de copia de seguridad en un bucket de Amazon S3. Para obtener más información, consulte el uso de Integración de Amazon S3.

Los archivos de copia de seguridad para copias de seguridad de RMAN permanecen en el host de instancias de bases de datos de Amazon RDS hasta que se eliminen manualmente. Puede utilizar el procedimiento `UTL_FILE.FREMOVE` de Oracle para eliminar archivos de un directorio. Para más información, consulte FREMOVE Procedure en la documentación de Oracle Database.

No puede utilizar el RMAN para restaurar instancias de base de datos de RDS para Oracle. Sin embargo, puede usar el RMAN para restaurar una copia de seguridad en una instancia en las instalaciones o de Amazon EC2. Para obtener más información, consulte el artículo del blog Restore an Amazon RDS for Oracle instance to a self-managed instance.

> **Note**
>
> Para hacer una copia de seguridad y restaurar en otra instancia de base de datos de Amazon RDS for Oracle, puede seguir usando las características de copia de seguridad y restauración de Amazon RDS. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

Temas

- Requisitos previos para las copias de seguridad de RMAN
- Parámetros comunes para procedimientos de RMAN
- Validación de archivos de base de datos en RDS para Oracle
- Activación y desactivación del seguimiento de cambio de bloques
- Comprobación cruzada de los registros REDO archivados
- Copia de seguridad de archivos de registro REDO
- Realización de una copia de seguridad completa de una base de datos

- Realización de una copia de seguridad completa de una base de datos de inquilinos
- Realización de una copia de seguridad incremental de una base de datos
- Realización de una copia de seguridad incremental de una base de datos de inquilinos
- Copia de seguridad de un espacio de tablas
- Copia de seguridad de un archivo de control
- Realización de la recuperación de medios en bloque

Requisitos previos para las copias de seguridad de RMAN

Antes de realizar una copia de seguridad de la base de datos mediante el paquete `rdsadmin.rdsadmin_rman_util`, asegúrese de cumplir los siguientes requisitos previos:

- Asegúrese de que su base de datos de RDS para Oracle esté en modo `ARCHIVELOG`. Para habilitar este modo, establezca el período de retención de la copia de seguridad en un valor distinto de cero.
- Al hacer copias de seguridad de registros REDO archivados o realizar una copia de seguridad completa o incremental que incluya registros REDO archivados y al hacer copias de seguridad de la base de datos, asegúrese de que la retención de registros REDO esté establecida en un valor distinto de cero. Los registros REDO archivados son necesarios para lograr la coherencia de los archivos de la base de datos durante la recuperación. Para obtener más información, consulte Retención de los registros REDO archivados.
- Asegúrese de que la instancia de base de datos tenga suficiente espacio libre para guardar las copias de seguridad. Cuando realiza una copia de seguridad de la base de datos, especifica un objeto de directorio de Oracle como un parámetro en la llamada al procedimiento. RMAN coloca los archivos en el directorio especificado. Puede utilizar los directorios predeterminados, como `DATA_PUMP_DIR` o crear un nuevo directorio. Para obtener más información, consulte Creación y eliminación de directorios en el espacio de almacenamiento de datos principal.

  Puede supervisar el espacio libre actual en una instancia de RDS para Oracle mediante la métrica de CloudWatch `FreeStorageSpace`. Se recomienda que el espacio libre supere el tamaño actual de la base de datos, aunque RMAN solo realiza copias de seguridad de bloques formateados y admite compresión.

Parámetros comunes para procedimientos de RMAN

Puede usar procedimientos del paquete de Amazon RDS `rdsadmin.rdsadmin_rman_util` para realizar tareas con RMAN. Varios parámetros son comunes en los procedimientos del paquete. El paquete tiene los siguientes parámetros comunes.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_directory_name`	varchar	Un nombre de directorio de base de datos válido.	—	Sí	El nombre del directorio que contendrá los archivos de copia de seguridad.
`p_label`	varchar	`a-z`, `A-Z`, `0-9`, `'_'`, `'-'`, `'.'`	—	No	Una cadena única que se incluye en los nombres de archivos de copia de seguridad. **Note** El límite es 30 caracteres.
`p_owner`	varchar	Un propietario válido del directorio especificado en `p_directory_name` .	—	Sí	El propietario del directorio que contendrá los archivos de copia de seguridad.
`p_tag`	varchar	`a-z`, `A-Z`, `0-9`, `'_'`, `'-'`, `'.'`	NULL	No	Una cadena que se puede usar para distinguir entre las copias de seguridad para indicar el propósito o el uso de las copias de seguridad, como las copias

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
					de seguridad diarias, semanales o de nivel incremental. El límite es 30 caracteres. La etiqueta no distingue entre mayúsculas y minúsculas. Las etiquetas siempre se guardan en mayúsculas, independientemente de cómo se hayan introducido. Las etiquetas no tienen que ser únicas, por lo que varias copias de seguridad pueden tener la misma etiqueta. Si no se especifica una etiqueta, RMAN asigna de forma automática una etiqueta predeterminada con el formato `TAG`*`YYYYMMDDTHHMMSS`*, donde *`YYYY`* es el año, *`MM`* es el mes, *`DD`* es el día, *`HH`* es la hora (en formato de 24 horas), *`MM`* son los minutos y *`SS`* son los segundos La fecha y la hora se refieren al momento en que RMAN inició la copia de seguridad. Por ejemplo, una copia de seguridad podría recibir una etiqueta `TAG20190927T214517` para una copia de seguridad iniciada el 27-09-2019 a las 21:45:17. El parámetro `p_tag` es compatible con las siguientes versiones del motor para

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
					bases de datos de Amazon RDS for Oracle: • Oracle Database 21c (21.0.0) • Base de datos Oracle 19c (19.0.0), que usa 19.0.0.0.ru-2021-10.rur-2021-10.r1 o versiones posteriores
p_compress	boolean	TRUE, FALSE	FALSE	No	Especifique TRUE para activar la compresión de copia de seguridad BÁSICA. Especifique FALSE para desactivar la compresión de copia de seguridad BÁSICA.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_include_archive_logs	boolean	TRUE, FALSE	FALSE	No	Especifique TRUE para incluir los registros REDO archivados en la copia de seguridad. Especifique FALSE para excluir los registros REDO archivados de la copia de seguridad. Si incluye los registros REDO archivados en la copia de seguridad, establezca la retención en una hora o más utilizando el procedimiento rdsadmin.rdsadmin_util.set_configuration. Asimismo, llame al procedimiento rdsadmin.rdsadmin_rman_util.crosscheck_archivelog inmediatamente antes de ejecutar la copia de seguridad. De lo contrario, podría producirse un error en la copia de seguridad debido a que faltan archivos REDO archivados que se han eliminado mediante los procedimientos de administración de Amazon RDS.
p_include_controlfile	boolean	TRUE, FALSE	FALSE	No	Especifique TRUE para incluir el archivo de control en la copia de seguridad. Especifique FALSE para excluir el archivo de control de la copia de seguridad.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_optimize	boolean	TRUE, FALSE	TRUE	No	Especifique TRUE para activar la optimización de copia de seguridad, si se incluyen los registros REDO archivados, para reducir el tamaño de la copia de seguridad. Especifique FALSE para desactivar la optimización de las copias de seguridad.
p_parallel	número	Un entero válido entre 1 y 254 para Oracle Database Enterprise Edition (EE) 1 para otras ediciones de Oracle Database	1	No	Número de canales.
p_rman_to_dbms_output	boolean	TRUE, FALSE	FALSE	No	Si es TRUE, la salida RMAN se envía al paquete DBMS_OUTPUT además de al archivo del directorio BDUMP. En SQL*Plus, use SET SERVEROUTPUT ON para ver la salida. Si es FALSE, la salida RMAN solo se envía a un archivo del directorio BDUMP.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_section_size_mb	número	Un entero válido	NULL	No	Tamaño de la sección en megabytes (MB). Se valida en paralelo dividiendo cada archivo en el tamaño de sección especificado. Si es NULL, se omite el parámetro.
p_validation_type	varchar	'PHYSICAL', 'PHYSICAL+LOGICAL'	'PHYS'	No	Nivel de detección de algún tipo de daño. Especifique 'PHYSICAL' para comprobar si hay daños físicos. Un ejemplo de daño físico es un bloque con una coincidencia en el encabezado y en el pie de página. Especifique 'PHYSICAL+LOGICAL' para comprobar si existen inconsistencias lógicas además del daño físico. Un ejemplo de daño lógico es un bloque dañado.

Validación de archivos de base de datos en RDS para Oracle

Puede utilizar el paquete `rdsadmin.rdsadmin_rman_util` de Amazon RDS para validar los archivos de base de datos de Amazon RDS para Oracle, como archivos de datos, tablespaces, archivos de control y archivos de parámetros de servidor (SPFILE).

Para obtener más información sobre la validación RMAN, consulte Validating Database Files and Backups y VALIDATE en la documentación de Oracle.

Temas

- Validación de una base de datos
- Validación de una base de datos de inquilinos
- Validación de un espacio de tabla
- Validación de un archivo de control
- Validación de un SPFILE
- Validación de un archivo de datos de Oracle

Validación de una base de datos

Para validar todos los archivos relevantes utilizados por una base de datos de Oracle en RDS for Oracle, utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_database`.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

El siguiente ejemplo valida la base de datos utilizando los valores predeterminados para los parámetros.

```
EXEC rdsadmin.rdsadmin_rman_util.validate_database;
```

El siguiente ejemplo valida la base de datos utilizando los valores especificados para los parámetros.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.validate_database(
        p_validation_type     => 'PHYSICAL+LOGICAL',
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_rman_to_dbms_output => FALSE);
END;
```

```
/
```

Si el parámetro `p_rman_to_dbms_output` se define como `FALSE`, la salida RMAN se escribe en un archivo del directorio `BDUMP`.

Para ver los archivos del directorio `BDUMP`, ejecute la siguiente instrucción `SELECT`.

```
SELECT * FROM table(rdsadmin.rds_file_util.listdir('BDUMP')) order by mtime;
```

Para ver los contenidos de un archivo del directorio `BDUMP`, ejecute la siguiente instrucción `SELECT`.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','rds-rman-validate-nnn.txt'));
```

Reemplace el nombre de archivo por el nombre del archivo que quiere visualizar.

Validación de una base de datos de inquilinos

Para validar los archivos de datos de la base de datos del inquilino en una base de datos de contenedor (CDB), utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_rman_util.validate_tenant`.

Este procedimiento solo se aplica a la base de datos del inquilino actual y utiliza los siguientes parámetros comunes para las tareas de RMAN:

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN. Este procedimiento es compatible con las siguientes versiones del motor de base de datos:

- Oracle Database 21c (21.0.0) CDB
- Oracle Database 19c (19.0.0) CDB

El siguiente ejemplo valida la base de datos de inquilinos actual utilizando los valores especificados para los parámetros.

```
EXEC rdsadmin.rdsadmin_rman_util.validate_tenant;
```

El siguiente ejemplo valida la base de datos de inquilinos actual utilizando los valores especificados para los parámetros.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.validate_tenant(
        p_validation_type     => 'PHYSICAL+LOGICAL',
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Si el parámetro `p_rman_to_dbms_output` se define como `FALSE`, la salida RMAN se escribe en un archivo del directorio BDUMP.

Para ver los archivos del directorio BDUMP, ejecute la siguiente instrucción `SELECT`.

```
SELECT * FROM table(rdsadmin.rds_file_util.listdir('BDUMP')) order by mtime;
```

Para ver los contenidos de un archivo del directorio BDUMP, ejecute la siguiente instrucción `SELECT`.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','rds-rman-
validate-nnn.txt'));
```

Reemplace el nombre de archivo por el nombre del archivo que quiere visualizar.

Validación de un espacio de tabla

Utilice el procedimiento de Amazon RDS para validar los archivos asociados a un espacio de tabl `rdsadmin.rdsadmin_rman_util.validate_tablespace`.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_tablespace_name`	varchar2	Nombre de un espacio de tabla válido	—	Sí	Nombre del espacio de tabla.

Validación de un archivo de control

Utilice el procedimiento `rdsadmin.rdsadmin_rman_util.validate_current_controlfile` de Amazon RDS para validar únicamente el archivo de control utilizado por una instancia de base de datos de Oracle en Amazon RDS.

Este procedimiento utiliza el siguiente parámetro común para tareas de RMAN:

- `p_validation_type`
- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Validación de un SPFILE

Utilice el procedimiento `rdsadmin.rdsadmin_rman_util.validate_spfile` de Amazon RDS para validar únicamente el archivo de parámetros de servidor (SPFILE) utilizado por una instancia de base de datos de Oracle en Amazon RDS.

Este procedimiento utiliza el siguiente parámetro común para tareas de RMAN:

- `p_validation_type`
- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Validación de un archivo de datos de Oracle

Utilice el procedimiento de Amazon RDS para validar un archivo de dato `rdsadmin.rdsadmin_rman_util.validate_datafile`.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_validation_type`
- `p_parallel`
- `p_section_size_mb`
- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_datafile`	varchar2	Un número de ID de archivo de datos válido o un nombre de archivo de datos válido, incluida su ruta completa	—	Sí	Número de ID del archivo de datos (de v `$datafile.file#`) o el nombre completo del archivo de datos, incluida su ruta (de v `$datafile.name`).

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_from_block	número	Un entero válido	NULL	No	Número del bloque donde se inicia la validación dentro del archivo de datos. Si esNULL, se utiliza 1.
p_to_block	número	Un entero válido	NULL	No	Número del bloque donde se inicia el fin de la validación dentro del archivo de datos. Si es NULL, se utiliza el bloque máximo del archivo de datos.

Activación y desactivación del seguimiento de cambio de bloques

Bloquear los registros del seguimiento de cambio de bloques cambió los bloques de un archivo de seguimiento. Esta técnica puede mejorar el rendimiento de las copias de seguridad RMAN incrementales. Para obtener más información, consulte Uso del seguimiento de cambio de bloque para aumentar el rendimiento de las copias de seguridad incrementales, en la Documentación de la base de datos de Oracle.

Las características de RMAN no se admiten en una réplica de lectura. Sin embargo, como parte de su estrategia de alta disponibilidad, podría optar por habilitar el seguimiento de cambios de bloques en una réplica de solo lectura mediante el procedimiento `rdsadmin.rdsadmin_rman_util.enable_block_change_tracking`. Si promueve esta réplica de solo lectura a una instancia de base de datos de origen, se habilita el seguimiento de cambio de bloques para la nueva instancia de origen. De este modo, su instancia puede beneficiarse de copias de seguridad incrementales rápidas.

Los procedimientos de seguimiento de cambio de bloques son compatibles en la Enterprise Edition solo para las siguientes versiones del motor de base de datos:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

> **Note**
>
> En un CDB de un solo propietario, funcionan las siguientes operaciones, pero ningún mecanismo visible por el cliente puede detectar el estado actual de las operaciones. Véase también Limitaciones de las CDB de RDS para Oracle.

Puede activar el seguimiento de cambio de bloques de una instancia de base de datos utilizando el procedimiento `rdsadmin.rdsadmin_rman_util.enable_block_change_tracking` de Amazon RDS. Para desactivar el seguimiento de cambio de bloques, utilice `disable_block_change_tracking`. Estos procedimientos no tienen ningún parámetro.

Para determinar si el seguimiento de cambios de bloques está activado para su instancia de base de datos, ejecute la siguiente consulta.

```
SELECT STATUS, FILENAME FROM V$BLOCK_CHANGE_TRACKING;
```

El siguiente ejemplo activa el seguimiento de cambios de bloque para una instancia de base de datos.

```
EXEC rdsadmin.rdsadmin_rman_util.enable_block_change_tracking;
```

El siguiente ejemplo desactiva el seguimiento de cambios de bloque para una instancia de DB.

```
EXEC rdsadmin.rdsadmin_rman_util.disable_block_change_tracking;
```

Comprobación cruzada de los registros REDO archivados

Puede hacer una comprobación cruzada de registros REDO archivados utilizando el procedimiento de Amazon RDS`rdsadmin.rdsadmin_rman_util.crosscheck_archivelog`.

Puede usar este procedimiento para hacer la comprobación cruzada de los registros REDO archivados en el archivo de control y, opcionalmente, eliminar los registros caducados. Cuando RMAN realiza una copia de seguridad, crea un registro en el archivo de control. Con el tiempo, estos

registros aumentan el tamaño del archivo de control. Le recomendamos que elimine los registros caducados periódicamente.

> **Note**
>
> Las copias estándar de Amazon RDS no utilizan RMAN y, por tanto, no crean registros en el archivo de control.

este procedimiento utiliza el parámetro común `p_rman_to_dbms_output` para tareas de RMAN.

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_delete_expired`	booleano	`TRUE`, `FALSE`	`TRUE`	No	Si es `TRUE`, elimina los registros REDO archivados caducados del archivo de control. Si es `FALSE`, retiene los registros REDO archivados en el archivo de control.

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

En el ejemplo siguiente se marcan registros redo log archivados en el archivo de control como caducados, pero no se eliminan los registros.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.crosscheck_archivelog(
        p_delete_expired      => FALSE,
        p_rman_to_dbms_output => FALSE);
END;
/
```

El siguiente ejemplo elimina registros REDO archivados caducados del archivo de control.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.crosscheck_archivelog(
        p_delete_expired      => TRUE,
        p_rman_to_dbms_output => FALSE);
END;
/
```

Copia de seguridad de archivos de registro REDO

Puede utilizar el paquete `rdsadmin.rdsadmin_rman_util` de Amazon RDS para hacer una copia de seguridad de los registros REDO archivados de una instancia de base de datos de Amazon RDS Oracle.

Los procedimientos para hacer copias de seguridad de registros REDO archivados son compatibles con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

Temas

- Copia de seguridad de todos los registros REDO archivados
- Copia de seguridad de un registro REDO archivado a partir de un intervalo de fechas
- Copia de seguridad de un registro REDO archivado a partir de un intervalo de SCN
- Copia de seguridad de un registro REDO archivado a partir de un intervalo de números secuenciales

Copia de seguridad de todos los registros REDO archivados

Utilice el procedimiento `rdsadmin.rdsadmin_rman_util.backup_archivelog_all` de Amazon RDS para hacer una copia de seguridad de todos los registros REDO archivados de una instancia de base de datos de Oracle en Amazon RDS.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

El siguiente ejemplo hace una copia de seguridad de todos los registros REDO archivados para la instancia de base de datos.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_all(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_parallel            => 4,
        p_tag                 => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Copia de seguridad de un registro REDO archivado a partir de un intervalo de fechas

Utilice el procedimiento `rdsadmin.rdsadmin_rman_util.backup_archivelog_date` de Amazon RDS para hacer una copia de seguridad de registros REDO archivados específicos de una instancia de base de datos de Oracle en Amazon RDS. El intervalo de fechas especifica los registros REDO archivados de los que se va a hacer una copia de seguridad.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_from_date`	date	Una fecha que se encuentra entre la `start_date` y la `next_date` de un registro REDO archivado que existe en el disco. El valor debe ser menor o	—	Sí	La fecha inicial de las copias de seguridad de registros archivados.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
		igual que el valor especificado para `p_to_date` .			
`p_to_date`	date	Una fecha que se encuentra entre la `start_date` y la `next_date` de un registro REDO archivado que existe en el disco. El valor debe ser mayor o igual que el valor especificado para `p_from_date` .	—	Sí	La fecha final de las copias de seguridad de registros archivados.

El siguiente ejemplo hace una copia de seguridad de todos los registros REDO archivados en el intervalo de fechas para la instancia de base de datos.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_date(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_from_date           => '03/01/2019 00:00:00',
        p_to_date             => '03/02/2019 00:00:00',
        p_parallel            => 4,
        p_tag                 => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Copia de seguridad de un registro REDO archivado a partir de un intervalo de SCN

Utilice el procedimiento de Amazon RDS para hacer una copia de seguridad de registros REDO archivados específicos de una instancia de base de datos de Oracle en Amazon RDS mediante la especificación de un intervalo de números de cambio del sistema (SCN `rdsadmin.rdsadmin_rman_util.backup_archivelog_scn`. El intervalo de SCN especifica qué registros REDO archivados incluir en la copia de seguridad.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_from_scn`	número	Un SCN de un registro REDO archivado que existe en el disco. El valor debe ser menor o igual que el valor especificado para `p_to_scn`.	—	Sí	El SCN inicial para las copias de seguridad de registros archivados.
`p_to_scn`	número	Un SCN de un registro REDO archivado que existe en el disco. El valor debe ser mayor o igual que el valor especificado para	—	Sí	El SCN final para las copias de seguridad de registros archivados.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
		p_from_scn .			

El siguiente ejemplo hace copia de seguridad de los registros REDO archivados en el intervalo de SCN para la instancia de base de datos.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_scn(
        p_owner                => 'SYS',
        p_directory_name       => 'MYDIRECTORY',
        p_from_scn             => 1533835,
        p_to_scn               => 1892447,
        p_parallel             => 4,
        p_tag                  => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Copia de seguridad de un registro REDO archivado a partir de un intervalo de números secuenciales

Utilice el procedimiento de Amazon RDS para hacer una copia de seguridad de registros REDO archivados específicos de una instancia de base de datos de Oracle en Amazon RDS mediante la especificación de un intervalo de números secuenciale `rdsadmin.rdsadmin_rman_util.backup_archivelog_sequence`. El intervalo de números secuenciales especifica qué registros REDO archivados incluir en la copia de seguridad.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_compress`

- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_from_sequence`	número	Un número secuencial de un registro REDO archivado que existe en el disco. El valor debe ser menor o igual que el valor especificado para `p_to_sequence` .	—	Sí	El número secuencial inicial para las copias de seguridad de registros archivados.
`p_to_sequence`	número	Un número secuencial de un registro REDO	—	Sí	El número secuencial final para las copias de seguridad de registros archivados.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
		archivado que existe en el disco. El valor debe ser mayor o igual que el valor especificado para p_from_sequence .			

El siguiente ejemplo hace copia de seguridad de los registros REDO archivados en el intervalo de número secuenciales para la instancia de base de datos.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_archivelog_sequence(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_from_sequence       => 11160,
        p_to_sequence         => 11160,
        p_parallel            => 4,
        p_tag                 => 'MY_LOG_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Realización de una copia de seguridad completa de una base de datos

Puede realizar una copia de seguridad de todos los bloques de archivos de datos incluidos en la copia de seguridad utilizando el procedimiento `rdsadmin.rdsadmin_rman_util.backup_database_full` de Amazon RDS.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- p_owner
- p_directory_name
- p_label
- p_parallel
- p_section_size_mb
- p_include_archive_logs
- p_optimize
- p_compress
- p_rman_to_dbms_output
- p_tag

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

El siguiente ejemplo realiza una copia de seguridad completa de la instancia de base de datos mediante el uso de valores específicos para los parámetros:

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_database_full(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_tag                 => 'FULL_DB_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Realización de una copia de seguridad completa de una base de datos de inquilinos

Puede realizar una copia de seguridad de todos los bloques de datos incluidos una base de datos de inquilinos en una base de datos de contenedores (CDB). Utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_tenant_full`. Este procedimiento solo se aplica a la copia de seguridad de la base de datos actual y utiliza los siguientes parámetros comunes para las tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_section_size_mb`
- `p_include_archive_logs`
- `p_optimize`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

El procedimiento `rdsadmin_rman_util.backup_tenant_full` es compatible con las siguientes versiones del motor para bases de datos de RDS for Oracle:

- Oracle Database 21c (21.0.0) CDB
- Oracle Database 19c (19.0.0) CDB

El siguiente ejemplo realiza una copia de seguridad completa de la base de datos del inquilino actual utilizando los valores especificados para los parámetros.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_tenant_full(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_parallel            => 4,
        p_section_size_mb     => 10,
```

```
        p_tag                 => 'FULL_TENANT_DB_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Realización de una copia de seguridad incremental de una base de datos

Puede realizar una copia de seguridad incremental de una instancia de base de datos utilizando el procedimiento `rdsadmin.rdsadmin_rman_util.backup_database_incremental` de Amazon RDS.

Para obtener información adicional sobre las copias de seguridad incrementales, consulte Incremental Backups en la documentación de Oracle.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_section_size_mb`
- `p_include_archive_logs`
- `p_include_controlfile`
- `p_optimize`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_level	número	0, 1	0	No	Especifique 0 para activar una copia de seguridad incremental completa. Especifique 1 para activar una copia de seguridad incremental no acumulativa.

El siguiente ejemplo realiza una copia de seguridad incremental de la instancia de base de datos mediante el uso de valores específicos para los parámetros:

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_database_incremental(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_level               => 1,
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_tag                 => 'MY_INCREMENTAL_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Realización de una copia de seguridad incremental de una base de datos de inquilinos

Puede realizar una copia de seguridad incremental de la base de datos del inquilino actual en su CDB. Utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_rman_util.backup_tenant_incremental`.

Para obtener información adicional sobre las copias de seguridad incrementales, consulte Incremental Backups en la documentación de Oracle Database.

Este procedimiento solo se aplica a la base de datos del inquilino actual y utiliza los siguientes parámetros comunes para las tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_section_size_mb`
- `p_include_archive_logs`
- `p_include_controlfile`
- `p_optimize`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0) CDB
- Oracle Database 19c (19.0.0) CDB

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_level`	número	`0`, `1`	`0`	No	Especifique `0` para activar una copia de seguridad incremental completa.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
					Especifique 1 para activar una copia de seguridad incremental no acumulativa.

El siguiente ejemplo realiza una copia de seguridad incremental de la base de datos del inquilino actual utilizando los valores especificados para los parámetros.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_tenant_incremental(
        p_owner                => 'SYS',
        p_directory_name       => 'MYDIRECTORY',
        p_level                => 1,
        p_parallel             => 4,
        p_section_size_mb      => 10,
        p_tag                  => 'MY_INCREMENTAL_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Copia de seguridad de un espacio de tablas

Puede realizar una copia de seguridad de un espacio de tablas mediante el procedimiento `rdsadmin.rdsadmin_rman_util.backup_tablespace` de Amazon RDS.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_parallel`
- `p_section_size_mb`
- `p_include_archive_logs`
- `p_include_controlfile`

- p_optimize
- p_compress
- p_rman_to_dbms_output
- p_tag

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento también utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_tablespace_name	varchar2	Nombre de un espacio de tabla válido.	—	Sí	Nombre del espacio de tabla para la copia de seguridad.

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

El siguiente ejemplo realiza una copia de seguridad del espacio de tabla mediante el uso de valores específicos para los parámetros:

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_tablespace(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_tablespace_name     => 'MYTABLESPACE',
        p_parallel            => 4,
        p_section_size_mb     => 10,
        p_tag                 => 'MYTABLESPACE_BACKUP',
```

```
        p_rman_to_dbms_output => FALSE);
END;
/
```

Copia de seguridad de un archivo de control

Puede realizar una copia de seguridad de un archivo de control mediante el procedimiento `rdsadmin.rdsadmin_rman_util.backup_current_controlfile` de Amazon RDS.

Este procedimiento utiliza los siguientes parámetros comunes para tareas de RMAN:

- `p_owner`
- `p_directory_name`
- `p_label`
- `p_compress`
- `p_rman_to_dbms_output`
- `p_tag`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

El siguiente ejemplo realiza una copia de seguridad de un archivo de control con los valores especificados para los parámetros.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.backup_current_controlfile(
        p_owner               => 'SYS',
        p_directory_name      => 'MYDIRECTORY',
        p_tag                 => 'CONTROL_FILE_BACKUP',
        p_rman_to_dbms_output => FALSE);
END;
/
```

Realización de la recuperación de medios en bloque

Puede recuperar bloques de datos individuales, lo que se conoce como recuperación de medios en bloque, mediante los procedimientos `rdsadmin.rdsadmin_rman_util.recover_datafile_block` de Amazon RDS. Puede utilizar este procedimiento sobrecargado para recuperar un bloque de datos individual o un rango de bloques de datos.

Este procedimiento utiliza el siguiente parámetro común para tareas de RMAN:

- `p_rman_to_dbms_output`

Para obtener más información, consulte Parámetros comunes para procedimientos de RMAN.

Este procedimiento utiliza los siguientes parámetros adicionales.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`p_datafile`	`NUMBER`	Un número de ID de archivo de datos válido.	—	Sí	El archivo de datos que contiene los bloques corruptos. Especifique el archivo de datos de cualquiera de las siguientes maneras: • El número de ID del archivo de datos, que se encuentra en `V$DATAFILE.FILE#` • El nombre completo del archivo de datos, incluida la ruta, ubicado en `V$DATAFILE.NAME`

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_block	NUMBER	Un número entero válido.	—	Sí	El número de un bloque individual que se va a recuperar. Los siguientes parámetros son mutuamente excluyentes. • p_block • p_from_block y p_to_block
p_from_block	NUMBER	Un número entero válido.	—	Sí	El primer número de bloque de un rango de bloques que se van a recuperar. Los siguientes parámetros son mutuamente excluyentes. • p_block • p_from_block y p_to_block

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
p_to_block	NUMBER	Un número entero válido.	—	Sí	El último número de bloque de un rango de bloques que se van a recuperar. Los siguientes parámetros son mutuamente excluyentes. • p_block • p_from_block y p_to_block

Este procedimiento es compatible con las siguientes versiones de motores de bases de datos de Amazon RDS for Oracle:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

El siguiente ejemplo recupera el bloque 100 del archivo de datos 5.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.recover_datafile_block(
        p_datafile            => 5,
        p_block               => 100,
        p_rman_to_dbms_output => TRUE);
END;
/
```

El siguiente ejemplo recupera los bloques del 100 al 150 del archivo de datos 5.

```
BEGIN
    rdsadmin.rdsadmin_rman_util.recover_datafile_block(
        p_datafile            => 5,
```

```
        p_from_block          => 100,
        p_to_block            => 150,
        p_rman_to_dbms_output => TRUE);
END;
/
```

Realización de tareas de programación comunes para instancias de base de datos de Oracle

Algunos trabajos del programador que pertenece a SYS pueden interferir con las operaciones normales de la base de datos. En estos casos, Oracle Support recomienda modificar la programación. Si necesita habilitar o deshabilitar los trabajos SYS, pruebe la operación en los trabajos programados en un entorno de prueba antes de implementarla en un entorno de producción. Puede utilizar el paquete `rdsadmin.rdsadmin_dbms_scheduler` de Amazon RDS para realizar tareas de los trabajos del Programador de Oracle que es propiedad de SYS.

Los procedimientos `rdsadmin.rdsadmin_dbms_scheduler` son compatibles con las versiones de motores de bases de datos de Amazon RDS para Oracle que aparecen en la siguiente tabla. Al utilizar este paquete, puede especificar los trabajos SYS que aparecen en la tabla.

Versión de base de datos	Trabajos habilitados de forma predeterminada	Trabajos deshabilitados de forma predeterminada
Oracle Database 19c	BSLN_MAINTAIN_STATS_JOB CLEANUP_NON_EXIST_OBJ CLEANUP_ONLINE_IND_BUILD CLEANUP_ONLINE_PMO CLEANUP_TAB_IOT_PMO CLEANUP_TRANSIENT_PKG CLEANUP_TRANSIENT_TYPE DRA_REEVALUATE_OPEN_FAILURES FILE_SIZE_UPD ORA$AUTOTASK_CLEAN PMO_DEFERRED_GIDX_MAINT_JOB PURGE_LOG RSE$CLEAN_RECOVERABLE_SCRIPT	FGR$AUTOPURGE_JOB FILE_WATCHER HM_CREATE_OFFLINE_DICTIONARY LOAD_OPATCH_INVENTORY ORA$PREPLUGIN_BACKUP_JOB XMLDB_NFS_CLEANUP_JOB

Versión de base de datos	Trabajos habilitados de forma predeterminada	Trabajos deshabilitados de forma predeterminada
	SM$CLEAN_AUTO_SPLIT_MERGE	
Oracle Database 21c	BSLN_MAINTAIN_STATS_JOB CLEANUP_NON_EXIST_OBJ CLEANUP_ONLINE_IND_BUILD CLEANUP_ONLINE_PMO CLEANUP_TAB_IOT_PMO CLEANUP_TRANSIENT_PKG CLEANUP_TRANSIENT_TYPE DRA_REEVALUATE_OPEN_FAILURES FILE_SIZE_UPD ORA$AUTOTASK_CLEAN PMO_DEFERRED_GIDX_MAINT_JOB PURGE_LOG	FGR$AUTOPURGE_JOB FILE_WATCHER HM_CREATE_OFFLINE_DICTIONARY LOAD_OPATCH_INVENTORY ORA$PREPLUGIN_BACKUP_JOB ORA$_ATSK_AUTOSTS XMLDB_NFS_CLEANUP_JOB

Parámetros comunes para los procedimientos del programador de Oracle

Utilice los procedimientos del paquete de Amazon RDS para realizar tareas con el programador de Oracl `rdsadmin.rdsadmin_dbms_scheduler`. Varios parámetros son comunes en los procedimientos del paquete. El paquete tiene los siguientes parámetros comunes.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`name`	varchar2	Los procedimientos enumerados en la tabla de Realización de	—	Sí	El nombre del trabajo que se va a modificar.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
		tareas de programación comunes para instancias de base de datos de Oracle			
`attribute`	varchar2	`'REPEAT_INTERVAL'` `_NAME'`	–	Sí	El atributo que se va a modificar. Especifique para modificar el intervalo de repetición del trabaj `'REPEAT_INTERVAL'` . Especifique para modificar el nombre de programación del trabaj `'SCHEDULE_NAME'` .

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`value`	varchar2	Un nombre de programación o intervalo de programación válidos, en función del atributo utilizado.	–	Sí	El nuevo valor del atributo.

Modificación de trabajos DBMS_SCHEDULER

Puede utilizar el procedimiento `dbms_scheduler.set_attribute` de Oracle para modificar determinados componentes de Oracle Scheduler. Para obtener más información, consulte DBMS_SCHEDULER y SET_ATTRIBUTE Procedure en la documentación de Oracle.

Cuando trabaje con instancias de bases de datos de Amazon RDS, anteponga el nombre del esquema SYS al nombre del objeto. En el siguiente ejemplo se establece el atributo RESOURCE_PLAN para el objeto MONDAY_WINDOW.

```
BEGIN
    DBMS_SCHEDULER.SET_ATTRIBUTE(
        name      => 'SYS.MONDAY_WINDOW',
        attribute => 'RESOURCE_PLAN',
        value     => 'resource_plan_1');
END;
/
```

Modificar las ventanas de mantenimiento de AutoTask

Las instancias de Amazon RDS for Oracle se crean con la configuración predeterminada de las ventanas de mantenimiento. Las tareas de mantenimiento automatizadas, como la recopilación de estadísticas del optimizador, se ejecutan durante estas ventanas. De forma predeterminada, las ventanas de mantenimiento activan Administrador de recursos de la base de datos de Oracle.

Para modificar la ventana, utilice el paquete `DBMS_SCHEDULER`. Es posible que tenga que modificar la configuración de la ventana de mantenimiento por las siguientes razones:

- Desea que los trabajos de mantenimiento se ejecuten en un momento diferente, con configuraciones diferentes o que no se ejecuten en absoluto. Por ejemplo, puede que desee modificar la duración de la ventana o cambiar el tiempo y el intervalo de repetición.
- Desea evitar el impacto en el rendimiento de habilitar el Administrador de Recursos durante el mantenimiento. Por ejemplo, si se especifica el plan de mantenimiento predeterminado y si la ventana de mantenimiento se abre mientras la base de datos está bajo carga, es posible que vea eventos de espera como `resmgr:cpu quantum`. Este evento de espera está relacionado con el Administrador de recursos de base de datos. Dispone de las opciones siguientes:
  - Asegúrese de que las ventanas de mantenimiento estén activas durante las horas de menor actividad de su instancia de base de datos.
  - Deshabilite el plan de mantenimiento predeterminado estableciendo el atributo `resource_plan` a una cadena vacía.
  - Establezca el parámetro `resource_manager_plan` en `FORCE:` en el grupo de parámetros. Si la instancia utiliza Enterprise Edition, esta configuración impide que se activen los planes del Administrador de recursos de base de datos.

Para modificar la configuración de la ventana de mantenimiento

1. Conexión a la base de datos mediante un cliente de Oracle SQL.
2. Consulte la configuración actual para una ventana del programador.

   En el siguiente ejemplo, se consulta la configuración de `MONDAY_WINDOW`.

   ```
   SELECT ENABLED, RESOURCE_PLAN, DURATION, REPEAT_INTERVAL
   FROM   DBA_SCHEDULER_WINDOWS
   WHERE  WINDOW_NAME='MONDAY_WINDOW';
   ```

El siguiente resultado muestra que la ventana está utilizando los valores predeterminados.

```
ENABLED         RESOURCE_PLAN                  DURATION         REPEAT_INTERVAL
--------------- ------------------------------ ---------------
 ------------------------------
TRUE            DEFAULT_MAINTENANCE_PLAN       +000 04:00:00
 freq=daily;byday=MON;byhour=22
                                                                 ;byminute=0;
 bysecond=0
```

3. Modifique la ventana mediante el paquete DBMS_SCHEDULER.

   En el siguiente ejemplo se establece el plan de recursos como nulo para que el Administrador de recursos no se ejecute durante la ventana de mantenimiento.

```
BEGIN
  -- disable the window to make changes
  DBMS_SCHEDULER.DISABLE(name=>'"SYS"."MONDAY_WINDOW"',force=>TRUE);

  -- specify the empty string to use no plan
  DBMS_SCHEDULER.SET_ATTRIBUTE(name=>'"SYS"."MONDAY_WINDOW"',
 attribute=>'RESOURCE_PLAN', value=>'');

  -- re-enable the window
  DBMS_SCHEDULER.ENABLE(name=>'"SYS"."MONDAY_WINDOW"');
END;
/
```

   En el siguiente ejemplo se establece la duración máxima de la ventana en 2 horas.

```
BEGIN
  DBMS_SCHEDULER.DISABLE(name=>'"SYS"."MONDAY_WINDOW"',force=>TRUE);
  DBMS_SCHEDULER.SET_ATTRIBUTE(name=>'"SYS"."MONDAY_WINDOW"',
 attribute=>'DURATION', value=>'0 2:00:00');
  DBMS_SCHEDULER.ENABLE(name=>'"SYS"."MONDAY_WINDOW"');
END;
/
```

   En el siguiente ejemplo se establece el intervalo de repetición en todos los lunes a las 10 AM.

```
BEGIN
```

```
  DBMS_SCHEDULER.DISABLE(name=>'"SYS"."MONDAY_WINDOW"',force=>TRUE);
  DBMS_SCHEDULER.SET_ATTRIBUTE(name=>'"SYS"."MONDAY_WINDOW"',
 attribute=>'REPEAT_INTERVAL',
 value=>'freq=daily;byday=MON;byhour=10;byminute=0;bysecond=0');
  DBMS_SCHEDULER.ENABLE(name=>'"SYS"."MONDAY_WINDOW"');
END;
/
```

Configuración de zona horaria para trabajos de Oracle Scheduler

Para modificar la zona horaria de Oracle Scheduler, puede utilizar el procedimiento de Oracle `dbms_scheduler.set_scheduler_attribute`. Para obtener más información sobre el paquete `dbms_scheduler`, consulte DBMS_SCHEDULER y SET_SCHEDULER_ATTRIBUTE en la documentación de Oracle.

Para modificar la configuración de zona horaria actual

1. Conéctese a la base de datos mediante un cliente como SQL Developer. Para obtener más información, consulte Conexión a la instancia de base de datos mediante Oracle SQL Developer.
2. Establezca la zona horaria predeterminada de la siguiente manera, sustituyendo su zona horaria por *time_zone_name*.

```
BEGIN
  DBMS_SCHEDULER.SET_SCHEDULER_ATTRIBUTE(
    attribute => 'default_timezone',
    value => 'time_zone_name'
  );
END;
/
```

En el siguiente ejemplo, debe cambiar la zona horaria a Asia/Shanghái.

Comience consultando la zona horaria actual, como se muestra a continuación.

```
SELECT VALUE FROM DBA_SCHEDULER_GLOBAL_ATTRIBUTE WHERE
 ATTRIBUTE_NAME='DEFAULT_TIMEZONE';
```

La salida muestra que la zona horaria actual es ETC/UTC.

```
VALUE
-------
Etc/UTC
```

A continuación, establece la zona horaria en Asia/Shanghái.

```
BEGIN
  DBMS_SCHEDULER.SET_SCHEDULER_ATTRIBUTE(
    attribute => 'default_timezone',
    value => 'Asia/Shanghai'
  );
END;
/
```

Para obtener más información sobre cómo cambiar la zona horaria del sistema, consulte Zona horaria Oracle.

Desactivación de los trabajos del programador de Oracle propiedad de SYS

Utilice el procedimiento `rdsadmin.rdsadmin_dbms_scheduler.disable` para desactivar un trabajo del programador de Oracle que pertenezca a SYS.

Este procedimiento utiliza el parámetro común `name` para las tareas del programador de Oracle. Para obtener más información, consulte Parámetros comunes para los procedimientos del programador de Oracle.

En el siguiente ejemplo se desactiva el trabajo del programador de Oracle `SYS.CLEANUP_ONLINE_IND_BUILD`.

```
BEGIN
   rdsadmin.rdsadmin_dbms_scheduler.disable('SYS.CLEANUP_ONLINE_IND_BUILD');
END;
/
```

Activación de los trabajos del programador de Oracle propiedad de SYS

Utilice el procedimiento `rdsadmin.rdsadmin_dbms_scheduler.enable` para activar un trabajo del programador de Oracle que pertenezca a SYS.

Este procedimiento utiliza el parámetro común `name` para las tareas del programador de Oracle. Para obtener más información, consulte Parámetros comunes para los procedimientos del programador de Oracle.

En el siguiente ejemplo se activa el trabajo del programador de Oracle `SYS.CLEANUP_ONLINE_IND_BUILD`.

```
BEGIN
   rdsadmin.rdsadmin_dbms_scheduler.enable('SYS.CLEANUP_ONLINE_IND_BUILD');
END;
/
```

Modificación del intervalo de repetición del programador de Oracle para los trabajos del tipo CALENDAR

Utilice el procedimiento `CALENDAR` para modificar el intervalo de repetición de un trabajo del programador de Oracle que pertenece a SYS del tipo `rdsadmin.rdsadmin_dbms_scheduler.disable`.

Este procedimiento utiliza los siguientes parámetros comunes para las tareas del programador de Oracle:

- `name`
- `attribute`
- `value`

Para obtener más información, consulte Parámetros comunes para los procedimientos del programador de Oracle.

En el siguiente ejemplo se modifica el intervalo de repetición del trabajo del programador de Oracle `SYS.CLEANUP_ONLINE_IND_BUILD`.

```
BEGIN
     rdsadmin.rdsadmin_dbms_scheduler.set_attribute(
          name      => 'SYS.CLEANUP_ONLINE_IND_BUILD',
          attribute => 'repeat_interval',
          value     => 'freq=daily;byday=FRI,SAT;byhour=20;byminute=0;bysecond=0');
END;
```

```
/
```

Modificación del intervalo de repetición del programador de Oracle para los trabajos del tipo NAMED

Algunos trabajos del programador de Oracle utilizan un nombre de programación en lugar de un intervalo. Debe crear una nueva programación NAMED en el esquema de usuario principal para este tipo de trabajos. Para ello, utilice el procedimiento estándar de Oracle `sys.dbms_scheduler.create_schedule`. Además, utilice el `rdsadmin.rdsadmin_dbms_scheduler.set_attribute procedure` para asignar la nueva programación con nombre asignado al trabajo.

Este procedimiento utiliza los siguientes parámetros comunes para las tareas del programador de Oracle:

- `name`
- `attribute`
- `value`

Para obtener más información, consulte Parámetros comunes para los procedimientos del programador de Oracle.

En el siguiente ejemplo se modifica el intervalo de repetición del trabajo del programador de Oracle `SYS.BSLN_MAINTAIN_STATS_JOB`.

```
BEGIN
     DBMS_SCHEDULER.CREATE_SCHEDULE (
          schedule_name   => 'rds_master_user.new_schedule',
          start_date      => SYSTIMESTAMP,
          repeat_interval =>
 'freq=daily;byday=MON,TUE,WED,THU,FRI;byhour=0;byminute=0;bysecond=0',
          end_date        => NULL,
          comments        => 'Repeats daily forever');
END;
/

BEGIN
     rdsadmin.rdsadmin_dbms_scheduler.set_attribute (
          name      => 'SYS.BSLN_MAINTAIN_STATS_JOB',
          attribute => 'schedule_name',
```

```
          value     => 'rds_master_user.new_schedule');
END;
/
```

Desactivación de la confirmación automática para la creación de trabajos del programador de Oracle

Cuando `DBMS_SCHEDULER.CREATE_JOB` crea trabajos del programador de Oracle, los crea inmediatamente y confirma los cambios. Puede que necesite incorporar la creación de trabajos del programador de Oracle en la transacción de usuario para hacer lo siguiente:

- Revertir el trabajo del programador de Oracle cuando se revierte la transacción del usuario.
- Crear el trabajo del programador de Oracle cuando se confirme la transacción principal del usuario.

Puede utilizar el procedimiento `rdsadmin.rdsadmin_dbms_scheduler.set_no_commit_flag` para activar este comportamiento. Este procedimiento no acepta parámetros. Puede utilizar este procedimiento en las siguientes versiones de RDS para Oracle:

- 21.0.0.0.ru-2022-07.rur-2022-07.r1 y posteriores
- 19.0.0.0.ru-2022-07.rur-2022-07.r1 y posteriores

El siguiente ejemplo desactiva la confirmación automática del programador de Oracle, crea un trabajo del programador de Oracle y, a continuación, revierte la transacción. Como la confirmación automática está desactivada, la base de datos también revierte la creación del trabajo del programador de Oracle.

```
BEGIN
  rdsadmin.rdsadmin_dbms_scheduler.set_no_commit_flag;
  DBMS_SCHEDULER.CREATE_JOB(job_name   => 'EMPTY_JOB',
                            job_type   => 'PLSQL_BLOCK',
                            job_action => 'begin null; end;',
                            auto_drop  => false);
  ROLLBACK;
END;
/

PL/SQL procedure successfully completed.

SELECT * FROM DBA_SCHEDULER_JOBS WHERE JOB_NAME='EMPTY_JOB';
```

```
no rows selected
```

Diagnóstico de problemas con instancias de bases de datos de RDS para Oracle

Oracle Database incluye una infraestructura de diagnóstico de fallos que puede utilizar para investigar problemas de bases de datos. En la terminología de Oracle, un problema es un error crítico, como un error de código o un daño en los datos. Un incidente es la existencia de un problema. Si el mismo error ocurre tres veces, la infraestructura muestra tres incidentes de este problema. Para obtener más información, consulte Diagnóstico y resolución de problemas en la documentación de Oracle Database.

La utilidad Automatic Diagnostic Repository Command Interpreter (ADRCI) es una herramienta de línea de comandos de Oracle que se utiliza para administrar datos de diagnóstico. Por ejemplo, puede utilizar esta herramienta para investigar problemas y empaquetar datos de diagnóstico. Un paquete de incidentes incluye datos de diagnóstico de un incidente o de todos los incidentes que hacen referencia a un problema específico. Puede cargar un paquete de incidentes, que se implementa como un archivo.zip, en Oracle Support.

Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a ADRCI. Para realizar tareas de diagnóstico en la instancia de base de datos de RDS para Oracle, utilice el paquete `rdsadmin.rdsadmin_adrci_util` de Amazon RDS.

Mediante el uso de las funciones de `rdsadmin_adrci_util`, puede obtener un listado de los problemas e incidentes y empaquetarlos, así como mostrar archivos de seguimiento. Todas las funciones devuelven un ID de tarea. Este ID forma parte del nombre del archivo de registro que contiene el resultado de ADRCI, como en `dbtask-`*`task_id`*`.log`. El archivo de registro reside en el directorio BDUMP. Puede descargar el archivo de registro siguiendo el procedimiento descrito en Descarga de un archivo de registro de base de datos.

Parámetros comunes para procedimientos de diagnóstico

Para realizar tareas de diagnóstico, utilice funciones del paquete `rdsadmin.rdsadmin_adrci_util` de Amazon RDS. El paquete tiene los siguientes parámetros comunes.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`incident_id`	número	Un ID de incidente válido o nulo	Null	No	Si el valor es nulo, la función muestra todos los incidentes. Si el valor no es nulo y representa un ID de incidente válido, la función muestra el incidente especificado.
`problem_id`	número	Un ID de problema válido o nulo	Null	No	Si el valor es nulo, la función muestra todos los problemas. Si el valor no es nulo y representa un ID de problema válido, la función muestra el problema especificado.
`last`	número	Un valor entero válido mayor que 0 o nulo	Null	No	Si el valor es nulo, la función muestra como máximo 50 elementos. Si el valor no es nulo, la función muestra el número especificado.

Descripción de incidentes

Para obtener un listado de los incidentes de diagnóstico para Oracle, utilice la función `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents` de Amazon RDS. Puede obtener

un listado de los incidentes en modo básico o detallado. De forma predeterminada, la función muestra los 50 incidentes más recientes.

Esta función utiliza los siguientes parámetros comunes:

- `incident_id`
- `problem_id`
- `last`

Si especifica `incident_id` y `problem_id`, `incident_id` anula a `problem_id`. Para obtener más información, consulte Parámetros comunes para procedimientos de diagnóstico.

Esta función utiliza el siguiente parámetro adicional.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`detail`	booleano	`TRUE` o `FALSE`	`FALSE`	No	Si `TRUE`, la función muestra los incidentes en modo detallado. Si `FALSE`, la función muestra los incidentes en modo básico.

Para enumerar todos los incidentes, consulte la función `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents` sin argumentos. La consulta devuelve el ID de tarea.

```
SQL> SELECT rdsadmin.rdsadmin_adrci_util.list_adrci_incidents AS task_id FROM DUAL;

TASK_ID
------------------
1590786706158-3126
```

O llame a la función `rdsadmin.rdsadmin_adrci_util.list_adrci_incidents` sin ningún argumento y almacene la salida en una variable de cliente SQL. Puede utilizar la variable en otras instrucciones.

```
SQL> VAR task_id VARCHAR2(80);
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_incidents;

PL/SQL procedure successfully completed.
```

Para leer el archivo de registro, llame al procedimiento `rdsadmin.rds_file_util.read_text_file` de Amazon RDS. Proporcione el identificador de la tarea como parte del nombre de archivo. El siguiente resultado muestra tres incidentes: 53523, 53522 y 53521.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log'));

TEXT
--------------------------------------------------------------------------------
2020-05-29 21:11:46.193 UTC [INFO ] Listing ADRCI incidents.
2020-05-29 21:11:46.256 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*********************************************************************
INCIDENT_ID PROBLEM_KEY                                                 CREATE_TIME
----------- ------------------------------------------------------------
 ----------------------------------------
53523       ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_003 2020-05-29
 20:15:20.928000 +00:00
53522       ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_002 2020-05-29
 20:15:15.247000 +00:00
53521       ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_001 2020-05-29
 20:15:06.047000 +00:00
3 rows fetched


2020-05-29 21:11:46.256 UTC [INFO ] The ADRCI incidents were successfully listed.
2020-05-29 21:11:46.256 UTC [INFO ] The task finished successfully.

14 rows selected.
```

Para enumerar un incidente concreto, especifique su ID mediante el parámetro `incident_id`. En el ejemplo siguiente, consulte el archivo de registro solo para el incidente 53523.

```
SQL> EXEC :task_id :=
 rdsadmin.rdsadmin_adrci_util.list_adrci_incidents(incident_id=>53523);

PL/SQL procedure successfully completed.

SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log'));

TEXT
--------------------------------------------------------------------------------
2020-05-29 21:15:25.358 UTC [INFO ] Listing ADRCI incidents.
2020-05-29 21:15:25.426 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*********************************************************************
INCIDENT_ID          PROBLEM_KEY
 CREATE_TIME
-------------------- ----------------------------------------------------------
 ---------------------------------
53523                ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_003
 2020-05-29 20:15:20.928000 +00:00
1 rows fetched


2020-05-29 21:15:25.427 UTC [INFO ] The ADRCI incidents were successfully listed.
2020-05-29 21:15:25.427 UTC [INFO ] The task finished successfully.

12 rows selected.
```

Descripción de problemas

Para enumerar los problemas de diagnóstico de Oracle, utilice la función `rdsadmin.rdsadmin_adrci_util.list_adrci_problems` de Amazon RDS.

De forma predeterminada, la función enumera los 50 problemas más recientes.

Esta función utiliza los parámetros comunes `problem_id` y `last`. Para obtener más información, consulte Parámetros comunes para procedimientos de diagnóstico.

Para obtener el ID de tarea de todos los problemas, llame a la función `rdsadmin.rdsadmin_adrci_util.list_adrci_problems` sin argumentos y almacene la salida en una variable de cliente SQL.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_problems;

PL/SQL procedure successfully completed.
```

Para leer el archivo de registro, llame a la función `rdsadmin.rds_file_util.read_text_file`, proporcionando el ID de tarea como parte del nombre del archivo. En el siguiente resultado, el archivo de registro muestra tres problemas: 1, 2 y 3.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log'));

TEXT
--------------------------------------------------------------------------------
2020-05-29 21:18:50.764 UTC [INFO ] Listing ADRCI problems.
2020-05-29 21:18:50.829 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*************************************************************************
PROBLEM_ID   PROBLEM_KEY                                                 LAST_INCIDENT
       LASTINC_TIME
---------- ------------------------------------------------------------ -------------
 -------------------------------
2          ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_003 53523
 2020-05-29 20:15:20.928000 +00:00
3          ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_002 53522
 2020-05-29 20:15:15.247000 +00:00
1          ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_001 53521
 2020-05-29 20:15:06.047000 +00:00
3 rows fetched


2020-05-29 21:18:50.829 UTC [INFO ] The ADRCI problems were successfully listed.
2020-05-29 21:18:50.829 UTC [INFO ] The task finished successfully.

14 rows selected.
```

En el ejemplo siguiente, solo muestra el problema 3.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.list_adrci_problems(problem_id=>3);
```

```
PL/SQL procedure successfully completed.
```

Para leer el archivo de registro del problema 3, llame `rdsadmin.rds_file_util.read_text_file`. Proporcione el identificador de la tarea como parte del nombre de archivo.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log'));

TEXT
--------------------------------------------------------------------------------
2020-05-29 21:19:42.533 UTC [INFO ] Listing ADRCI problems.
2020-05-29 21:19:42.599 UTC [INFO ]
ADR Home = /rdsdbdata/log/diag/rdbms/orcl_a/ORCL:
*********************************************************************
PROBLEM_ID PROBLEM_KEY                                                 LAST_INCIDENT
 LASTINC_TIME
---------- ------------------------------------------------------------ -------------
 -------------------------------
3          ORA 700 [EVENT_CREATED_INCIDENT] [942] [SIMULATED_ERROR_002 53522
 2020-05-29 20:15:15.247000 +00:00
1 rows fetched


2020-05-29 21:19:42.599 UTC [INFO ] The ADRCI problems were successfully listed.
2020-05-29 21:19:42.599 UTC [INFO ] The task finished successfully.

12 rows selected.
```

Creación de paquetes de incidentes

Puede crear paquetes de incidentes utilizando la función `rdsadmin.rdsadmin_adrci_util.create_adrci_package` de Amazon RDS. El resultado es un archivo.zip que puede proporcionar a Oracle Support.

Esta función utiliza los siguientes parámetros comunes:

- `problem_id`
- `incident_id`

Asegúrese de especificar uno de los parámetros anteriores. Si especifica ambos, el parámetro `incident_id` anula el parámetro `problem_id`. Para obtener más información, consulte Parámetros comunes para procedimientos de diagnóstico.

Para crear un paquete para un incidente específico, llame a la función `rdsadmin.rdsadmin_adrci_util.create_adrci_package` de Amazon RDS con el parámetro `incident_id`. En el ejemplo siguiente se crea un paquete para el incidente 53523.

```
SQL> EXEC :task_id :=
 rdsadmin.rdsadmin_adrci_util.create_adrci_package(incident_id=>53523);

PL/SQL procedure successfully completed.
```

Para leer el archivo de registro, llame a `rdsadmin.rds_file_util.read_text_file`. Puede proporcionar el ID de tarea como parte del nombre de archivo. El resultado muestra que se ha generado el paquete de incidentes `ORA700EVE_20200529212043_COM_1.zip`.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log'));

TEXT
--------------------------------------------------------------------------------
2020-05-29 21:20:43.031 UTC [INFO ] The ADRCI package is being created.
2020-05-29 21:20:47.641 UTC [INFO ] Generated package 1 in file /rdsdbdata/log/trace/
ORA700EVE_20200529212043_COM_1.zip, mode complete
2020-05-29 21:20:47.642 UTC [INFO ] The ADRCI package was successfully created.
2020-05-29 21:20:47.642 UTC [INFO ] The task finished successfully.
```

Para empaquetar los datos de diagnóstico de un problema concreto, especifique su ID mediante el parámetro `problem_id`. En el ejemplo siguiente, solo se empaquetan datos del problema 3.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.create_adrci_package(problem_id=>3);

PL/SQL procedure successfully completed.
```

Para leer la salida de la tarea, llame a `rdsadmin.rds_file_util.read_text_file` y proporcione el ID de la tarea como parte del nombre del archivo. El resultado muestra que se ha generado el paquete de incidentes `ORA700EVE_20200529212111_COM_1.zip`.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log'));

TEXT
--------------------------------------------------------------------------------
2020-05-29 21:21:11.050 UTC [INFO ] The ADRCI package is being created.
2020-05-29 21:21:15.646 UTC [INFO ] Generated package 2 in file /rdsdbdata/log/trace/
ORA700EVE_20200529212111_COM_1.zip, mode complete
2020-05-29 21:21:15.646 UTC [INFO ] The ADRCI package was successfully created.
2020-05-29 21:21:15.646 UTC [INFO ] The task finished successfully.
```

También puede descargar el archivo de registro. Para obtener más información, consulte Descarga de un archivo de registro de base de datos.

Mostrar archivos de seguimiento

Puede utilizar la función de Amazon RDS `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile` para enumerar los archivos de seguimiento en el directorio de seguimiento y todos los directorios de incidentes en la página de inicio del ADR actual. También puede mostrar el contenido de los archivos de seguimiento y de los archivos de seguimiento de incidentes.

Esta función utiliza el siguiente parámetro.

Nombre del parámetro	Tipo de datos	Valores válidos	Valor predeterminado	Obligatorio	Descripción
`filename`	varchar2	Un nombre de archivo de seguimiento válido	Null	No	Si el valor es nulo, la función muestra todos los archivos de seguimiento. Si no es nulo, la función muestra el archivo especificado.

Para mostrar el archivo de seguimiento, llame a la función de Amazon RDS `rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile`.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile;

PL/SQL procedure successfully completed.
```

Para enumerar los nombres de archivo de seguimiento, llame al procedimiento `rdsadmin.rds_file_util.read_text_file` de Amazon RDS, y proporcione el identificador de tarea como parte del nombre de archivo.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log')) WHERE TEXT LIKE '%/alert_%';

TEXT
--------------------------------------------------------------
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-28
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-27
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-26
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-25
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-24
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-23
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-22
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log.2020-05-21
     diag/rdbms/orcl_a/ORCL/trace/alert_ORCL.log

9 rows selected.
```

En el ejemplo siguiente, se genera un resultado para `alert_ORCL.log`.

```
SQL> EXEC :task_id := rdsadmin.rdsadmin_adrci_util.show_adrci_tracefile('diag/rdbms/
orcl_a/ORCL/trace/alert_ORCL.log');

PL/SQL procedure successfully completed.
```

Para leer el archivo de registro, llame a `rdsadmin.rds_file_util.read_text_file`. Proporcione el identificador de la tarea como parte del nombre de archivo. El resultado muestra las primeras 10 líneas de alert_ORCL.log.

```
SQL> SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||:task_id||'.log')) WHERE ROWNUM <= 10;

TEXT
```

```
--------------------------------------------------------------------------------
2020-05-29 21:24:02.083 UTC [INFO ] The trace files are being displayed.
2020-05-29 21:24:02.128 UTC [INFO ] Thu May 28 23:59:10 2020
Thread 1 advanced to log sequence 2048 (LGWR switch)
  Current log# 3 seq# 2048 mem# 0: /rdsdbdata/db/ORCL_A/onlinelog/o1_mf_3_hbl2p8xs_.log
Thu May 28 23:59:10 2020
Archived Log entry 2037 added for thread 1 sequence 2047 ID 0x5d62ce43 dest 1:
Fri May 29 00:04:10 2020
Thread 1 advanced to log sequence 2049 (LGWR switch)
  Current log# 4 seq# 2049 mem# 0: /rdsdbdata/db/ORCL_A/onlinelog/o1_mf_4_hbl2qgmh_.log
Fri May 29 00:04:10 2020

10 rows selected.
```

También puede descargar el archivo de registro. Para obtener más información, consulte Descarga de un archivo de registro de base de datos.

Realización de tareas diversas para instancias de base de datos de Oracle

A continuación, puede encontrar cómo realizar varias tareas de DBA en las instancias de base de datos de Amazon RDS que ejecutan Oracle. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a las instancias de bases de datos y restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados.

Temas

- Creación y eliminación de directorios en el espacio de almacenamiento de datos principal
- Descripción de los archivos de un directorio de instancia de base de datos
- Lectura de archivos de un directorio de instancia de base de datos
- Acceso a los archivos de Opatch
- Administrar tareas del asesor
- Transporte de espacios de tabla

Creación y eliminación de directorios en el espacio de almacenamiento de datos principal

Utilice el procedimiento de Amazon RDS para crear directorio `rdsadmin.rdsadmin_util.create_directory`. Puede crear hasta 10 000 directorios, todos

ellos en el espacio principal de almacenamiento de datos. Para eliminar directorios, utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_util.drop_directory`.

Los procedimientos `create_directory` y `drop_directory` tienen el siguiente parámetro requerido.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_directory_name`	VARCHAR2	—	Sí	El nombre del directorio.

En el siguiente ejemplo se crea un directorio denominado `PRODUCT_DESCRIPTIONS`.

```
EXEC rdsadmin.rdsadmin_util.create_directory(p_directory_name =>
 'product_descriptions');
```

El diccionario de datos almacena el nombre del directorio en mayúsculas. Es posible obtener un listado de los directorios consultando `DBA_DIRECTORIES`. El sistema elige automáticamente la ruta de acceso real del host. En el ejemplo siguiente se obtiene la ruta del directorio denominado `PRODUCT_DESCRIPTIONS`:

```
SELECT DIRECTORY_PATH
  FROM DBA_DIRECTORIES
 WHERE DIRECTORY_NAME='PRODUCT_DESCRIPTIONS';

DIRECTORY_PATH
----------------------------------------
/rdsdbdata/userdirs/01
```

El nombre de usuario maestro de la instancia de base de datos tiene privilegios de lectura y escritura en el nuevo directorio y puede conceder acceso a otros usuarios. Los privilegios de `EXECUTE` no están disponibles para directorios en una instancia de base de datos. Los directorios se crean en el espacio principal de almacenamiento de datos, y consumen espacio y ancho de banda de E/S.

En el ejemplo siguiente se elimina el directorio denominado `PRODUCT_DESCRIPTIONS`.

```
EXEC rdsadmin.rdsadmin_util.drop_directory(p_directory_name => 'product_descriptions');
```

> **Note**
>
> También puede eliminar un directorio mediante el comando de Oracle SQL `DROP DIRECTORY`.

Al eliminar un directorio, no se elimina su contenido. Debido a que el procedimiento `rdsadmin.rdsadmin_util.create_directory` puede reutilizar los nombres de ruta, los archivos de los directorios eliminados pueden aparecer en un directorio que se acaba de crear. Antes de eliminar un directorio, recomendamos que utilice `UTL_FILE.FREMOVE` para eliminar los archivos del directorio. Para más información, consulte FREMOVE Procedure en la documentación de Oracle.

Descripción de los archivos de un directorio de instancia de base de datos

Utilice el procedimiento de Amazon RDS para obtener un listado de los archivos de un directori `rdsadmin.rds_file_util.listdir`. No se admite este procedimiento en una réplica de Oracle. El procedimiento `listdir` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_directory`	varchar2	—	Sí	El nombre del directorio cuyo listado se desea obtener.

El siguiente ejemplo concede privilegios de lectura o escritura en el directorio `PRODUCT_DESCRIPTIONS` al usuario `rdsadmin` y, luego, enumera los archivos de este directorio.

```
GRANT READ,WRITE ON DIRECTORY PRODUCT_DESCRIPTIONS TO rdsadmin;
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory =>
 'PRODUCT_DESCRIPTIONS'));
```

Lectura de archivos de un directorio de instancia de base de datos

Utilice el procedimiento de Amazon RDS para leer un archivo de text `rdsadmin.rds_file_util.read_text_file`. El procedimiento `read_text_file` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_directory	varchar2	—	Sí	El nombre del directorio que contiene el archivo.
p_filename	varchar2	—	Sí	El nombre del archivo que se va a leer.

En el ejemplo siguiente se crea el archivo `rice.txt` en el directorio `PRODUCT_DESCRIPTIONS`.

```
declare
  fh sys.utl_file.file_type;
begin
  fh := utl_file.fopen(location=>'PRODUCT_DESCRIPTIONS', filename=>'rice.txt',
 open_mode=>'w');
  utl_file.put(file=>fh, buffer=>'AnyCompany brown rice, 15 lbs');
  utl_file.fclose(file=>fh);
end;
/
```

En el siguiente ejemplo se lee el archivo `rice.txt` del directorio `PRODUCT_DESCRIPTIONS`.

```
SELECT * FROM TABLE
    (rdsadmin.rds_file_util.read_text_file(
        p_directory => 'PRODUCT_DESCRIPTIONS',
        p_filename  => 'rice.txt'));
```

Acceso a los archivos de Opatch

Opatch es una utilidad de Oracle que permite la aplicación y la restauración de parches en el software de Oracle. El mecanismo de Oracle para determinar qué parches se han aplicado a una base de datos es el comando `opatch lsinventory`. Para abrir solicitudes de servicio para clientes de Bring Your Own License (BYOL), Oracle Support solicita el archivo `lsinventory` y a veces el archivo `lsinventory_detail` generado por Opatch.

Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso mediante shell a Opatch. En su lugar, el `lsinventory-`*`dbv`*`.txt` en el directorio BDUMP

contiene la información del parche relacionada con la versión actual del motor. Cuando realiza una actualización menor o importante, Amazon RDS actualiza `lsinventory-dbv.txt` dentro de una hora después de aplicar el parche. Para verificar los parches aplicados, lea`lsinventory-dbv.txt`. Esta acción es similar a ejecutar el comando `opatch lsinventory`.

> **Note**
>
> Los ejemplos de esta sección suponen que el directorio BDUMP se llama `BDUMP`. En una réplica de lectura, el nombre del directorio BDUMP es diferente. Para obtener información sobre cómo obtener el nombre BDUMP mediante una consulta `V$DATABASE.DB_UNIQUE_NAME` en una réplica de lectura, consulte Descripción de archivos.

Los archivos de inventario utilizan la convención de nomenclatura de Amazon RDS `lsinventory-dbv.txt` y `lsinventory_detail-dbv.txt`, donde *dbv* es el nombre completo de su versión de base de datos. El archivo `lsinventory-dbv.txt` está disponible en todas las versiones de base de datos. El correspondiente `lsinventory_detail-dbv.txt` está disponible en 19.0.0.0, ru-2020-01.rur-2020-01.r1 o versiones posteriores.

Por ejemplo, si su versión de base de datos es 19.0.0.0.ru-2021-07.rur-2021-07.r1, los archivos de inventario tienen los siguientes nombres.

```
lsinventory-19.0.0.0.ru-2021-07.rur-2021-07.r1.txt
lsinventory_detail-19.0.0.0.ru-2021-07.rur-2021-07.r1.txt
```

Asegúrese de descargar los archivos que coinciden con la versión actual de su motor de base de datos.

Consola

Para descargar un archivo de inventario mediante la consola

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione el nombre de la instancia de base de datos que tiene el archivo de registro que desea visualizar.
4. Seleccione la pestaña Logs & events (Registros y eventos).
5. Desplácese hacia abajo hasta la sección Logs.

6. En la sección Registros, busque `lsinventory`.
7. Seleccione el archivo al que desea acceder y, a continuación, elija Descargar.

SQL

Para leer `lsinventory-`*`dbv`*`.txt` en un cliente SQL, puede utilizar una instrucción `SELECT`. Para esta técnica, utilice cualquiera de las siguientes funciones de `rdsadmin`: `rdsadmin.rds_file_util.read_text_file` o `rdsadmin.tracefile_listing`.

En la siguiente consulta de ejemplo, reemplace *dbv* por la versión de la base de datos de Oracle. Por ejemplo, es posible que su versión de base de datos sea 19.0.0.0.ru-2020-04.rur-2020-04.r1.

```
SELECT text
FROM   TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP', 'lsinventory-dbv.txt'));
```

PL/SQL

Para leer `lsinventory-`*`dbv`*`.txt` en un cliente SQL, puede escribir un programa PL/SQL. Este programa utiliza `utl_file` para leer el archivo y `dbms_output` para imprimirlo. Estos son paquetes suministrados por Oracle.

En el siguiente programa de ejemplo, reemplace *dbv* por la versión de base de datos de Oracle. Por ejemplo, es posible que su versión de base de datos sea 19.0.0.0.ru-2020-04.rur-2020-04.r1.

```
SET SERVEROUTPUT ON
DECLARE
  v_file              SYS.UTL_FILE.FILE_TYPE;
  v_line              VARCHAR2(1000);
  v_oracle_home_type  VARCHAR2(1000);
  c_directory         VARCHAR2(30) := 'BDUMP';
  c_output_file       VARCHAR2(30) := 'lsinventory-dbv.txt';
BEGIN
  v_file := SYS.UTL_FILE.FOPEN(c_directory, c_output_file, 'r');
  LOOP
    BEGIN
      SYS.UTL_FILE.GET_LINE(v_file, v_line,1000);
      DBMS_OUTPUT.PUT_LINE(v_line);
    EXCEPTION
      WHEN no_data_found THEN
        EXIT;
```

```
    END;
  END LOOP;
END;
/
```

O consulta `rdsadmin.tracefile_listing` e incorpora la salida a un archivo. En el ejemplo siguiente se incorpora la salida a `/tmp/tracefile.txt`.

```
SPOOL /tmp/tracefile.txt
SELECT *
FROM   rdsadmin.tracefile_listing
WHERE  FILENAME LIKE 'lsinventory%';
SPOOL OFF;
```

Administrar tareas del asesor

Oracle Database incluye varios asesores. Cada asesor soporta tareas automatizadas y manuales. Puede utilizar procedimientos en el paquete `rdsadmin.rdsadmin_util` para administrar algunas tareas del asesor.

Los procedimientos de tareas del asesor están disponibles en las siguientes versiones del motor:

- Oracle Database 21c (21.0.0)
- Versión 19.0.0.0.ru-2021-01.rur-2021-01.r1 Oracle Database 19c y versiones posteriores

  Para obtener más información, consulte la sección sobre la versión 19.0.0.0.ru-2021-01.rur-2021-01.r1 en las notas de la versión de Amazon RDS for Oracle.

Temas

- Configuración de parámetros para tareas del asesor
- Desactivación de AUTO_STATS_ADVISOR_TASK
- Volver a habilitar AUTO_STATS_ADVISOR_TASK

Configuración de parámetros para tareas del asesor

A fin de establecer parámetros para algunas tareas del asesor, utilice el Amazon RDS procedimiento `rdsadmin.rdsadmin_util.advisor_task_set_parameter`. El procedimiento `advisor_task_set_parameter` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_task_name	varchar2	—	Sí	El nombre de la tarea del asesor cuyos parámetros desea cambiar. Los siguientes valores son válidos: • AUTO_STATS_ADVISOR_TASK • INDIVIDUAL_STATS_ADVISOR_TASK • SYS_AUTO_SPM_EVOLVE_TASK • SYS_AUTO_SQL_TUNING_TASK

p_parameter	varchar2	—	Sí	El nombre del parámetro de la tarea. A fin de buscar parámetros válidos para una tarea del asesor, ejecute la siguiente consulta. Sustituya *p_task_name* con un valor válido para p_task_name :
				`COL PARAMETER_NAME FORMAT a30`
				`COL PARAMETER_VALUE FORMAT a30`
				`SELECT PARAMETER_NAME, PARAMETER _VALUE`
				`FROM DBA_ADVISOR_PARAMETERS`
				`WHERE TASK_NAME=' p_task_name '`
				`AND PARAMETER_VALUE != 'UNUSED'`
				`ORDER BY PARAMETER_NAME;`

p_value	varchar2	—	Sí	El valor de un parámetro de tarea. Para buscar valores válidos para los parámetros de tarea, ejecute la siguiente consulta. Sustituya *p_task_name* con un valor válido para p_task_name :
				`COL PARAMETER_NAME FORMAT a30`
				`COL PARAMETER_VALUE FORMAT a30`
				`SELECT PARAMETER_NAME, PARAMETER _VALUE`

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				FROM DBA_ADVISOR_PARAMETERS WHERE TASK_NAME=' *p_task_name* ' AND PARAMETER_VALUE != 'UNUSED' ORDER BY PARAMETER_NAME;

El siguiente programa PL/SQL establece `ACCEPT_PLANS` a `FALSE` para `SYS_AUTO_SPM_EVOLVE_TASK`. La tarea automatizada de administración de planes SQL verifica los planes y genera un informe de sus conclusiones, pero no evoluciona los planes automáticamente. Puede utilizar un informe para identificar nuevas líneas base de plan SQL y aceptarlas manualmente.

```
BEGIN
  rdsadmin.rdsadmin_util.advisor_task_set_parameter(
    p_task_name => 'SYS_AUTO_SPM_EVOLVE_TASK',
    p_parameter => 'ACCEPT_PLANS',
    p_value     => 'FALSE');
END;
```

El siguiente programa PL/SQL establece `EXECUTION_DAYS_TO_EXPIRE` a `10` para `AUTO_STATS_ADVISOR_TASK`. La tarea predefinida `AUTO_STATS_ADVISOR_TASK` se ejecuta automáticamente en el periodo de mantenimiento una vez al día. En el ejemplo se establece el periodo de retención para la ejecución de la tarea en 10 días.

```
BEGIN
  rdsadmin.rdsadmin_util.advisor_task_set_parameter(
    p_task_name => 'AUTO_STATS_ADVISOR_TASK',
    p_parameter => 'EXECUTION_DAYS_TO_EXPIRE',
    p_value     => '10');
END;
```

Desactivación de AUTO_STATS_ADVISOR_TASK

Para deshabilitar `AUTO_STATS_ADVISOR_TASK`, utilice el Amazon RDS procedimiento `rdsadmin.rdsadmin_util.advisor_task_drop`. El procedimiento `advisor_task_drop` acepta el siguiente parámetro.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_task_name	varchar2	—	Sí	El nombre de la tarea del asesor que se va a deshabilitar. El único valor válido es AUTO_STATS_ADVISOR_TASK .

El siguiente comando se coloca AUTO_STATS_ADVISOR_TASK.

```
EXEC rdsadmin.rdsadmin_util.advisor_task_drop('AUTO_STATS_ADVISOR_TASK')
```

Puede volver a habilitar AUTO_STATS_ADVISOR_TASK con rdsadmin.rdsadmin_util.dbms_stats_init.

Volver a habilitar AUTO_STATS_ADVISOR_TASK

Para volver a habilitar AUTO_STATS_ADVISOR_TASK, utilice el Amazon RDS procedimiento rdsadmin.rdsadmin_util.dbms_stats_init. El procedimiento dbms_stats_init no acepta parámetros.

El siguiente comando vuelve a habilitar AUTO_STATS_ADVISOR_TASK.

```
EXEC rdsadmin.rdsadmin_util.dbms_stats_init()
```

Transporte de espacios de tabla

Utilice el paquete Amazon RDS rdsadmin.rdsadmin_transport_util para copiar un conjunto de espacios de tabla de una base de datos Oracle en las instalaciones a una instancia de base de datos de RDS para Oracle. A nivel físico, la característica de espacio de tabla transportable copia de forma incremental los archivos de datos de origen y los archivos de metadatos en la instancia de destino. Puede transferir los archivos mediante Amazon EFS o Amazon S3. Para obtener más información, consulte Migración mediante espacios de tabla transportables de Oracle.

Temas

- Importación de espacios de tabla transportados a su instancia de base de datos

- Importación de metadatos de espacios de tabla transportables a su instancia de base de datos
- Enumeración de los archivos huérfanos después de importar un espacio de tabla
- Eliminación de los archivos de datos huérfanos después de importar un espacio de tabla

Importación de espacios de tabla transportados a su instancia de base de datos

Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces` para restaurar los espacios de tabla que haya exportado anteriormente desde una instancia de base de datos de origen. En la fase de transporte, se realiza una copia de seguridad de los espacios de tabla de solo lectura y se exportan los metadatos de Data Pump, se transfiere estos archivos a su instancia de base de datos de destino y se importan tanto los espacios de tabla. Para obtener más información, consulte Fase 4: Transportar los espacios de tabla.

Sintaxis

```
FUNCTION import_xtts_tablespaces(
    p_tablespace_list IN CLOB,
    p_directory_name  IN VARCHAR2,
    p_platform_id     IN NUMBER DEFAULT 13,
    p_parallel        IN INTEGER DEFAULT 0) RETURN VARCHAR2;
```

Parámetros

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_tablespace_list`	`CLOB`	—	Sí	La lista de espacios de tabla que se van a importar.
`p_directory_name`	`VARCHAR2`	—	Sí	El directorio que contiene las copias de seguridad del espacio de tabla.
`p_platform_id`	`NUMBER`	`13`	No	Proporcione un ID de plataforma que coincida

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				con el especificado durante la fase de copia de seguridad. Para encontrar una lista de plataformas, consulte V$TRANSPORTABLE_PLATFORM . La plataforma predeterminada es Linux x86 de 64 bits, que tiene un formato little endian.
p_parallel	INTEGER	0	No	El grado de paralelismo. De forma predeterminada, el paralelismo está desactivado.

Ejemplos

En el siguiente ejemplo se importan los espacios de tabla *TBS1*, *TBS2* y *TBS3* del directorio *DATA_PUMP_DIR*. La plataforma de origen es AIX-Based Systems (64 bits), con el id. de plataforma 6. Puede encontrar los id. de plataforma consultando V$TRANSPORTABLE_PLATFORM.

```
VAR task_id CLOB

BEGIN
  :task_id:=rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces(
        'TBS1,TBS2,TBS3',
        'DATA_PUMP_DIR',
        p_platform_id => 6);
END;
/

PRINT task_id
```

Importación de metadatos de espacios de tabla transportables a su instancia de base de datos

Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_metadata` para importar los metadatos del espacio de tabla transportable a su instancia de base de datos de RDS para Oracle. Durante la operación, el estado de la importación de metadatos se muestra en la tabla `rdsadmin.rds_xtts_operation_info`. Para obtener más información, consulte Paso 5: Importar los metadatos del espacio de tabla en la instancia de base de datos de destino.

Sintaxis

```
PROCEDURE import_xtts_metadata(
    p_datapump_metadata_file IN SYS.DBA_DATA_FILES.FILE_NAME%TYPE,
    p_directory_name         IN VARCHAR2,
    p_exclude_stats          IN BOOLEAN DEFAULT FALSE,
    p_remap_tablespace_list  IN CLOB DEFAULT NULL,
    p_remap_user_list        IN CLOB DEFAULT NULL);
```

Parámetros

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_datapump_metadata_file`	`SYS.DBA_DATA_FILES.FILE_NAME%TYPE`	—	Sí	El nombre del archivo de Oracle Data Pump que contiene los metadatos de los espacios de tabla transportables.
`p_directory_name`	`VARCHAR2`	—	Sí	El nombre del directorio que contiene el archivo de Data Pump.
`p_exclude_stats`	`BOOLEAN`	`FALSE`	No	Indicador que señala si se deben excluir las estadísticas.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_remap_tablespace_list`	`CLOB`	NULL	No	Una lista de espacios de tabla que se van a reasignar durante la importación de metadatos. Utilice el formato *`from_tbs`*`:`*`to_tbs`*. Por ejemplo, especifique `users:user_data`.
`p_remap_user_list`	`CLOB`	NULL	No	Una lista de esquemas de usuario que se van a reasignar durante la importación de metadatos. Utilice el formato *`from_schema_name`*`:`*`to_schema_name`*. Por ejemplo, especifique `hr:human_resources`.

Ejemplos

El ejemplo importa los metadatos del espacio de tabla del archivo *`xttdump.dmp`*, que se encuentra en el directorio *`DATA_PUMP_DIR`*.

```
BEGIN
  rdsadmin.rdsadmin_transport_util.import_xtts_metadata('xttdump.dmp','DATA_PUMP_DIR');
END;
```

```
/
```

Enumeración de los archivos huérfanos después de importar un espacio de tabla

Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files` para enumerar los archivos de datos que quedaron huérfanos tras la importación de un espacio de tabla. Después de identificar los archivos de datos, puede eliminarlos llamando a `rdsadmin.rdsadmin_transport_util.cleanup_incomplete_xtts_import`.

Sintaxis

```
FUNCTION list_xtts_orphan_files RETURN xtts_orphan_files_list_t PIPELINED;
```

Ejemplos

En el siguiente ejemplo se ejecuta el procedimiento `rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files`. El resultado muestra dos archivos de datos huérfanos.

```
SQL> SELECT * FROM TABLE(rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files);

FILENAME       FILESIZE
-------------- ---------
datafile_7.dbf 104865792
datafile_8.dbf 104865792
```

Eliminación de los archivos de datos huérfanos después de importar un espacio de tabla

Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files` para eliminar los archivos de datos que quedaron huérfanos tras la importación de un espacio de tabla. La ejecución de este comando genera un archivo de registro que usa el formato de nombre `rds-xtts-delete_xtts_orphaned_files-`*`YYYY-MM-DD.HH24-MI-SS.FF`*`.log` en el directorio BDUMP. Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.cleanup_incomplete_xtts_import` para buscar los archivos huérfanos. Para leer el archivo de registro, llame al procedimiento `rdsadmin.rds_file_util.read_text_file`. Para obtener más información, consulte Fase 6: Limpiar los archivos sobrantes.

Sintaxis

```
PROCEDURE cleanup_incomplete_xtts_import(
    p_directory_name IN VARCHAR2);
```

Parámetros

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_directory_name	VARCHAR2	—	Sí	El directorio que contiene los archivos de datos huérfanos.

Ejemplos

En el siguiente ejemplo se eliminan los archivos de datos huérfanos en *DATA_PUMP_DIR*.

```
BEGIN
  rdsadmin.rdsadmin_transport_util.cleanup_incomplete_xtts_import('DATA_PUMP_DIR');
END;
/
```

En el siguiente ejemplo se lee el archivo de registro generado por el comando anterior.

```
SELECT *
FROM TABLE(rdsadmin.rds_file_util.read_text_file(
       p_directory => 'BDUMP',
       p_filename  => 'rds-xtts-
delete_xtts_orphaned_files-2023-06-01.09-33-11.868894000.log'));

TEXT
--------------------------------------------------------------------------------
orphan transported datafile datafile_7.dbf deleted.
orphan transported datafile datafile_8.dbf deleted.
```

Configuración de características avanzadas de RDS para Oracle

RDS para Oracle admite varias funciones avanzadas, como HugePages, un almacén de instancias y tipos de datos extendidos.

Temas

- Almacenamiento de datos temporales en un almacén de instancias de RDS para Oracle
- Activación de páginas de gran tamaño para una instancia de RDS para Oracle
- Activación de tipos de datos extendidos en RDS para Oracle

Almacenamiento de datos temporales en un almacén de instancias de RDS para Oracle

Utilice un almacén de instancias para los espacios de tabla temporales y la caché flash inteligente de base de datos (la caché flash) en clases de instancia de base de datos de RDS para Oracle admitidas.

Temas

- Descripción general del almacén de instancias de RDS para Oracle
- Activación de un almacén de instancias de RDS para Oracle
- Configuración de un almacén de instancias de RDS para Oracle
- Trabajo con un almacén de instancias en una réplica de lectura de Oracle
- Configuración de un grupo de espacio de tablas temporal en un almacén de instancias y Amazon EBS
- Eliminación de un almacén de instancias de RDS para Oracle

Descripción general del almacén de instancias de RDS para Oracle

El almacén de instancias ofrece un almacenamiento de nivel de bloques temporal para la instancia de base de datos de RDS para Oracle. Puede usar un almacén de instancias para almacenar temporalmente la información que cambia con frecuencia.

Un almacén de instancias se basa en dispositivos de memoria rápida no volátil (NVMe) que están conectados físicamente al equipo host. El almacenamiento está optimizado para una latencia baja, un rendimiento de E/S aleatorio y un rendimiento de lectura secuencial.

El tamaño del almacén de instancias varía según el tipo de instancia de base de datos. Para obtener más información sobre el almacén de instancias, consulte Almacén de instancias de Amazon EC2 en la Guía del usuario de Amazon Elastic Compute Cloud para las instancias de Linux.

Temas

- Tipos de datos en el almacén de instancias de RDS para Oracle
- Beneficios del almacén de instancias de RDS para Oracle
- Clases de instancia admitidas para el almacén de instancias de RDS para Oracle
- Versiones de motor para el almacén de instancias de RDS para Oracle
- Regiones de AWS admitidas para el almacén de instancias de RDS para Oracle
- Coste del almacén de instancias de RDS para Oracle

Tipos de datos en el almacén de instancias de RDS para Oracle

Puede colocar los siguientes tipos de datos temporales de RDS para Oracle en un almacén de instancias:

Un espacio de tabla temporal

Oracle Database utiliza espacios de tablas temporales para almacenar los resultados de las consultas intermedias que no caben en la memoria. Las consultas más grandes pueden generar grandes cantidades de datos intermedios que deben almacenarse en caché temporalmente, pero no es necesario que persistan. En particular, un espacio de tablas temporal es útil para ordenaciones, agregaciones de hash y uniones. Si su instancia de base de datos de RDS para Oracle usa la Enterprise Edition o la Standard Edition 2, puede colocar un espacio de tablas temporal en un almacén de instancias.

Memoria caché flash

La memoria caché flash mejora el rendimiento de las lecturas aleatorias de un solo bloque en la ruta convencional. Se recomienda ajustar el tamaño de la memoria caché para que se adapte a la mayoría del conjunto de datos activo. Si su instancia de RDS para la base de datos de Oracle utiliza la Enterprise Edition, puede colocar la memoria caché flash en un almacén de instancias.

De forma predeterminada, un almacén de instancias está configurado para un espacio de tablas temporal, pero no para la memoria caché flash. No puede colocar archivos de datos de Oracle y archivos de registro de base de datos en un almacén de instancias.

Beneficios del almacén de instancias de RDS para Oracle

Puede considerar usar un almacén de instancias para almacenar archivos y memorias caché temporales que pueda permitirse perder. Si desea mejorar el rendimiento de la base de datos o si el aumento de la carga de trabajo está causando problemas de rendimiento en su almacenamiento de Amazon EBS, considere la posibilidad de escalar a una clase de instancias que admita un almacén de instancias.

Al colocar el espacio de tablas temporal y la memoria caché flash en un almacén de instancias, obtendrá las siguientes ventajas:

- Latencias de lectura más bajas
- Mayor rendimiento
- Carga reducida en sus volúmenes de Amazon EBS
- Costos de almacenamiento e instantáneas más bajos gracias a la reducción de la carga de Amazon EBS
- Menor necesidad de aprovisionar IOPS elevadas, lo que posiblemente reduzca el costo total

Al colocar su espacio de tablas temporal en el almacén de instancias, aumenta de forma inmediata el rendimiento de las consultas que utilizan espacio temporal. Al colocar la memoria caché flash en el almacén de instancias, las lecturas de bloques en caché suelen tener una latencia mucho más baja que las lecturas de Amazon EBS. La memoria caché flash debe «calentarse» antes de ofrecer beneficios de rendimiento. La memoria caché se calienta por sí sola porque la base de datos escribe bloques en la caché flash a medida que se agotan en la memoria caché del búfer de la base de datos.

> **Note**
>
> En algunos casos, la caché flash ocasiona una sobrecarga de rendimiento debido a la administración de la memoria caché. Antes de activar la caché flash en un entorno de producción, le recomendamos que analice su carga de trabajo y pruebe la caché en un entorno de prueba.

Clases de instancia admitidas para el almacén de instancias de RDS para Oracle

Amazon RDS admite el almacén de instancias para las siguientes clases de instancia de base de datos:

- db.m5d
- db.r5d
- db.x2idn
- db.x2iedn

RDS para Oracle solo admite las clases de instancia de base de datos anteriores para el modelo de licencias BYOL. Para obtener más información, consulte Clases de instancias admitidas de RDS para Oracle y Traiga su propia licencia (BYOL) para EE y SE2.

Para ver el almacenamiento de instancias total de los tipos de instancia de base de datos admitidas, ejecute el siguiente comando en la CLI de AWS.

Example

```
aws ec2 describe-instance-types \
  --filters "Name=instance-type,Values=*5d.*large*" \
  --query "InstanceTypes[?contains(InstanceType,'m5d')||contains(InstanceType,'r5d')]
[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
  --output table
```

El comando anterior devuelve el tamaño de dispositivo sin procesar del almacén de instancias. RDS para Oracle utiliza una pequeña parte de este espacio para la configuración. El espacio en el almacén de instancias que está disponible para los espacios de tablas temporales o la memoria caché flash es un poco más pequeño.

Versiones de motor para el almacén de instancias de RDS para Oracle

El almacén de instancias es compatible con las siguientes versiones de motor de RDS para Oracle

- Versiones 21.0.0.0.ru-2022-01.rur-2022-01.r1 o posteriores de Oracle Database 21c
- Versiones 19.0.0.0.ru-2021-10.rur-2021-10.r1 o posteriores de Oracle Database 19c

Regiones de AWS admitidas para el almacén de instancias de RDS para Oracle

El almacén de instancias está disponible en todas las Regiones de AWS donde se admite uno o más de estos tipos de instancia. Para obtener más información sobre las clases de instancia db.m5d y db.r5d, consulte Clases de instancia de base de datos de . Para obtener más información sobre las clases de instancia admitidas por Amazon RDS para Oracle, consulte Clases de instancias de base de datos de RDS para Oracle.

Coste del almacén de instancias de RDS para Oracle

El coste del almacén de instancias se incluye en el coste de las instancias activadas en el almacén de instancias. No incurre en costes adicionales al habilitar un almacén de instancias en una instancia de base de datos de RDS para Oracle. Para obtener más información acerca de las instancias activadas del el almacén de instancias, consulte Clases de instancia admitidas para el almacén de instancias de RDS para Oracle.

Activación de un almacén de instancias de RDS para Oracle

Para activar el almacén de instancias para datos temporales de RDS para Oracle, realice una de las siguientes operaciones:

- Cree una instancia de base de datos de RDS para Oracle mediante una clase de instancia compatible. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de RDS para Oracle existente para usar una clase de instancia compatible. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Configuración de un almacén de instancias de RDS para Oracle

De forma predeterminada, el 100 % del espacio del almacén de instancias se asigna al espacio de tablas temporal. Para configurar el almacén de instancias para asignar espacio a la memoria caché flash y al espacio de tablas temporal, establezca los siguientes parámetros en el grupo de parámetros de su instancia:

db_flash_cache_size={DBInstanceStore*{0,2,4,6,8,10}/10}

Este parámetro especifica la cantidad de espacio de almacenamiento asignado a la memoria caché flash. Este parámetro solo es válido para Oracle Database Enterprise Edition. El valor predeterminado es `{DBInstanceStore*0/10}`. Si establece un valor distinto de cero para `db_flash_cache_size`, la instancia de RDS para Oracle habilita la memooria caché flash después de reiniciar la instancia.

rds.instance_store_temp_size={DBInstanceStore*{0,2,4,6,8,10}/10}

Este parámetro especifica la cantidad de espacio de almacenamiento asignado a la tabla de espacio temporal. El valor predeterminado es `{DBInstanceStore*10/10}`. Este parámetro se puede modificar para Oracle Database Enterprise Edition y es de solo lectura para la Standard

Edition 2. Si establece un valor distinto de cero para `rds.instance_store_temp_size`, Amazon RDS asigna espacio en el almacén de instancias para el espacio de tablas temporal.

Puede establecer los parámetros `db_flash_cache_size` y `rds.instance_store_temp_size` para las instancias de base de datos que no utilizan un almacén de instancias. En este caso, ambos ajustes se evalúan en `0`, lo que desactiva la función. En este caso, puede usar el mismo grupo de parámetros para instancias de diferentes tamaños y para instancias que no usen un almacén de instancias. Si modifica estos parámetros, asegúrese de reiniciar las instancias asociadas para que los cambios surtan efecto.

> **Important**
>
> Si asigna espacio a un espacio de tablas temporal, Amazon RDS no crea el espacio de tablas temporal automáticamente. Para obtener información sobre cómo crear el espacio de tablas temporal en el almacén de instancias, consulte Creación de un espacio de tablas temporal en el almacén de instancias.

El valor combinado de los parámetros anteriores no debe superar el 10/10 o el 100 %. En la tabla siguiente se muestran las configuraciones de parámetros válidas y no válidas.

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explicación
db_flash_cache_size={DBInstanceStore*0/10}	rds.instance_store_temp_size={DBInstanceStore*10/10}	Esta es una configuración válida para todas las ediciones de Oracle Database. Amazon RDS asigna el 100 % del espacio del almacén de instancias al espacio de tablas temporal. Esta

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explicación
		es la opción predeterminada.
db_flash_cache_size={DBInstanceStore*10/10}	rds.instance_store_temp_size={DBInstanceStore*0/10}	Esta es una configuración válida para Oracle Database Enterprise Edition. Amazon RDS asigna el 100 % del espacio del almacén de instancias a la memoria caché flash.

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explicación
db_flash_cache_size={DBInstanceStore*2/10}	rds.instance_store_temp_size={DBInstanceStore*8/10}	Esta es una configuración válida solo para Oracle Database Enterprise Edition. Amazon RDS asigna el 20 % del espacio del almacén de instancias a la memoria caché flash y el 80 % del espacio del almacén de instancias al espacio de tablas temporal.

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explicación
db_flash_cache_size={DBInstanceStore*6/10}	rds.instance_store_temp_size={DBInstanceStore*4/10}	Esta es una configuración válida solo para Oracle Database Enterprise Edition. Amazon RDS asigna el 60 % del espacio del almacén de instancias a la memoria caché flash y el 40 % del espacio del almacén de instancias al espacio de tablas temporal.

db_flash_cache_size setting	rds.instance_store_temp_size setting	Explicación
db_flash_cache_size={DBInstanceStore*2/10}	rds.instance_store_temp_size={DBInstanceStore*4/10}	Esta es una configuración válida solo para Oracle Database Enterprise Edition. Amazon RDS asigna el 20 % del espacio del almacén de instancias a la memoria caché flash y el 40 % del espacio del almacén de instancias al espacio de tablas temporal.
db_flash_cache_size={DBInstanceStore*8/10}	rds.instance_store_temp_size={DBInstanceStore*8/10}	Esta configuración no es válida porque el porcentaje combinado del espacio del almacén de instancias supera el 100 %. En esos casos, Amazon RDS no logra realizar el intento.

Consideraciones a la hora de cambiar el tipo de instancia

Si cambia el tipo de instancia de base de datos, esto puede afectar a la configuración de la memoria caché flash o al espacio de tablas temporal del almacén de instancias. Tenga en cuenta las siguientes modificaciones y sus efectos:

Puede escalar verticalmente o reducir verticalmente la instancia de base de datos que admite el almacén de instancias.

Los siguientes valores aumentan o disminuyen proporcionalmente al nuevo tamaño del almacén de instancias:

- El nuevo tamaño de la memoria caché flash.
- El espacio asignado a los espacios de tablas temporales que residen en el almacén de instancias.

Por ejemplo, el ajuste `db_flash_cache_size={DBInstanceStore*6/10}` de una instancia db.m5d.4xlarge proporciona alrededor de 340 GB de espacio de memoria caché flash. Si aumentas el tipo de instancia a db.m5d.8xlarge, el espacio de la caché flash aumenta hasta unos 680 GB.

Modifica una instancia de base de datos que no usa un almacén de instancias en una instancia que sí usa un almacén de instancias.

Si `db_flash_cache_size` se establece en un valor superior a `0`, se configura la memoria caché flash. Si `rds.instance_store_temp_size` se establece en un valor mayor que `0`, el espacio del almacén de instancias se asigna para que lo use un espacio de tablas temporal. RDS for Oracle no mueve automáticamente los archivos temporales al almacén de instancias. Para obtener información sobre el uso del espacio asignado, consulte Creación de un espacio de tablas temporal en el almacén de instancias o Adición de un archivo temporal al almacén de instancias en una réplica de lectura.

Una instancia de base de datos que no usa un almacén de instancias se modifica en una instancia que sí usa un almacén de instancias.

En este caso, RDS para Oracle elimina la memoria caché flash. RDS vuelve a crear el archivo temporal que se encuentra actualmente en el almacén de instancias de un volumen de Amazon EBS. El tamaño máximo del nuevo archivo temporal es el tamaño anterior del parámetro `rds.instance_store_temp_size`.

Trabajo con un almacén de instancias en una réplica de lectura de Oracle

Las réplicas de lectura admiten la memoria caché flash y los espacios de tablas temporales de un almacén de instancias. Si bien la memoria caché flash funciona de la misma manera que en la instancia de base de datos principal, tenga en cuenta las siguientes diferencias en los espacios de tablas temporales:

- No puede crear un espacio de tabla temporal existente en una réplica de lectura. Si crea un nuevo espacio de tablas temporal en la instancia principal, RDS para Oracle replica la información del espacio de tablas sin archivos temporales. Para agregar un archivo temporal nuevo, utilice cualquiera de las siguientes técnicas:
  - Utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_util.add_inst_store_tempfile`. RDS para Oracle crea un archivo temporal en el almacén de instancias de la réplica de lectura y lo agrega al espacio de tablas temporal especificado.
  - Ejecute el comando `ALTER TABLESPACE … ADD TEMPFILE`. RDS para Oracle coloca el archivo temporal en el almacenamiento de Amazon EBS.

  > **Note**
  >
  > Los tamaños de los archivos temporales y los tipos de almacenamiento pueden ser diferentes en la instancia de base de datos principal y en la réplica de lectura.

- Puede administrar la configuración predeterminada del espacio de tablas temporal solo en la instancia de base de datos principal. RDS para Oracle replica la configuración en todas las réplicas de lectura.
- Puede configurar grupos de espacio de tablas temporal solo en la instancia de base de datos principal. RDS para Oracle replica el ajuste en todas las réplicas de lectura.

Configuración de un grupo de espacio de tablas temporal en un almacén de instancias y Amazon EBS

Puede configurar un grupo de espacios de tablas temporal para que incluya espacios de tablas temporales tanto en un almacén de instancias como en Amazon EBS. Esta técnica es útil cuando se desea disponer de más almacenamiento temporal del permitido por el ajuste máxima de `rds.instance_store_temp_size`.

Al configurar un grupo de espacios de tablas temporal tanto en un almacén de instancias como en Amazon EBS, los dos espacios de tablas tienen características de rendimiento significativamente diferentes. Oracle Database elige el espacio de tablas para atender las consultas en función de un algoritmo interno. Por lo tanto, el rendimiento de consultas similares puede variar.

Por lo general, se crea un espacio de tablas temporal en el almacén de instancias de la siguiente manera:

1. Cree un espacio de tablas temporal en el almacén de instancias.
2. Configure el nuevo espacio de tablas como el espacio de tabla temporal predeterminado de la base de datos.

Si el tamaño del espacio de tablas del almacén de instancias es insuficiente, puede crear almacenamiento temporal adicional de la siguiente manera:

1. Asigne el espacio de tablas temporal del almacén de instancias a un grupo de espacios de tablas temporales.
2. Cree un nuevo espacio de tablas temporal en Amazon EBS si no existe ninguno.
3. Asigne el espacio de tablas temporal de Amazon EBS al mismo grupo de espacios de tablas que incluye el espacio de tablas del almacén de instancias.
4. Configure el grupo de espacios de tablas como el espacio de tabla temporal predeterminado.

En el siguiente ejemplo, se suponeque el tamaño del espacio de tablas temporal del almacén de instancias no cumple con los requisitos de la aplicación. En el ejemplo se crea el espacio de tablas temporal `temp_in_inst_store` en el almacén de instancias, se asigna al grupo de espacios de tablas `temp_group`, se agrega el espacio de tablas de Amazon EBS existente denominado `temp_in_ebs` a este grupo y se establece este grupo como el espacio de tablas temporal predeterminado.

```
SQL> EXEC rdsadmin.rdsadmin_util.create_inst_store_tmp_tblspace('temp_in_inst_store');

PL/SQL procedure successfully completed.

SQL> ALTER TABLESPACE temp_in_inst_store TABLESPACE GROUP temp_group;

Tablespace altered.

SQL> ALTER TABLESPACE temp_in_ebs TABLESPACE GROUP temp_group;
```

```
Tablespace altered.

SQL> EXEC rdsadmin.rdsadmin_util.alter_default_temp_tablespace('temp_group');

PL/SQL procedure successfully completed.

SQL> SELECT * FROM DBA_TABLESPACE_GROUPS;

GROUP_NAME                     TABLESPACE_NAME
------------------------------ ------------------------------
TEMP_GROUP                     TEMP_IN_EBS
TEMP_GROUP                     TEMP_IN_INST_STORE

SQL> SELECT PROPERTY_VALUE FROM DATABASE_PROPERTIES WHERE
 PROPERTY_NAME='DEFAULT_TEMP_TABLESPACE';

PROPERTY_VALUE
--------------
TEMP_GROUP
```

Eliminación de un almacén de instancias de RDS para Oracle

Para quitar el almacén de instancias, modifique la instancia de base de datos de RDS para Oracle para utilizar un tipo de instancia que no admita el almacén de instancias, como db.m5 o db.r5.

Activación de páginas de gran tamaño para una instancia de RDS para Oracle

Amazon RDS for Oracle es compatible con las páginas enormes del kernel de Linux para aumentar la escalabilidad de la base de datos. El uso de HugePages deriva en tablas de páginas más pequeñas y menos tiempo dedicado por la CPU a la administración de memoria, lo que aumenta el rendimiento de instancias de base de datos grandes. Para obtener más información, consulte Overview of HugePages en la documentación de Oracle.

Puede utilizar HugePages con todas las versiones y ediciones compatibles de RDS para Oracle.

El parámetro `use_large_pages` controla si las páginas de gran tamaño están activadas para una instancia de base de datos. Los valores posibles para este parámetro son `ONLY`, `FALSE` y `{DBInstanceClassHugePagesDefault}`. El parámetro `use_large_pages` se define

en {DBInstanceClassHugePagesDefault} en el grupo de parámetros de base de datos predeterminado para Oracle.

Para comprobar si se han activado las páginas de gran tamaño para una instancia de base de datos de forma automática, puede utilizar la variable de la fórmula DBInstanceClassHugePagesDefault en los grupos de parámetros. El valor se determina de la siguiente manera:

- Para las clases de instancia de base de datos mencionadas en la tabla siguiente, DBInstanceClassHugePagesDefault siempre toma el valor FALSE de forma predeterminada y use_large_pages toma el valor FALSE. Puede activar páginas de gran tamaño manualmente para estas clases de instancia de base de datos si la clase de instancia de base de datos dispone de al menos 14 GiB de memoria.
- Para las clases de instancia de base de datos no mencionadas en la tabla siguiente, si la clase de instancia de base de datos tiene menos de 14 GiB de memoria, DBInstanceClassHugePagesDefault siempre toma el valor FALSE. Además, use_large_pages toma el valor FALSE.
- Para las clases de instancia de base de datos no mencionadas en la tabla siguiente, si la clase de instancia tiene al menos 14 GiB de memoria y menos de 100 GiB de memoria, DBInstanceClassHugePagesDefault toma el valor TRUE de forma predeterminada. Además, use_large_pages toma el valor ONLY. Puede desactivar las páginas de gran tamaño manualmente estableciendo use_large_pages en FALSE.
- Para las clases de instancia de base de datos no mencionadas en la tabla siguiente, si la clase de instancia tiene al menos 100 GiB de memoria, DBInstanceClassHugePagesDefault siempre toma el valor TRUE. Además, use_large_pages toma el valor ONLY y las páginas de gran tamaño no se pueden desactivar.

Las páginas de gran tamaño no están activadas de forma predeterminada para las siguientes clases de instancia de base de datos.

Familia de clase de instancia de base de datos	Las clases de instancia de base de datos con páginas de gran tamaño no están activadas de forma predeterminada
db.m5	db.m5.large

Familia de clase de instancia de base de datos	Las clases de instancia de base de datos con páginas de gran tamaño no están activadas de forma predeterminada
db.m4	db.m4.large, db.m4.xlarge, db.m4.2xlarge, db.m4.4xlarge, db.m4.10xlarge
db.t3	db.t3.micro, db.t3.small, db.t3.medium, db.t3.large

Para obtener más información acerca de las clases de instancias de bases de datos, consulte Especificaciones de hardware para clases de instancia de base de datos .

Para activar manualmente las páginas de gran tamaño para las instancias de bases de datos nuevas o existentes, establezca el parámetro `use_large_pages` en `ONLY`. No es posible utilizar las páginas enormes con Oracle Automatic Memory Management (AMM). Si establece el parámetro `use_large_pages` en `ONLY`, también debe establecer `memory_target` y `memory_max_target` en `0`. Para obtener más información acerca de cómo configurar parámetros de base de datos para la instancia de base de datos, consulte Grupos de parámetros para Amazon RDS.

También puede configurar los parámetros `sga_target`, `sga_max_size` y `pga_aggregate_target`. Cuando establezca los parámetros de memoria de área global del sistema (SGA) y de área global del programa (PGA), sume ambos valores. Reste este total de la memoria disponible en la instancia (`DBInstanceClassMemory`) para determinar la memoria que queda libre después de la asignación de las páginas enormes. Debe dejar libres como mínimo 2 GiB, o el 10 por ciento de la memoria total disponible de la instancia, lo que sea menor.

Después de configurar los parámetros, debe reiniciar la instancia de base de datos para que los cambios surtan efecto. Para obtener más información, consulte Reinicio de una instancia de base de datos.

> **Note**
>
> La instancia de base de datos de Oracle aplaza los cambios en los parámetros de inicialización relacionados con SGA hasta que se reinicie la instancia sin conmutación por error. En la consola de Amazon RDS, elija Reiniciar pero no elija Reiniciar con conmutación por error. En la AWS CLI, llame al comando `reboot-db-instance` con el parámetro `--no-force-failover`. La instancia de base de datos no procesa los parámetros

relacionados con SGA durante la conmutación por error o durante otras operaciones de mantenimiento que hacen que la instancia se reinicie.

A continuación se muestra una configuración de parámetros de ejemplo de páginas de gran tamaño que habilita las páginas de gran tamaño manualmente. Debe establecer los valores de acuerdo con sus necesidades.

```
memory_target            = 0
memory_max_target        = 0
pga_aggregate_target     = {DBInstanceClassMemory*1/8}
sga_target               = {DBInstanceClassMemory*3/4}
sga_max_size             = {DBInstanceClassMemory*3/4}
use_large_pages          = ONLY
```

Suponga que se definen los siguientes valores de parámetro en un grupo de parámetros.

```
memory_target            = IF({DBInstanceClassHugePagesDefault}, 0,
 {DBInstanceClassMemory*3/4})
memory_max_target        = IF({DBInstanceClassHugePagesDefault}, 0,
 {DBInstanceClassMemory*3/4})
pga_aggregate_target     = IF({DBInstanceClassHugePagesDefault},
 {DBInstanceClassMemory*1/8}, 0)
sga_target               = IF({DBInstanceClassHugePagesDefault},
 {DBInstanceClassMemory*3/4}, 0)
sga_max_size             = IF({DBInstanceClassHugePagesDefault},
 {DBInstanceClassMemory*3/4}, 0)
use_large_pages          = {DBInstanceClassHugePagesDefault}
```

El grupo de parámetros es utilizado por una clase de instancia db.r4 DB que tiene menos de 100 GiB de memoria. Con esta configuración de parámetros y `use_large_pages` establecido en `{DBInstanceClassHugePagesDefault}`, las páginas de gran tamaño están activadas en la instancia db.r4.

Vea otro ejemplo con los siguientes valores de parámetros definidos en un grupo de parámetros.

```
memory_target           = IF({DBInstanceClassHugePagesDefault}, 0,
 {DBInstanceClassMemory*3/4})
memory_max_target       = IF({DBInstanceClassHugePagesDefault}, 0,
 {DBInstanceClassMemory*3/4})
```

```
pga_aggregate_target    = IF({DBInstanceClassHugePagesDefault},
 {DBInstanceClassMemory*1/8}, 0)
sga_target              = IF({DBInstanceClassHugePagesDefault},
 {DBInstanceClassMemory*3/4}, 0)
sga_max_size            = IF({DBInstanceClassHugePagesDefault},
 {DBInstanceClassMemory*3/4}, 0)
use_large_pages         = FALSE
```

Una clase de instancia de base de datos db.r4 y db.r5 usa el grupo de parámetros, ambas con menos de 100 GiB de memoria. Con esta configuración de parámetros, las páginas de gran tamaño están desactivadas en las instancias db.r4 y db.r5.

> **Note**
>
> Si una clase de instancia de base de datos db.r4 o db.r5 DB con al menos 100 GiB de memoria utiliza este grupo de parámetros, se anula el valor `FALSE` de `use_large_pages` y se cambia por `ONLY`. En este caso, se envía una notificación de cliente sobre la anulación.

Después de activar las páginas de gran tamaño en la instancia de base de datos, puede ver la información sobre las páginas de gran tamaño activando el monitoreo mejorado. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Activación de tipos de datos extendidos en RDS para Oracle

Amazon RDS for Oracle es compatible con tipos de datos extendidos. Con tipos de datos extendidos, el tamaño máximo es 32 767 bytes para los tipos de datos `VARCHAR2`, `NVARCHAR2` y `RAW`. Para usar tipos de datos extendidos, configure el parámetro `MAX_STRING_SIZE` como `EXTENDED`. Para obtener más información, consulte Extended Data Types en la documentación de Oracle.

Si no desea utilizar tipos de datos extendidos, mantenga el parámetro `MAX_STRING_SIZE` establecido en `STANDARD`. En este caso, los límites de tamaño son de 4000 bytes para los tipos de datos `VARCHAR2` y `NVARCHAR2`, y de 2000 bytes para el tipo de datos RAW.

Puede activar tipos de datos extendidos en una instancia de base de datos nueva o existente. Para instancias de base de datos nuevas, el tiempo de creación de instancias de base de datos suele ser más largo cuando se activan tipos de datos extendidos. Para instancias de base de datos existentes, la instancia de base de datos no está disponible durante el proceso de conversión.

Consideraciones sobre los tipos de datos extendidos

Tenga en cuenta lo siguiente al habilitar los tipos de datos extendidos para su instancia de base de datos:

- Cuando activa tipos de datos nuevos o existentes para una instancia de base de datos nueva o existente, debe reiniciar la instancia para que el cambio se aplique.
- Cuando active tipos de datos extendidos, no podrá volver a cambiar la instancia de base de datos para usar el tamaño estándar de los tipos de datos. Si vuelve a configurar el parámetro `MAX_STRING_SIZE` en `STANDARD`, se obtendrá el estado `incompatible-parameters`.
- Cuando restaura una instancia de base de datos que utilizado tipos de datos extendidos, tiene que especificar un grupo de parámetros con el parámetro `MAX_STRING_SIZE` establecido en `EXTENDED`. Durante la restauración, si especifica el grupo de parámetros predeterminado o cualquier grupo de parámetros con `MAX_STRING_SIZE` establecido en `STANDARD` produce el estado `incompatible-parameters`.
- Cuando el estado de la instancia de base de datos es `incompatible-parameters` debido al ajuste `MAX_STRING_SIZE`, la instancia de la base de datos se mantiene no disponible hasta que estable el parámetro `MAX_STRING_SIZE` en `EXTENDED` y reinicia la instancia de base de datos.

Activación de tipos de datos extendidos para una instancia de base de datos nueva

Al crear una instancia de base de datos con `MAX_STRING_SIZE` establecido en `EXTENDED`, la instancia muestra `MAX_STRING_SIZE` con el valor predeterminado `STANDARD`. Reinicie la instancia para aplicar el cambio.

Para activar tipos de datos extendidos para una instancia de base de datos nueva

1. Establezca en el parámetro `MAX_STRING_SIZE` en `EXTENDED` en un grupo de parámetros.

   Para establecer el parámetro, puede crear un grupo de parámetros nuevo o modificar un grupo de parámetros existente.

   Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
2. Cree una nueva instancia de base de datos de RDS para Oracle.

   Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

3. Asocie el nuevo grupo de parámetros con `MAX_STRING_SIZE` establecido en `EXTENDED` con la instancia de base de datos.

   Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

4. Reinicie la instancia de base de datos para que el cambio de parámetro tenga efecto.

   Para obtener más información, consulte Reinicio de una instancia de base de datos.

Activación de tipos de datos extendidos para una instancia de base de datos existente

Cuando modifique una instancia de base de datos para activar tipos de datos extendidos, RDS convierte los datos de la base de datos para que usen los tamaños extendidos. La conversión y el tiempo de inactividad se producen la próxima vez que se reinicie la base de datos tras el cambio de parámetro. La instancia de base de datos no está disponible durante la conversión.

La cantidad de tiempo que lleva convertir los datos depende de la clase de instancia de base de datos, el tamaño de la base de datos y el tiempo de la instantánea de la base de datos. Para reducir el tiempo de inactividad, considere la posibilidad de tomar una instantánea inmediatamente antes de reiniciar. Esto acorta el tiempo de la copia de seguridad que se produce durante el flujo de trabajo de conversión.

> **Note**
>
> Después de activar tipos de datos extendidos, no es posible realizar una restauración a un momento coincidente con la conversión. Puede realizar la restauración a un momento inmediatamente antes de la conversión o después de la conversión.

Para activar tipos de datos extendidos para una instancia de base de datos existente

1. Tome una instantánea de la base de datos.

   Si hay objetos no válidos en la base de datos, Amazon RDS intenta volver a compilarlos. La conversión a tipos de datos extendidos puede producir error si Amazon RDS no puede volver a compilar un objeto no válido. La instantánea le permite restaurar la base de datos si se produce un problema con la conversión. Compruebe siempre la presencia de objetos no válidos antes de la conversión y corrija o elimine esos objetos no válidos. Para bases de datos de producción,

recomendamos poner a prueba el proceso de conversión en una copia de su instancia de base de datos en primer lugar.

Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

2. Establezca en el parámetro `MAX_STRING_SIZE` en `EXTENDED` en un grupo de parámetros.

   Para establecer el parámetro, puede crear un grupo de parámetros nuevo o modificar un grupo de parámetros existente.

   Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

3. Modifique la instancia de base de datos para asociarla con el grupo de parámetros con `MAX_STRING_SIZE` establecido en `EXTENDED`.

   Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

4. Reinicie la instancia de base de datos para que el cambio de parámetro tenga efecto.

   Para obtener más información, consulte Reinicio de una instancia de base de datos.

Importación de datos a Oracle en Amazon RDS

La forma de importar datos a una instancia de base de datos de Amazon RDS para Oracle depende de lo siguiente

- La cantidad de datos que tiene
- El número de objetos de base de datos en la base de datos
- La variedad de objetos de base de datos en la base de datos

Por ejemplo, puede utilizar las siguientes herramientas, en funcion de sus requisitos:

- Oracle SQL Developer: importe una base de datos sencilla de 20 MB.
- Oracle Data Pump: importe bases de datos complejas o con un tamaño de varios cientos de megabytes o varios terabytes. Por ejemplo, puede transportar espacios de tabla desde una base de datos en las instalaciones a su instancia de base de datos de RDS para Oracle. Puede utilizar Amazon S3 o Amazon EFS para transferir los archivos de datos y los metadatos. Para obtener más información, consulte Migración mediante espacios de tabla transportables de Oracle, Integración de Amazon EFS y Integración de Amazon S3.
- AWS Database Migration Service (AWS DMS): migre bases de datos sin tiempo de inactividad. Para obtener más información acerca de AWS DMS, consulte ¿Qué es AWS Database Migration Service y la publicación del blog sobre la migración de bases de datos de Oracle con tiempo de inactividad casi nulo mediante DMS de AWS.

> **Important**
>
> Antes de utilizar estas técnicas de migración, le recomendamos que realice una copia de seguridad de la base de datos. Después de importar los datos, puede realizar una copia de seguridad de sus instancias de base de datos de RDS para Oracle creando instantáneas. Posteriormente, puede restaurar las instantáneas. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

Para muchos motores de base de datos, la replicación continua puede continuar hasta que esté listo para cambiar a la base de datos de destino. Puede utilizar AWS DMS para migrar a RDS para Oracle desde el mismo motor de base de datos o desde un motor diferente. Si migra desde un motor

de base de datos diferente, puede utilizar AWS Schema Conversion Tool para migrar objetos de esquema que AWS DMS no migra.

Temas

- Importación mediante Oracle SQL Developer
- Migración mediante espacios de tabla transportables de Oracle
- Importación mediante Oracle Data Pump
- Importación mediante exportación/importación de Oracle
- Importación mediante Oracle SQL*Loader
- Migración de vistas materializadas de Oracle

Importación mediante Oracle SQL Developer

Oracle SQL Developer es una herramienta gráfica desarrollada en Java y distribuida sin coste por Oracle. SQL Developer proporciona opciones para migrar datos entre dos bases de datos de Oracle o para migrar datos de otras bases de datos, como MySQL, a una base de datos Oracle. Esta herramienta es la opción más adecuada para migrar bases de datos pequeñas.

Puede instalar esta herramienta en un equipo de escritorio (Windows, Linux o Mac) o en uno de sus servidores. Después de instalar SQL Developer, puede utilizarlo para conectarse a las bases de datos de origen y de destino. Utilice el comando Copia de base de datos del menú Herramientas para copiar datos en la instancia de base de datos de RDS para Oracle.

Para descargar SQL Developer, vaya a http://www.oracle.com/technetwork/developer-tools/sql-developer.

Recomendamos que lea la documentación del producto Oracle SQL Developer antes de comenzar a migrar datos. Oracle también tiene documentación acerca de cómo migrar desde otras bases de datos, como MySQL y SQL Server. Para obtener más información, consulte http://www.oracle.com/technetwork/database/migration en la documentación de Oracle.

Migración mediante espacios de tabla transportables de Oracle

Puede utilizar la característica de espacios de tabla transportables de Oracle para copiar un conjunto de espacios de tabla de una base de datos de Oracle en las instalaciones a una instancia de base de datos de RDS para Oracle. En el nivel físico, los archivos de datos de origen y los archivos de metadatos se transfieren a la instancia de base de datos de destino mediante Amazon

EFS o Amazon S3. La característica de espacios de tabla transportables utiliza el paquete `rdsadmin.rdsadmin_transport_util`. Para obtener información sobre la sintaxis y la semántica de este paquete, consulte Transporte de espacios de tabla.

Para ver publicaciones de blog que explican cómo transportar espacios de tabla, consulte Migrate Oracle Databases to AWS using transportable tablespace y Amazon RDS for Oracle Transportable Tablespaces using RMAN.

Temas

- Descripción general de los espacios de tabla transportables de Oracle
- Fase 1: Configurar el host de origen
- Fase 2: Preparar la copia de seguridad completa del espacio de tabla
- Fase 3: Realizar y transferir copias de seguridad incrementales
- Fase 4: Transportar los espacios de tabla
- Fase 5: Validar los espacios de tabla transportados
- Fase 6: Limpiar los archivos sobrantes

Descripción general de los espacios de tabla transportables de Oracle

Un conjunto de espacios de tabla transportables consta de archivos de datos para el conjunto de espacios de tabla que se transportan y un archivo de volcado de exportación que contiene los metadatos del espacio de tabla. En una solución de migración física, como los espacios de tabla transportables, se transfieren archivos físicos: archivos de datos, archivos de configuración y archivos de volcado de Data Pump.

Temas

- Ventajas y desventajas de los espacios de tabla transportables
- Limitaciones de los espacios de tabla transportables
- Requisitos previos para los espacios de tabla transportables

Ventajas y desventajas de los espacios de tabla transportables

Le recomendamos que utilice espacios de tabla transportables cuando tenga que migrar uno o más espacios de tabla grandes a RDS con un tiempo de inactividad mínimo. Los espacios de tabla transportables ofrecen las siguientes ventajas con respecto a la migración lógica:

- El tiempo de inactividad es inferior al de la mayoría de las demás soluciones de migración de Oracle.
- Dado que la característica de espacio de tabla transportable solo copia archivos físicos, evita los errores de integridad de los datos y la corrupción lógica que pueden producirse en la migración lógica.
- No se requiere ninguna licencia adicional.
- Puede migrar un conjunto de espacios de tabla en diferentes plataformas y tipos de endianness, por ejemplo, de una plataforma Oracle Solaris a Linux. Sin embargo, no se admite el transporte de espacios de tabla hacia y desde servidores Windows.

> **Note**
>
> Linux está totalmente probado y es compatible. No se han probado todas las variantes de UNIX.

Si usa espacios de tabla transportables, puede transportar datos mediante Amazon S3 o Amazon EFS:

- Si utiliza EFS, las copias de seguridad permanecen en el sistema de archivos EFS durante la importación. Podrá eliminar los archivos después. En esta técnica, no es necesario aprovisionar el almacenamiento de EBS para la instancia de base de datos. Por este motivo, se recomienda utilizar Amazon EFS en lugar de S3. Para obtener más información, consulte Integración de Amazon EFS.
- Si usa S3, debe descargar las copias de seguridad de RMAN al almacenamiento de EBS adjunto a su instancia de base de datos. Los archivos permanecerán en su almacenamiento de EBS durante la importación. Tras la importación, puede liberar este espacio, que sigue asignado a la instancia de base de datos.

La principal desventaja de los espacios de tabla transportables es que se necesitan conocimientos relativamente avanzados de Oracle Database. Para obtener más información, consulte el tema sobre cómo transportar espacios de tabla entre bases de datos en la Guía del administrador de bases de datos de Oracle.

Limitaciones de los espacios de tabla transportables

Las limitaciones de Oracle Database para los espacios de tabla transportables se aplican cuando se utiliza esta característica en RDS para Oracle. Para obtener más información, consulte los apartados sobre limitaciones de los espacios de tabla transportables y limitaciones generales del transporte de datos en la Guía del administrador de bases de datos de Oracle. Tenga en cuenta las siguientes limitaciones adicionales para los espacios de tabla transportables en RDS para Oracle:

- Ni la base de datos de origen ni la de destino pueden utilizar Standard Edition 2 (SE2). Solo se admite la edición Enterprise.
- No puede utilizar una base de datos Oracle Database 11g como origen. La característica de espacios de tablas transportables multiplataforma de RMAN se basa en el mecanismo de transporte RMAN, que Oracle Database 11g no admite.
- No puede migrar datos de una instancia de base de datos de RDS para Oracle mediante espacios de tabla transportables. Solo puede usar espacios de tabla transportables para migrar datos a una instancia de base de datos de RDS para Oracle.
- No admite el sistema operativo Windows.
- No puede transportar espacios de tabla a una base de datos con un nivel de versión inferior. La base de datos de destino debe estar en el mismo nivel de versión o en una versión posterior que la base de datos de origen. Por ejemplo, no puede transportar espacios de tabla de Oracle Database 21c a Oracle Database 19c.
- No puede transportar espacios de tablas administrativas como `SYSTEM` y `SYSAUX`.
- No puede transportar objetos que no sean de datos, como paquetes PL/SQL, clases de Java, vistas, desencadenadores, secuencias, usuarios, roles y tablas temporales. Para transportar objetos que no sean de datos, créelos manualmente o utilice la exportación e importación de metadatos de Data Pump. Para obtener más información, consulte My Oracle Support Note 1454872.1.
- No puede transportar espacios de tabla cifrados ni utilizar columnas cifradas.
- Si transfiere archivos mediante Amazon S3, el tamaño máximo de archivo admitido será de 5 TiB.
- Si la base de datos de origen utiliza opciones de Oracle, como Spatial, no podrá transportar espacios de tabla a menos que se configuren las mismas opciones en la base de datos de destino.
- No puede transportar espacios de tabla a una instancia de base de datos de RDS para Oracle en una configuración de réplica de Oracle. Como solución alternativa, puede eliminar todas las réplicas, transportar los espacios de tabla y, a continuación, volver a crear las réplicas.

Requisitos previos para los espacios de tabla transportables

Antes de empezar, complete las siguientes tareas:

- Revise los requisitos de los espacios de tabla transportables que se describen en los siguientes documentos de My Oracle Support:
  - Reduzca el tiempo de inactividad del espacio de tabla transportable mediante la copia de seguridad incremental multiplataforma (ID del documento 2471245.1)
  - Restricciones y limitaciones del espacio de tabla transportable (TTS): detalles, referencia y versión, según corresponda (ID del documento 1454872.1)
  - Nota principal sobre los espacios de tabla transportables (TTS): preguntas y problemas frecuentes (ID del documento 1166564.1)
- Planifique la conversión de endianness. Si especifica el ID de la plataforma de origen, RDS para Oracle convierte el endianness automáticamente. Para obtener información sobre cómo encontrar los ID de plataforma, consulte Data Guard Support for Heterogeneous Primary and Physical Standbys in Same Data Guard Configuration (Doc ID 413484.1) (Compatibilidad de Data Guard para instancias en espera principales y físicas heterogéneos en la misma configuración de Data Guard).
- Asegúrese de que la característica de espacio de tabla transportable esté habilitada en la instancia de base de datos de destino. La característica solo está habilitada si no reciben ningún error `ORA-20304` al ejecutar la siguiente consulta:

  ```
  SELECT * FROM TABLE(rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files);
  ```

  Si la característica de espacio de tabla transportable no está habilitada, reinicie la instancia de base de datos. Para obtener más información, consulte Reinicio de una instancia de base de datos.
- Compruebe que el archivo de zona horaria sea el mismo en las bases de datos de origen y destino.
- Compruebe que los juegos de caracteres de las bases de datos de origen y destino cumplen alguno de los siguientes requisitos:
  - Los conjuntos de caracteres son los mismos.
  - Los conjuntos de caracteres son compatibles. Para obtener una lista de los requisitos de compatibilidad, consulte General Limitations on Transporting Data en la documentación de Oracle Database.

- Si tiene previsto transferir archivos mediante Amazon S3, haga lo siguiente:
  - Asegúrese de que haya un bucket de Amazon S3 disponible para las transferencias de archivos, y de que el bucket de Amazon S3 esté en la misma región de AWS que la instancia de base de datos. Para ver las instrucciones, consulte Crear un bucket en la Guía de introducción de Amazon Simple Storage Service.
  - Debe preparar el bucket de Amazon S3 para la integración de Amazon RDS siguiendo las instrucciones de Configuración de permisos IAM para la integración de RDS para Oracle con Amazon S3.
- Si tiene previsto transferir archivos mediante Amazon EFS, asegúrese de haber configurado EFS según las instrucciones de Integración de Amazon EFS.
- Le recomendamos encarecidamente que active las copias de seguridad automáticas en la instancia de base de datos de destino. Dado que el paso de importación de metadatos puede fallar, es importante poder restaurar la instancia de base de datos al estado anterior a la importación, para evitar la necesidad de realizar copias de seguridad, transferir e importar los espacios de tabla de nuevo.

Fase 1: Configurar el host de origen

En este paso, se copian los scripts de espacios de tabla transportables proporcionados por My Oracle Support y se configuran los archivos de configuración necesarios. En los siguientes pasos, el host de origen ejecuta la base de datos que contiene los espacios de tabla que se transportarán a la instancia de destino.

Para configurar el host de origen

1. Inicie sesión en su host de origen como propietario de su inicio de Oracle.
2. Asegúrese de que sus variables de entorno `ORACLE_HOME` y `ORACLE_SID` apunten hacia la base de datos de origen.
3. Inicie sesión en la base de datos como administrador y compruebe que la versión de zona horaria, el juego de caracteres de la base de datos y el conjunto de caracteres nacionales sean los mismos que los de la base de datos de destino.

```
SELECT * FROM V$TIMEZONE_FILE;
SELECT * FROM NLS_DATABASE_PARAMETERS
  WHERE PARAMETER IN ('NLS_CHARACTERSET','NLS_NCHAR_CHARACTERSET');
```

4. Configure la utilidad de espacio de tabla transportable tal como se describe en la nota de soporte de Oracle 2471245.1.

   La configuración incluye la edición del archivo `xtt.properties` en el host de origen. El siguiente archivo `xtt.properties` de ejemplo especifica las copias de seguridad de tres espacios de tabla del directorio `/dsk1/backups`. Estos son los espacios de tabla que pretende transportar a la instancia de base de datos de destino. También especifica el ID de la plataforma de origen para convertir el endianness automáticamente.

   > **Note**
   >
   > Para encontrar los ID de plataforma válidos, consulte Data Guard Support for Heterogeneous Primary and Physical Standbys in Same Data Guard Configuration (Doc ID 413484.1) (Compatibilidad de Data Guard para instancias en espera principales y físicas heterogéneos en la misma configuración de Data Guard).

```
#linux system
platformid=13
#list of tablespaces to transport
tablespaces=TBS1,TBS2,TBS3
#location where backup will be generated
src_scratch_location=/dsk1/backups
#RMAN command for performing backup
usermantransport=1
```

Fase 2: Preparar la copia de seguridad completa del espacio de tabla

En esta fase, realiza una copia de seguridad de los espacios de tabla por primera vez, transfiere las copias de seguridad al host de destino y, a continuación, las restaura siguiendo el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces`. Cuando se complete esta fase, las copias de seguridad iniciales del espacio de tabla estarán en la instancia de base de datos de destino y se podrán actualizar con copias de seguridad incrementales.

Temas

- Paso 1: realice copias de seguridad de los espacios de tabla en el host de origen
- Paso 2: transfiera los archivos de copia de seguridad a la instancia de base de datos de destino

- Paso 3: importe los espacios de tabla en la instancia de base de datos de destino

Paso 1: realice copias de seguridad de los espacios de tabla en el host de origen

En este paso, utilizará el script `xttdriver.pl` para hacer una copia de seguridad completa de sus espacios de tabla. La salida de `xttdriver.pl` se almacena en la variable de entorno `TMPDIR`.

Para hacer una copia de seguridad de los espacios de tabla

1. Si los espacios de tabla están en modo de solo lectura, inicie sesión en la base de datos de origen como usuario con el privilegio `ALTER TABLESPACE` y coloque los espacios de tabla en modo de lectura/escritura. De no ser así, vaya al siguiente paso.

   En el siguiente ejemplo se establecen `tbs1`, `tbs2` y `tbs3` en modo de lectura/escritura.

   ```
   ALTER TABLESPACE tbs1 READ WRITE;
   ALTER TABLESPACE tbs2 READ WRITE;
   ALTER TABLESPACE tbs3 READ WRITE;
   ```

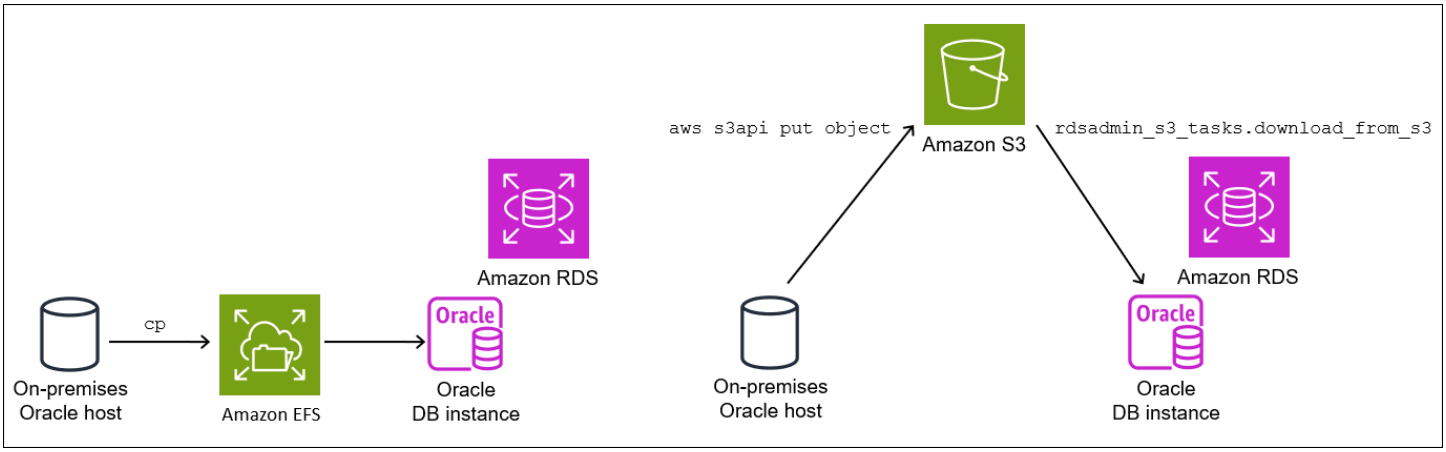
2. Realice una copia de seguridad de los espacios de tabla con el script `xttdriver.pl`. Si lo desea, puede especificar `--debug` para que ejecute el script en modo de depuración.

   ```
   export TMPDIR=location_of_log_files
   cd location_of_xttdriver.pl
   $ORACLE_HOME/perl/bin/perl xttdriver.pl --backup
   ```

Paso 2: transfiera los archivos de copia de seguridad a la instancia de base de datos de destino

En este paso, debe copiar los archivos de copia de seguridad y de configuración de la ubicación inicial a la instancia de base de datos de destino. Seleccione una de las siguientes opciones:

- Si los hosts de origen y destino comparten un sistema de archivos de Amazon EFS, use una utilidad del sistema operativo, por ejemplo, `cp`, para copiar los archivos de copia de seguridad y el archivo `res.txt` de su ubicación inicial a un directorio compartido. A continuación, diríjase a Paso 3: importe los espacios de tabla en la instancia de base de datos de destino.
- Si necesita organizar sus copias de seguridad en un bucket de Amazon S3, siga estos pasos.



Paso 2.2: Cargar las copias de seguridad en el bucket de Amazon S3

Cargue las copias de seguridad y el archivo `res.txt` del directorio inicial al bucket de Amazon S3. Para obtener más información, consulte Carga de objetos en la Guía del desarrollador de Amazon Simple Storage Service.

Paso 2.3: Descargar las copias de seguridad desde el bucket de Amazon S3 a la instancia de base de datos de destino

En este paso, utilizará el procedimiento `rdsadmin.rdsadmin_s3_tasks.download_from_s3` para descargar las copias de seguridad en la instancia de base de datos de RDS para Oracle.

Para descargar las copias de seguridad del bucket de Amazon S3

1. Inicie SQL*Plus u Oracle SQL Developer e inicie sesión en la instancia de base de datos de destino de RDS para Oracle.
2. Descargue las copias de seguridad del bucket de Amazon S3 en la instancia de base de datos de destino mediante el procedimiento de Amazon RDS `rdsadmin.rdsadmin_s3_tasks.download_from_s3` para d. En el siguiente ejemplo se descargan todos los archivos de un bucket de Amazon S3 denominado *`amzn-s3-demo-bucket`* en el directorio *`DATA_PUMP_DIR`*.

```
EXEC UTL_FILE.FREMOVE ('DATA_PUMP_DIR', 'res.txt');
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
  p_bucket_name    =>  'amzn-s3-demo-bucket',
  p_directory_name =>  'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

La instrucción SELECT devuelve el identificador de la tarea en un tipo de datos VARCHAR2. Para obtener más información, consulte Descarga de archivos desde un bucket de Amazon S3 en una instancia de base de datos de Oracle.

Paso 3: importe los espacios de tabla en la instancia de base de datos de destino

Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces` para restaurar los espacios de tabla en la instancia de base de datos de destino. Este procedimiento convierte automáticamente los archivos de datos al formato endian correcto.

Si realiza la importación desde una plataforma que no sea Linux, especifique la plataforma de origen mediante el parámetro `p_platform_id` cuando llame a `import_xtts_tablespaces`. Asegúrese de que el id. de plataforma coincida con el especificado en el archivo `xtt.properties` en Paso 2: exporte los metadatos del espacio de tabla en el host de origen.

Importar los espacios de tabla en la instancia de base de datos de destino

1. Inicie un cliente de Oracle SQL e inicie sesión como usuario maestro en su instancia de base de datos de destino de RDS para Oracle.
2. Ejecute el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces` y especifique los espacios de tabla que se van a importar y el directorio que contiene las copias de seguridad.

   En el siguiente ejemplo se importan los espacios de tabla *TBS1*, *TBS2* y *TBS3* del directorio *DATA_PUMP_DIR*. La plataforma de origen es AIX-Based Systems (64 bits), con el id. de plataforma 6. Puede encontrar los id. de plataforma consultando `V$TRANSPORTABLE_PLATFORM`.

```
VAR task_id CLOB

BEGIN
  :task_id:=rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces(
        'TBS1,TBS2,TBS3',
        'DATA_PUMP_DIR',
        p_platform_id => 6);
END;
/
```

```
PRINT task_id
```

3. (Opcional) Supervise el progreso consultando la tabla `rdsadmin.rds_xtts_operation_info`. La columna `xtts_operation_state` muestra el valor `EXECUTING`, `COMPLETED` o `FAILED`.

```
SELECT * FROM rdsadmin.rds_xtts_operation_info;
```

> **Note**
>
> Para operaciones de larga duración, también puede consultar `V$SESSION_LONGOPS`, `V$RMAN_STATUS` y `V$RMAN_OUTPUT`.

4. Para ver el registro de la importación finalizada, utilice el ID de la tarea del paso anterior.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||'&task_id'||'.log'));
```

Asegúrese de que se haya completado correctamente la importación antes de continuar con el siguiente paso.

Fase 3: Realizar y transferir copias de seguridad incrementales

En esta fase, se realizan y transfieren copias de seguridad incrementales periódicamente mientras la base de datos de origen esté activa. Esta técnica reduce el tamaño de la copia de seguridad final del espacio de tabla. Si realiza varias copias de seguridad incrementales, debe copiar el archivo `res.txt` después de la última copia de seguridad incremental antes de poder aplicarlo en la instancia de destino.

Los pasos son los mismos que en Fase 2: Preparar la copia de seguridad completa del espacio de tabla, excepto que el paso de importación es opcional.

Fase 4: Transportar los espacios de tabla

En esta fase, se realiza una copia de seguridad de los espacios de tabla de solo lectura y se exportan los metadatos de Data Pump, se transfiere estos archivos al host de destino y se importan tanto los espacios de tabla como los metadatos.

Temas

- Paso 1: realice una copia de seguridad de los espacios de tabla de solo lectura
- Paso 2: exporte los metadatos del espacio de tabla en el host de origen
- Paso 3: (solo Amazon S3) transfiera los archivos de copia de seguridad y exporte los archivos a la instancia de base de datos de destino
- Paso 4: Importar los espacios de tabla en la instancia de base de datos de destino
- Paso 5: Importar los metadatos del espacio de tabla en la instancia de base de datos de destino

Paso 1: realice una copia de seguridad de los espacios de tabla de solo lectura

Este paso es idéntico al Paso 1: realice copias de seguridad de los espacios de tabla en el host de origen, salvo que aquí se establecen los espacios de tabla en modo de solo lectura antes de hacer una copia de seguridad de los espacios de tabla por última vez.

En el siguiente ejemplo se establecen `tbs1`, `tbs2` y `tbs3` en modo de solo lectura.

```
ALTER TABLESPACE tbs1 READ ONLY;
ALTER TABLESPACE tbs2 READ ONLY;
ALTER TABLESPACE tbs3 READ ONLY;
```

Paso 2: exporte los metadatos del espacio de tabla en el host de origen

Para exportar los metadatos del espacio de tabla, ejecute la utilidad `expdb` en el host de origen. En el siguiente ejemplo se exportan los espacios de tabla *`TBS1`*, *`TBS2`* y *`TBS3`* al archivo de volcado *`xttdump.dmp`* en el directorio *`DATA_PUMP_DIR`*.

```
expdp username/pwd \
dumpfile=xttdump.dmp \
directory=DATA_PUMP_DIR \
statistics=NONE \
transport_tablespaces=TBS1,TBS2,TBS3 \
transport_full_check=y \
logfile=tts_export.log
```

Si *`DATA_PUMP_DIR`* es un directorio compartido en Amazon EFS, vaya a Paso 4: Importar los espacios de tabla en la instancia de base de datos de destino.

Paso 3: (solo Amazon S3) transfiera los archivos de copia de seguridad y exporte los archivos a la instancia de base de datos de destino

Si utiliza Amazon S3 para organizar las copias de seguridad del espacio de tabla y el archivo de exportación de Data Pump, siga estos pasos.

Paso 3.1: cargue las copias de seguridad y el archivo de volcado del host de origen en el bucket de Amazon S3

Cargue las copias de seguridad y los archivos de volcado del host de origen en el bucket de Amazon S3. Para obtener más información, consulte Carga de objetos en la Guía del desarrollador de Amazon Simple Storage Service.

Paso 3.2: Descargar las copias de seguridad y el archivo de volcado desde el bucket de Amazon S3 a la instancia de base de datos de destino

En este paso, se utiliza el procedimiento `rdsadmin.rdsadmin_s3_tasks.download_from_s3` para descargar las copias de seguridad y el archivo de volcado en la instancia de base de datos de RDS para Oracle. Siga los pasos de Paso 2.3: Descargar las copias de seguridad desde el bucket de Amazon S3 a la instancia de base de datos de destino.

Paso 4: Importar los espacios de tabla en la instancia de base de datos de destino

Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces` para restaurar los espacios de tabla. Para obtener información sobre la semántica de este procedimiento, consulte Importación de espacios de tabla transportados a su instancia de base de datos.

Important

Tras completar la importación final del espacio de tabla, el siguiente paso es importar los metadatos de Oracle Data Pump. Si se produce un error en la importación, es importante que la instancia de base de datos vuelva a su estado anterior al error. Por lo tanto, le recomendamos que cree una instantánea de base de datos de la instancia de base de datos siguiendo las instrucciones de Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS. La instantánea contendrá todos los espacios de tabla importados, por lo que si se produce un error en la importación, no tendrá que repetir el proceso de copia de seguridad e importación.
Si la instancia de base de datos de destino tiene activadas las copias de seguridad automáticas y Amazon RDS no detecta que se haya iniciado una instantánea válida antes

de importar los metadatos, RDS intentará crear una instantánea. En función de la actividad de la instancia, esta instantánea puede o no funcionar correctamente. Si no se detecta una instantánea válida o no se puede iniciar una instantánea, la importación de metadatos se cerrará con errores.

Importar los espacios de tabla en la instancia de base de datos de destino

1. Inicie un cliente de Oracle SQL e inicie sesión como usuario maestro en su instancia de base de datos de destino de RDS para Oracle.
2. Ejecute el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces` y especifique los espacios de tabla que se van a importar y el directorio que contiene las copias de seguridad.

   En el siguiente ejemplo se importan los espacios de tabla *TBS1*, *TBS2* y *TBS3* del directorio *DATA_PUMP_DIR*.

   ```
   BEGIN

    :task_id:=rdsadmin.rdsadmin_transport_util.import_xtts_tablespaces('TBS1,TBS2,TBS3','DATA_
   END;
   /
   PRINT task_id
   ```
3. (Opcional) Supervise el progreso consultando la tabla `rdsadmin.rds_xtts_operation_info`. La columna `xtts_operation_state` muestra el valor `EXECUTING`, `COMPLETED` o `FAILED`.

   ```
   SELECT * FROM rdsadmin.rds_xtts_operation_info;
   ```

   > **Note**
   >
   > Para operaciones de larga duración, también puede consultar `V$SESSION_LONGOPS`, `V$RMAN_STATUS` y `V$RMAN_OUTPUT`.
4. Para ver el registro de la importación finalizada, utilice el ID de la tarea del paso anterior.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file('BDUMP',
 'dbtask-'||'&task_id'||'.log'));
```

Asegúrese de que se haya completado correctamente la importación antes de continuar con el siguiente paso.

5. Realice una instantánea manual de la base de datos siguiendo las instrucciones de Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Paso 5: Importar los metadatos del espacio de tabla en la instancia de base de datos de destino

En este paso, se importan los metadatos del espacio de tabla transportables a la instancia de base de datos de RDS para Oracle mediante el procedimiento `rdsadmin.rdsadmin_transport_util.import_xtts_metadata`. Para obtener información sobre la sintaxis y la semántica de este procedimiento, consulte Importación de metadatos de espacios de tabla transportables a su instancia de base de datos. Durante la operación, el estado de la importación se muestra en la tabla `rdsadmin.rds_xtts_operation_info`.

> **Important**
>
> Antes de importar los metadatos, le recomendamos encarecidamente que confirme la creación correcta de la instantánea de base de datos después de importar los espacios de tabla. Si se produce un error en el paso de importación, restaure la instancia de base de datos, corrija los errores de importación y, a continuación, vuelva a intentar la importación.

Importar los metadatos de Data Pump a la instancia de base de datos de RDS para Oracle

1. Inicie el cliente de Oracle SQL e inicie sesión como usuario maestro en su instancia de base de datos de destino.
2. Cree los usuarios que posean esquemas en los espacios de tabla transportados, si estos usuarios aún no existen.

```
CREATE USER tbs_owner IDENTIFIED BY password;
```

3. Importe los metadatos, especificando el nombre del archivo de volcado y su ubicación en el directorio.

```
BEGIN

 rdsadmin.rdsadmin_transport_util.import_xtts_metadata('xttdump.dmp','DATA_PUMP_DIR');
END;
/
```

4. (Opcional) Consulte la tabla del historial de espacios de tabla transportables para ver el estado de la importación de los metadatos.

   ```
   SELECT * FROM rdsadmin.rds_xtts_operation_info;
   ```

   Cuando finalice la operación, los espacios de tabla estarán en modo de solo lectura.

5. (Opcional) Vea el archivo de registro.

   En el ejemplo siguiente se muestra el contenido del directorio BDUMP y, a continuación, se consulta el registro de importación.

   ```
   SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => 'BDUMP'));

   SELECT * FROM TABLE(rdsadmin.rds_file_util.read_text_file(
     p_directory => 'BDUMP',
     p_filename => 'rds-xtts-
   import_xtts_metadata-2023-05-22.01-52-35.560858000.log'));
   ```

Fase 5: Validar los espacios de tabla transportados

En este paso opcional, se validan los espacios de tabla transportados mediante el procedimiento `rdsadmin.rdsadmin_rman_util.validate_tablespace` y, a continuación, los espacios de tabla se establecen en modo de lectura/escritura.

Para validar los datos transportados

1. Inicie SQL*Plus o SQL Developer e inicie sesión como usuario maestro en su instancia de base de datos de destino.
2. Valide los espacios de tabla mediante el procedimiento `rdsadmin.rdsadmin_rman_util.validate_tablespace`.

   ```
   SET SERVEROUTPUT ON
   ```

```
BEGIN
    rdsadmin.rdsadmin_rman_util.validate_tablespace(
        p_tablespace_name     => 'TBS1',
        p_validation_type     => 'PHYSICAL+LOGICAL',
        p_rman_to_dbms_output => TRUE);
    rdsadmin.rdsadmin_rman_util.validate_tablespace(
        p_tablespace_name     => 'TBS2',
        p_validation_type     => 'PHYSICAL+LOGICAL',
        p_rman_to_dbms_output => TRUE);
    rdsadmin.rdsadmin_rman_util.validate_tablespace(
        p_tablespace_name     => 'TBS3',
        p_validation_type     => 'PHYSICAL+LOGICAL',
        p_rman_to_dbms_output => TRUE);
END;
/
```

3. Coloque los espacios de tabla en modo de lectura/escritura.

```
ALTER TABLESPACE TBS1 READ WRITE;
ALTER TABLESPACE TBS2 READ WRITE;
ALTER TABLESPACE TBS3 READ WRITE;
```

Fase 6: Limpiar los archivos sobrantes

En este paso opcional, se eliminan los archivos innecesarios. Utilice el procedimiento `rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files` para enumerar los archivos de datos que quedaron huérfanos tras la importación de un espacio de tabla y, a continuación, utilice el procedimiento `rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files` para eliminarlos. Para obtener información sobre la sintaxis y la semántica de estos procedimientos, consulte Enumeración de los archivos huérfanos después de importar un espacio de tabla y Eliminación de los archivos de datos huérfanos después de importar un espacio de tabla.

Para limpiar los archivos sobrantes

1. Elimine las copias de seguridad antiguas en *DATA_PUMP_DIR* de la siguiente manera:

    a. Para enumerar los archivos de copia de seguridad, ejecute `rdsadmin.rdsadmin_file_util.listdir`.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory =>
 'DATA_PUMP_DIR'));
```

b. Para eliminar las copias de seguridad una por una, llame a `UTL_FILE.FREMOVE`.

```
EXEC UTL_FILE.FREMOVE ('DATA_PUMP_DIR', 'backup_filename');
```

2. Si ha importado espacios de tabla pero no ha importado metadatos para estos espacios de tabla, puede eliminar los archivos de datos huérfanos de la siguiente manera:

a. Haga una lista de los archivos de datos huérfanos que debe eliminar. En el siguiente ejemplo se ejecuta el procedimiento `rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files`.

```
SQL> SELECT * FROM
 TABLE(rdsadmin.rdsadmin_transport_util.list_xtts_orphan_files);

FILENAME       FILESIZE
-------------- ---------
datafile_7.dbf 104865792
datafile_8.dbf 104865792
```

b. Para eliminar los archivos huérfanos, ejecute el procedimiento `rdsadmin.rdsadmin_transport_util.cleanup_incomplete_xtts_import`.

```
BEGIN

 rdsadmin.rdsadmin_transport_util.cleanup_incomplete_xtts_import('DATA_PUMP_DIR');
END;
/
```

La operación de limpieza genera un archivo de registro que utiliza el formato de nombre `rds-xtts-delete_xtts_orphaned_files-`*`YYYY-MM-DD.HH24-MI-SS.FF`*`.log` del directorio BDUMP.

c. Lea el archivo de registro generado en el paso anterior. En el siguiente ejemplo se lee el registro `rds-xtts-delete_xtts_orphaned_files-`*`2023-06-01.09-33-11.868894000`*`.log`.

```
SELECT *
```

```
FROM TABLE(rdsadmin.rds_file_util.read_text_file(
       p_directory => 'BDUMP',
       p_filename  => 'rds-xtts-
delete_xtts_orphaned_files-2023-06-01.09-33-11.868894000.log'));

TEXT
--------------------------------------------------------------------------------
orphan transported datafile datafile_7.dbf deleted.
orphan transported datafile datafile_8.dbf deleted.
```

3. Si ha importado espacios de tabla y metadatos para estos espacios de tabla, pero se ha topado con errores de compatibilidad u otros problemas de Oracle Data Pump, limpie los archivos de datos parcialmente transportados de la siguiente manera:

   a. Enumere los espacios de tabla que contienen archivos de datos parcialmente transportados mediante consultas DBA_TABLESPACES.

   ```
   SQL> SELECT TABLESPACE_NAME FROM DBA_TABLESPACES WHERE PLUGGED_IN='YES';

   TABLESPACE_NAME
   --------------------------------------------------------------------------------
   TBS_3
   ```

   b. Elimine los espacios de tabla y los archivos de datos parcialmente transportados.

   ```
   DROP TABLESPACE TBS_3 INCLUDING CONTENTS AND DATAFILES;
   ```

Importación mediante Oracle Data Pump

Oracle Data Pump es una utilidad que le permite exportar datos de Oracle a un archivo de volcado e importarlos a otra base de datos de Oracle. Es un reemplazo a largo plazo de las utilidades de exportación e importación de Oracle. Oracle Data Pump es la forma preferida de trasladar grandes cantidades de datos desde una base de datos Oracle a una instancia de base de datos de Amazon RDS.

Los ejemplos de esta sección muestran una forma de importar datos a una base de datos Oracle, pero Oracle Data Pump admite otras técnicas. Para obtener más información, consulte la documentación de Oracle Database.

En los ejemplos de esta sección se utiliza el paquete `DBMS_DATAPUMP`. Puede realizar las mismas tareas con las utilidades de línea de comandos de Oracle Data Pump `impdp` y `expdp`. Puede instalar estas utilidades en un host remoto como parte de una instalación de Oracle Client, incluido Oracle Instant Client. Para obtener más información, consulte How do I use Oracle Instant Client to run Data Pump Import or Export for my Amazon RDS for Oracle DB instance? (¿Cómo utilizo Oracle Instant Client para ejecutar la importación o exportación de Data Pump para mi instancia de base de datos de Amazon RDS para Oracle?)

Temas

- Información general sobre Oracle Data Pump
- Importación de datos con Oracle Data Pump y un bucket de Amazon S3
- Importación de datos con Oracle Data Pump y un enlace de base de datos

Información general sobre Oracle Data Pump

Oracle Data Pump consta de los siguientes componentes:

- Clientes de línea de comandos `expdp` y `impdp`
- El paquete PL/SQL `DBMS_DATAPUMP`
- El paquete PL/SQL `DBMS_METADATA`

Puede utilizar Oracle Data Pump en los siguientes casos:

- Importación de datos desde una base de datos de Oracle (en las instalaciones o en una instancia de Amazon EC2) a una instancia de base de datos de Amazon RDS para Oracle
- Importación de datos desde una instancia de base de datos de RDS para Oracle a una base de datos Oracle, ya sea en las instalaciones o en una instancia de Amazon EC2
- Importación de datos entre instancias de base de datos de RDS para Oracle (por ejemplo, para migrar datos desde EC2-Classic a una VPC).

Para descargar utilidades de Oracle Data Pump, consulte Oracle Database Software Downloads (Descargas de software de base de datos de Oracle) en el sitio web de Oracle Technology Network. Para conocer aspectos sobre compatibilidad al migrar entre versiones de Oracle Database, consulte la documentación de Oracle Database.

Flujo de trabajo de Oracle Data Pump

Por lo general, se utiliza Oracle Data Pump en las siguientes etapas:

1. Exporte sus datos a un archivo de volcado en la base de datos de origen.
2. Cargue el archivo de volcado en la instancia de base de datos de RDS para Oracle Puede transferirlo mediante un bucket de Amazon S3 o mediante un enlace de base de datos entre dos bases de datos.
3. Importe los datos desde el archivo de volcado a la instancia de base de RDS para Oracle.

Prácticas recomendadas de Oracle Data Pump

Cuando utiliza Oracle Data Pump para importar datos en una instancia de RDS para Oracle, se recomiendan las siguientes prácticas recomendadas:

- Realice importaciones en el modo `schema` o `table` para importar esquemas y objetos específicos.
- Limite los esquemas que importe a los que necesita su aplicación.
- No los importe en el modo `full` ni en esquemas de importación para componentes mantenidos por el sistema.

  Puesto que RDS para Oracle no permite el acceso a usuarios administrativos `SYS` o `SYSDBA`, estas acciones pueden dañar el diccionario de datos de Oracle y afectar a la estabilidad de su base de datos.
- Al cargar grandes cantidades de datos, haga lo siguiente:
  1. Transfiera el archivo de volcado a la instancia de base de datos de RDS para Oracle.
  2. Cree una instantánea de base de datos de su instancia.
  3. Pruebe la importación para comprobar que se realiza correctamente.

  Si se invalidan los componentes de la base de datos, puede eliminar la instancia de base de datos y volver a crearla a partir de la instantánea de base de datos. La instancia de base de datos restaurada incluye los archivos de volcado preparados en la instancia de base de datos cuando realice una instantánea de base de datos.
- No importe archivos de volcado creados con parámetros `TRANSPORT_TABLESPACES`, `TRANSPORTABLE` o `TRANSPORT_FULL_CHECK` de exportación de Oracle Data Pump. Las instancias de bases de datos de RDS para Oracle no admiten la importación de estos archivos de volcado.

- No importe archivos de volcado que contengan objetos del programador de Oracle en `SYS`, `SYSTEM`, `RDSADMIN`, `RDSSEC` y `RDS_DATAGUARD` y que pertenezcan a las categorías siguientes:
  - Tareas
  - Programas
  - Programas
  - Cadenas
  - Reglas
  - Contextos de evaluación
  - Conjunto de reglas

  Las instancias de bases de datos de RDS para Oracle no admiten la importación de estos archivos de volcado.
- Para excluir objetos de Oracle Scheduler no admitidos, utilice directivas adicionales durante la exportación de Data Pump. Si utiliza `DBMS_DATAPUMP`, añada un `METADATA_FILTER` adicional antes de `DBMS_METADATA.START_JOB`:

```
DBMS_DATAPUMP.METADATA_FILTER(
  v_hdnl,
  'EXCLUDE_NAME_EXPR',
  q'[IN (SELECT NAME FROM SYS.OBJ$
         WHERE TYPE# IN (66,67,74,79,59,62,46)
         AND OWNER# IN
           (SELECT USER# FROM SYS.USER$
            WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC')
            )
        )
  ]',
  'PROCOBJ'
);
```

  Si utiliza `expdp`, cree un archivo de parámetros que contenga la directiva `exclude` que se muestra en el siguiente ejemplo. Luego `PARFILE=`*`parameter_file`* utilícelo con su `expdp` comando.

```
exclude=procobj:"IN
  (SELECT NAME FROM sys.OBJ$
   WHERE TYPE# IN (66,67,74,79,59,62,46)
   AND OWNER# IN
```

```
    (SELECT USER# FROM SYS.USER$
     WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC')
    )
)"
```

Importación de datos con Oracle Data Pump y un bucket de Amazon S3

El siguiente proceso de importación utiliza Oracle Data Pump y un bucket de Amazon S3. Los pasos son los siguientes:

1. Exporte datos en la base de datos de origen mediante el paquete DBMS_DATAPUMP de Oracle.
2. Coloque el archivo de volcado en un bucket de Amazon S3.
3. A continuación, descargue el archivo de volcado del bucket de Amazon S3 al directorio `DATA_PUMP_DIR` en la instancia de base de datos de RDS para Oracle de destino.
4. Importe los datos del archivo de volcado copiado a la instancia de base de datos de RDS para Oracle utilizando el paquete `DBMS_DATAPUMP`.

Temas

- Requisitos para la importación de datos con Oracle Data Pump y un bucket de Amazon S3
- Paso 1: Conceda privilegios al usuario de la base de datos en la instancia de base de datos de destino de RDS para Oracle
- Paso 2: Exporte datos a un archivo de volcado mediante DBMS_DATAPUMP
- Paso 3: carga del archivo de volcado a su bucket de Amazon S3
- Paso 4: Descargue el archivo de volcado desde su bucket de Amazon S3 a la instancia de base de datos de destino.
- Paso 5: Importe el archivo de volcado a la instancia de base de datos de destino mediante DBMS_DATAPUMP
- Paso 6: Limpieza

Requisitos para la importación de datos con Oracle Data Pump y un bucket de Amazon S3

El proceso tiene los siguientes requisitos:

- Asegúrese de que hay un bucket de Amazon S3 disponible para las transferencias de archivos, y que el bucket de Amazon S3 está en la misma Región de AWS que la instancia de base de datos.

Para ver las instrucciones, consulte Crear un bucket en la Guía de introducción de Amazon Simple Storage Service.

- El objeto que cargue en el bucket de Amazon S3 debe ser de 5 TB o menos. Para obtener más información acerca de cómo trabajar con objetos en Amazon S3, consulte Guía del usuario de Amazon Simple Storage Service.

> **Note**
>
> Si el archivo de volcado supera los 5 TB, puede ejecutar la exportación de Oracle Data Pump con la opción paralela. Esta operación distribuye los datos en varios archivos de volcado para que no supere el límite de 5 TB para archivos individuales.

- Debe preparar el bucket de Amazon S3 para la integración de Amazon RDS siguiendo las instrucciones en Configuración de permisos IAM para la integración de RDS para Oracle con Amazon S3.
- Debe asegurarse de que tiene suficiente espacio de almacenamiento para almacenar el archivo de volcado en la instancia de origen y en la instancia de base de datos de destino.

> **Note**
>
> Este proceso importa un archivo de volcado en el directorio `DATA_PUMP_DIR`, un directorio preconfigurado en todas las instancias de bases de datos de Oracle. Este directorio se encuentra en el mismo volumen de almacenamiento que los archivos de datos. Cuando importe el archivo de volcado, los archivos de datos de Oracle existentes utilizarán más espacio. Por lo tanto, debe asegurarse de que su instancia de base de datos pueda dar cabida a ese uso de espacio adicional. El archivo de volcado importado no se elimina ni se purga automáticamente del directorio `DATA_PUMP_DIR`. Para quitar el archivo de volcado importado, utilice UTL_FILE.FREMOVE, que se encuentra en el sitio web de Oracle.

Paso 1: Conceda privilegios al usuario de la base de datos en la instancia de base de datos de destino de RDS para Oracle

En este paso, debe crear los esquemas en los que tiene pensado importar datos y conceder a los usuarios los privilegios necesarios.

Para crear usuarios y conceder los privilegios necesarios en la instancia de destino de RDS para Oracle

1. Utilice SQL*Plus u Oracle SQL Developer para iniciar sesión como usuario maestro en la instancia de base de datos de RDS para Oracle en la que se importarán los datos. Para obtener más información acerca de la conexión a una instancia de base de datos, consulte Conexión a una instancia de base de datos de Oracle.
2. Cree el espacio de tabla necesario antes de importar los datos. Para obtener más información, consulte Creación y especificación del tamaño de los espacios de tablas.
3. Cree la cuenta de usuario y conceda los permisos y roles necesarios si la cuenta de usuario a la que se importan los datos no existe. Si piensa importar datos en varios esquemas de usuario, cree cada cuenta de usuario y otórguele los permisos y roles necesarios.

   Por ejemplo, las siguientes instrucciones SQL crean un nuevo usuario y conceden los permisos y roles necesarios para importar los datos en el esquema propiedad de este usuario. Reemplace *schema_1* por el nombre de su esquema en este paso y en los siguientes.

   ```
   CREATE USER schema_1 IDENTIFIED BY my_password;
   GRANT CREATE SESSION, RESOURCE TO schema_1;
   ALTER USER schema_1 QUOTA 100M ON users;
   ```

   > **Note**
   >
   > Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

   Las instrucciones anteriores conceden al nuevo usuario el privilegio `CREATE SESSION` y el rol `RESOURCE`. Es probable que necesite más privilegios y roles en función de los objetos de base de datos que importe.

Paso 2: Exporte datos a un archivo de volcado mediante DBMS_DATAPUMP

Para crear un archivo de volcado, utilice el paquete `DBMS_DATAPUMP`.

Para exportar datos de Oracle a un archivo de volcado

1. Utilice SQL Plus u Oracle SQL Developer para conectarse a la instancia de base de datos de RDS para Oracle de origen con un usuario administrativo. Si la base de datos de origen es una instancia de base de datos de RDS para Oracle, conéctese con el usuario maestro de Amazon RDS.
2. Exporte los datos llamando a los procedimientos `DBMS_DATAPUMP`.

   El siguiente script exporta el esquema *SCHEMA_1* a un archivo de volcado denominado `sample.dmp` en el directorio `DATA_PUMP_DIR`. Reemplace *SCHEMA_1* por el nombre del esquema que desea exportar.

```
DECLARE
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(
    operation => 'EXPORT',
    job_mode  => 'SCHEMA',
    job_name  => null
  );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl         ,
    filename  => 'sample.dmp'   ,
    directory => 'DATA_PUMP_DIR',
    filetype  => dbms_datapump.ku$_file_type_dump_file
  );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample_exp.log',
    directory => 'DATA_PUMP_DIR' ,
    filetype  => dbms_datapump.ku$_file_type_log_file
  );
  DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''SCHEMA_1'')');
  DBMS_DATAPUMP.METADATA_FILTER(
    v_hdnl,
    'EXCLUDE_NAME_EXPR',
    q'[IN (SELECT NAME FROM SYS.OBJ$
           WHERE TYPE# IN (66,67,74,79,59,62,46)
           AND OWNER# IN
             (SELECT USER# FROM SYS.USER$
              WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC')
             )
```

```
          )
    ]',
    'PROCOBJ'
  );
  DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

> **Note**
>
> Data Pump inicia los trabajos de forma asíncrona Para obtener información sobre la supervisión de un trabajo de Data Pump, consulte Monitoring job status (Supervisión del estado del trabajo) en la documentación de Oracle.

3. (Opcional) Puede ver el contenido del registro de exportación llamando al procedimiento `rdsadmin.rds_file_util.read_text_file`. Para obtener más información, consulte Lectura de archivos de un directorio de instancia de base de datos.

Paso 3: carga del archivo de volcado a su bucket de Amazon S3

Utilice el procedimiento de Amazon RDS `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` para copiar el archivo de volcado en el bucket de Amazon S3. En el siguiente ejemplo se cargan todos los archivos del directorio `DATA_PUMP_DIR` en un bucket de Amazon S3 denominado *amzn-s3-demo-bucket*.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
  p_bucket_name    =>  'amzn-s3-demo-bucket',
  p_directory_name =>  'DATA_PUMP_DIR')
AS TASK_ID FROM DUAL;
```

La instrucción `SELECT` devuelve el identificador de la tarea en un tipo de datos `VARCHAR2`. Para obtener más información, consulte Carga de archivos desde la instancia de base de datos de RDS para Oracle en un bucket de Amazon S3.

Paso 4: Descargue el archivo de volcado desde su bucket de Amazon S3 a la instancia de base de datos de destino.

Realice este paso mediante el procedimiento de Amazon RDS `rdsadmin.rdsadmin_s3_tasks.download_from_s3`. Al descargar un archivo en un

directorio, el procedimiento `download_from_s3` omite la descarga si ya existe un archivo con el mismo nombre en el directorio. Para quitar el archivo del directorio de descarga, utilice UTL_FILE.FREMOVE, que se encuentra en el sitio web de Oracle.

Para descargar el archivo de volcado

1. Inicie SQL*Plus u Oracle SQL Developer e inicie sesión como usuario maestro en su instancia de base de datos de destino de Amazon RDS
2. Descargue el archivo de volcado mediante el procedimiento de Amazon RDS `rdsadmin.rdsadmin_s3_tasks.download_from_s3`.

   En el siguiente ejemplo, se descargan todos los archivos de un bucket de Amazon S3 denominado *`amzn-s3-demo-bucket`* en el directorio `DATA_PUMP_DIR`.

   ```
   SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
     p_bucket_name    =>  'amzn-s3-demo-bucket',
     p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
   ```

   La instrucción `SELECT` devuelve el identificador de la tarea en un tipo de datos `VARCHAR2`. Para obtener más información, consulte Descarga de archivos desde un bucket de Amazon S3 en una instancia de base de datos de Oracle.

Paso 5: Importe el archivo de volcado a la instancia de base de datos de destino mediante DBMS_DATAPUMP

Utilice `DBMS_DATAPUMP` para importar el esquema a la instancia de base de datos de RDS para Oracle. Podrían ser necesarias opciones adicionales, como `METADATA_REMAP`.

Para importar datos a la instancia de base de datos de destino

1. Inicie SQL*Plus u Oracle SQL Developer e inicie sesión como usuario maestro en su instancia de base de datos de destino de RDS para Oracle.
2. Importe los datos llamando a los procedimientos `DBMS_DATAPUMP`.

   En el siguiente ejemplo se importan los datos de *`SCHEMA_1`* de `sample_copied.dmp` en la instancia de base de datos de destino.

   ```
   DECLARE
   ```

```
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(
    operation => 'IMPORT',
    job_mode  => 'SCHEMA',
    job_name  => null);
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample_copied.dmp',
    directory => 'DATA_PUMP_DIR',
    filetype  => dbms_datapump.ku$_file_type_dump_file);
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample_imp.log',
    directory => 'DATA_PUMP_DIR',
    filetype  => dbms_datapump.ku$_file_type_log_file);
  DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''SCHEMA_1'')');
  DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

> **Note**
>
> Los trabajos de Data Pump se inician de modo asincrónico. Para obtener información sobre el monitoreo de un trabajo de Data Pump, consulte Monitorización del estado del trabajo en la documentación de Oracle. Puede ver el contenido del registro de importación mediante el procedimiento `rdsadmin.rds_file_util.read_text_file`. Para obtener más información, consulte Lectura de archivos de un directorio de instancia de base de datos.

3. Para comprobar la importación de datos, enumere las tablas de esquemas de la instancia de base de datos de destino.

   Por ejemplo, la siguiente consulta devuelve el número de tablas de *SCHEMA_1*.

   ```
   SELECT COUNT(*) FROM DBA_TABLES WHERE OWNER='SCHEMA_1';
   ```

Paso 6: Limpieza

Después de importar los datos, puede eliminar los archivos que no desee conservar.

Para eliminar archivos innecesarios

1. Inicie SQL*Plus u Oracle SQL Developer e inicie sesión como usuario maestro en su instancia de base de datos de destino de RDS para Oracle.
2. Enumere los archivos en DATA_PUMP_DIR mediante el siguiente comando.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('DATA_PUMP_DIR')) ORDER BY
 MTIME;
```

3. Elimine los archivos de DATA_PUMP_DIR que ya no sean necesarios con el siguiente comando.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','filename');
```

   Por ejemplo, el siguiente comando elimina el archivo denominado sample_copied.dmp.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample_copied.dmp');
```

Importación de datos con Oracle Data Pump y un enlace de base de datos

El siguiente proceso de importación utiliza Oracle Data Pump y el paquete DBMS_FILE_TRANSFER de Oracle. Los pasos son los siguientes:

1. Conéctese a una base de datos Oracle de origen, que puede ser una base de datos en las instalaciones, una instancia de Amazon EC2 o una instancia de base de datos de RDS para Oracle.
2. Exporte los datos mediante el paquete DBMS_DATAPUMP.
3. Utilice DBMS_FILE_TRANSFER.PUT_FILE para copiar el archivo de volcado desde la base de datos Oracle al directorio DATA_PUMP_DIR de la instancia de base de datos de RDS para Oracle de destino que está conectada mediante un enlace de base de datos.
4. Importe los datos del archivo de volcado copiado a la instancia de base de datos de RDS para Oracle utilizando el paquete DBMS_DATAPUMP.

El proceso de importación mediante Oracle Data Pump y un paquete de DBMS_FILE_TRANSFER tiene los siguientes pasos.

Temas

- Requisitos de importación de datos con Oracle Data Pump y un enlace de base de datos
- Paso 1: Conceda privilegios al usuario en la instancia de base de datos de destino de RDS para Oracle
- Paso 2: concesión de privilegios al usuario en la base de datos de origen
- Paso 3: Cree un archivo de volcado utilizando DBMS_DATAPUMP
- Paso 4: Crear un enlace de base de datos a la instancia de base de datos de destino
- Paso 5: Copie el archivo de volcado exportado a la instancia de base de datos de destino utilizando DBMS_FILE_TRANSFER
- Paso 6: Importe el archivo de datos a la instancia de base de datos de destino utilizando DBMS_DATAPUMP
- Paso 7: Limpieza

Requisitos de importación de datos con Oracle Data Pump y un enlace de base de datos

El proceso tiene los siguientes requisitos:

- Debe tener privilegios de ejecución en los paquetes `DBMS_FILE_TRANSFER` y `DBMS_DATAPUMP`.
- Debe tener privilegios de escritura en el directorio `DATA_PUMP_DIR` de la instancia de base de datos de origen.
- Debe asegurarse de que tiene suficiente espacio de almacenamiento para almacenar el archivo de volcado en la instancia de origen y en la instancia de base de datos de destino.

> **Note**
>
> Este proceso importa un archivo de volcado en el directorio `DATA_PUMP_DIR`, un directorio preconfigurado en todas las instancias de bases de datos de Oracle. Este directorio se encuentra en el mismo volumen de almacenamiento que los archivos de datos. Cuando importe el archivo de volcado, los archivos de datos de Oracle existentes utilizarán más espacio. Por lo tanto, debe asegurarse de que su instancia de base de datos pueda dar cabida a ese uso de espacio adicional. El archivo de volcado importado no se elimina ni se purga automáticamente del directorio `DATA_PUMP_DIR`. Para quitar el archivo de volcado importado, utilice UTL_FILE.FREMOVE, que se encuentra en el sitio web de Oracle.

Paso 1: Conceda privilegios al usuario en la instancia de base de datos de destino de RDS para Oracle

Para conceder privilegios al usuario en la instancia de base de datos de destino de RDS para Oracle, realice los siguientes pasos:

1. Utilice SQL Plus u Oracle SQL Developer para conectarse a la instancia de base de datos de RDS para Oracle a la que desea importar los datos. Conéctese con el usuario maestro de Amazon RDS. Para obtener más información acerca de la conexión a la instancia de base de datos, consulte Conexión a una instancia de base de datos de Oracle.
2. Cree el espacio de tabla necesario antes de importar los datos. Para obtener más información, consulte Creación y especificación del tamaño de los espacios de tablas.
3. Si la cuenta de usuario a la que se van a importar los datos no existe, cree la cuenta y otórguele los permisos y roles necesarios. Si piensa importar datos en varios esquemas de usuario, cree cada cuenta de usuario y otórguele los permisos y roles necesarios.

   Por ejemplo, los siguientes comandos crean un nuevo usuario denominado *schema_1* y otorgan los permisos y roles necesarios para importar los datos al esquema de este usuario.

   ```
   CREATE USER schema_1 IDENTIFIED BY my-password;
   GRANT CREATE SESSION, RESOURCE TO schema_1;
   ALTER USER schema_1 QUOTA 100M ON users;
   ```

   > **Note**
   >
   > Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

   En el ejemplo anterior, se otorga el privilegio `CREATE SESSION` y el rol `RESOURCE` al nuevo usuario. Es probable que necesite más privilegios y roles en función de los objetos de base de datos que importe.

   > **Note**
   >
   > Reemplace *schema_1* por el nombre de su esquema en este paso y en los siguientes.

Paso 2: concesión de privilegios al usuario en la base de datos de origen

Utilice SQL*Plus u Oracle SQL Developer para conectarse a la instancia de base de datos de RDS para Oracle que contiene los datos que va a importar. Si es necesario, cree una cuenta de usuario con los permisos necesarios.

> **Note**
>
> Si la base de datos de origen es una instancia de Amazon RDS, puede omitir este paso. Para realizar la exportación utilizará la cuenta de usuario maestra de Amazon RDS.

Los siguientes comandos crean un usuario y le conceden los permisos necesarios.

```
CREATE USER export_user IDENTIFIED BY my-password;
GRANT CREATE SESSION, CREATE TABLE, CREATE DATABASE LINK TO export_user;
ALTER USER export_user QUOTA 100M ON users;
GRANT READ, WRITE ON DIRECTORY data_pump_dir TO export_user;
GRANT SELECT_CATALOG_ROLE TO export_user;
GRANT EXECUTE ON DBMS_DATAPUMP TO export_user;
GRANT EXECUTE ON DBMS_FILE_TRANSFER TO export_user;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Paso 3: Cree un archivo de volcado utilizando DBMS_DATAPUMP

Para crear el archivo de volcado, haga lo siguiente:

1. Utilice SQL*Plus u Oracle SQL Developer para conectarse a la instancia de Oracle de origen con un usuario administrativo o con el usuario creado en el paso 2. Si la base de datos de origen es una instancia de base de datos de Amazon RDS for Oracle, conéctese con el usuario maestro de Amazon RDS.
2. Cree un archivo de volcado mediante la utilidad Oracle Data Pump.

   El siguiente script crea un archivo de volcado denominado sample.dmp en el directorio `DATA_PUMP_DIR`.

```
DECLARE
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(
    operation => 'EXPORT' ,
    job_mode  => 'SCHEMA' ,
    job_name  => null
  );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample.dmp'    ,
    directory => 'DATA_PUMP_DIR' ,
    filetype  => dbms_datapump.ku$_file_type_dump_file
  );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl           ,
    filename  => 'sample_exp.log' ,
    directory => 'DATA_PUMP_DIR'  ,
    filetype  => dbms_datapump.ku$_file_type_log_file
  );
  DBMS_DATAPUMP.METADATA_FILTER(
    v_hdnl              ,
    'SCHEMA_EXPR'       ,
    'IN (''SCHEMA_1'')'
  );
  DBMS_DATAPUMP.METADATA_FILTER(
    v_hdnl,
    'EXCLUDE_NAME_EXPR',
    q'[IN (SELECT NAME FROM sys.OBJ$
           WHERE TYPE# IN (66,67,74,79,59,62,46)
           AND OWNER# IN
             (SELECT USER# FROM SYS.USER$
              WHERE NAME IN ('RDSADMIN','SYS','SYSTEM','RDS_DATAGUARD','RDSSEC')
             )
         )
    ]',
    'PROCOBJ'
  );
  DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

> **Note**
>
> Los trabajos de Data Pump se inician de modo asincrónico. Para obtener información sobre la supervisión de un trabajo de Data Pump, consulte Monitoring job status (Supervisión del estado del trabajo) en la documentación de Oracle. Puede ver el contenido del registro de exportación mediante el procedimiento `rdsadmin.rds_file_util.read_text_file`. Para obtener más información, consulte Lectura de archivos de un directorio de instancia de base de datos.

Paso 4: Crear un enlace de base de datos a la instancia de base de datos de destino

Cree un enlace de base de datos entre la instancia de base de datos de origen y la instancia de base de datos de destino. La instancia local de Oracle debe tener conectividad de red con la instancia de base de datos para poder crear un enlace de base de datos y transferir el archivo de volcado de exportación.

Para realizar este paso, conéctese con la misma cuenta de usuario del paso anterior.

Si está creando un enlace de base de datos entre dos instancias de bases de datos dentro de la misma VPC o en VPC interconectadas, debe existir una ruta válida entre las dos instancias de bases de datos. El grupo de seguridad de cada instancia de base de datos debe permitir la entrada y la salida desde la otra instancia de base de datos. Las reglas de entrada y salida del grupo de seguridad pueden referirse a grupos de seguridad de la misma VPC o de una VPC interconectada. Para obtener más información, consulte Ajuste de los enlaces de base de datos para usarlos con las instancias de bases de datos de una VPC.

El siguiente comando crea un enlace de base de datos denominado `to_rds` que se conecta con un usuario maestro de Amazon RDS de la instancia de base de datos de destino.

```
CREATE DATABASE LINK to_rds
  CONNECT TO <master_user_account> IDENTIFIED BY <password>
  USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns or ip address of remote db>)
         (PORT=<listener port>))(CONNECT_DATA=(SID=<remote SID>)))';
```

Paso 5: Copie el archivo de volcado exportado a la instancia de base de datos de destino utilizando DBMS_FILE_TRANSFER

Utilice `DBMS_FILE_TRANSFER` para copiar el archivo de volcado desde la instancia de base de datos de origen en la instancia de base de datos de destino. El siguiente script copia un archivo de volcado denominado sample.dmp desde la instancia de origen en un enlace de la base de datos de destino denominado to_rds (creado en el paso anterior).

```
BEGIN
  DBMS_FILE_TRANSFER.PUT_FILE(
    source_directory_object       => 'DATA_PUMP_DIR',
    source_file_name              => 'sample.dmp',
    destination_directory_object  => 'DATA_PUMP_DIR',
    destination_file_name         => 'sample_copied.dmp',
    destination_database          => 'to_rds' );
END;
/
```

Paso 6: Importe el archivo de datos a la instancia de base de datos de destino utilizando DBMS_DATAPUMP

Utilice Oracle Data Pump para importar el esquema en la instancia de base de datos. Pueden ser necesarias opciones adicionales, como METADATA_REMAP.

Para llevar a cabo la importación, conéctese a la instancia de base de datos con la cuenta de usuario maestro de Amazon RDS.

```
DECLARE
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(
    operation => 'IMPORT',
    job_mode  => 'SCHEMA',
    job_name  => null);
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'sample_copied.dmp',
    directory => 'DATA_PUMP_DIR',
    filetype  => dbms_datapump.ku$_file_type_dump_file );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
```

```
    filename  => 'sample_imp.log',
    directory => 'DATA_PUMP_DIR',
    filetype  => dbms_datapump.ku$_file_type_log_file);
  DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''SCHEMA_1'')');
  DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

> **Note**
>
> Los trabajos de Data Pump se inician de modo asincrónico. Para obtener información sobre el monitoreo de un trabajo de Data Pump, consulte Monitorización del estado del trabajo en la documentación de Oracle. Puede ver el contenido del registro de importación mediante el procedimiento `rdsadmin.rds_file_util.read_text_file`. Para obtener más información, consulte Lectura de archivos de un directorio de instancia de base de datos.

Puede verificar la importación de datos viendo las tablas de usuario en la instancia de base de datos. Por ejemplo, la siguiente consulta devuelve el número de tablas de *schema_1*.

```
SELECT COUNT(*) FROM DBA_TABLES WHERE OWNER='SCHEMA_1';
```

Paso 7: Limpieza

Después de importar los datos, puede eliminar los archivos que no desee conservar. Puede enumerar los archivos en `DATA_PUMP_DIR` mediante el siguiente comando.

```
SELECT * FROM TABLE(rdsadmin.rds_file_util.listdir('DATA_PUMP_DIR')) ORDER BY MTIME;
```

Para eliminar archivos de `DATA_PUMP_DIR` que ya no sean necesarios, utilice el siguiente comando.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','<file name>');
```

Por ejemplo, el siguiente comando elimina el archivo denominado `"sample_copied.dmp"`.

```
EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample_copied.dmp');
```

Importación mediante exportación/importación de Oracle

Puede considerar las utilidades de exportación/importación de Oracle para migraciones en las siguientes condiciones:

- El tamaño de los datos es pequeño.
- Los tipos de datos, como binario flotante y doble, no son necesarios.

El proceso de importación crea los objetos de esquema necesarios. Por lo tanto, no es necesario ejecutar un script para crear los objetos de antemano.

La forma más sencilla de instalar las utilidades de exportación e importación de Oracle es instalar Oracle Instant Client. Para descargar el software, vaya a https://www.oracle.com/database/technologies/instant-client.html. Para obtener documentación, consulte Instant Client for SQL*Loader, Export and Import (Instant Client para SQL*Loader, exportación e importación) en el manual de Oracle Database Utilities.

Para exportar tablas y, a continuación, importarlas

1. Exporte las tablas de la base de datos de origen con el comando `exp`.

   El siguiente comando exporta las tablas denominadas `tab1`, `tab2` y `tab3`. El archivo de volcado es `exp_file.dmp`.

   ```
   exp cust_dba@ORCL FILE=exp_file.dmp TABLES=(tab1,tab2,tab3) LOG=exp_file.log
   ```

   La exportación crea un archivo de volcado binario que contiene el esquema y los datos de las tablas especificadas.
2. Importe el esquema y los datos a una base de datos de destino utilizando el comando `imp`.

   El siguiente comando importa las tablas `tab1`, `tab2` y`tab3` desde el archivo de volcado `exp_file.dmp`.

   ```
   imp cust_dba@targetdb FROMUSER=cust_schema TOUSER=cust_schema \
   TABLES=(tab1,tab2,tab3) FILE=exp_file.dmp LOG=imp_file.log
   ```

La utilidad de exportación e importación tiene otras variaciones que podrían adaptarse mejor a sus necesidades. Consulte la documentación de Oracle para obtener toda la información.

Importación mediante Oracle SQL*Loader

Puede considerar Oracle SQL*Loader para bases de datos de gran tamaño que contienen un número limitado de objetos. Dado que el proceso de exportación desde una base de datos de origen y de carga en una base de datos de destino es específico del esquema, el siguiente ejemplo crea los objetos del esquema de ejemplo, exporta desde un origen y luego carga los datos en una base de datos de destino.

La forma más sencilla de instalar Oracle SQL*Loader es instalar Oracle Instant Client. Para descargar el software, vaya a https://www.oracle.com/database/technologies/instant-client.html. Para obtener documentación, consulte Instant Client for SQL*Loader, Export and Import (Instant Client para SQL*Loader, exportación e importación) en el manual de Oracle Database Utilities.

Para importar datos mediante Oracle SQL*Loader

1. Cree una tabla de origen de ejemplo con la siguiente instrucción SQL.

```
CREATE TABLE customer_0 TABLESPACE users
   AS (SELECT ROWNUM id, o.*
       FROM   ALL_OBJECTS o, ALL_OBJECTS x
       WHERE  ROWNUM <= 1000000);
```

2. En la instancia de base de datos de RDS para Oracle de destino, cree una tabla de destino para cargar los datos. La cláusula `WHERE 1=2` garantiza que copia la estructura de `ALL_OBJECTS`, pero no copia ninguna de las filas.

```
CREATE TABLE customer_1 TABLESPACE users
  AS (SELECT 0 AS ID, OWNER, OBJECT_NAME, CREATED
      FROM   ALL_OBJECTS
      WHERE  1=2);
```

3. Exporte los datos desde la base de datos de origen a un archivo de texto. En el siguiente ejemplo se utiliza SQL*Plus. Para sus datos, es probable que tenga que generar una script que realice la exportación de todos los objetos de la base de datos.

```
ALTER SESSION SET NLS_DATE_FORMAT = 'YYYY/MM/DD HH24:MI:SS'

SET LINESIZE 800 HEADING OFF FEEDBACK OFF ARRAY 5000 PAGESIZE 0
SPOOL customer_0.out
SET MARKUP HTML PREFORMAT ON
SET COLSEP ','
```

```
SELECT id, owner, object_name, created
FROM   customer_0;

SPOOL OFF
```

4. Cree un archivo de control para describir los datos. Es posible que tenga que escribir un script para realizar este paso.

```
cat << EOF > sqlldr_1.ctl
load data
infile customer_0.out
into table customer_1
APPEND
fields terminated by "," optionally enclosed by '"'
(
  id           POSITION(01:10)    INTEGER EXTERNAL,
  owner        POSITION(12:41)    CHAR,
  object_name  POSITION(43:72)    CHAR,
  created      POSITION(74:92)    date "YYYY/MM/DD HH24:MI:SS"
)
```

   Si es necesario, copie los archivos generados por el código anterior en un área de ensayo, como una instancia Amazon EC2.

5. Importe los datos usando SQL*Loader con el nombre de usuario y la contraseña apropiados para la base de datos de destino.

```
sqlldr cust_dba@targetdb CONTROL=sqlldr_1.ctl BINDSIZE=10485760 READSIZE=10485760
 ROWS=1000
```

Migración de vistas materializadas de Oracle

Para migrar grandes conjuntos de datos de forma eficaz, puede utilizar la replicación de vistas materializadas de Oracle. Con la replicación, puede mantener las tablas de destino sincronizadas con las tablas de origen. Por lo tanto, puede cambiar a Amazon RDS más adelante, si es necesario.

Antes de migrar mediante vistas materializadas, asegúrese de cumplir los siguientes requisitos:

- Configure el acceso desde la base de datos de destino a la base de datos de origen En el siguiente ejemplo, se han activado reglas de acceso en la base de datos de origen para permitir

que la base de datos de destino de RDS para Oracle se conecte a la de origen a través de SQL*Net.

- Cree un enlace de base de datos desde la instancia de base de datos de RDS para Oracle a la base de datos de origen.

Para migrar datos mediante vistas materializadas

1. Cree una cuenta de usuario en las instancias de origen y de destino de RDS para Oracle que pueda autenticarse con la misma contraseña. El siguiente ejemplo crea una usuario denominado `dblink_user`.

```
CREATE USER dblink_user IDENTIFIED BY my-password
  DEFAULT TABLESPACE users
  TEMPORARY TABLESPACE temp;

GRANT CREATE SESSION TO dblink_user;

GRANT SELECT ANY TABLE TO dblink_user;

GRANT SELECT ANY DICTIONARY TO dblink_user;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

2. Cree un enlace de base de datos desde la instancia de destino de RDS para Oracle a la instancia de origen utilizando el usuario recién creado.

```
CREATE DATABASE LINK remote_site
  CONNECT TO dblink_user IDENTIFIED BY my-password
  USING '(description=(address=(protocol=tcp) (host=my-host)
    (port=my-listener-port)) (connect_data=(sid=my-source-db-sid)))';
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

3. Pruebe el enlace:

```
SELECT * FROM V$INSTANCE@remote_site;
```

4. Cree una tabla de ejemplo con la clave principal y el log de vistas materializadas en la instancia de origen.

```
CREATE TABLE customer_0 TABLESPACE users
  AS (SELECT ROWNUM id, o.*
      FROM   ALL_OBJECTS o, ALL_OBJECTS x
      WHERE  ROWNUM <= 1000000);

ALTER TABLE customer_0 ADD CONSTRAINT pk_customer_0 PRIMARY KEY (id) USING INDEX;

CREATE MATERIALIZED VIEW LOG ON customer_0;
```

5. En la instancia de base de datos de RDS para Oracle, cree una vista materializada.

```
CREATE MATERIALIZED VIEW customer_0
  BUILD IMMEDIATE REFRESH FAST
  AS (SELECT *
      FROM   cust_dba.customer_0@remote_site);
```

6. En la instancia de base de datos de RDS para Oracle, actualice la vista materializada.

```
EXEC DBMS_MVIEW.REFRESH('CUSTOMER_0', 'f');
```

7. Arrastre la vista materializada e incluya la cláusula `PRESERVE TABLE` para retener la tabla del contenedor de la vista materializada y su contenido.

```
DROP MATERIALIZED VIEW customer_0 PRESERVE TABLE;
```

   La tabla conservada tiene el mismo nombre que la vista materializada eliminada.

Trabajo con las réplicas de lectura para Amazon RDS para Oracle

Para configurar la replicación entre instancias de base de datos de Oracle, puede crear bases de datos de réplica. Para obtener información general sobre las réplicas de lectura de Amazon RDS, consulte Información general de las réplicas de lectura de Amazon RDS. Para obtener un resumen de las diferencias entre las réplicas de Oracle y otros motores de base de datos, consulte Diferencias entre réplicas de lectura para motores de base de datos.

Temas

- Descripción general de las réplicas de RDS para Oracle
- Requisitos y consideraciones sobre réplicas de RDS para Oracle
- Preparación para crear una réplica de Oracle
- Creación de una réplica de RDS para Oracle en modo montado
- Modificación del modo de réplica de RDS para Oracle
- Trabajo con copias de seguridad de réplicas de RDS para Oracle
- Realización de una conmutación de Oracle Data Guard
- Solución de problemas de réplicas de RDS para Oracle

Descripción general de las réplicas de RDS para Oracle

La base de datos de una réplica de Oracle es una copia física de la base de datos principal. Una réplica de Oracle en modo de solo lectura se denomina réplica de lectura. Una réplica de Oracle en modo montado se denomina réplica montada. La base de datos de Oracle no permite escribir en una réplica, pero puede promocionar una réplica para hacerla de escritura. La réplica de lectura promocionada tiene los datos replicados hasta el momento en el que se hizo la solicitud para promocionarla.

En el siguiente video, se proporciona información general útil de la recuperación de desastres de RDS para Oracle.

Para obtener más información, consulte las publicaciones del blog Recuperación de desastres administrada con copias de seguridad automatizadas de Amazon RDS for Oracle entre regiones - Parte 1 y Recuperación de desastres administrada con copias de seguridad automatizadas de Amazon RDS for Oracle entre regiones - Parte 2.

Temas

- Réplicas de solo lectura y montadas
- Leer réplicas de CDB
- Retención de registros REDO archivados
- Interrupciones durante la replicación de Oracle

Réplicas de solo lectura y montadas

Al crear o modificar una réplica de Oracle, puede colocarla en cualquiera de los modos siguientes:

Solo lectura

Esta es la opción predeterminada. Active Data Guard transmite y aplica los cambios de la base de datos de origen a todas las bases de datos de réplica de lectura.

Puede crear hasta cinco réplicas de lectura a partir de una instancia de base de datos de origen. Para obtener información general acerca de las réplicas de lectura que se aplican a todos los motores de base de datos, consulte Trabajo con réplicas de lectura de instancias de base de datos. Para obtener información acerca de Oracle Data Guard, consulte la sección sobre administración y conceptos de Oracle Data Guard en la documentación de Oracle.

Montado

En este caso, la replicación utiliza Oracle Data Guard, pero la base de datos de réplica no acepta conexiones de usuario. El uso principal de las réplicas montadas es la recuperación de desastres entre regiones.

Una réplica montada no puede servir una carga de trabajo de solo lectura. La réplica montada elimina los archivos de registro REDO archivados después de aplicarlos, independientemente de la política de retención de registros archivados.

Puede crear una combinación de réplicas de base de datos montadas y de solo lectura para la misma instancia de base de datos de origen. Puede cambiar una réplica de solo lectura al modo montado o cambiar una réplica montada al modo de solo lectura. En cualquier caso, la base de datos Oracle conserva la configuración de retención de registros archivados.

Leer réplicas de CDB

RDS para Oracle admite las réplicas de lectura de Data Guard para las CDB de Oracle Database 19c y 21c, pero solo en la configuración de un solo inquilino. Puede crear, administrar y promover

réplicas de lectura en una CDB del mismo modo que en una no CDB. También se admiten réplicas montadas. Logra los siguientes beneficios:

- Recuperación de desastres administrada, alta disponibilidad y acceso de solo lectura a las réplicas.
- La posibilidad de crear réplicas de lectura en una Región de AWS diferente.
- Integración con las API de réplica de lectura de RDS existentes: CreateDBInstanceReadReplica, PromoteReadReplica y SwitchoverReadReplica.

Para utilizar esta característica, necesita una licencia de Active Data Guard y una licencia de Oracle Database Enterprise Edition tanto para la réplica como para la instancia de base de datos principal. No hay costes adicionales relacionados con el uso de la arquitectura de CDB. Solo paga por sus instancias de base de datos.

Para obtener más información sobre las configuraciones de un inquilino y de varios inquilinos de la arquitectura CDB, consulte Descripción general de las CDB de RDS para Oracle.

Retención de registros REDO archivados

Si una instancia de base de datos principal no tiene réplicas de lectura entre regiones, Amazon RDS para Oracle mantiene durante un mínimo de dos horas los registros REDO en la instancia de base de datos de origen. Esto es cierto independientemente de la configuración de `archivelog retention hours` en `rdsadmin.rdsadmin_util.set_configuration`.

RDS purga los registros de la instancia de base de datos de origen después de dos horas o cuando hayan pasado las horas de retención del registro del archivo establecidas, lo que lleve más tiempo. RDS purga los registros de la réplica de lectura después de haber pasado las horas de retención del registro del archivo establecidas solo si se han aplicado correctamente a la base de datos.

En algunos casos, es posible que una instancia de base de datos principal tenga una o más réplicas de lectura entre regiones. Si esto ocurre, Amazon RDS para Oracle mantiene los registros de transacción en la instancia de base de datos de origen hasta que se hayan transmitido y aplicado a todas las réplicas de lectura entre regiones. Para obtener información sobre `rdsadmin.rdsadmin_util.set_configuration`, consulte Retaining archived redo logs (Retención de los registros de recuperación de cambios archivados).

Interrupciones durante la replicación de Oracle

Cuando se crea una réplica de lectura, Amazon RDS realiza una instantánea de base de datos de la instancia de base de datos de origen y comienza la replicación. La instancia de base de datos de origen experimenta una suspensión de E/S muy breve cuando comienza la operación de instantánea de base de datos. La suspensión de E/S suele durar un segundo. Puede evitar la suspensión de E/S si la instancia de base de datos de origen es una implementación Multi-AZ, porque en ese caso la instantánea se toma de la instancia de base de datos secundaria.

La instantánea de base de datos se convierte en la réplica de Oracle. Amazon RDS establece los parámetros y permisos necesarios para la instancia de base de datos de origen y la réplica sin interrupción del servicio. Del mismo modo, si elimina una réplica, no se produce ninguna interrupción.

Requisitos y consideraciones sobre réplicas de RDS para Oracle

Antes de crear una réplica de Oracle, familiarícese con los siguientes requisitos y consideraciones.

Temas

- Requisitos de versión y licencia para réplicas de RDS para Oracle
- Limitaciones de grupos de opciones para réplicas de RDS para Oracle
- Consideraciones sobre copias de seguridad y restauración para réplicas de RDS para Oracle
- Requisitos y limitaciones de replicación de RDS Custom para Oracle
- Otros aspectos para réplicas de RDS para Oracle

Requisitos de versión y licencia para réplicas de RDS para Oracle

Antes de crear una réplica de RDS para Oracle, tenga en cuenta lo siguiente:

- Si la réplica está en modo de solo lectura, asegúrese de que tiene una licencia de Active Data Guard. Si coloca la réplica en modo montado, no necesita una licencia de Active Data Guard. Solo el motor de base de datos de Oracle admite réplicas montadas.
- Las réplicas de Oracle solo se admiten para el motor de Oracle Enterprise Edition (EE).
- Las réplicas de Oracle que no son CDB solo son compatibles con instancias de bases de datos creadas con instancias que no son CDB y que se ejecutan en Oracle Database 19c.
- Las réplicas de Oracle están disponibles para instancias de base de datos que se ejecutan solo en clases de instancia de base de datos con dos o más vCPU. Una instancia de base de datos de origen no puede utilizar la clase de instancia db.t3.small.

- La versión del motor de base de datos de Oracle de la instancia de base de datos de origen y todas sus réplicas deben ser iguales. Amazon RDS actualiza las replicas inmediatamente después de actualizar la instancia de base de datos de origen, independientemente del periodo de mantenimiento de la replica. Para las actualizaciones de versiones principales de réplicas entre regiones, Amazon RDS hace automáticamente lo siguiente:
  - Genera un grupo de opciones para la versión de destino.
  - Copia todas las opciones y configuraciones de opciones del grupo de opciones original al nuevo grupo de opciones.
  - Asocia la réplica entre regiones actualizada con el nuevo grupo de opciones.

  Para obtener más información acerca de cómo actualizar la versión del motor de base de datos, consulte Actualización del motor de base de datos de RDS para Oracle.

Limitaciones de grupos de opciones para réplicas de RDS para Oracle

Cuando trabaje con grupos de opciones para la réplica de RDS para Oracle, tenga en cuenta lo siguiente:

- No puede utilizar un grupo de opciones de réplica distinto del grupo de opciones de la instancia de base de datos de origen cuando el origen y la réplica se encuentran en la misma región de AWS.

  Las modificaciones en el grupo de opciones de origen o en la suscripción a grupos de opciones de origen se propagan a las réplicas de Oracle. Estos cambios se aplican a las réplicas inmediatamente después de su aplicación a la instancia de base de datos de origen, con independencia del periodo de mantenimiento de la réplica. Para obtener más información acerca de los grupos de opciones, consulte Trabajo con grupos de opciones.
- No puede eliminar una réplica entre regiones de RDS para Oracle desde su grupo de opciones dedicado, que se crea automáticamente para la réplica.
- No puede añadir el grupo de opciones dedicado para una réplica entre regiones de RDS para Oracle en una instancia de base de datos diferente.
- No puede agregar o quitar las opciones no replicadas de un grupo de opciones dedicado para una réplica entre regiones de RDS para Oracle, con la excepción de las siguientes opciones:
  - `NATIVE_NETWORK_ENCRYPTION`
  - `OEM`
  - `OEM_AGENT`

- SSL

  Para agregar otras opciones a una réplica entre regiones de RDS para Oracle, agréguelas al grupo de opciones de la instancia de base de datos de origen. La opción también está instalada en todas las réplicas de la instancia de base de datos de origen. Para las opciones con licencia, asegúrese de que haya licencias suficientes para las réplicas.

  Al promocionar una réplica entre regiones de RDS para Oracle, la réplica promocionada se comporta igual que las otras instancias de base de datos de Oracle, incluida la administración de sus opciones. Puede promocionar una réplica de manera explícita o implícita al eliminar su instancia de base de datos de origen.

  Para obtener más información acerca de los grupos de opciones, consulte Trabajo con grupos de opciones.

- No puede agregar la opción `EFS_INTEGRATION` a las réplicas entre regiones de RDS para Oracle.

Consideraciones sobre copias de seguridad y restauración para réplicas de RDS para Oracle

Antes de crear una réplica de RDS para Oracle, tenga en cuenta lo siguiente:

- Para crear instantáneas de réplicas de RDS para Oracle o activar copias de seguridad automáticas, asegúrese de configurar el período de retención de copias de seguridad manualmente. Las copias de seguridad automáticas no están activadas de forma predeterminada.
- Cuando se restaura una copia de seguridad de réplicas, esta se restaura a la hora de la base de datos, no a la hora en que se realizó la copia de seguridad. El tiempo de base de datos se refiere a la última hora de la transacción aplicada de los datos de la copia de seguridad. La diferencia es importante, porque una réplica puede tener un retardo con respecto a la principal de minutos u horas.

  Para encontrar la diferencia, utilice el comando `describe-db-snapshots`. Compare `snapshotDatabaseTime`, que es la hora de la base de datos de la copia de seguridad de réplicas, con `OriginalSnapshotCreateTime`, que es la última transacción aplicada en la base de datos principal.

Requisitos y limitaciones de replicación de RDS Custom para Oracle

Antes de crear una réplicas de RDS para Oracle, tenga en cuenta los siguientes requisitos y limitaciones:

- Si la instancia de base de datos principal usa la configuración de inquilino único de la arquitectura multitenencia, tenga en cuenta lo siguiente:
  - Debe utilizar Oracle Database 19c o una versión posterior con la Enterprise Edition.
  - Su instancia de CDB principal debe estar en un ciclo de vida `ACTIVE`.
  - No puedes convertir una instancia principal que no sea de CDB en una instancia de CDB y convertir sus réplicas en la misma operación. En cambio, elimine las réplicas que no sean de CDB, convierta la instancia de base de datos principal en una CDB y, a continuación, cree réplicas nuevas
- Asegúrese de que el desencadenador de inicio de sesión en una instancia de base de datos principal permita el acceso al usuario de `RDS_DATAGUARD` y a cualquier usuario cuyo valor `AUTHENTICATED_IDENTITY` sea `RDS_DATAGUARD` o `rdsdb`. Además, el desencadenador no debe establecer el esquema actual para el usuario de `RDS_DATAGUARD`.
- Para evitar el bloqueo de conexiones desde el proceso de Data Guard Broker, no habilite las sesiones restringidas. Para obtener más información acerca de las sesiones restringidas, consulte Activación y desactivación de sesiones restringidas.

Otros aspectos para réplicas de RDS para Oracle

Antes de crear una réplica de RDS para Oracle, tenga en cuenta lo siguiente:

- Si su instancia de base de datos es un origen para una o más réplicas entre regiones, la base de datos de origen retiene sus archivos de registros REDO hasta que se apliquen en todas las réplicas entre regiones. Los registros REDO archivados podrían provocar un incremento del consumo del almacenamiento.
- Para evitar interrumpir la automatización de RDS, los desencadenadores del sistema deben permitir a usuarios específicos iniciar sesión en la base de datos principal y de réplica. Los desencadenadores del sistema incluyen desencadenadores de DDL, inicio de sesión y función de base de datos. Le recomendamos que agregue código a los desencadenadores para excluir a los usuarios enumerados en el siguiente código de ejemplo:

```
-- Determine who the user is
```

```
SELECT SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') INTO CURRENT_USER FROM DUAL;
-- The following users should always be able to login to either the Primary or
 Replica
IF CURRENT_USER IN ('master_user', 'SYS', 'SYSTEM', 'RDS_DATAGUARD', 'rdsdb') THEN
RETURN;
END IF;
```

- El seguimiento de cambios de bloque es compatible con réplicas de solo lectura, pero no para réplicas montadas. Puede cambiar una réplica montada a una réplica de solo lectura y, a continuación, habilitar el seguimiento de cambios de bloque. Para obtener más información, consulte Activación y desactivación del seguimiento de cambio de bloques.
- No puede crear una réplica de lectura de Oracle cuando la base de datos de origen administra las credenciales de usuario principal con Secrets Manager.

Preparación para crear una réplica de Oracle

Antes de empezar a utilizar la réplica, realice las siguientes tareas.

Temas

- Habilitación de copias de seguridad automáticas
- Activación del modo Force Logging
- Cambio de la configuración de registro
- Configuración del parámetro MAX_STRING_SIZE
- Planificación de los recursos informáticos y de almacenamiento

Habilitación de copias de seguridad automáticas

Para que una instancia de base de datos pueda servir como instancia de base de datos de origen, asegúrese de habilitar las copias de seguridad automáticas en la instancia de base de datos de origen. Para obtener información sobre cómo realizar este procedimiento, consulte Habilitar las copias de seguridad automatizadas.

Activación del modo Force Logging

Le recomendamos que habilite el modo Force Logging. En el modo Force Logging, la base de datos Oracle escribe registros REDO incluso cuando `NOLOGGING` se utiliza con instrucciones de lenguaje de definición de datos (DDL).

Para habilitar el modo Force Logging

1. Inicie sesión en la base de datos Oracle mediante una herramienta de cliente como SQL Developer.
2. Active el modo Force Logging ejecutando el siguiente procedimiento.

```
exec rdsadmin.rdsadmin_util.force_logging(p_enable => true);
```

Para obtener más información acerca de este procedimiento, consulte Activación del modo force logging.

Cambio de la configuración de registro

Para n registros REDO en línea de tamaño m, RDS crea automáticamente n+1 registros en espera de tamaño m en la instancia de base de datos principal y en todas las réplicas. Siempre que cambie la configuración de registro en la principal, los cambios se propagarán automáticamente a las réplicas.

Si cambia la configuración de registro, tenga en cuenta las directrices siguientes:

- Recomendamos que realice dichos cambios antes de hacer que una instancia de base de datos sea el origen de las réplicas. RDS para Oracle también admite la actualización de la instancia una vez que se convierte en origen.
- Antes de cambiar la configuración de registro en la instancia de base de datos principal, compruebe que cada réplica tenga suficiente espacio de almacenamiento para adaptarse a la nueva configuración.

Puede modificar la configuración de registro de una instancia de base de datos mediante los procedimientos de Amazon RDS `rdsadmin.rdsadmin_util.add_logfile` y `rdsadmin.rdsadmin_util.drop_logfile`. Para obtener más información, consulte Adición de registros REDO en línea y Eliminación de registros REDO en línea.

Configuración del parámetro MAX_STRING_SIZE

Antes de crear una réplica de Oracle, asegúrese de que el valor del parámetro `MAX_STRING_SIZE` sea el mismo en la réplica y la instancia de base de datos de origen. Puede hacerlo asociándolas al mismo grupo de parámetros. Si tiene grupos de parámetros distintos para el origen y la réplica,

puede establecer `MAX_STRING_SIZE` en el mismo valor. Para obtener más información sobre este parámetro, consulte Activación de tipos de datos extendidos para una instancia de base de datos nueva.

Planificación de los recursos informáticos y de almacenamiento

Asegúrese de que la instancia de base de datos de origen y sus réplicas tengan el tamaño adecuado, en términos de informática y almacenamiento, para adaptarse a su carga operativa. Si una réplica llega a su capacidad en materia de recursos de cómputo, de red o de almacenamiento, dejará de recibir o aplicar los cambios desde su origen. Amazon RDS for Oracle no interviene para mitigar el retraso de réplica elevado entre una instancia de base de datos de origen y sus réplicas. Puede modificar los recursos de CPU y almacenamiento de una réplica independientemente de su origen y otras réplicas.

Creación de una réplica de RDS para Oracle en modo montado

De forma predeterminada, las réplicas de Oracle son de solo lectura. Para crear una réplica en modo montado, utilice la consola, la AWS CLI o la API de RDS.

Consola

Para crear una réplica montada a partir de una instancia de base de datos de Oracle de origen

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Seleccione la instancia de base de datos de Oracle que desea utilizar como origen de una réplica montada.
4. En Actions (Acciones), elija Create read replica (Crear réplica de lectura).
5. En Replica mode (Modo de réplica), elija Mounted (Montado).
6. Elija los ajustes que desee usar. En DB instance identifier (Identificador de instancias de bases de datos), escriba un nombre para la réplica de lectura. Ajuste otros valores como considere necesario.
7. En Regions (Regiones), elija la región donde se lanzará la réplica montada.
8. Elija el tamaño de la instancia y el tipo de almacenamiento. Es recomendable usar la misma clase de instancia de base de datos y el mismo tipo de almacenamiento que la instancia de base de datos de origen para la réplica de lectura.

9. En Multi-AZ deployment (Implementación Multi-AZ), elija Create a standby instance (Crear una instancia en espera) para crear una réplica en espera en otra zona de disponibilidad para permitir la conmutación por error de la réplica montada. La creación de su réplica montada como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.
10. Elija los demás ajustes que desee usar.
11. Elija Create replica (Crear réplica).

En la página Databases (Bases de datos), la réplica montada tiene el rol Réplica.

AWS CLI

Para crear una réplica de Oracle en modo montado, establezca `--replica-mode` en `mounted` en el comando create-db-instance-read-replica de la AWS CLI.

Example

Para Linux, macOS o:Unix

```
aws rds create-db-instance-read-replica \
    --db-instance-identifier myreadreplica \
    --source-db-instance-identifier mydbinstance \
    --replica-mode mounted
```

En:Windows

```
aws rds create-db-instance-read-replica ^
    --db-instance-identifier myreadreplica ^
    --source-db-instance-identifier mydbinstance ^
    --replica-mode mounted
```

Para cambiar una réplica de solo lectura a un estado montado, establezca `--replica-mode` en `mounted` en el comando modify-db-instance de la AWS CLI. Para colocar una réplica montada en modo de solo lectura, establezca `--replica-mode` en `open-read-only`.

API de RDS

Para crear una réplica de Oracle en modo montado, especifique `ReplicaMode=mounted` en la operación de API de RDS CreateDBInstanceReadReplica.

Modificación del modo de réplica de RDS para Oracle

Para cambiar el modo de réplica de una réplica existente, utilice la consola, la AWS CLI o la API de RDS. Al cambiar al modo montado, la réplica desconecta todas las conexiones activas. Cuando cambie al modo de solo lectura, Amazon RDS inicializa Active Data Guard.

La operación de cambio puede tardar unos minutos. Durante la operación, el estado de la instancia de base de datos cambia a modifying (modificando). Para obtener más información acerca de los cambios de estado, consulte Visualización del estado de la instancia de base de datos de en un clúster de Aurora.

Consola

Para cambiar el modo de réplica de una réplica de Oracle de montada a de sólo lectura

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la base de datos de réplica montada
4. Elija Modify.
5. En Replica mode (Modo de réplica), elija Read-only (Solo lectura).
6. Elija los demás ajustes que desee usar.
7. Elija Continue.
8. En Programación de modificaciones, elija Aplicar inmediatamente.
9. Elija Modificar la instancia de base de datos.

AWS CLI

Para cambiar una réplica de lectura al modo montado, establezca `--replica-mode` en `mounted` en el comando modify-db-instance de la AWS CLI. Para cambiar una réplica montada al modo de solo lectura, establezca `--replica-mode` en `open-read-only`.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
```

```
    --db-instance-identifier myreadreplica \
    --replica-mode mode
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier myreadreplica ^
    --replica-mode mode
```

API de RDS

Para cambiar una réplica de solo lectura al modo montado, establezca `ReplicaMode=mounted` en ModifyDBInstance. Para cambiar una réplica montada al modo de solo lectura, establezca `ReplicaMode=read-only`.

Trabajo con copias de seguridad de réplicas de RDS para Oracle

Puede crear y restaurar copias de seguridad de una réplica de RDS para Oracle. Se admiten tanto copias de seguridad automáticas como instantáneas manuales. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos. En las siguientes secciones se describen las diferencias clave entre la administración de copias de seguridad de una réplica principal y una de RDS para Oracle.

Activación de copias de seguridad de réplicas de RDS para Oracle

Una réplica de Oracle no tiene activadas las copias de seguridad automáticas de forma predeterminada. Para activar las copias de seguridad automáticas, establezca el periodo de retención de copia de seguridad en un valor positivo distinto de cero.

Consola

Para habilitar las copias de seguridad automatizadas inmediatamente

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija la instancia de base de datos o el clúster de base de datos Multi-AZ que desea modificar.
3. Elija Modificar.

4. En Periodo de retención de copia de seguridad, elija un valor positivo distinto de cero, por ejemplo, tres días.
5. Elija Continue.
6. Seleccione Apply immediately (Aplicar inmediatamente).
7. Elija Modificar la instancia de base de datos o Modificar clúster para guardar los cambios y habilitar las copias de seguridad automáticas.

AWS CLI

Para habilitar las copias de seguridad automáticas, utilice el comando modify-db-instance o modify-db-cluster de AWS CLI.

Incluya los siguientes parámetros:

- `--db-instance-identifier` (o `--db-cluster-identifier` para un clúster de base de datos Multi-AZ)
- `--backup-retention-period`
- `--apply-immediately` o `--no-apply-immediately`

En este ejemplo, habilitaremos las copias de seguridad automatizadas estableciendo el periodo de retención de copia de seguridad en 3 días. Los cambios se aplican inmediatamente.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier my_db_instance  \
    --backup-retention-period 3 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier my_db_instance  ^
    --backup-retention-period 3 ^
    --apply-immediately
```

API de RDS

Para habilitar las copias de seguridad automáticas, utilice la operación ModifyDBInstance o ModifyDBCluster de la API de RDS con los siguientes parámetros obligatorios:

- `DBInstanceIdentifier` o `DBClusterIdentifier`
- `BackupRetentionPeriod`

Restauración de una copia de seguridad de réplicas de RDS para Oracle

Puede restaurar una copia de seguridad de réplicas de Oracle del mismo modo que puede restaurar una copia de seguridad de la instancia principal. Para obtener más información, consulte los siguientes temas:

- Restauración a una instancia de base de datos
- Restauración de una instancia de base de datos a un momento especificado para Amazon RDS

La consideración principal a la hora de restaurar una copia de seguridad de réplicas es determinar el punto en el tiempo en el que se va a restaurar. El tiempo de base de datos se refiere a la última hora de la transacción aplicada de los datos de la copia de seguridad. Cuando restaura una copia de seguridad de réplicas, se restaura la hora de la base de datos, no la hora en que se realizó la copia de seguridad. La diferencia es importante, porque una réplica de RDS para Oracle puede tener un retardo con respecto a la principal de minutos u horas. Por lo tanto, la hora de la base de datos de una copia de seguridad de réplicas y, por lo tanto, el punto en el tiempo en el que se restaura, puede ser mucho más anterior a la hora de creación

Para encontrar la diferencia entre la hora de la base de datos y la hora de creación, utilice el comando `describe-db-snapshots`. Compare `SnapshotDatabaseTime`, que es la hora de la base de datos de la copia de seguridad de réplicas, con `OriginalSnapshotCreateTime`, que es la última transacción aplicada en la base de datos principal. El siguiente ejemplo muestra la diferencia entre las dos horas:

```
aws rds describe-db-snapshots \
    --db-instance-identifier my-oracle-replica
    --db-snapshot-identifier my-replica-snapshot

{
    "DBSnapshots": [
```

```
        {
            "DBSnapshotIdentifier": "my-replica-snapshot",
            "DBInstanceIdentifier": "my-oracle-replica",
            "SnapshotDatabaseTime": "2022-07-26T17:49:44Z",
            ...
            "OriginalSnapshotCreateTime": "2021-07-26T19:49:44Z"
        }
    ]
}
```

Realización de una conmutación de Oracle Data Guard

Una conmutación es una inversión de roles entre una base de datos principal y una base de datos en espera. Durante una conmutación, la base de datos principal original pasa a un rol en espera, mientras que la base de datos en espera original pasa al rol primerio.

En un entorno de Oracle Data Guard, una base de datos principal admite una o más bases de datos en espera. Puede realizar una transición de roles administrada y basada en conmutaciones de una base de datos principal a una base de datos en espera. Una conmutación es una inversión de roles entre una base de datos principal y una base de datos en espera. Durante una conmutación, la base de datos principal original pasa a un rol en espera, mientras que la base de datos en espera original pasa al rol primerio.

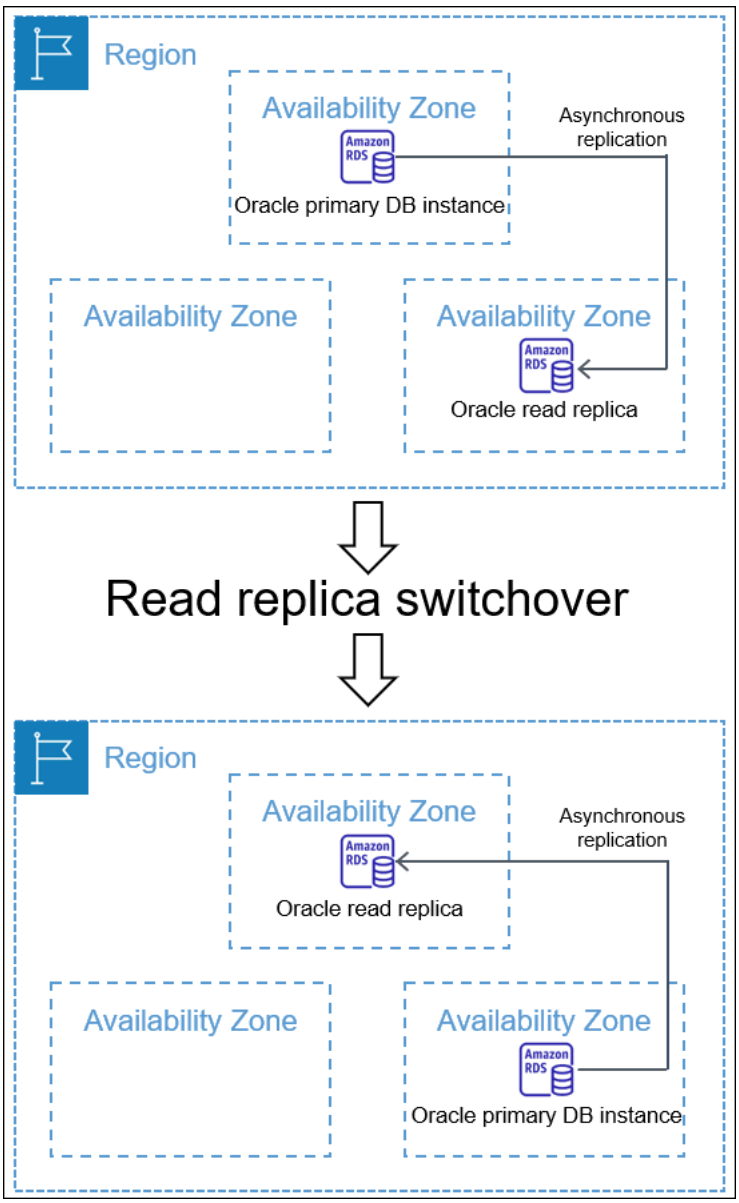
Temas

- Información general sobre conmutaciones de Oracle Data Guard
- Requisitos para la transición de Oracle Data Guard
- Inicio de la conmutación de Oracle Data Guard
- Monitorización de la conmutación de Oracle Data Guard

Información general sobre conmutaciones de Oracle Data Guard

Amazon RDS admite una transición de roles totalmente administrada y basada en conmutaciones para las réplicas de Oracle Database. Solo puede iniciar una conmutación a una base de datos secundaria que esté montada o abierta en modo de solo lectura.

Las réplicas pueden residir en Regiones de AWS distintas o en diferentes zonas de disponibilidad (AZ) de una sola región. Se admiten todas las Regiones de AWS.



Una transición difiere de una promoción de réplicas de lectura. En una transición, las instancias de base de datos de origen y réplica cambian de rol. En una promoción, una réplica de lectura se convierte en una instancia de base de datos de origen, pero la instancia de base de datos de origen no se convierte en una réplica. Para obtener más información, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

Temas

- Beneficios de las conmutaciones de Oracle Data Guard
- Versiones de Oracle Database compatibles
- Coste de las conmutaciones de Oracle Data Guard

- Cómo funcionan las conmutaciones de Oracle Data Guard

Beneficios de las conmutaciones de Oracle Data Guard

Al igual que para las réplicas de lectura de RDS para Oracle, una conmutación administrada se basa en Oracle Data Guard. La operación está diseñada para tener cero pérdida de datos. Amazon RDS automatiza los siguientes aspectos de la conmutación:

- Invierte los roles de la base de datos principal y la base de datos en espera especificada, poniendo la nueva base de datos en espera en el mismo estado (montada o de solo lectura) que la base de datos en espera original
- Garantiza la coherencia de datos
- Mantiene la configuración de replicación después de la transición
- Admite reversiones repetidas, lo que permite que la nueva base de datos en espera vuelva a su rol principal original

Versiones de Oracle Database compatibles

La transición de Oracle Data Guard se admite en Oracle Database 19c y en versiones posteriores.

Coste de las conmutaciones de Oracle Data Guard

La característica de la conmutación de Oracle Data Guard no implica costes adicionales. Oracle Database Enterprise Edition es compatible con bases de datos en espera en modo montado. Para abrir bases de datos en espera en modo de solo lectura, necesita la opción Oracle Active Data Guard.

Cómo funcionan las conmutaciones de Oracle Data Guard

La conmutación de Oracle Data Guard es una operación totalmente administrada. Para iniciar la conmutación de una base de datos en espera, ejecute el comando de la CLI `switchover-read-replica`. A continuación, Amazon RDS modifica los roles principal y en espera en la configuración de replicación.

El modo de espera original y principal original son los roles que existen antes de la conmutación. El modo de espera original y principal nuevo son los roles que existen después de la conmutación. Una réplica de espectador es una base de datos de réplica que funciona como base de datos en espera en el entorno de Oracle Data Guard, pero no cambia de rol.

Temas

- Fases de las conmutaciones de Oracle Data Guard
- Después de la conmutación de Oracle Data Guard

Fases de las conmutaciones de Oracle Data Guard

Para realizar la conmutación, Amazon RDS debe seguir estos pasos:

1. Bloquee nuevas transacciones en la base de datos principal original. Durante la conmutación, Amazon RDS interrumpe la replicación de todas las bases de datos de la configuración de Oracle Data Guard. Durante la conmutación, la base de datos principal original no puede procesar solicitudes de escritura.
2. Envíe las transacciones no aplicadas a la base de datos en espera original y aplíquelas.
3. Reinicie la nueva base de datos en espera en modo de solo lectura o montado. El modo depende del estado abierto de la base de datos en espera original antes de la conmutación.
4. Abra la nueva base de datos principal en el modo lectura/escritura.

Después de la conmutación de Oracle Data Guard

Amazon RDS cambia los roles de la base de datos principal y en espera. Usted es responsable de volver a conectar la aplicación y de realizar cualquier otra configuración que desee.

Temas

- Criterios correctos
- Conexión a la nueva base de datos principal
- Configuración de la nueva base de datos principal

Criterios correctos

La conmutación de Oracle Data Guard se realiza correctamente cuando la base de datos en espera original hace lo siguiente:

- Transiciones a su rol como nueva base de datos principal
- Completa su reconfiguración

Para limitar el tiempo de inactividad, la nueva base de datos principal se activa lo antes posible. Dado que Amazon RDS configura las réplicas de espectadores de forma asíncrona, estas réplicas pueden activarse después de la base de datos principal original.

Conexión a la nueva base de datos principal

Amazon RDS no propagará las conexiones de base de datos actuales a la nueva base de datos principal tras el cambio. Una vez completada la conmutación de Oracle Data Guard, vuelva a conectar la aplicación a la nueva base de datos principal.

Configuración de la nueva base de datos principal

Para realizar una conmutación a la nueva base de datos principal, Amazon RDS cambia el modo de la base de datos en espera original a abierta. El cambio de rol es el único cambio en la base de datos. Amazon RDS no configura características como la replicación Multi-AZ.

Si realiza una conmutación a una réplica entre regiones con diferentes opciones, la nueva base de datos principal conserva sus propias opciones. Amazon RDS no migra las opciones de la base de datos principal original. Si la base de datos principal original tenía opciones como SSL, NNE, OEM y OEM_AGENT, Amazon RDS no las propaga a la nueva base de datos principal.

Requisitos para la transición de Oracle Data Guard

Antes de iniciar la conmutación de Oracle Data Guard, asegúrese de que el entorno de replicación cumple los siguientes requisitos:

- La base de datos en espera original está montada o abierta en modo de solo lectura.
- Las copias de seguridad automáticas están activadas en la base de datos en espera original
- La base de datos principal original y la base de datos en espera original están en estado `available`.
- La base de datos principal original y la base de datos en espera original no tienen acciones de mantenimiento pendientes en alguno de los estados siguientes: `required`, `next window` o `in progress`. Las acciones en estos estados bloquean la transición. Para obtener información sobre cómo comprobar el estado de las actualizaciones de mantenimiento pendientes, consulte Visualización de actualizaciones de mantenimiento pendientes.

  Las acciones de mantenimiento pendientes en el estado `available` no bloquean la transición. RDS para Oracle publica con frecuencia actualizaciones del sistema operativo (SO) en el estado `available`. Estas actualizaciones pendientes del sistema operativo no bloquearán la transición

a menos que las programe para el siguiente periodo de mantenimiento, que las colocará en el estado `next window`.

> **Note**
>
> Si desea aplazar una acción de mantenimiento programada para poder ejecutar una transición, elija Acciones y, a continuación, Aplazar la actualización en la consola de RDS. También puede evitar que se bloquee una transición aplicando una acción de mantenimiento pendiente o desplazando el periodo de mantenimiento a un intervalo anterior a la transición. Para obtener más información, consulte el artículo de re:Post Cómo eliminar los elementos de mantenimiento pendientes de RDS.

- La base de datos en espera original está en estado de replicación.
- No está intentando iniciar una conmutación cuando la base de datos principal o la base de datos en espera se encuentran actualmente en un ciclo de vida de conmutación. Si una base de datos de réplicas se está reconfigurando después de una conmutación, Amazon RDS le impide iniciar otra conmutación.

> **Note**
>
> Una réplica de espectador es una réplica en la configuración de Oracle Data Guard que no es el destino de la conmutación. Las réplicas de espectador pueden estar en cualquier estado durante la conmutación.

- La base de datos en espera original tiene una configuración que es lo más parecida a la base de datos principal original. Supongamos un escenario en el que las bases de datos principal y en espera originales tienen diferentes opciones. Una vez completada la conmutación, Amazon RDS no vuelve a configurar automáticamente la nueva base de datos principal para que tenga las mismas opciones que la base de datos principal original.
- Configure la implementación multi-AZ que desee antes de iniciar la conmutación. Amazon RDS no administra Multi-AZ como parte de la conmutación. La implementación multi-AZ permanecerá inalterada.

  Supongamos que db_maz es la base de datos principal en una implementación multi-AZ y que db_saz es una réplica single-AZ. Usted inicia una conmutación de de db_maz a db_saz. Posteriormente, db_maz es una base de datos de réplica multi-AZ y db_saz es una base de

datos principal single-AZ. La nueva base de datos principal ahora no está protegida por una implementación multi-AZ.

- Como preparación para una conmutación entre regiones, la base de datos principal no usa el mismo grupo de opciones que una instancia de base de datos fuera de la configuración de replicación. Para que la conmutación entre regiones se realice correctamente, la base de datos principal actual y sus réplicas de lectura deben ser las únicas instancias de base de datos que utilicen el grupo de opciones de la base de datos principal actual. De lo contrario, Amazon RDS impedirá la conmutación.

Inicio de la conmutación de Oracle Data Guard

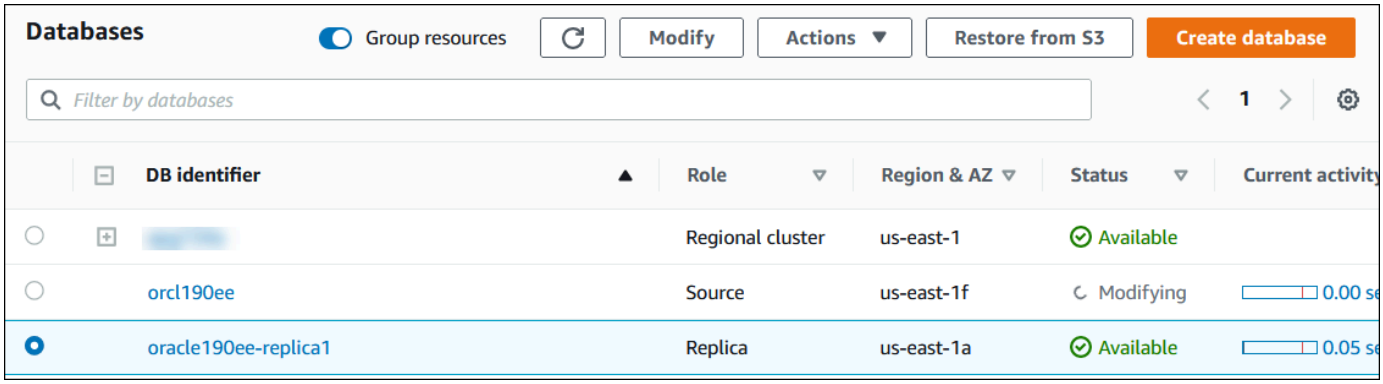
Puede cambiar una réplica de lectura de RDS para Oracle al rol principal y la anterior instancia de base de datos principal a un rol de réplica.

Consola

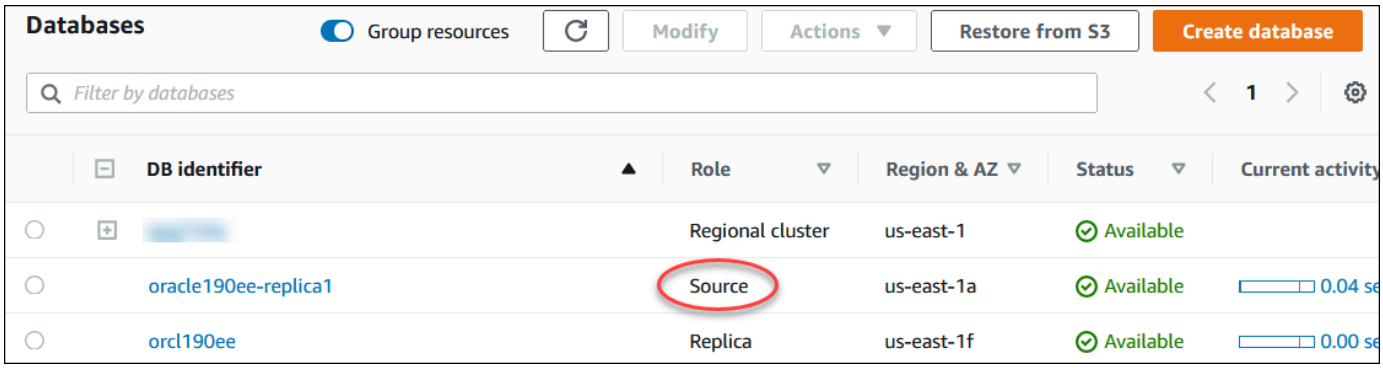
Para cambiar una réplica de lectura de Oracle al rol de la base de datos principal

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la consola de Amazon RDS, seleccione Databases (Bases de datos).

   Aparece el panel Databases (Bases de datos). Cada réplica de lectura muestra Replica (Réplica) en la columna Role (Rol).
3. Elija la réplica de lectura que desea cambiar al rol principal.
4. En Actions (Acciones), elija Switch over replica (Réplica de conmutación).
5. Elija I acknowledge (Confirmo). A continuación, elija Switch over replica (Réplica de conmutación).
6. En la página Databases (Bases de datos), supervise el progreso de la conmutación.



Cuando se complete la conmutación, el rol del objetivo de la conmutación cambiará de Replica (Réplica) a Primary (Principal).



AWS CLI

Para cambiar una réplica de Oracle al rol de la base de datos principal, utilice el comando `switchover-read-replica` de la AWS CLI. Los siguientes ejemplos hacen que la réplica de Oracle se llame *`replica-to-be-made-primary`* en la nueva base de datos principal.

Example

Para Linux, macOS o:Unix

```
aws rds switchover-read-replica \
    --db-instance-identifier replica-to-be-made-primary
```

En:Windows

```
aws rds switchover-read-replica ^
    --db-instance-identifier replica-to-be-made-primary
```

API de RDS

Para cambiar una réplica de Oracle al rol de base de datos principal, llame a la operación `SwitchoverReadReplica` de la API de Amazon RDS con el parámetro requerido `DBInstanceIdentifier`. Este parámetro especifica el nombre de la réplica de Oracle que desea que asuma el rol de base de datos principal.

Monitorización de la conmutación de Oracle Data Guard

Para comprobar el estado de las instancias, utilice el comando `describe-db-instances` de AWS CLI. El siguiente comando comprueba el estado de la instancia de base de datos *`orcl2`*. Esta base de datos era una base de datos en espera antes de la conmutación, pero es la nueva base de datos principaldespués de la conmutación.

```
aws rds describe-db-instances \
    --db-instance-identifier orcl2
```

Para confirmar que la conmutación se ha completado correctamente, consulte `V$DATABASE.OPEN_MODE`. Compruebe que el valor de la nueva base de datos principal sea `READ WRITE`.

```
SELECT OPEN_MODE FROM V$DATABASE;
```

Para buscar eventos relacionados con la conmutación, utilice el comando `describe-events` de AWS CLI. El siguiente ejemplo busca eventos en la instancia *`orcl2`*.

```
aws rds describe-events \
    --source-identifier orcl2 \
    --source-type db-instance
```

Solución de problemas de réplicas de RDS para Oracle

En esta sección se describen los posibles problemas y soluciones de replicación.

Temas

- Supervisión del retardo de replicación de Oracle
- Solución de problemas de error de replicación después de agregar o modificar desencadenadores

Supervisión del retardo de replicación de Oracle

Para supervisar el retraso de replicación en Amazon CloudWatch, consulte la métrica `ReplicaLag` de Amazon RDS. Para obtener información sobre el retardo de replicación, consulte Monitoreo de la replicación de lectura y Métricas de Amazon CloudWatch para Amazon RDS.

En un replicación de lectura, si el retraso es demasiado largo, consulte las siguientes vistas:

- `V$ARCHIVED_LOG`: muestra qué confirmaciones se han aplicado a la réplica de lectura.
- `V$DATAGUARD_STATS`: muestra un desglose detallado de los componentes que conforman la métrica `ReplicaLag`.
- `V$DATAGUARD_STATUS`: muestra el resultado de registro de los procesos de replicación internos de Oracle.

Para una réplica montada, si el tiempo de retardo es demasiado largo, no puede consultar las vistas de `V$`. En su lugar, haga lo siguiente:

- Compruebe la métrica `ReplicaLag` en CloudWatch.
- Compruebe el archivo de registro de alertas de la réplica en la consola. Busque errores en los mensajes de recuperación. Los mensajes incluyen el número de secuencia de registro, que se puede comparar con el número de secuencia principal. Para obtener más información, consulte Archivos de registro de base de datos de Amazon RDS para Oracle.

Solución de problemas de error de replicación después de agregar o modificar desencadenadores

Si se agrega o modifica cualquier desencadenador, y si la replicación falla posteriormente, los desencadenadores podrían ser el problema. Asegúrese de que el desencadenador excluye las siguientes cuentas de usuarios que RDS requiere para la replicación:

- Cuentas de usuario con privilegios de administrador
- `SYS`
- `SYSTEM`
- `RDS_DATAGUARD`
- `rdsdb`

Para obtener más información, consulte Otros aspectos para réplicas de RDS para Oracle.

Adición de opciones a instancias de base de datos de Oracle

En Amazon RDS, una opción es una característica adicional. A continuación, puede encontrar una descripción de las opciones que puede agregar a Amazon RDS que ejecutan el motor de base de datos de Oracle.

Temas

- Información general sobre las opciones de Oracle DB
- Integración de Amazon S3
- Oracle Application Express
- Integración de Amazon EFS
- Máquina virtual Oracle Java
- Oracle Enterprise Manager
- Oracle Label Security
- Oracle Locator
- Oracle Native Network Encryption
- Oracle OLAP
- Capa de conexión segura de Oracle
- Oracle Spatial
- Oracle SQLT
- Oracle Statspack
- Zona horaria Oracle
- Actualización automática del archivo de zona horaria de Oracle
- Cifrado de datos transparente de Oracle
- Oracle UTL_MAIL
- Oracle XML DB

Información general sobre las opciones de Oracle DB

Para habilitar opciones para su base de datos Oracle, puede añadirlas a un grupo de opciones y, a continuación, asociar el grupo de opciones a la instancia de base de datos. Para obtener más información, consulte Trabajo con grupos de opciones.

Temas

- Resumen de las opciones de Oracle Database
- Opciones admitidas para diferentes ediciones
- Requisitos de memoria para opciones específicas

Resumen de las opciones de Oracle Database

Puede agregar las siguientes opciones para instancias de base de datos de Oracle.

Opción	ID de la opción
Integración de Amazon S3	`S3_INTEGRATION`
Oracle Application Express	`APEX` `APEX-DEV`
Oracle Enterprise Manager	`OEM` `OEM_AGENT`
Máquina virtual Oracle Java	`JVM`
Oracle Label Security	`OLS`
Oracle Locator	`LOCATOR`
Oracle Native Network Encryption	`NATIVE_NETWORK_ENCRYPTION`
Oracle OLAP	`OLAP`
Capa de conexión segura de Oracle	`SSL`
Oracle Spatial	`SPATIAL`
Oracle SQLT	`SQLT`
Oracle Statspack	`STATSPACK`

Opción	ID de la opción
Zona horaria Oracle	`Timezone`
Actualización automática del archivo de zona horaria de Oracle	`TIMEZONE_FILE_AUTOUPGRADE`
Cifrado de datos transparente de Oracle	`TDE`
Oracle UTL_MAIL	`UTL_MAIL`
Oracle XML DB	`XMLDB`

Opciones admitidas para diferentes ediciones

RDS para Oracle le impide agregar opciones a una edición si no se admiten. Para averiguar qué opciones de RDS se admiten en diferentes ediciones de Oracle Database, utilice el comando`aws rds describe-option-group-options`. En el siguiente ejemplo se enumeran las opciones admitidas para Oracle Database 19c Enterprise Edition.

```
aws rds describe-option-group-options \
    --engine-name oracle-ee \
    --major-engine-version 19
```

Para obtener más información, consulte describe-option-group-options en la Referencia de los comandos de la CLI de AWS.

Requisitos de memoria para opciones específicas

Algunas opciones necesitan memoria adicional para ejecutarse en la instancia de base de datos. Por ejemplo, Oracle Enterprise Manager Database Control utiliza unos 300 MB de RAM. Si activa esta opción para una instancia de base de datos pequeña, puede encontrar problemas de desempeño debido a restricciones de memoria. Puede ajustar los parámetros de Oracle de manera que la base de datos requiera menos RAM. También puede escalar a una instancia de base de datos mayor tamaño.

Integración de Amazon S3

Puede transferir archivos entre una instancia de RDS para Oracle BD y un bucket de Amazon S3. Puede usar la integración de Amazon S3 con características de Oracle Batabase como Oracle Data Pump. Por ejemplo, puede descargar archivos de Data Pump desde Amazon S3 en su instancia de base de datos de RDS para Oracle. Para obtener más información, consulte Importación de datos a Oracle en Amazon RDS.

> **Note**
>
> Su instancia de base de datos y el bucket de Amazon S3 deben estar en la misma Región de AWS.

Temas

- Configuración de permisos IAM para la integración de RDS para Oracle con Amazon S3
- Adición de la opción de integración con Amazon S3
- Transferencia de archivos entre Amazon RDS para Oracle y un bucket de Amazon S3
- Solución de problemas de la integración de Amazon S3
- Eliminación de la opción de integración con Amazon S3

Configuración de permisos IAM para la integración de RDS para Oracle con Amazon S3

Para que RDS para Oracle se integre con Amazon S3, su instancia de base de datos debe tener acceso a un bucket Amazon S3. La Amazon VPC utilizada por la instancia de base de datos no necesita ofrecer acceso a los puntos de enlace de Amazon S3.

RDS para Oracle admite la transferencia de archivos entre una instancia de base de datos en una cuenta y un bucket de Amazon S3 en una cuenta diferente. En los casos en que se requieren pasos adicionales, se indican en las siguientes secciones.

Temas

- Paso 1: Crear una política de IAM para su rol de Amazon RDS
- Paso 2: (Opcional) Crear una política de IAM para su bucket de Amazon S3
- Paso 3: Crear un rol de IAM para la instancia de base de datos y asociar la política

- Paso 4: Asocie su rol de IAM a su instancia de base de datos de RDS para Oracle

Paso 1: Crear una política de IAM para su rol de Amazon RDS

En este paso, cree una política AWS Identity and Access Management (IAM) con los permisos necesarios para transferir archivos entre el bucket de Amazon S3 a la instancia de base de datos de RDS. En este paso, también se asume que ya ha creado un bucket de S3.

Antes de crear la política, anote la siguiente información:

- El nombre de recurso de Amazon (ARN) del bucket
- El ARN para su clave de AWS KMS, si el bucket utiliza el cifrado SSE-KMS o SSE-S3

> **Note**
>
> Una instancia de base de datos de RDS para Oracle no puede acceder a los buckets de Amazon S3 cifrados con SSE-C.

Para obtener más información, consulta Protección de los datos con el cifrado de servidor en la Guía del usuario de Amazon Simple Storage Service.

Consola

Para crear una política de IAM que permita a Amazon RDS acceder a un bucket de Amazon S3

1. Abra la consola de administración de IAM.
2. En Access management (Administración de acceso), seleccione Policies (Políticas).
3. Elija Crear política.
4. En la pestaña Visual editor (Editor visual), seleccione Choose a service (Elegir un servicio) y, a continuación, S3.
5. En Actions (Acciones), seleccione Expand all (Expandir todo)y, a continuación, elija los permisos de bucket y los permisos de objeto necesarios para transferir archivos de un bucket Amazon S3 a Amazon RDS. Por ejemplo, haga lo siguiente:
   - Expanda List (Lista)y, a continuación, seleccione ListBucket.
   - Expanda Read (Lectura)y, a continuación, seleccione GetObject.
   - Expanda Write (Escritura) y, a continuación, seleccione PutObject y DeleteObject.

- Expanda Permissions management (Administración de permisos)y, a continuación, seleccione PutObjectAcl. Este permiso es necesario si planea cargar archivos en un bucket propiedad de otra cuenta y esta cuenta necesita un control total del contenido del bucket.

Los permisos de objeto son permisos para operaciones de objeto en Amazon S3. Debe concederlos para los objetos de un bucket, y no para el bucket en sí. Para más información, consulte Permisos para operaciones con objetos.

6. Elija Recursos y, a continuación, haga lo siguiente:

   a. Elija Específico.

   b. En el bucket, seleccione Agregar ARN. Introduzca el ARN de su bucket. El nombre del bucket se rellena automáticamente. A continuación, elija Add (Añadir).

   c. Si se muestra el recurso del objeto, elija Agregar ARN para añadir recursos manualmente o elija Cualquiera.

   > **Note**
   >
   > Puede establecer en Amazon Resource Name (ARN) (Nombre de recurso de Amazon [ARN]) un valor de ARN más específico y que así Amazon RDS solo tenga acceso a archivos o carpetas determinados de un bucket de Amazon S3. Para obtener más información acerca del modo de definir una política de acceso en Amazon S3, consulte Administración de permisos de acceso para los recursos de Amazon S3.

7. (Opcional) Elija Add additional permissions (Agregar permisos adicionales) para agregar recursos a la política. Por ejemplo, haga lo siguiente:

   a. Si el bucket está cifrado con una clave KMS personalizada, seleccione KMS para el servicio.

   b. En Acciones manuales, seleccione lo siguiente:

      - Encrypt
      - Volver a cifrar desde y Volver a cifrar a
      - Decrypt
      - DescribeKey
      - GenerateDataKey

   c. En Recursos, elija Específico.

d. En la clave, seleccione Agregar ARN. Introduzca el ARN de su clave personalizada como recurso y luego elija Añadir.

   Para obtener más información, consulte Protección de datos con el cifrado en el servidor mediante claves de KMS almacenadas en AWS Key Management Service (SSE-KMS) en la guía del usuario de Amazon Simple Storage Service.

e. Si desea que Amazon RDS acceda a otros buckets, agregue los ARN de estos buckets. Opcionalmente, también puede conceder acceso a todos los buckets y objetos de Amazon S3.

8. Elija Next: Tags (Siguiente: Etiquetas) y, a continuación, Next: Review (Siguiente: Revisar).
9. En Name (Nombre), escriba un nombre para la política de IAM, por ejemplo, `rds-s3-integration-policy`. Utilizará este nombre al crear un rol de IAM y asociarlo a la instancia de base de datos. También puede añadir una descripción opcional en Description (Descripción).
10. Elija Create Policy (Crear política).

AWS CLI

Cree una política de AWS Identity and Access Management (IAM) que conceda a Amazon RDS acceso a un bucket de Amazon S3. Después de crear la política, apunte el ARN de esta. Necesita el ARN para un paso posterior.

Incluya las acciones adecuadas en la política en función del tipo de acceso necesario:

- `GetObject`: se requiere para transferir archivos desde un bucket de Amazon S3 a Amazon RDS.
- `ListBucket`: se requiere para transferir archivos desde un bucket de Amazon S3 a Amazon RDS.
- `PutObject`: se requiere para transferir archivos desde Amazon RDS a un bucket de Amazon S3.

El siguiente comando de la AWS CLI crea una política de IAM denominada *`rds-s3-integration-policy`* con estas opciones. Otorga acceso a un bucket denominado *`amzn-s3-demo-bucket`*.

Example

Para Linux, macOS o Unix:

```
aws iam create-policy \
   --policy-name rds-s3-integration-policy \
   --policy-document '{
```

```
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "s3integration",
        "Action": [
          "s3:GetObject",
          "s3:ListBucket",
          "s3:PutObject"
        ],
        "Effect": "Allow",
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket",
          "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
      }
    ]
  }'
```

En el ejemplo siguiente se incluyen permisos para claves KMS personalizadas.

```
aws iam create-policy \
   --policy-name rds-s3-integration-policy \
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3integration",
         "Action": [
           "s3:GetObject",
           "s3:ListBucket",
           "s3:PutObject",
           "kms:Decrypt",
           "kms:Encrypt",
           "kms:ReEncrypt*",
           "kms:GenerateDataKey",
           "kms:DescribeKey",
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket",
           "arn:aws:s3:::amzn-s3-demo-bucket/*",
           "arn:aws:kms:::your-kms-arn"
         ]
```

```
      }
    ]
  }'
```

Para Windows:

```
aws iam create-policy ^
   --policy-name rds-s3-integration-policy ^
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3integration",
         "Action": [
           "s3:GetObject",
           "s3:ListBucket",
           "s3:PutObject"
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket",
           "arn:aws:s3:::amzn-s3-demo-bucket/*"
         ]
       }
     ]
   }'
```

En el ejemplo siguiente se incluyen permisos para claves KMS personalizadas.

```
aws iam create-policy ^
   --policy-name rds-s3-integration-policy ^
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3integration",
         "Action": [
           "s3:GetObject",
           "s3:ListBucket",
           "s3:PutObject",
           "kms:Decrypt",
           "kms:Encrypt",
           "kms:ReEncrypt",
```

```
            "kms:GenerateDataKey",
            "kms:DescribeKey",
          ],
          "Effect": "Allow",
          "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "arn:aws:kms:::your-kms-arn"
          ]
        }
      ]
    }'
```

Paso 2: (Opcional) Crear una política de IAM para su bucket de Amazon S3

Este paso solo es necesario en las siguientes condiciones:

- Tiene previsto cargar archivos en un bucket de Amazon S3 desde una cuenta (cuenta A) y acceder a ellos desde otra cuenta (cuenta B).
- La cuenta A es la propietaria del bucket.
- La cuenta B necesita un control total de los objetos cargados en el bucket.

Si las condiciones anteriores no le atañen, vaya a Paso 3: Crear un rol de IAM para la instancia de base de datos y asociar la política.

Para crear la política del bucket, asegúrese de que dispone de lo siguiente:

- El ID de cuenta de la cuenta A
- El nombre de usuario de la cuenta A
- El valor ARN para el bucket de Amazon S3 en la cuenta B

Consola

Para crear o editar una política de bucket

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket para el que desea crear una política de bucket o cuya política de bucket quiera editar.

3. Elija Permisos.
4. En Bucket Policy (Política de bucket), elija Edit (Editar). Se abre la página Edit bucket policy (Editar política de bucket).
5. En la página Edit bucket policy (Editar política de bucket), examine Policy examples (Ejemplos de políticas) en la Guía del usuario de Amazon S3. Elija Policy generator (Generador de políticas) para generar una política automáticamente o edite el JSON en la sección Policy (Política).

   Si elige Policy generator (Generador de políticas), se abre el generador de políticas de AWS en una ventana nueva:

   a. En la página AWS Policy Generator (Generador de políticas de AWS), en Select Type of Policy (Seleccionar tipo de política), elija S3 Bucket Policy (Política de bucket de S3).
   b. Agregue una instrucción ingresando la información en los campos proporcionados y, a continuación, elija Add Statement (Agregar declaración). Repita el procedimiento para tantas instrucciones como desee agregar. Para obtener más información acerca de estos campos, consulte la Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

      > **Note**
      >
      > Para mayor comodidad, la página Edit bucket policy (Editar política de bucket) muestra el Bucket ARN (nombre de recurso de Amazon [ARN]) del bucket actual encima del campo de texto Policy (Política). Puede copiar este ARN para utilizarlo en las instrucciones de la página AWS Policy Generator (Generador de políticas de AWS).

   c. Una vez que haya terminado de agregar instrucciones, elija Generar política.
   d. Copie el texto de la política generada, elija Cerrar y vuelva a la página Editar política de bucket en la consola de Amazon S3.
6. En el cuadro Policy (Política), edite la política existente o pegue la política de bucket desde el generador de políticas. Asegúrese de resolver advertencias de seguridad, errores, advertencias generales y sugerencias antes de guardar la política.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Example permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-A-ID:account-A-user"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

7. Elija Save changes (Guardar cambios), que lo redirecciona a la página Bucket Permissions (Permisos de bucket).

Paso 3: Crear un rol de IAM para la instancia de base de datos y asociar la política

En este paso se supone que se ha creado la política de IAM en Paso 1: Crear una política de IAM para su rol de Amazon RDS. En este paso, creará un rol para la instancia de base de datos de RDS para Oracle y, a continuación, asociará la política al rol.

Consola

Para crear un rol de IAM que permita el acceso de Amazon RDS a un bucket de Amazon S3

1. Abra la consola de administración de IAM.
2. Seleccione Roles en el panel de navegación.
3. Elija Crear rol.

4. Elija Servicio de AWS.
5. En Casos de uso de otros servicios de:AWS, elija RDS y, a continuación, RDS: Añadir rol a la base de datos. A continuación, elija Siguiente.
6. En Buscar, en Políticas de permisos, escriba el nombre de la política de IAM que ha creado en Paso 1: Crear una política de IAM para su rol de Amazon RDS y elija la política cuando aparezca en la lista. A continuación, elija Siguiente.
7. En Nombre del rol, escriba un nombre para el rol de IAM, por ejemplo, `rds-s3-integration-role`. También puede añadir una descripción opcional en Description (Descripción).
8. Seleccione Crear rol.

AWS CLI

Para crear un rol de IAM y asociarle su política

1. Cree un rol de IAM que Amazon RDS pueda asumir en su nombre para acceder a sus buckets de Amazon S3.

   Se recomienda usar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las relaciones de confianza basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

   Puede utilizar claves de contexto de condición globales y hacer que el valor de `aws:SourceArn` contenga el ID de cuenta. En estos casos, el valor de `aws:SourceAccount` y la cuenta del valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilizan en la misma instrucción.

   - Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
   - Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

   En la relación de confianza, asegúrese de usar la clave de contexto de la condición global `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo de los recursos que acceden al rol.

   El siguiente comando AWS CLI crea el rol nombrado *`rds-s3-integration-role`* para este propósito.

Example

Para Linux, macOS o Unix:

```
aws iam create-role \
   --role-name rds-s3-integration-role \
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                 "aws:SourceAccount": "my_account_ID",
                 "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
             }
         }
       }
     ]
   }'
```

Para Windows:

```
aws iam create-role ^
   --role-name rds-s3-integration-role ^
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                 "aws:SourceAccount": "my_account_ID",
                 "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
```

```
            }
          }
        }
      ]
    }'
```

Para obtener más información, consulte Creación de un rol para delegar permisos a un usuario de IAM en la Guía del usuario de IAM.

2. Después de crear el rol, anote el ARN del rol. Necesita el ARN para un paso posterior.
3. Asocie la política que ha creado al rol que ha creado.

   El siguiente comando de la AWS CLI asocia la política al rol denominado *rds-s3-integration-role*.

   Example

   Para Linux, macOS o Unix:

```
aws iam attach-role-policy \
   --policy-arn your-policy-arn \
   --role-name rds-s3-integration-role
```

   Para Windows:

```
aws iam attach-role-policy ^
   --policy-arn your-policy-arn ^
   --role-name rds-s3-integration-role
```

   Sustituya *your-policy-arn* por el ARN de la política anotado en el paso anterior.

Paso 4: Asocie su rol de IAM a su instancia de base de datos de RDS para Oracle

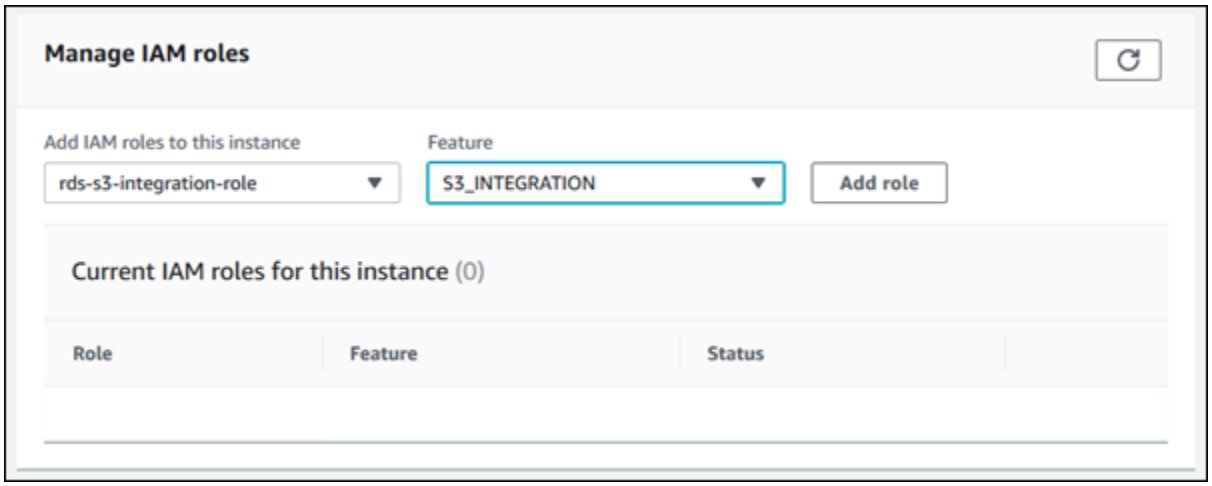
El último paso para configurar los permisos para la integración de Amazon S3 es asociar el rol de IAM con la instancia de base de datos. Tenga en cuenta los siguientes requisitos:

- Debe tener acceso a un rol de IAM con la política de permisos de Amazon S3 requerida adjunta.
- Solo puede asociar un rol de IAM a su instancia de base de datos de RDS para Oracle cada vez.
- Su instancia de base de datos debe tener el estado Disponible.

Consola

Para asociar su rol de IAM a su instancia de base de datos de RDS para Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Bases de datos en el panel de navegación.
3. Seleccione el nombre de la instancia de base de datos de RDS para Oracle para ver sus detalles.
4. En la pestaña Connectivity & Security (Conectividad y seguridad), desplácese hacia abajo hasta la sección Manage IAM roles (Administrar roles de IAM) de la parte inferior de la página.
5. En Añadir roles de IAM a esta instancia, elija el rol que creó en Paso 3: Crear un rol de IAM para la instancia de base de datos y asociar la política.
6. En Feature (Característica), elija S3_INTEGRATION.



7. Seleccione Add role (Añadir rol).

AWS CLI

El siguiente comando de la AWS CLI añade el rol a una instancia de base de datos de Oracle denominada *mydbinstance*.

Example

Para Linux, macOS o Unix:

```
aws rds add-role-to-db-instance \
   --db-instance-identifier mydbinstance \
```

```
    --feature-name S3_INTEGRATION \
    --role-arn your-role-arn
```

Para Windows:

```
aws rds add-role-to-db-instance ^
    --db-instance-identifier mydbinstance ^
    --feature-name S3_INTEGRATION ^
    --role-arn your-role-arn
```

Sustituya *your-role-arn* por el ARN del rol anotado en el paso anterior. `S3_INTEGRATION` debe especificarse para la opción `--feature-name`.

Adición de la opción de integración con Amazon S3

Para integrar Amazon RDS para Oracle con Amazon S3, su instancia de base de datos debe estar asociada a un grupo de opciones que incluya la opción `S3_INTEGRATION`.

Consola

Para configurar un grupo de opciones para la integración con Simple Storage Service (Amazon S3)

1. Cree un nuevo grupo de opciones o identifique uno ya existente al que pueda añadir la opción `S3_INTEGRATION`.

   Para obtener información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.
2. Añada la opción `S3_INTEGRATION` al grupo de opciones.

   Para obtener información acerca de cómo añadir una opción a un grupo de opciones, consulte Agregar una opción a un grupo de opciones.
3. Cree una nueva instancia de base de datos de RDS para Oracle y asocie el grupo de opciones a ella, o bien modifique una instancia de base de datos de RDS para Oracle para asociarla al grupo de opciones.

   Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

   Para obtener más información acerca de la modificación de una instancia de base de datos , consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

Para configurar un grupo de opciones para la integración con Simple Storage Service (Amazon S3)

1. Cree un nuevo grupo de opciones o identifique uno ya existente al que pueda añadir la opción `S3_INTEGRATION`.

   Para obtener información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.

2. Añada la opción `S3_INTEGRATION` al grupo de opciones.

   Por ejemplo, el siguiente comando de la AWS CLI añade la opción `S3_INTEGRATION` a un grupo de opciones denominado **`myoptiongroup`**.

   Example

   Para Linux, macOS o:Unix

   ```
   aws rds add-option-to-option-group \
      --option-group-name myoptiongroup \
      --options OptionName=S3_INTEGRATION,OptionVersion=1.0
   ```

   En:Windows

   ```
   aws rds add-option-to-option-group ^
      --option-group-name myoptiongroup ^
      --options OptionName=S3_INTEGRATION,OptionVersion=1.0
   ```

3. Cree una nueva instancia de base de datos de RDS para Oracle y asocie el grupo de opciones a ella, o bien modifique una instancia de base de datos de RDS para Oracle para asociarla al grupo de opciones.

   Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

   Para obtener información acerca de cómo modificar una instancia de base de datos de RDS para Oracle, consulte Modificación de una instancia de base de datos de Amazon RDS.

Transferencia de archivos entre Amazon RDS para Oracle y un bucket de Amazon S3

Para transferir archivos entre una instancia de base de datos de RDS para Oracle y un bucket Amazon S3, puede utilizar el paquete `rdsadmin_s3_tasks` de Amazon RDS. Puede comprimir archivos con GZIP al cargarlos y descomprimirlos durante la descarga.

Temas

- Requisitos y limitaciones de la transferencia de archivos
- Carga de archivos desde la instancia de base de datos de RDS para Oracle en un bucket de Amazon S3
- Descarga de archivos desde un bucket de Amazon S3 en una instancia de base de datos de Oracle
- Monitoreo del estado de una transferencia de archivos

Requisitos y limitaciones de la transferencia de archivos

Antes de transferir archivos entre una instancia de base de datos y un bucket de Amazon S3, tenga en cuenta lo siguiente:

- El paquete `rdsadmin_s3_tasks` transfiere los archivos que se encuentran en un único directorio. No puede incluir subdirectorios en una transferencia.
- El tamaño máximo de objeto en un bucket de Amazon S3 es de 5 TB.
- Las tareas creadas por `rdsadmin_s3_tasks` se ejecutan de forma asíncrona.
- Puede cargar archivos desde el directorio de Data Pump, como `DATA_PUMP_DIR`, o desde cualquier directorio creado por el usuario. No puede cargar archivos desde un directorio que utilizan los procesos en segundo plano de Oracle, como los directorios `adump`, `bdump` o `trace`.
- El límite de descargas es de 2000 archivos por llamada a procedimiento para `download_from_s3`. Si necesita descargar más de 2000 archivos de Amazon S3, divida la descarga en acciones independientes, con un máximo de 2000 archivos por llamada al procedimiento.
- Si existe un archivo en la carpeta de descargas e intenta descargar un archivo con el mismo nombre, `download_from_s3` omite la descarga. Para quitar un archivo del directorio de descarga, utilice el procedimiento PL/SQL UTL_FILE.FREMOVE.

Carga de archivos desde la instancia de base de datos de RDS para Oracle en un bucket de Amazon S3

Para cargar archivos desde una instancia de base de datos en un bucket de Amazon S3, use el procedimiento `rdsadmin.rdsadmin_s3_tasks.upload_to_s3`. Por ejemplo, puede cargar archivos de copia de seguridad de Oracle Recovery Manager (RMAN) o archivos de Oracle Data Pump. Para obtener información acerca del uso de objetos, consulte Guía del usuario de Amazon Simple Storage Service. Para obtener más información acerca de cómo realizar copias de seguridad de RMAN, consulte Realización de tareas RMAN comunes para instancias de base de datos de Oracle.

El procedimiento `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_bucket_name`	VARCHAR2	–	obligatorio	Nombre del bucket de Amazon S3 en el que cargar archivos.
`p_directory_name`	VARCHAR2	–	obligatorio	Nombre del objeto de directorio de Oracle desde el que cargar archivos. El directorio puede ser cualquier objeto de directorio creado por el usuario o el directorio Data Pump, como `DATA_PUMP_DIR` . No puede cargar archivos desde un directorio que utilizan los procesos en segundo plano, como `adump`, `bdump` y `trace`.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				Note Solo puede cargar archivos desde el directorio especificado. No puede cargar archivos en subdirectorios en el directorio especificado.
`p_s3_prefix`	VARCHAR2	–	obligatorio	Prefijo del nombre de archivo de Amazon S3 en el que se cargan los archivos. Un prefijo vacío carga todos los archivos en el nivel superior en el bucket de Amazon S3 especificado y no añade un prefijo a los nombres de archivo. Por ejemplo, si el prefijo es `folder_1/oradb` , los archivos se cargan en `folder_1`. En este caso, el prefijo `oradb` se añade a cada archivo.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_prefix	VARCHAR2	–	obligatorio	Prefijo del nombre de archivo con el que deben coincidir los nombres de archivo para cargarse. Un prefijo vacío carga todos los archivos en el directorio especificado.
p_compression_level	NUMBER	0	opcional	El nivel de compresión GZIP. Los valores válidos van de 0 a:9 • 0: sin compresión • 1: la compresión más rápida • 9: la compresión más alta
p_bucket_owner_full_control	VARCHAR2	–	opcional	Configuración de control de acceso para el bucket. Los únicos valores válidos son null o FULL_CONTROL . Esta configuración solo es obligatoria si carga archivos de una cuenta (cuenta A) en un bucket propiedad de otra cuenta (cuenta B) y la cuenta B necesita el control total de los archivos.

El valor devuelto para el procedimiento `rdsadmin.rdsadmin_s3_tasks.upload_to_s3` es un ID de tarea.

En el siguiente ejemplo, se cargan todos los archivos del directorio *DATA_PUMP_DIR* en el bucket de Amazon S3 denominado *amzn-s3-demo-bucket*. Los archivos no están comprimidos.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name    =>  'amzn-s3-demo-bucket',
      p_prefix         =>  '',
      p_s3_prefix      =>  '',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

En el siguiente ejemplo se cargan todos los archivos con el prefijo *db* del directorio *DATA_PUMP_DIR* en el bucket de Amazon S3 denominado *amzn-s3-demo-bucket*. Amazon RDS aplica el nivel más alto de compresión GZIP a los archivos.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name       =>  'amzn-s3-demo-bucket',
      p_prefix            =>  'db',
      p_s3_prefix         =>  '',
      p_directory_name    =>  'DATA_PUMP_DIR',
      p_compression_level =>  9)
   AS TASK_ID FROM DUAL;
```

En el siguiente ejemplo se cargan todos los archivos del directorio *DATA_PUMP_DIR* en el bucket de Amazon S3 denominado *amzn-s3-demo-bucket*. Los archivos se cargan en una carpeta `dbfiles`. En este ejemplo, el nivel de compresión GZIP es *1*, que es el nivel de compresión más rápido.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name       =>  'amzn-s3-demo-bucket',
      p_prefix            =>  '',
      p_s3_prefix         =>  'dbfiles/',
      p_directory_name    =>  'DATA_PUMP_DIR',
      p_compression_level =>  1)
   AS TASK_ID FROM DUAL;
```

En el siguiente ejemplo se cargan todos los archivos del directorio *DATA_PUMP_DIR* en el bucket de Amazon S3 denominado *amzn-s3-demo-bucket*. Los archivos se cargan en una carpeta `dbfiles` y `ora` se añade al principio de cada nombre de archivo. No se aplica compresión.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name    =>  'amzn-s3-demo-bucket',
      p_prefix         =>  '',
      p_s3_prefix      =>  'dbfiles/ora',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

En el ejemplo siguiente se supone que el comando se ejecuta en la cuenta A, pero la cuenta B requiere un control total del contenido del bucket. El comando `rdsadmin_s3_tasks.upload_to_s3` transfiere todos los archivos del directorio *DATA_PUMP_DIR* al bucket denominado *s3bucket0wnedByAccountB*. El control de acceso está configurado en `FULL_CONTROL` para que la cuenta B pueda acceder a los archivos del bucket. El nivel de compresión GZIP es *6*, que equilibra la velocidad y el tamaño del archivo.

```
SELECT rdsadmin.rdsadmin_s3_tasks.upload_to_s3(
      p_bucket_name               =>  's3bucket0wnedByAccountB',
      p_prefix                    =>  '',
      p_s3_prefix                 =>  '',
      p_directory_name            =>  'DATA_PUMP_DIR',
      p_bucket_owner_full_control =>  'FULL_CONTROL',
      p_compression_level         =>  6)
   AS TASK_ID FROM DUAL;
```

En cada ejemplo, la instrucción `SELECT` devuelve el identificador de la tarea en un tipo de datos `VARCHAR2`.

Para ver el resultado, visualice el archivo de salida de la tarea.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-id.log'));
```

Reemplace *task-id* con el ID de tarea devuelto por el procedimiento.

> **Note**
>
> Las tareas se ejecutan de forma asíncrona.

Descarga de archivos desde un bucket de Amazon S3 en una instancia de base de datos de Oracle

Para descargar archivos desde un bucket de Amazon S3 en una instancia de RDS para Oracle, use el procedimiento de Amazon RDS `rdsadmin.rdsadmin_s3_tasks.download_from_s3`.

El procedimiento `download_from_s3` tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_bucket_name`	VARCHAI	–	Obligatoria	Nombre del bucket de Amazon S3 desde el que descargar archivos.
`p_directory_name`	VARCHAI	–	Obligatoria	Nombre del directorio de Oracle en el que descargar archivos. El directorio puede ser cualquier objeto de directorio creado por el usuario o el directorio Data Pump, como `DATA_PUMP_DIR` .
`p_error_on_zero_downloads`	VARCHAI	FALSO	Opcional	Indicador que determina si la tarea genera un error cuando ningún objeto del bucket de Amazon S3 coincide con el prefijo. Si este parámetro no está establecido o se establece en FALSE (predeterminado), la tarea imprime un mensaje en el que se indica que no se ha encontrado ningún objeto, pero no genera ninguna excepción ni se produce un error. Si este parámetro es TRUE, la tarea genera una excepción y se produce un error. Algunos ejemplos de especificaciones de prefijos que no superan las pruebas de coincidencia son los espacios en los prefijos, como en `' import/test9.log'` , y los desajustes de

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
				mayúsculas y minúsculas, como en `test9.log` y `test9.LOG`.
`p_s3_prefix`	VARCHAR	–	Obligatoria	Prefijo del nombre de archivo con el que deben coincidir los nombres de archivo para descargarse. Un prefijo vacío descarga todos los archivos de nivel superior en el bucket de Amazon S3 especificado pero no los archivos en las carpetas en el bucket. El procedimiento descarga objetos de Amazon S3 solo desde la primera carpeta de nivel que coincide con el prefijo. Las estructuras de directorios anidados que coinciden con el prefijo especificado no se descargan. Por ejemplo, supongamos que un bucket de Amazon S3 tiene la estructura de carpetas `folder_1/folder_2/folder_3`. Especifique el prefijo `'folder_1/folder_2/'`. En este caso, solo se descargan los archivos de `folder_2`, no los archivos de `folder_1` ni de `folder_3`. Si, de lo contrario, especifico el prefijo `'folder_1/folder_2'`, se descargan todos los archivos en `folder_1` que coincidan con el prefijo `'folder_2'` y no se descarga ningún archivo en `folder_2`.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
p_decompression_format	VARCHAR	–	Opcional	El formato de compresión. Los valores válidos son NONE sin descompresión y GZIP para descompresión.

El valor devuelto para el procedimiento rdsadmin.rdsadmin_s3_tasks.download_from_s3 es un ID de tarea.

En el siguiente ejemplo se descargan todos los archivos del bucket de Amazon S3 denominado *amzn-s3-demo-bucket* en el directorio *DATA_PUMP_DIR*. Los archivos no están comprimidos, por lo que no se aplica descompresión.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name    =>  'amzn-s3-demo-bucket',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

En el siguiente ejemplo se descargan todos los archivos con el prefijo *db* del bucket de Amazon S3 denominado *amzn-s3-demo-bucket* en el directorio *DATA_PUMP_DIR*. Los archivos están comprimidos con GZIP, por lo que se aplica descompresión. El parámetro p_error_on_zero_downloads activa la comprobación de errores de prefijos, de modo que si el prefijo no coincide con ningún archivo del bucket, la tarea generará una excepción y fallará.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name               =>  'amzn-s3-demo-bucket',
      p_s3_prefix                 =>  'db',
      p_directory_name            =>  'DATA_PUMP_DIR',
      p_decompression_format      =>  'GZIP',
      p_error_on_zero_downloads   =>  'TRUE')
   AS TASK_ID FROM DUAL;
```

En el siguiente ejemplo se descargan todos los archivos de la carpeta *myfolder/* del bucket de Amazon S3 denominado *amzn-s3-demo-bucket* en el directorio *DATA_PUMP_DIR*. Use el parámetro p_s3_prefix para especificar la carpeta de Amazon S3. Los archivos cargados se comprimen con GZIP, pero no se descomprimen durante la descarga.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name          =>  'amzn-s3-demo-bucket',
      p_s3_prefix            =>  'myfolder/',
      p_directory_name       =>  'DATA_PUMP_DIR',
      p_decompression_format =>  'NONE')
   AS TASK_ID FROM DUAL;
```

El siguiente ejemplo descarga el archivo *mydumpfile.dmp* en el bucket de Simple Storage Service (Amazon S3) con el nombre *amzn-s3-demo-bucket* del directorio *DATA_PUMP_DIR*. No se aplica descompresión.

```
SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3(
      p_bucket_name    =>  'amzn-s3-demo-bucket',
      p_s3_prefix      =>  'mydumpfile.dmp',
      p_directory_name =>  'DATA_PUMP_DIR')
   AS TASK_ID FROM DUAL;
```

En cada ejemplo, la instrucción `SELECT` devuelve el identificador de la tarea en un tipo de datos `VARCHAR2`.

Para ver el resultado, visualice el archivo de salida de la tarea.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-id.log'));
```

Reemplace *task-id* con el ID de tarea devuelto por el procedimiento.

> **Note**
>
> Las tareas se ejecutan de forma asíncrona.
> Puede utilizar el procedimiento `UTL_FILE.FREMOVE` de Oracle para eliminar archivos de un directorio. Para más información, consulte FREMOVE Procedure en la documentación de Oracle.

Monitoreo del estado de una transferencia de archivos

Las tareas de transferencia de archivos publican eventos de Amazon RDS al comenzar y al completarse. El mensaje de evento contiene el identificador de la tarea para la transferencia del

archivo. Para obtener información acerca de cómo ver los eventos, consulte Consulta de eventos de Amazon RDS.

Puede ver el estado de una tarea continua en un archivo bdump. Los archivos bdump están ubicados en el directorio `/rdsdbdata/log/trace`. El nombre del archivo bdump está en el siguiente formato.

```
dbtask-task-id.log
```

Reemplace *`task-id`* por el ID de la tarea que desea monitorizar.

> **Note**
>
> Las tareas se ejecutan de forma asíncrona.

Puede utilizar el procedimiento almacenado `rdsadmin.rds_file_util.read_text_file` para ver el contenido de los archivos bdump. Por ejemplo, la siguiente consulta devuelve el contenido del archivo bdump *`dbtask-1234567890123-1234.log`*.

```
SELECT text FROM
 table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1234567890123-1234.log'));
```

A continuación, se muestra un ejemplo de archivo de registro de una transferencia fallida.

```
TASK_ID




                                                
```

```
------------------------------------------------------------------------------------------
2023-04-17 18:21:33.993 UTC [INFO ] File #1: Uploading the file /rdsdbdata/datapump/
A123B4CDEF567890G1234567890H1234/sample.dmp to Amazon S3 with bucket name amzn-s3-demo-
bucket and key sample.dmp.
2023-04-17 18:21:34.188 UTC [ERROR] RDS doesn't have permission to write to Amazon S3
 bucket name amzn-s3-demo-bucket and key sample.dmp.
2023-04-17 18:21:34.189 UTC [INFO ] The task failed.
```

Solución de problemas de la integración de Amazon S3

Para obtener consejos sobre la solución de problemas, consulte el artículo de AWS re:post ¿Cómo puedo solucionar los problemas al integrar Amazon RDS para Oracle con Amazon S3?

Eliminación de la opción de integración con Amazon S3

Puede eliminar la opción de integración con Amazon S3 de una instancia de base de datos.

Para eliminar la opción de integración con Amazon S3 de una instancia de base de datos, realice una de las siguientes acciones:

- Para eliminar la opción de integración con Amazon S3 de varias instancias de base de datos, elimine la opción `S3_INTEGRATION` del grupo de opciones al que pertenecen las instancias de base de datos. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
- Para eliminar la opción de integración con Amazon S3 de una sola instancia, modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción `S3_INTEGRATION`. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle Application Express

Amazon RDS es compatible con Oracle Application Express (APEX) mediante el uso de las opciones `APEX` y `APEX-DEV`. Oracle APEX puede implementarse como un entorno de tiempo de ejecución o como un entorno de desarrollo completo para aplicaciones basadas en web. Con Oracle APEX, puede crear aplicaciones de principio a fin en el navegador web. Para obtener más información, consulte Oracle Application Express en la documentación de Oracle.

Temas

- Componentes de Oracle APEX
- Requisitos y limitaciones
- Configuración de Oracle APEX y Oracle Rest Data Services (ORDS)
- Configuración de Oracle Rest Data Services (ORDS)
- Actualización y eliminación de Oracle APEX

Componentes de Oracle APEX

Oracle APEX consta de los siguientes componentes principales:

- Un repositorio que almacena los metadatos para las aplicaciones y los componentes de Oracle APEX. El repositorio se compone de tablas, índices y otros objetos que están instalados en la instancia de base de datos de Amazon RDS.
- Un agente de escucha que administra las comunicaciones HTTP con los clientes de Oracle APEX. El oyente está en un host independiente como, por ejemplo, una instancia de Amazon EC2, un servidor en las instalaciones de su empresa o un equipo de escritorio. El agente de escucha acepta las conexiones entrantes de los navegadores web, las reenvía a la instancia de base de datos de Amazon RDS para su procesamiento y, después, envía los resultados del repositorio de vuelta a los navegadores.

  RDS para Oracle admite los siguientes tipos de oyente:

  - Para Oracle APEX versión 5.0 y posteriores, utilice Oracle REST Data Services (ORDS), versión 19.1 y posteriores. Le recomendamos utilizar la última versión compatible de Oracle APEX y ORDS. Esta documentación describe versiones anteriores solo para compatibilidad con versiones anteriores.
  - Para la versión 4.1.1 de Oracle APEX, puede utilizar Oracle APEX Listener versión 1.1.4.
  - Puede utilizar Oracle HTTP Server y agentes de escucha `mod_plsql`.

> **Note**
>
> Amazon RDS no es compatible con el servidor HTTP de base de datos XML de Oracle con la puerta de enlace PL/SQL integrada como oyente para Oracle APEX. En general, Oracle recomienda evitar el uso de la gateway PL/SQL integrada para las aplicaciones que se ejecutan en Internet.

Para obtener más información sobre estos tipos de agentes de escucha, consulte Elección de un agente de escucha web en la documentación de Oracle.

Cuando se agregan las opciones de `APEX` y `APEX-DEV` a la instancia de base de datos de RDS para Oracle, Amazon RDS instala solo el repositorio de Oracle APEX. Instale su oyente en un host independiente.

Requisitos y limitaciones

En el siguiente tema se muestran los requisitos y las limitaciones para Oracle APEX y ORDS.

Requisitos de versiones de Oracle APEX

La opción de `APEX` utiliza el almacenamiento en la clase de instancia de base de datos para la instancia de base de datos. Estas son las versiones admitidas y los requisitos de almacenamiento aproximados para Oracle APEX.

Versión de Oracle APEX	Requisitos de almacenamiento	Versiones de Oracle Database compatibles	Notas
Oracle APEX versión 24.2.v1	114 MiB	Todos	Esta versión incluye el parche 37885097: PSE BUNDLE FOR APEX 24,2 (PSES ON TOP OF 24,2.0), PATCH_VERSION 4.
Oracle APEX versión 24.1.v1	112 MiB	Todos	Esta versión incluye el parche 36695709: PSE BUNDLE FOR APEX 24.1 (PSES ON TOP OF 24.1.0), PATCH_VERSION 3. Si necesita instalar exactamente la misma versión de imágenes

Versión de Oracle APEX	Requisitos de almacenamiento	Versiones de Oracle Database compatibles	Notas
			APEX en la instancia EC2, descargue la revisión 37544819: 24.1.3 PAQUETE PSE PARA APEX 24.1 (PSES SOBRE 24.1.0).
Oracle APEX versión 23.2.v1	110 MiB	Todos	Esta versión incluye el parche 35895964: PSE BUNDLE FOR APEX 23.2 (PSES ON TOP OF 23.2.0), PATCH_VERSION 6. Si necesita instalar exactamente la misma versión de imágenes APEX en la instancia EC2, descargue la revisión 37593125: 23.2.6 PAQUETE PSE PARA APEX 23.2 (PSES SOBRE 23.2.0).
Oracle APEX versión 23.1.v1	106 MiB	Todos	Esta versión incluye el parche 35283657: PSE BUNDLE FOR APEX 23.1 (PSES ON TOP OF 23.1.0), PATCH_VERSION 2.
Oracle APEX, versión 22.2.v1	106 MiB	Todos	Esta versión incluye el parche 34628174: PSE BUNDLE FOR APEX 22,2 (PSES ON TOP OF 22,2.0), PATCH_VERSION 4.
Oracle APEX, versión 22.1.v1	124 MiB	Todos	Esta versión incluye el parche 34020981: PSE BUNDLE FOR APEX 22.1 (PSES ON TOP OF 22.1.0), PATCH_VERSION 6.
Oracle APEX, versión 21.2.v1	125 MiB	Todos	Esta versión incluye el parche 33420059: PSE BUNDLE FOR APEX 21,2 (PSES ON TOP OF 21,2.0), PATCH_VERSION 8.
Oracle APEX, versión 21.1.v1	125 MiB	Todos	Esta versión incluye la revisión 32598392: PSE BUNDLE FOR APEX 21.1, PATCH_VERSION 3.

Versión de Oracle APEX	Requisitos de almacenamiento	Versiones de Oracle Database compatibles	Notas
Oracle APEX versión 20.2.v1	148 MiB	Todas excepto Oracle Database 21c	Esta versión incluye la revisión 32006852: PSE BUNDLE FOR APEX 20.2, PATCH_VERSION 2020.11.12. Puede consultar el número de parche y la fecha ejecutando la siguiente consulta: `SELECT PATCH_VERSION, PATCH_NUMBER FROM APEX_PATCHES;`
Oracle APEX versión 20.1.v1	173 MiB	Todas excepto Oracle Database 21c	Esta versión incluye la revisión 30990551: PSE BUNDLE FOR APEX 20.1, PATCH_VERSION 2020.07.15.
Oracle APEX versión 19.2.v1	149 MiB	Todas excepto Oracle Database 21c	
Oracle APEX, versión 19.1.v1	148 MiB	Todas excepto Oracle Database 21c	

Para ver los archivos .zip de Oracle APEX descargables, consulte los archivos de versiones anteriores de Oracle APEX en el sitio web de Oracle.

Requisitos previos para Oracle APEX y ORDS

Tenga en cuenta los siguientes requisitos previos para Oracle APEX y ORDS:

- El sistema debe utilizar el entorno de ejecución de Java (JRE).
- Una instalación de cliente de Oracle debe incluir lo siguiente:

- SQL*Plus o SQL Developer para tareas de administración
- Oracle Net Services para configurar conexiones a su instancia de base de datos de RDS para Oracle

Limitaciones de Oracle APEX

No puede modificar la cuenta de usuario `APEX_version`, que administra Amazon RDS. Por lo tanto, no puede aplicar perfiles de bases de datos ni imponer reglas de contraseñas a este usuario. Oracle y AWS predefinen la configuración de perfiles y contraseñas para `APEX_version`, que se ha diseñado para cumplir con los requisitos de seguridad de Amazon RDS.

Configuración de Oracle APEX y Oracle Rest Data Services (ORDS)

En el siguiente tema se muestran los pasos necesarios para configurar Oracle APEX y ORDS

Temas

- Cómo añadir las opciones de APEX y APEX-DEV a una instancia de base de datos
- Desbloqueo de la cuenta de usuario pública en una instancia de base de datos
- Configuración de los servicios RESTful para Oracle APEX
- Preparativos para la instalación de ORDS en un host independiente
- Configuración del agente de escucha de Oracle APEX

Cómo añadir las opciones de APEX y APEX-DEV a una instancia de base de datos

Para añadir las opciones `APEX` y `APEX-DEV` a la instancia de base de datos de RDS para Oracle, haga lo siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Agregue las opciones `APEX` y `APEX-DEV` al grupo de opciones.
3. Asocie el grupo de opciones con la instancia de base de datos.

Cuando se agregan las opciones `APEX` y `APEX-DEV`, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente.

> **Note**
>
> `APEX_MAIL` está disponible cuando la opción `APEX` está instalada. El privilegio de ejecución del paquete `APEX_MAIL` se concede a `PUBLIC`por lo que no necesita la cuenta administrativa de APEX para usarlo.

Agregación de las opciones de APEX y APEX-DEV a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine, elija la edición de Oracle que desea utilizar. Las opciones de `APEX` y `APEX-DEV` se admiten en todas las ediciones.

   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada las opciones al grupo de opciones. Si desea implementar únicamente el entorno de tiempo de ejecución de Oracle APEX, añada solo la opción `APEX`. Si desea implementar el entorno de desarrollo completo, añada las opciones `APEX` y `APEX-DEV`.

   Para Versión, elija la versión de Oracle APEX que desea utilizar.

   > **Important**
   >
   > Si agrega las opciones de `APEX` y `APEX-DEV` a un grupo de opciones existente que ya se ha adjuntado a una o varias instancias de base de datos, se producirá una breve interrupción. Durante esa interrupción, se reinician automáticamente todas las instancias de base de datos.

   Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

- Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Cuando se agregan las opciones de APEX o APEX-DEV a una instancia de base de datos existente, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Desbloqueo de la cuenta de usuario pública en una instancia de base de datos

Después de instalar las opciones de APEX o APEX-DEV para la instancia de base de datos, asegúrese de hacer lo siguiente:

1. Cambie la contraseña de la cuenta APEX_PUBLIC_USER.
2. Desbloquee la cuenta.

Para ello, puede usar la utilidad de línea de comandos Oracle SQL*Plus. Conéctese a la instancia de base de datos como usuario maestro y ejecute los siguientes comandos. Reemplace new_password por una contraseña de su elección.

```
ALTER USER APEX_PUBLIC_USER IDENTIFIED BY new_password;
ALTER USER APEX_PUBLIC_USER ACCOUNT UNLOCK;
```

Configuración de los servicios RESTful para Oracle APEX

Para configurar los servicios RESTful en Oracle APEX (no es necesario para Oracle APEX 4.1.1.V1), utilice SQL*Plus para conectarse a la instancia de base de datos como usuario maestro. Una vez realizado ese paso, ejecute el procedimiento almacenado rdsadmin.rdsadmin_run_apex_rest_config. Cuando ejecute el procedimiento almacenado, proporcione contraseñas para los siguientes usuarios:

- APEX_LISTENER
- APEX_REST_PUBLIC_USER

El procedimiento almacenado ejecuta el script `apex_rest_config.sql`, que crea cuentas de base de datos nuevas para estos usuarios.

> **Note**
>
> La configuración no es necesaria para Oracle APEX versión 4.1.1.v1. No es necesario ejecutar el procedimiento almacenado únicamente para esta versión de Oracle APEX.

El comando siguiente ejecuta el procedimiento almacenado.

```
EXEC rdsadmin.rdsadmin_run_apex_rest_config('apex_listener_password',
 'apex_rest_public_user_password');
```

Preparativos para la instalación de ORDS en un host independiente

Instale ORDS en un host independiente, como una instancia de Amazon EC2, un servidor en las instalaciones de su empresa o un equipo de escritorio. En los ejemplos de esta sección, se supone que el host ejecuta Linux y tiene el nombre `myapexhost.example.com`.

Antes de poder instalar ORDS, tiene que crear un usuario de SO sin privilegios y, a continuación, descargar y descomprimir el archivo de instalación de Oracle APEX.

Para prepararse para la instalación de ORDS

1. Inicie sesión en `myapexhost.example.com` como `root`.
2. Cree un usuario de SO sin privilegios que sea el propietario de la instalación del agente de escucha. El siguiente comando crea un nuevo usuario llamado apexuser.

   ```
   useradd -d /home/apexuser apexuser
   ```

   El siguiente comando asigna una contraseña al nuevo usuario.

   ```
   passwd apexuser;
   ```

3. Inicie sesión en `myapexhost.example.com` como `apexuser` y descargue los archivos de instalación de Oracle APEX desde Oracle en su directorio `/home/apexuser`:

   - http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html

- Archivos de liberación previos de Oracle Application Express

4. Descomprima el archivo en el directorio `/home/apexuser`.

```
unzip apex_version.zip
```

Tras descomprimir el archivo, hay un directorio `apex` en el directorio `/home/apexuser`.

5. Mientras siga con la sesión iniciada en `myapexhost.example.com` como `apexuser`, descargue el archivo de Oracle REST Data Services de Oracle a su directorio:`/home/apexuser` http://www.oracle.com/technetwork/developer-tools/apex-listener/downloads/index.html.

Configuración del agente de escucha de Oracle APEX

> **Note**
>
> Oracle APEX Listener está obsoleto.

Amazon RDS para Oracle sigue siendo compatible con Oracle APEX versión 4.1.1 y Oracle APEX Listener versión 1.1.4. Se recomienda utilizar las últimas versiones compatibles de Oracle APEX y ORDS.

Instale Oracle APEX Listener en un host independiente, como, por ejemplo, una instancia Amazon EC2, un servidor en las instalaciones en su empresa o un equipo de sobremesa. Suponemos que el nombre del host es `myapexhost.example.com` y que el host ejecuta Linux.

Preparación para instalar el agente de escucha de Oracle APEX

Antes de instalar Oracle APEX Listener, debe crear un usuario de SO sin privilegios y, a continuación, descargar y descomprimir el archivo de instalación de Oracle APEX.

Para prepararse para la instalación del agente de escucha de Oracle APEX

1. Inicie sesión en `myapexhost.example.com` como `root`.
2. Cree un usuario de SO sin privilegios que sea el propietario de la instalación del agente de escucha. El siguiente comando crea un nuevo usuario llamado apexuser.

```
useradd -d /home/apexuser apexuser
```

El siguiente comando asigna una contraseña al nuevo usuario.

```
passwd apexuser;
```

3. Inicie sesión en `myapexhost.example.com` como `apexuser` y descargue los archivos de instalación de Oracle APEX desde Oracle en su directorio `/home/apexuser`:
   - http://www.oracle.com/technetwork/developer-tools/apex/downloads/index.html
   - Archivos de liberación previos de Oracle Application Express
4. Descomprima el archivo en el directorio `/home/apexuser`.

   ```
   unzip apex_<version>.zip
   ```

   Tras descomprimir el archivo, hay un directorio `apex` en el directorio `/home/apexuser`.
5. Mientras sigue con la sesión iniciada en `myapexhost.example.com` como `apexuser`, descargue el archivo de Oracle APEX Listener desde Oracle a su directorio `/home/apexuser`.

Instalación y configuración del agente de escucha de Oracle APEX

Antes de poder utilizar Oracle APEX, debe descargar el archivo `apex.war`, usar Java para instalar Oracle APEX Listener y, a continuación, iniciar el oyente.

Para instalar y configurar el agente de escucha de Oracle APEX

1. Cree un nuevo directorio basado en Oracle APEX Listener y abra el archivo del agente de escucha.

   Ejecute el siguiente código:

   ```
   mkdir /home/apexuser/apexlistener
   cd /home/apexuser/apexlistener
   unzip ../apex_listener.version.zip
   ```
2. Ejecute el siguiente código.

   ```
   java -Dapex.home=./apex -Dapex.images=/home/apexuser/apex/images -Dapex.erase -
   jar ./apex.war
   ```
3. Introduzca la siguiente información que el programa le solicita:

- Nombre de usuario del administrador del agente de escucha de APEX. El valor predeterminado es adminlistener.
- Contraseña del administrador del agente de escucha de APEX.
- Nombre de usuario del gestor del agente de escucha de APEX. El valor predeterminado es managerlistener.
- Contraseña del administrador del agente de escucha de APEX.

El programa imprime una dirección URL que se necesita para completar la configuración, tal y como se indica a continuación.

```
INFO: Please complete configuration at: http://localhost:8080/apex/
listenerConfigure
Database is not yet configured
```

4. Deje Oracle APEX Listener en ejecución para que pueda utilizar Oracle Application Express. Cuando haya completado este procedimiento de configuración, podrá ejecutar el agente de escucha en segundo plano.
5. Desde el navegador web, vaya a la dirección URL proporcionada por el programa del oyente de Oracle APEX. Aparece la ventana de administración de Oracle Application Express Listener. Introduzca la información siguiente:
   - Username (Nombre de usuario – `APEX_PUBLIC_USER`
   - Password (Contraseña): la contraseña de APEX_PUBLIC_USER. Esta contraseña es la que especificó antes cuando configuró el repositorio de Oracle APEX. Para obtener más información, consulte Desbloqueo de la cuenta de usuario pública en una instancia de base de datos.
   - Connection Type (Tipo de conexión): Basic (Básica)
   - Hostname (Nombre de host): el punto de enlace de su instancia de base de datos de Amazon RDS, como `mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com`.
   - Port (Puerto – 1521
   - SID: el nombre de la base de datos de la instancia de base de datos de Amazon RDS, como `mydb`.
6. Seleccione Apply. Aparece la ventana de administración de Oracle APEX.

7. Establezca una contraseña para el usuario `admin` de Oracle APEX. Para ello, use SQL*Plus para conectarse a la instancia de base de datos como usuario principal y, a continuación, ejecute los siguientes comandos.

   ```
   EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
   grant APEX_ADMINISTRATOR_ROLE to master;
   @/home/apexuser/apex/apxchpwd.sql
   ```

   Sustituya *`master`* por el nombre de usuario maestro. Cuando el script de `apxchpwd.sql` se lo solicite, introduzca una nueva contraseña de `admin`.

8. Vuelva a la ventana de administración de Oracle APEX en el navegador y elija Administración. A continuación, elija Application Express Internal Administration. Cuando se le soliciten las credenciales, introduzca la siguiente información:

   - User name (Nombre de usuario – `admin`
   - Password (Contraseña): la contraseña que se estableció con el script `apxchpwd.sql`

   Elija Login y a continuación defina una nueva contraseña para el usuario `admin`.

El agente de escucha ya está listo para utilizarse.

Configuración de Oracle Rest Data Services (ORDS)

En el siguiente tema se enumeran las opciones de configuración de ORDS 21 y 22:

Temas

- Instalación y configuración de ORDS 21 y versiones anteriores
- Instalación y configuración de ORDS 22 y versiones posteriores

Instalación y configuración de ORDS 21 y versiones anteriores

Ahora está listo para instalar y configurar Oracle Rest Data Services (ORDS) para su uso con Oracle APEX. Para Oracle APEX versión 5.0 y posteriores, utilice las versiones 19.1 a 21 de ORDS. Para obtener información sobre cómo instalar ORDS 22 y versiones posteriores, consulte Instalación y configuración de ORDS 22 y versiones posteriores.

Instale el agente de escucha en un host independiente como, por ejemplo, una instancia Amazon EC2, un servidor en las instalaciones de su empresa o un equipo de escritorio. Para los ejemplos de esta sección, suponemos que el nombre de su host es `myapexhost.example.com` y que su host está ejecutando Linux.

Instalación y configuración de ORDS 21 y versiones anteriores para usarse con Oracle APEX

1. Consulte Oracle REST data services y examine el archivo Readme. Asegúrese de que tiene instalada la versión de Java necesaria.
2. Cree un nuevo directorio para su instalación de ORDS.

```
mkdir /home/apexuser/ORDS
cd /home/apexuser/ORDS
```

3. Descargue el archivo `ords.`*`version.number`*`.zip` en Oracle REST data services (Servicios de datos REST de Oracle).
4. Descomprima el archivo en el directorio `/home/apexuser/ORDS`.
5. Si va a instalar ORDS en una base de datos multiusuario, agregue la siguiente línea al archivo:`/home/apexuser/ORDS/params/ords_params.properties`

```
pdb.disable.lockdown=false
```

6. Conceda al usuario principal los privilegios necesarios para instalar ORDS.

   Una vez instaladas las opciones para Oracle APEX, conceda al usuario principal los privilegios necesarios para instalar el esquema de ORDS. Para ello, conéctese a la base de datos y ejecute los siguientes comandos. Sustituya *`MASTER_USER`* por el nombre del usuario principal en mayúsculas.

   > **Important**
   >
   > Al ingresar el nombre de usuario, utilice mayúsculas, a menos que haya creado el usuario con un identificador que distingue entre mayúsculas y minúsculas. Por ejemplo, si ejecuta `CREATE USER myuser` o `CREATE USER MYUSER`, el diccionario de datos almacena `MYUSER`. Sin embargo, si utiliza comillas dobles en `CREATE USER "MyUser"`, el diccionario de datos almacena `MyUser`. Para obtener más información, consulte Concesión de privilegios SELECT o EXECUTE para objetos SYS.

```
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_OBJECTS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_ROLE_PRIVS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_COLUMNS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_CONS_COLUMNS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_CONSTRAINTS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_OBJECTS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_PROCEDURES', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_TAB_COLUMNS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_TABLES', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_VIEWS', 'MASTER_USER', 'SELECT',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('WPIUTL', 'MASTER_USER', 'EXECUTE',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_SESSION', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_UTILITY', 'MASTER_USER',
 'EXECUTE', true);
```

> **Note**
>
> Estos comandos se aplican a las versiones 19.1 y posteriores de ORDS.

7. Instale el esquema de ORDS mediante el archivo ords.war descargado.

```
java -jar ords.war install advanced
```

El programa le pedirá la siguiente información. Los valores predeterminados aparecen entre corchetes. Para obtener más información, consulte Introduction to Oracle REST Data Services en la documentación de Oracle.

- Escriba la ubicación para almacenar los datos de configuración:

  Ingrese */home/apexuser/ORDS*. Esta es la ubicación de los archivos de configuración ORDS.

- Especifique el tipo de conexión de base de datos que se va a utilizar. Escriba un número: [1] Basic [2] TNS [3] URL personalizada [1]:

  Elija el tipo de conexión deseado.

- Escriba el nombre del servidor de la base de datos [localhost]: *punto_de_enlace_de_instancia_de_base_de_datos*

  Elija el valor predeterminado o introduzca el valor correcto.

- Escriba el puerto del agente de escucha de la base de datos [1521]: *puerto_de_instancia_de_base_de_datos*

  Elija el valor predeterminado o introduzca el valor correcto.

- Escriba 1 para especificar el nombre del servicio de base de datos o elija 2 para especificar el SID de la base de datos [1]:

  Elija 2 para especificar el SID de la base de datos.

- SID de la base de datos [xe]

  Elija el valor predeterminado o introduzca el valor correcto.

- Escriba 1 si desea verificar/instalar el esquema de Oracle REST Data Services o escriba 2 para omitir este paso [1]:

  Elija 1. Este paso crea el usuario del proxy de Oracle REST Data Services denominado ORDS_PUBLIC_USER.

- Escriba la contraseña de la base de datos para ORDS_PUBLIC_USER:

  Escriba la contraseña y, a continuación, confírmela.

- Es necesario iniciar sesión con privilegios de administrador para verificar el esquema de Oracle REST Data Services.

  Introduzca el nombre del usuario administrador: *master_user*

  Introduzca la contraseña de la base de datos para *master_user*: *master_user_password*

Confirme la contraseña: *master_user_password*

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

- Introduzca el espacio de tabla predeterminado de ORDS_METADATA [SYSAUX].

  Introduzca el espacio de tabla temporal de ORDS_METADATA [TEMP].

  Introduzca el espacio de tabla predeterminado de ORDS_PUBLIC_USER [USERS].

  Introduzca el espacio de tabla temporal de ORDS_PUBLIC_USER [TEMP].
- Introduzca 1 si desea utilizar la gateway PL/SQL o 2 para omitir este paso. Si utiliza Oracle Application Express o migra desde mod_plsql, debe introducir 1 [1].

  Elija el valor predeterminado.
- Escriba el nombre de usuario de la base de datos de la gateway PL/SQL [APEX_PUBLIC_USER]

  Elija el valor predeterminado.
- Escriba la contraseña de la base de datos para APEX_PUBLIC_USER:

  Escriba la contraseña y, a continuación, confírmela.
- Escriba 1 para especificar contraseñas para los usuarios de la base de datos de los servicios RESTful de Application Express (APEX_LISTENER, APEX_REST_PUBLIC_USER) o escriba 2 para omitir este paso [1]:

  Elija 2 para APEX 4.1.1.V1; elija 1 para todas las demás versiones de APEX.
- [No es necesario para APEX 4.1.1.v1] Contraseña de la base de datos para APEX_LISTENER

  Escriba la contraseña (si es necesario) y, a continuación, confírmela.
- [No es necesario para APEX 4.1.1.v1] Contraseña de la base de datos para APEX_REST_PUBLIC_USER

  Escriba la contraseña (si es necesario) y, a continuación, confírmela.
- Escriba un número para seleccionar una característica para habilitar:

Escriba 1 para habilitar todas las características: SQL Developer Web, SQL habilitado para REST y API de base de datos.

- Escriba 1 si desea comenzar en modo autónomo o 2 para salir [1]:

  Escriba 1.

- Escriba la ubicación de recursos estáticos de APEX:

  Si descomprimió los archivos de instalación de APEX en `/home/apexuser`, escriba `/home/apexuser/apex/images`. De lo contrario, escriba *`unzip_path`*`/apex/images`, donde *`unzip_path`* es el directorio donde descomprimió el archivo.

- Escriba 1 si usa HTTP o escriba 2 si usa HTTPS [1]:

  Si escribe 1, especifique el puerto HTTP. Si escribe 2, especifique el puerto HTTPS y el nombre del host de SSL. La opción HTTPS le pide que especifique cómo proporcionará el certificado:

  - Escriba 1 para usar el certificado autofirmado.
  - Escriba 2 para proporcionar su propio certificado. Si escribe 2, especifique la ruta de acceso del certificado SSL y la ruta de acceso de la clave privada del certificado SSL.

8. Establezca una contraseña para el usuario `admin` de APEX. Para ello, use SQL*Plus para conectarse a la instancia de base de datos como usuario principal y, a continuación, ejecute los siguientes comandos.

   ```
   EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
   grant APEX_ADMINISTRATOR_ROLE to master;
   @/home/apexuser/apex/apxchpwd.sql
   ```

   Sustituya *`master`* por el nombre de usuario maestro. Cuando el script de `apxchpwd.sql` se lo solicite, introduzca una nueva contraseña de `admin`.

9. Inicie el agente de escucha ORDS. Ejecute el siguiente código.

   ```
   java -jar ords.war
   ```

   La primera vez que inicie ORDS, se le pedirá que proporcione la ubicación de los recursos estáticos de APEX. Esta carpeta de imágenes se encuentra en el directorio `/apex/images` en el directorio de instalación de APEX.

10. Vuelva a la ventana de administración de Oracle APEX en el navegador y elija Administración. A continuación, elija Application Express Internal Administration. Cuando se le soliciten las credenciales, introduzca la siguiente información:

    - User name (Nombre de usuario – `admin`
    - Password (Contraseña): la contraseña que se estableció con el script `apxchpwd.sql`

    Elija Login y a continuación defina una nueva contraseña para el usuario `admin`.

El agente de escucha ya está listo para utilizarse.

Instalación y configuración de ORDS 22 y versiones posteriores

Ahora está listo para instalar y configurar Oracle Rest Data Services (ORDS) para su uso con Oracle APEX. Para los ejemplos de esta sección, suponemos que el nombre del host independiente es `myapexhost.example.com` y que está ejecutando Linux. Las instrucciones de ORDS 22 difieren de las instrucciones de las versiones anteriores.

Instalación y configuración de ORDS 22 y versiones posteriores para usarse con Oracle APEX

1. Visite Oracle REST data services y examine el archivo Readme de la versión de ORDS que tiene pensado descargar. Asegúrese de que tiene instalada la versión de Java necesaria.
2. Cree un nuevo directorio para su instalación de ORDS.

   ```
   mkdir /home/apexuser/ORDS
   cd /home/apexuser/ORDS
   ```

3. Descargue el archivo `ords.version.number.zip` o `ords-latest.zip` de Oracle REST data services.
4. Descomprima el archivo en el directorio `/home/apexuser/ORDS`.
5. Conceda al usuario principal los privilegios necesarios para instalar ORDS.

   Una vez instalada la opción APEX, conceda al usuario principal los privilegios necesarios para instalar el esquema de ORDS. Puede hacerlo conectándose a la base de datos y ejecutando los siguientes comandos. Sustituya *MASTER_USER* por el nombre del usuario principal en mayúsculas.

> **Important**
>
> Al ingresar el nombre de usuario, utilice mayúsculas, a menos que haya creado el usuario con un identificador que distingue entre mayúsculas y minúsculas. Por ejemplo, si ejecuta `CREATE USER myuser` o `CREATE USER MYUSER`, el diccionario de datos almacena `MYUSER`. Sin embargo, si utiliza comillas dobles en `CREATE USER "MyUser"`, el diccionario de datos almacena `MyUser`. Para obtener más información, consulte Concesión de privilegios SELECT o EXECUTE para objetos SYS.

```
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_OBJECTS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_ROLE_PRIVS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_COLUMNS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_CONS_COLUMNS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_CONSTRAINTS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_OBJECTS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_PROCEDURES', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_TAB_COLUMNS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_TABLES', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('USER_VIEWS', 'MASTER_USER', 'SELECT',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('WPIUTL', 'MASTER_USER', 'EXECUTE',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_SESSION', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_UTILITY', 'MASTER_USER',
 'EXECUTE', true);

exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_LOB', 'MASTER_USER', 'EXECUTE',
 true);
```

```
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_ASSERT', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_OUTPUT', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_SCHEDULER', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('HTP', 'MASTER_USER', 'EXECUTE',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('OWA', 'MASTER_USER', 'EXECUTE',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('WPG_DOCLOAD', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_CRYPTO', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_METADATA', 'MASTER_USER',
 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_SQL', 'MASTER_USER', 'EXECUTE',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('UTL_SMTP', 'MASTER_USER', 'EXECUTE',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_NETWORK_ACL_ADMIN',
 'MASTER_USER', 'EXECUTE', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('SESSION_PRIVS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_USERS', 'MASTER_USER', 'SELECT',
 true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_NETWORK_ACL_PRIVILEGES',
 'MASTER_USER', 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_NETWORK_ACLS', 'MASTER_USER',
 'SELECT', true);
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_REGISTRY', 'MASTER_USER',
 'SELECT', true);
```

> **Note**
>
> Los comandos anteriores se aplican a las versiones 22 y posteriores de ORDS.

6. Instale el esquema de ORDS mediante el script `ords` descargado. Especifique los directorios que deben contener los archivos de configuración y los archivos de registro. Oracle Corporation recomienda no colocar estos directorios dentro del directorio que contiene el software del producto ORDS.

```
mkdir -p /home/apexuser/ords_config /home/apexuser/ords_logs

/home/apexuser/ORDS/bin/ords \
  --config /home/apexuser/ords_config \
  install --interactive --log-folder /home/apexuser/ords_logs
```

Para las instancias de base de datos que ejecutan la arquitectura de base de datos de contenedores (CDB), utilice ORDS 23.2 y versiones posteriores y pase el argumento `--pdb-skip-disable-lockdown` al instalar ORDS.

```
/home/apexuser/ORDS/bin/ords \
  --config /home/apexuser/ords_config \
  install --interactive --log-folder /home/apexuser/ords_logs --pdb-skip-disable-
lockdown
```

El programa le pedirá la siguiente información. Los valores predeterminados aparecen entre corchetes. Para obtener más información, consulte Introduction to Oracle REST Data Services en la documentación de Oracle.

- `Choose the type of installation:`

  Elija **2** para instalar los esquemas de ORDS en la base de datos y crear un grupo de conexiones de base de datos en los archivos de configuración de ORDS locales.

- `Specify the database connection type to use. Enter number for [1] Basic [2] TNS [3] Custom URL:`

  Elija el tipo de conexión deseado. En este ejemplo se supone que elige **1**.

- `Enter the name of the database server [localhost]:` ***`DB_instance_endpoint`***

  Elija el valor predeterminado o introduzca el valor correcto.

- `Enter the database listener port [1521]:` ***`DB_instance_port`***

  Elija el valor predeterminado **1521** o introduzca el valor correcto.

- `Enter the database service name [orcl]:`

  Introduzca el nombre de base de datos que utiliza la instancia de base de datos de RDS para Oracle.

- `Provide database user name with administrator privileges`

  Introduzca el nombre de usuario maestro para la instancia de base de datos de RDS para Oracle.

- `Enter the database password for [username]:`

  Introduzca la contraseña de usuario maestro para la instancia de base de datos de RDS para Oracle.

- `Enter the default tablespace for ORDS_METADATA and ORDS_PUBLIC_USER [SYSAUX]:`
- `Enter the temporary tablespace for ORDS_METADATA [TEMP]. Enter the default tablespace for ORDS_PUBLIC_USER [USERS]. Enter the temporary tablespace for ORDS_PUBLIC_USER [TEMP].`
- `Enter a number to select additional feature(s) to enable [1]:`
- `Enter a number to configure and start ORDS in standalone mode [1]:`

  Elija **2** para omitir inmediatamente el inicio de ORDS en modo independiente.

- `Enter a number to select the protocol [1] HTTP`
- `Enter the HTTP port [8080]:`
- `Enter the APEX static resources location:`

  Ingrese la ruta a los archivos de instalación de Oracle APEX (`/home/apexuser/apex/images`).

7. Establezca una contraseña para el usuario `admin` de Oracle APEX. Para ello, use SQL*Plus para conectarse a la instancia de base de datos como usuario principal y, a continuación, ejecute los siguientes comandos.

   ```
   EXEC rdsadmin.rdsadmin_util.grant_apex_admin_role;
   grant APEX_ADMINISTRATOR_ROLE to master;
   @/home/apexuser/apex/apxchpwd.sql
   ```

   Sustituya *`master`* por el nombre de usuario maestro. Cuando el script de `apxchpwd.sql` se lo solicite, introduzca una nueva contraseña de `admin`.

8. Ejecute ORDS en modo independiente mediante el script `ords` con el comando `serve`. Para las implementaciones de producción, plantéese la posibilidad de utilizar servidores de aplicaciones Java EE admitidos, como Apache Tomcat u Oracle WebLogic Server. Para obtener información,

consulte Deploying and Monitoring Oracle REST Data Services en la documentación de Oracle Database.

```
/home/apexuser/ORDS/bin/ords \
  --config /home/apexuser/ords_config serve \
  --port 8193 \
  --apex-images /home/apexuser/apex/images
```

Si ORDS se está ejecutando pero no puede acceder a la instalación de Oracle APEX, es posible que aparezca el siguiente error, sobre todo en las instancias que no son CDB.

```
The procedure named apex_admin could not be accessed, it may not be declared,
 or the user executing this request may not have been granted execute privilege
 on the procedure, or a function specified by security.requestValidationFunction
 configuration property has prevented access.
```

Para corregir este error, cambie la función de validación de solicitudes utilizada por ORDS ejecutando el script `ords` con el comando `config`. De forma predeterminada, ORDS usa el procedimiento `ords_util.authorize_plsql_gateway`, que solo se admite en las instancias de CDB. En el caso de las instancias que no son de CDB, puede cambiar este procedimiento por el paquete `wwv_flow_epg_include_modules.authorize`. Consulte la documentación de Oracle Database y Oracle Support para conocer las mejores prácticas a la hora de configurar la función de validación de solicitudes adecuada para su caso de uso.

9. Vuelva a la ventana de administración de Oracle APEX en el navegador y elija Administración. A continuación, elija Application Express Internal Administration. Cuando se le soliciten las credenciales, introduzca la siguiente información:

   - User name (Nombre de usuario – `admin`
   - Password (Contraseña): la contraseña que se estableció con el script `apxchpwd.sql`

   Elija Login y a continuación defina una nueva contraseña para el usuario `admin`.

El agente de escucha ya está listo para utilizarse.

Actualización y eliminación de Oracle APEX

Para actualizar o eliminar Oracle APEX, siga las instrucciones de este tema:

Temas

- Actualización de la versión de Oracle APEX
- Eliminación de las opciones de APEX y APEX-DEV

Actualización de la versión de Oracle APEX

> **Important**
>
> Realice una copia de seguridad de la instancia de base de datos antes de actualizar Oracle APEX. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS y Prueba de una actualización de base de datos de Oracle.

Para actualizar Oracle APEX con la instancia de base de datos, realice lo siguiente:

- Cree un nuevo grupo de opciones para la versión actualizada de la instancia de base de datos.
- Agregue las versiones actualizadas de `APEX` y `APEX-DEV` al nuevo grupo de opciones. Asegúrese de incluir todas las opciones que utiliza la instancia de base de datos. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.
- Al actualizar la instancia de base de datos, especifique el nuevo grupo de opciones para la instancia de base de datos actualizada.

Después de actualizar la versión de Oracle APEX, el esquema de Oracle APEX de la versión anterior puede seguir en la base de datos. Si ya no lo necesita, puede eliminar el antiguo esquema de Oracle APEX de la base de datos después de actualizar la versión.

Si actualiza la versión de Oracle APEX, pero los servicios RESTful no se habían configurado en la versión anterior de Oracle APEX, le recomendamos que configure los servicios RESTful. Para obtener más información, consulte Configuración de los servicios RESTful para Oracle APEX.

En algunos casos, cuando piensa realizar una actualización a la versión principal de la instancia de base de datos, puede que detecte que está usando una versión de OracleAPEX que no es compatible con la versión de base de datos de destino. En esos casos, puede actualizar la versión de Oracle APEX antes de actualizar la instancia de base de datos. Si actualiza Oracle APEX primero, puede reducirse el tiempo necesario para actualizar la instancia de base de datos.

> **Note**
>
> Tras actualizar Oracle APEX, instale y configure un oyente para usarlo con la versión actualizada. Para obtener instrucciones, consulte Configuración del agente de escucha de Oracle APEX.

Eliminación de las opciones de APEX y APEX-DEV

Puede eliminar las opciones de `APEX` y `APEX-DEV` de una instancia de base de datos. Para eliminar estas opciones de la instancia de base de datos, realice una de las siguientes operaciones:

- Para eliminar las opciones de `APEX` y `APEX-DEV` de varias instancias de bases de datos, elimine las opciones del grupo de opciones al que pertenecen. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Cuando elimine las opciones de un grupo de opciones que esté asociado a varias instancias de base de datos, se producirá una breve interrupción mientras se reinician las instancias de base de datos.

  Para obtener más información, consulte Quitar una opción de un grupo de opciones.
- Para eliminar las opciones de `APEX` y `APEX-DEV` de una sola instancia de base de datos, modifique la instancia de base de datos y especifique otro grupo de opciones diferente que no incluya estas opciones. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Cuando se eliminan las opciones, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente.

  Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Al eliminar las opciones de `APEX` y `APEX-DEV` de una instancia de base de datos, el esquema de APEX se elimina de la base de datos.

Integración de Amazon EFS

Amazon Elastic File System (Amazon EFS) proporciona un almacenamiento de archivos totalmente elástico y sin servidor para que pueda compartir datos de archivos sin aprovisionar ni administrar la capacidad de almacenamiento ni el rendimiento. Con Amazon EFS, puede crear un sistema de archivos y, a continuación, montarlo en su VPC mediante el protocolo de las versiones 4.0 y 4.1 (NFSv4) de NFS. A continuación, puede utilizar el sistema de archivos EFS como cualquier otro sistema de archivos compatible con POSIX. Para obtener información general, consulte la sección sobre ¿qué es Amazon Elastic File System? y la publicación del blog de AWS sobre integrar Amazon RDS para Oracle con Amazon EFS.

Temas

- Descripción general de la integración de Amazon EFS
- Configuración de permisos de red para la integración de RDS para Oracle con Amazon EFS
- Configuración de permisos de IAM para la integración de RDS para Oracle con Amazon EFS
- Adición de la opción EFS_INTEGRATION
- Configuración de permisos del sistema de archivos Amazon EFS
- Transferencia de archivos entre RDS para Oracle y un sistema de archivos Amazon EFS
- Eliminación de la opción EFS_INTEGRATION
- Solución de problemas de la integración de Amazon EFS

Descripción general de la integración de Amazon EFS

Amazon EFS le permite transferir archivos entre su instancia de base de datos de RDS para Oracle y un archivo de sistemas EFS. Por ejemplo, puede usar EFS para admitir los siguientes casos de uso:

- Compartir un sistema de archivos entre aplicaciones y varios servidores de bases de datos.
- Crear un directorio compartido para los archivos relacionados con la migración, incluidos los archivos de datos transportables del espacio de tablas. Para obtener más información, consulte Migración mediante espacios de tabla transportables de Oracle.
- Almacenar y compartir archivos de registro redo archivados sin asignar espacio de almacenamiento adicional en el servidor.
- Utilice las utilidades de Oracle Database, por ejemplo, `UTL_FILE`, para leer y escribir archivos.

Ventajas de la integración con Amazon EFS

Al elegir un sistema de archivos EFS en lugar de soluciones de transferencia de datos alternativas, obtiene las siguientes ventajas:

- Puede transferir archivos de Oracle Data Pump entre Amazon EFS y su instancia de base de datos de RDS para Oracle. No necesita copiar estos archivos localmente porque Data Pump los importa directamente desde el sistema de archivos EFS. Para obtener más información, consulte Importación de datos a Oracle en Amazon RDS.
- La migración de datos es más rápida que usar un enlace a una base de datos.
- Evita asignar espacio de almacenamiento en su instancia de base de datos de RDS para Oracle para retener los archivos.
- Un sistema de archivos EFS puede escalar automáticamente el almacenamiento sin necesidad de aprovisionarlo.
- La integración de Amazon EFS no tiene tarifas ni costos de configuración mínimos. Solo paga por lo que utiliza.
- La integración de Amazon EFS admite dos formas de cifrado: cifrado de datos en tránsito y cifrado en reposo. El cifrado de datos en tránsito se habilita de forma predeterminada mediante TLS versión 1.2. Puede habilitar el cifrado de datos en reposo al crear un sistema de archivos de Amazon EFS. Para obtener más información, consulte Encrypting data at rest (Cifrado de datos en reposo) en la Guía del usuario de Amazon Elastic File System.

Requisitos para la integración de Amazon EFS

Asegúrese de cumplir los siguientes requisitos:

- La base de datos debe ejecutar la versión 19.0.0.0.ru-2022-07.rur-2022-07.r1 o una versión posterior.
- La instancia de base de datos y el sistema de archivos EFS deben estar en la misma Región de AWS, la misma VPC y la misma Cuenta de AWS. RDS para Oracle no admite el acceso entre cuentas y entre regiones para EFS.
- En la VPC deben estar habilitadas las opciones Resolución de DNS y Nombres de host de DNS. Para obtener más información, consulte DNS attributes in your VPC (Atributos de DNS en su VPC) en la Guía del usuario de Amazon Virtual Private Cloud.
- El sistema de archivos EFS debe utilizar la clase de almacenamiento Estándar o Estándar - Acceso poco frecuente.

- Si utiliza un nombre de DNS en el comando `mount`, asegúrese de que la VPC esté configurada para utilizar el servidor DNS proporcionado por Amazon. No se admiten servidores DNS personalizados.
- Debe utilizar soluciones que no son de RDS para hacer copias de seguridad del sistema de archivos EFS. RDS para Oracle no admite copias de seguridad automatizadas ni instantáneas manuales de bases de datos de un sistema de archivos EFS. Para obtener más información, consulte Backing up your Amazon EFS file systems (Copias de seguridad de los sistemas de archivos Amazon EFS).

Configuración de permisos de red para la integración de RDS para Oracle con Amazon EFS

Para que RDS para Oracle se integre con Amazon EFS, asegúrese de que la instancia de base de datos tenga acceso de red a un sistema de archivos EFS. Para obtener más información, consulte Control del acceso a la red a los sistemas de archivos Amazon EFS para clientes NFS en la Guía del usuario de Amazon Elastic File System.

Temas

- Control del acceso a la red con grupos de seguridad
- Control del acceso a la red con políticas de sistema de archivos

Control del acceso a la red con grupos de seguridad

Para controlar el acceso a la instancia de base de datos de los sistemas de archivos EFS puede usar mecanismos de seguridad de la capa de red, como los grupos de seguridad de VPC. Para permitir el acceso a un sistema de archivos EFS para la instancia de base de datos, asegúrese de que el sistema de archivos EFS cumpla los siguientes requisitos:

- Debe existir un destino de montaje EFS en cada zona de disponibilidad que utilice una instancia de base de datos de RDS para Oracle.

  Un destino de montaje de EFS proporciona una dirección IP para un punto de conexión de NFSv4 en el que puede montar un sistema de archivos de EFS. Debe montar el sistema de archivos con su nombre de DNS, que se resolverá en la dirección IP del destino de montaje de EFS en la misma zona de disponibilidad que su instancia EC2.

Puede configurar instancias de base de datos en diferentes AZ para que utilicen el mismo sistema de archivos EFS. Para multi-AZ, necesita un punto de montaje para cada AZ de su implementación. Puede que tenga que trasladar una instancia de base de datos a una AZ diferente. Por estos motivos, recomendamos que cree un punto de montaje EFS en cada AZ de su VPC. De forma predeterminada, al crear un nuevo sistema de archivos EFS mediante la consola, RDS crea destinos de montaje para todas las AZ.

- Se debe adjuntar un grupo de seguridad al destino de montaje.
- El grupo de seguridad tiene una regla de entrada que permite la subred de red o el grupo de seguridad de la instancia de base de datos de RDS para Oracle en TCP/2049 (tipo NFS).

Para obtener más información, consulte Creación de sistemas de archivos de Amazon EFS y Creación y administración de objetivos de montaje y grupos de seguridad en la Guía del usuario de Amazon Elastic File System.

Control del acceso a la red con políticas de sistema de archivos

La integración de Amazon EFS con RDS para Oracle funciona con la política del sistema de archivos EFS predeterminada (vacía). La política predeterminada no usa IAM para autenticarse. En su lugar, otorga acceso total a cualquier cliente anónimo que pueda conectarse al sistema de archivos mediante un destino de montaje. La política predeterminada se aplica siempre que no se aplique una política de sistema de archivos configurada por el usuario, incluso al crear el sistema de archivos. Para obtener más información, consulte Política del sistema de archivos EFS por defecto en la Guía del usuario de Amazon Elastic File System.

Para reforzar el acceso a su sistema de archivos EFS para todos los clientes, incluido RDS para Oracle, puede configurar los permisos de IAM. En este enfoque, debe crear una política de sistema de archivos. Para obtener más información, consulte Creación de políticas de sistemas de archivos en la Guía del usuario de Amazon Elastic File System.

Configuración de permisos de IAM para la integración de RDS para Oracle con Amazon EFS

De forma predeterminada, la característica de integración de Amazon EFS no utiliza un rol de IAM: la configuración de la opción `USE_IAM_ROLE` es `FALSE`. Para integrar RDS para Oracle con Amazon EFS y un rol de IAM, su instancia de base de datos debe tener permisos de IAM para acceder a un sistema de archivos de Amazon EFS.

Temas

- Paso 1: crear un rol de IAM para la instancia de base de datos y asociarle la política
- Paso 2: crear una política de sistema de archivos para su sistema de archivos Amazon EFS
- Paso 3: asociar el rol de IAM a la instancia de base de datos de RDS para Oracle

Paso 1: crear un rol de IAM para la instancia de base de datos y asociarle la política

En este paso, creará un rol para su instancia de base de datos de RDS para Oracle para permitir que Amazon RDS acceda a su sistema de archivos EFS.

Consola

Para crear un rol de IAM que permita a Amazon RDS acceder a un sistema de archivos EFS

1. Abra la consola de administración de IAM.
2. Seleccione Roles en el panel de navegación.
3. Elija Create role (Crear rol).
4. Para obtener el servicio de AWS, elija RDS.
5. En Select your use case (Seleccionar su caso de uso), elija RDS: Add Role to Database (RDS: Añadir rol a base de datos).
6. Elija Siguiente.
7. No añada ninguna política de permisos. Elija Siguiente.
8. En Role name (Nombre de rol), escriba un nombre para el rol de IAM, por ejemplo, `rds-efs-integration-role`. También puede añadir una descripción opcional en Description (Descripción).
9. Seleccione Crear rol.

AWS CLI

Para limitar los permisos del servicio a un recurso específico, le recomendamos que utilice las claves de contexto de condición globales `aws:SourceArn` y `aws:SourceAccount` en las relaciones de confianza basadas en recursos. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

Puede utilizar claves de contexto de condición globales y hacer que el valor de `aws:SourceArn` contenga el ID de cuenta. En estos casos, el valor de `aws:SourceAccount` y la cuenta del valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilizan en la misma instrucción.

- Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
- Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En la relación de confianza, asegúrese de usar la clave de contexto de la condición global `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo de los recursos que acceden al rol.

El siguiente comando AWS CLI crea el rol nombrado *`rds-efs-integration-role`* para este propósito.

Example

Para Linux, macOS o Unix:

```
aws iam create-role \
   --role-name rds-efs-integration-role \
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                 "aws:SourceAccount": my_account_ID,
                 "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
             }
         }
       }
     ]
   }'
```

Para Windows:

```
aws iam create-role ^
   --role-name rds-efs-integration-role ^
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                 "aws:SourceAccount": my_account_ID,
                 "aws:SourceArn": "arn:aws:rds:Region:my_account_ID:db:dbname"
             }
         }
       }
     ]
   }'
```

Para obtener más información, vea Crear un rol para delegar permisos a un usuario de IAM en Guía del usuario de IAM.

Paso 2: crear una política de sistema de archivos para su sistema de archivos Amazon EFS

En este paso, creará una política de sistema de archivos para su sistema de archivos EFS.

Para crear o editar una política del sistema de archivos EFS

1. Abra la consola de administración de EFS.
2. Elija File Systems (Sistemas de archivos).
3. En la página File systems (Sistemas de archivos) elija el sistema de archivos que quiere editar o para el que desea crear una política de sistema de archivos. Aparece la página de detalles de ese sistema de archivos.
4. Seleccione la pestaña File system policy (Política del sistema de archivos).

   Si la política está vacía, significa que se está utilizando la política del sistema de archivos EFS predeterminada. Para obtener más información, consulte Política del sistema de archivos EFS por defecto en la Guía del usuario de Amazon Elastic File System.

5. Seleccione Editar. Aparece la página File system policy (Política del sistema de archivos).
6. En Policy editor (Editor de políticas), introduzca una política como la siguiente y, a continuación, seleccione Save (Guardar).

   JSON

```
{
    "Version": "2012-10-17",
    "Id": "ExamplePolicy01",
    "Statement": [
        {
            "Sid": "ExampleStatement01",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/rds-efs-integration-
role"
            },
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite",
                "elasticfilesystem:ClientRootAccess"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-
east-1:123456789012:file-system/fs-1234567890abcdef0"
        }
    ]
}
```

Paso 3: asociar el rol de IAM a la instancia de base de datos de RDS para Oracle

En este paso, asociará el rol de IAM a su instancia de base de datos. Tenga en cuenta los siguientes requisitos:

- Debe tener acceso a un rol de IAM con la política de permisos de Amazon EFS requerida adjunta.
- Solo puede asociar un rol de IAM a su instancia de base de datos de RDS para Oracle cada vez.
- El estado de la instancia debe ser Available (Disponible).

Para obtener más información, consulte Identity and access management for Amazon EFS (Administración de identidades y accesos para Amazon EFS) en la Guía del usuario de Amazon Elastic File System.

Consola

Para asociar su rol de IAM a su instancia de base de datos de RDS para Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione Bases de datos.
3. Si la instancia de base de datos no está disponible, elija Actions (Acciones) y, a continuación, Start (Inicio). Cuando el estado de la instancia muestre Started (Iniciada), vaya al paso siguiente.
4. Seleccione el nombre de la instancia de base de datos Oracle para mostrar sus detalles.
5. En la pestaña Connectivity & Security (Conectividad y seguridad), desplácese hacia abajo hasta la sección Manage IAM roles (Administrar roles de IAM) de la parte inferior de la página.
6. Elija el rol que se va a añadir en la sección Add IAM roles to this instance (Agregar roles de IAM a esta instancia).
7. En Feature (Característica), elija EFS_INTEGRATION.
8. Seleccione Add role (Añadir rol).

AWS CLI

El siguiente comando de la AWS CLI añade el rol a una instancia de base de datos de Oracle denominada *mydbinstance*.

Example

Para Linux, macOS o Unix:

```
aws rds add-role-to-db-instance \
   --db-instance-identifier mydbinstance \
   --feature-name EFS_INTEGRATION \
   --role-arn your-role-arn
```

Para Windows:

```
aws rds add-role-to-db-instance ^
```

```
    --db-instance-identifier mydbinstance ^
    --feature-name EFS_INTEGRATION ^
    --role-arn your-role-arn
```

Sustituya *your-role-arn* por el ARN del rol anotado en el paso anterior. `EFS_INTEGRATION` debe especificarse para la opción `--feature-name`.

Adición de la opción EFS_INTEGRATION

Para integrar Amazon RDS para Oracle con Amazon EFS, su instancia de base de datos debe estar asociada a un grupo de opciones que incluya la opción `EFS_INTEGRATION`.

Varias instancias de base de datos de Oracle que pertenecen al mismo grupo de opciones comparten el mismo sistema de archivos EFS. Las distintas instancias de base de datos pueden acceder a los mismos datos, pero el acceso se puede dividir mediante diferentes directorios de Oracle. Para obtener más información, consulte Transferencia de archivos entre RDS para Oracle y un sistema de archivos Amazon EFS.

Consola

Para configurar un grupo de opciones para la integración con Amazon EFS

1. Cree un nuevo grupo de opciones o identifique uno ya existente al que pueda añadir la opción `EFS_INTEGRATION`.

   Para obtener información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.
2. Agregue la opción `EFS_INTEGRATION` al grupo de opciones. Debe especificar el ID del sistema de archivos `EFS_ID` y configurar el indicador `USE_IAM_ROLE`.

   Para obtener más información, consulte Agregar una opción a un grupo de opciones.
3. Asocie el grupo de opciones a su instancia de base de datos de cualquiera de las siguientes maneras:

   - Cree una nueva instancia de base de datos de Oracle y asóciele el grupo de opciones. Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Modifique la instancia de base de datos de Oracle para asociarle el grupo de opciones. Para obtener información acerca de cómo modificar una instancia de base de datos de Oracle, consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

Para configurar un grupo de opciones para la integración EFS

1. Cree un nuevo grupo de opciones o identifique uno ya existente al que pueda añadir la opción `EFS_INTEGRATION`.

   Para obtener información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.

2. Añada la opción `EFS_INTEGRATION` al grupo de opciones.

   Por ejemplo, el siguiente comando de la AWS CLI añade la opción `EFS_INTEGRATION` a un grupo de opciones denominado **`myoptiongroup`**.

   Example

   Para Linux, macOS o:Unix

   ```
   aws rds add-option-to-option-group \
      --option-group-name myoptiongroup \
      --options "OptionName=EFS_INTEGRATION,OptionSettings=\
      [{Name=EFS_ID,Value=fs-1234567890abcdef0},{Name=USE_IAM_ROLE,Value=TRUE}]"
   ```

   En:Windows

   ```
   aws rds add-option-to-option-group ^
      --option-group-name myoptiongroup ^
      --options "OptionName=EFS_INTEGRATION,OptionSettings=^
      [{Name=EFS_ID,Value=fs-1234567890abcdef0},{Name=USE_IAM_ROLE,Value=TRUE}]"
   ```

3. Asocie el grupo de opciones a su instancia de base de datos de cualquiera de las siguientes maneras:

   - Cree una nueva instancia de base de datos de Oracle y asóciele el grupo de opciones. Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Modifique la instancia de base de datos de Oracle para asociarle el grupo de opciones. Para obtener información acerca de cómo modificar una instancia de base de datos de Oracle, consulte Modificación de una instancia de base de datos de Amazon RDS.

Configuración de permisos del sistema de archivos Amazon EFS

De forma predeterminada, solo el usuario raíz (UID `0`) dispone de permisos de lectura, escritura y ejecución para un sistema de archivos EFS creado recientemente. Para que otros usuarios modifiquen el sistema de archivos, el usuario raíz debe concederles acceso de forma explícita. El usuario de la instancia de base de datos de RDS para Oracle tiene la categoría `others`. Para obtener más información, consulte Trabajar con usuarios, grupos y permisos en el nivel del sistema de archivos de red (NFS) en la Guía del usuario de Amazon Elastic File System.

Para permitir que su instancia de base de datos de RDS para Oracle pueda leer y escribir archivos en un sistema de archivos EFS, haga lo siguiente:

- Monte un sistema de archivos EFS localmente en su instancia de Amazon EC2 en las instalaciones.
- Configure permisos detallados.

Por ejemplo, para conceder a `other` usuarios permisos para escribir en la raíz del sistema de archivos EFS, ejecute `chmod 777` en este directorio. Para obtener más información, consulte Ejemplos de casos de uso y permisos del sistema de archivos de Amazon EFS en la Guía del usuario de Amazon Elastic File System.

Transferencia de archivos entre RDS para Oracle y un sistema de archivos Amazon EFS

Para transferir archivos entre una instancia de RDS para Oracle y un sistema de archivos Amazon EFS, cree al menos un directorio de Oracle y configure los permisos del sistema de archivos EFS para controlar el acceso a la instancia de base de datos.

Temas

- Creación de un directorio de Oracle
- Transferencia de datos hacia y desde un sistema de archivos EFS: ejemplos

Creación de un directorio de Oracle

Utilice el procedimiento `rdsadmin.rdsadmin_util.create_directory_efs` para crear un directorio de Oracle. El procedimiento tiene los siguientes parámetros.

Nombre del parámetro	Tipo de datos	Valor predeterminado	Obligatorio	Descripción
`p_directory_name`	VARCHAR	–	Sí	Nombre del directorio de Oracle.
`p_path_on_efs`	VARCHAR	–	Sí	Ruta al sistema de archivos EFS. El prefijo del nombre de la ruta usa el patrón `/rdsefs-`*`fsid`*`/`, donde *`fsid`* es un marcador de posición para el ID del sistema de archivos EFS. Por ejemplo, si su sistema de archivos EFS se denomina `fs-1234567890abcdef0` y usted crea un subdirectorio en ese sistema de archivos denominado `mydir`, puede especificar el siguiente valor: `/rdsefs-fs-1234567890abcdef0/mydir`

Suponga que crea un subdirectorio denominado `/datapump1` en el sistema de archivos EFS `fs-1234567890abcdef0`. El siguiente ejemplo crea un directorio de Oracle `DATA_PUMP_DIR_EFS` que apunta al directorio `/datapump1` del sistema de archivos EFS. El valor de la ruta del sistema de archivos para el parámetro `p_path_on_efs` lleva el prefijo de cadena`/rdsefs-`.

```
BEGIN
  rdsadmin.rdsadmin_util.create_directory_efs(
    p_directory_name => 'DATA_PUMP_DIR_EFS',
    p_path_on_efs    => '/rdsefs-fs-1234567890abcdef0/datapump1');
END;
/
```

Transferencia de datos hacia y desde un sistema de archivos EFS: ejemplos

El siguiente ejemplo utiliza Oracle Data Pump para exportar la tabla denominada `MY_TABLE` a un archivo `datapump.dmp`. Este archivo reside en un sistema de archivos EFS.

```
DECLARE
```

```
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'EXPORT', job_mode => 'TABLE',
 job_name=>null);
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'datapump.dmp',
    directory => 'DATA_PUMP_DIR_EFS',
    filetype  => dbms_datapump.ku$_file_type_dump_file);
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'datapump-exp.log',
    directory => 'DATA_PUMP_DIR_EFS',
    filetype  => dbms_datapump.ku$_file_type_log_file);
  DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'NAME_EXPR','IN (''MY_TABLE'')');
  DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

El siguiente ejemplo utiliza Oracle Data Pump para importar la tabla denominada `MY_TABLE` desde el archivo `datapump.dmp`. Este archivo reside en un sistema de archivos EFS.

```
DECLARE
  v_hdnl NUMBER;
BEGIN
  v_hdnl := DBMS_DATAPUMP.OPEN(
    operation => 'IMPORT',
    job_mode  => 'TABLE',
    job_name  => null);
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'datapump.dmp',
    directory => 'DATA_PUMP_DIR_EFS',
    filetype  => dbms_datapump.ku$_file_type_dump_file );
  DBMS_DATAPUMP.ADD_FILE(
    handle    => v_hdnl,
    filename  => 'datapump-imp.log',
    directory => 'DATA_PUMP_DIR_EFS',
    filetype  => dbms_datapump.ku$_file_type_log_file);
  DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'NAME_EXPR','IN (''MY_TABLE'')');
  DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Para obtener más información, consulte Importación de datos a Oracle en Amazon RDS.

Eliminación de la opción EFS_INTEGRATION

Los pasos para eliminar la opción `EFS_INTEGRATION` dependen de si se va a eliminar la opción de varias instancias de base de datos o de una sola instancia.

Número de instancias de base de datos	Acción	Información relacionada
Múltiple	Elimine la opción `EFS_INTEGRATION` del grupo de opciones al que pertenecen las instancias de base de datos. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones.	Quitar una opción de un grupo de opciones
Única	Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción `EFS_INTEGRATION` . Puede especificar el grupo de opciones predeterm inado (vacío) u otro grupo de opciones personalizado.	Modificación de una instancia de base de datos de Amazon RDS

Tras eliminar la opción `EFS_INTEGRATION`, también puede eliminar el sistema de archivos EFS que estaba conectado a las instancias de base de datos.

Solución de problemas de la integración de Amazon EFS

Su instancia de base de datos de RDS para Oracle supervisa la conectividad a un sistema de archivos Amazon EFS. Cuando la supervisión detecta un problema, puede intentar corregirlo y publicar un evento en la consola de RDS. Para obtener más información consulte Consulta de eventos de Amazon RDS.

Utilice la información de esta sección como ayuda para diagnosticar y solucionar problemas comunes cuando trabaje con la integración de Amazon EFS.

Notification	Descripción	Acción
`The EFS for RDS Oracle instance` *`instance_name`* `isn't available on the primary host. NFS port 2049 of your EFS isn't reachable.`	La instancia de base de datos no se puede comunicar con el sistema de archivos EFS.	Asegúrese de lo siguiente: • El sistema de archivos EFS debe existir. • El grupo de seguridad vinculado al destino de montaje debe tener una regla de entrada que permita la subred de red o el grupo de seguridad de la instancia de base de datos de RDS para Oracle en TCP/2049 (tipo NFS).
`The EFS isn't reachable.`	Se ha producido un error al instalar la opción `EFS_INTEGRATION` .	Asegúrese de lo siguiente: • El sistema de archivos EFS debe existir. • El grupo de seguridad vinculado al destino de montaje debe tener una regla de entrada que permita la subred de red o el grupo de seguridad de la instancia de base de datos de RDS para Oracle en TCP/2049 (tipo NFS). • El atributo `enableDnsSupport` debe estar activado en su VPC. • Está utilizando el servidor DNS proporcionado por Amazon en la VPC. La integración de Amazon EFS

Notification	Descripción	Acción
		no funciona con un DNS de DHCP personalizado.
`The associated role with your DB instance wasn't found.`	Se ha producido un error al instalar la opción `EFS_INTEGRATION` .	Asegúrese de haber asociado su rol de IAM a su instancia de base de datos de RDS para Oracle.
`The associated role with your DB instance wasn't found.`	Se ha producido un error al instalar la opción `EFS_INTEGRATION` . RDS para Oracle se restauró a partir de una instantánea de base de datos con la opción `USE_IAM_ROLE` configurada en `TRUE`.	Asegúrese de haber asociado su rol de IAM a su instancia de base de datos de RDS para Oracle.
`The associated role with your DB instance wasn't found.`	Se ha producido un error al instalar la opción `EFS_INTEGRATION` . RDS para Oracle se creó a partir de una plantilla de CloudFormation integral con la opción `USE_IAM_ROLE` configurada en `TRUE`.	Como solución alternativa, realice los siguientes pasos: 1. Cree una instancia de base de datos con el rol de IAM y el grupo de opciones predeterminado. 2. En una actualización posterior de la pila, añada el grupo de opciones personalizado con la opción `EFS_INTEGRATION` .
`PLS-00302: component 'CREATE_DIRECTORY_EFS' must be declared`	Este error puede producirse cuando utilice una versión de RDS para Oracle que no admite Amazon EFS.	Asegúrese de utilizar la instancia de base de datos de RDS para Oracle versión 19.0.0.0.ru-2022-07.rur-2022-07.r1 o posterior.

Notification	Descripción	Acción
`Read access of your EFS is denied. Check your file system policy.`	La instancia de base de datos no puede leer el sistema de archivos EFS.	Asegúrese de que su sistema de archivos EFS permita el acceso de lectura a través del rol de IAM o en el nivel del sistema de archivos EFS.
N/A	La instancia de base de datos no puede escribir el sistema de archivos EFS.	Siga estos pasos: 1. Asegúrese de que el sistema de archivos EFS esté montado en una instancia de Amazon EC2. 2. Otorgue al grupo `others` acceso de escritura a su usuario de RDS. La técnica más sencilla consiste en ejecutar el comando `chmod 777` en el directorio superior del sistema de archivos EFS.

Máquina virtual Oracle Java

Amazon RDS admite Oracle Java Virtual Machine (JVM) mediante el uso de la opción `JVM`. Mediante Oracle Java se suministran un esquema SQL y funciones que facilitan el uso de las características de Oracle Java en una base de datos Oracle. Para obtener más información, consulte Introduction to Java in Oracle Database en la documentación de Oracle. Puede utilizar Oracle JVM con todas las versiones de Oracle Database 21c (21.0.0) y Oracle Database 19c (19.0.0).

Consideraciones para Oracle JVM

La implementación de Java en Amazon RDS dispone de un conjunto limitado de permisos. Se concede al usuario maestro el rol `RDS_JAVA_ADMIN`, que proporciona un subconjunto de privilegios gracias al rol `JAVA_ADMIN`. Para enumerar los privilegios concedidos al rol `RDS_JAVA_ADMIN`, ejecute la siguiente consulta en su instancia de base de datos:

```
SELECT * FROM dba_java_policy
   WHERE grantee IN ('RDS_JAVA_ADMIN', 'PUBLIC')
   AND enabled = 'ENABLED'
   ORDER BY type_name, name, grantee;
```

Requisitos previos para Oracle JVM

A continuación se indican los requisitos previos para utilizar Oracle Java:

- Su instancia de base de datos debe ser de una clase suficientemente grande. Oracle Java no es compatible con la clase de instancia de base de datos db.t3.small. Para obtener más información, consulte Clases de instancia de base de datos de .
- Su instancia de base de datos debe tener Auto Minor Version Upgrade habilitada. Esta opción permite que la instancia de base de datos reciba automáticamente las actualizaciones de la versión secundaria del motor de base de datos cuando estén disponibles. Amazon RDS utiliza esta opción para actualizar su instancia de base de datos a la PSU (Patch Set Update) de Oracle más reciente o actualización de la versión (RU). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Prácticas recomendadas para Oracle JVM

A continuación, se indican las prácticas recomendadas para utilizar Oracle Java:

- Para que la seguridad sea máxima, use la opción `JVM` con Capa de conexión segura (SSL). Para obtener más información, consulte Capa de conexión segura de Oracle.
- Configure su instancia de base de datos para restringir el acceso a la red. Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC y Uso de una instancia de base de datos en una VPC.
- Actualice la configuración de los puntos de enlace HTTPS para admitir TLSv1.2 si cumple las siguientes condiciones:
  - Utilice la máquina virtual de Oracle Java (JVM) para conectar un punto de enlace HTTPS a través de los protocolos TLSv1 o TLSv1.1.
  - El punto de enlace no admite el protocolo TLSv1.2.
  - No ha aplicado la actualización de la versión de abril de 2021 a Oracle Database.

  Al actualizar la configuración del punto de enlace, se asegura de que la conectividad de la JVM con el punto de enlace HTTPS siga en funcionamiento. Para obtener más información sobre los cambios de TLS en Oracle JRE y JDK, consulte Plan de desarrollo criptográfico de Oracle JRE y JDK.

Adición de la opción Oracle JVM

A continuación se muestra el proceso general para añadir la opción `JVM` a una instancia de base de datos:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Se produce una breve interrupción mientras se añade la opción `JVM`. Después de añadir la opción , no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, Oracle Java estará disponible.

> **Note**
>
> Durante esta interrupción, las funciones de verificación de contraseña se deshabilitan brevemente. También puede esperar ver eventos relacionados con las funciones de verificación de contraseña durante la interrupción. Las funciones de verificación de

contraseña se vuelven a habilitar antes de que la instancia de base de datos de Oracle esté disponible.

Para añadir la opción JVM a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   - Para Engine (Motor), elija el motor de base de datos utilizado por la instancia de base de datos (oracle-ee, oracle-se, oracle-se1 o bien oracle-se2).
   - En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.
2. Añada la opción JVM al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
4. Concesión de permisos necesarios a los usuarios.

   El usuario maestro de Amazon RDS tiene los permisos para usar la opción `JVM` de forma predeterminada. Si otros usuarios necesitan estos permisos, conéctese a la instancia de base de datos como usuario maestro en un cliente SQL y conceda los permisos a los usuarios.

   En el siguiente ejemplo se conceden permisos para usar la opción `JVM` al usuario `test_proc`.

```
create user test_proc identified by password;
```

```
CALL dbms_java.grant_permission('TEST_PROC',
 'oracle.aurora.security.JServerPermission', 'LoadClassInPackage.*', '');
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Una vez que se conceden los permisos al usuario, la siguiente consulta debería devolver el resultado.

```
select * from dba_java_policy where grantee='TEST_PROC';
```

> **Note**
>
> El nombre de usuario de Oracle distingue entre mayúsculas y minúsculas; normalmente todos los caracteres están en mayúsculas.

Eliminación de la opción Oracle JVM

Puede quitar la opción `JVM` de una instancia de base de datos. Se produce una breve interrupción mientras se quita la opción. Después de quitar la opción `JVM`, no es necesario reiniciar la instancia de base de datos.

> **Warning**
>
> La eliminación de la opción `JVM` puede dar lugar a la pérdida de datos si la instancia de base de datos usa los tipos de datos habilitados como parte de la opción. Realice copias de seguridad de los datos antes de continuar. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

Para quitar la opción `JVM` de una instancia de base de datos, realice una de las siguientes operaciones:

- Quite la opción `JVM` del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
- Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción `JVM`. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle Enterprise Manager

Amazon RDS es compatible con Oracle Enterprise Manager (OEM). OEM es la línea de productos de Oracle para la administración integrada de tecnología de la información empresarial.

Amazon RDS solo admite OEM en Oracle Database 19c (CDB o no CDB). En la tabla siguiente se describen las opciones de OEM admitidas.

Opción	ID de la opción	Versiones OEM compatibles
OEM Database Express	`OEM`	OEM Database Express 19c
OEM Management Agent	`OEM_AGENT`	OEM Cloud Control for 13c

> **Note**
>
> Puede utilizar OEM Database u OEM Management Agent, pero no ambos.

Oracle Enterprise Manager Database Express

Amazon RDS es compatible con Oracle Enterprise Manager Database Express (EM Express) mediante la opción OEM. Amazon RDS admite EM Express para Oracle Database 19c tanto con la arquitectura de CDB como con una arquitectura que no sea de CDB.

EM Express es una herramienta web de administración de bases de datos que está incluida en su base de datos y que solo está disponible cuando está abierta. Es compatible con las funciones clave de administración del rendimiento y de administración básica de bases de datos. Para obtener más información, consulte Introduction to Oracle Enterprise Manager Database Express en la documentación de Oracle Database.

> **Note**
>
> No se admite EM Express para la clase de instancia de base de datos db.t3.small. Para obtener más información sobre las clases de instancias de bases de datos, consulte Clases de instancias de base de datos de RDS para Oracle.

Configuración de la opción OEM

Amazon RDS admite los siguientes valores para las opciones de OEM.

Ajuste de la opción	Valores válidos	Descripción
Puerto	Un valor entero	El puerto en la instancia de base de datos de RDS para Oracle que escucha para EM Express. El valor predeterm inado es 5500.
Grupos de seguridad	—	Un grupo de seguridad que tiene acceso a Port.

Paso 1: añadir la opción OEM

El proceso general para añadir la opción OEM a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.

2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones con la instancia de base de datos.

Cuando se agrega la opción OEM, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente.

Para añadir la opción OEM a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine, elija la edición de Oracle que corresponda a la instancia de base de datos.

   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada la opción OEM al grupo de opciones y ajuste la configuración de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones. Para obtener más información acerca de cada opción, consulte Configuración de la opción OEM.

   > **Note**
   >
   > Si agrega la opción OEM a un grupo de opciones existente que ya se ha adjuntado a una o varias instancias de base de datos, se producirá una breve interrupción mientras reinician todas las instancias de base de datos.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Cuando se agrega la opción OEM, se produce una breve interrupción mientras la instancia de base de datos se reinicia

automáticamente. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

> **Note**
>
> También puede utilizar la AWS CLI para agregar la opción OEM. Para ver ejemplos, consulte Agregar una opción a un grupo de opciones.

Paso 2 (solo CDB): desbloquear la cuenta de usuario de DBSNMP

Si su instancia de base de datos utiliza la arquitectura de CDB, debe iniciar sesión en EM Express como `DBSNMP`. En una CDB, `DBSNMP` es un usuario común. De forma predeterminada, esta cuenta está bloqueada. Si la instancia de base de datos no utiliza la arquitectura de CDB, omita este paso.

Desbloqueo de la cuenta de usuario de DBSNMP en una instancia de CDB

1. En SQL*Plus u otra aplicación de Oracle SQL, inicie sesión como usuario maestro en su instancia de base de datos.
2. Ejecute el siguiente procedimiento almacenado para desbloquear la cuenta de `DBSNMP`:

   ```
   EXEC rdsadmin.rdsadmin_util.reset_oem_agent_password('new_password');
   ```

   Si recibe un error que indica que el procedimiento no existe, reinicie la instancia de CDB para instalarla automáticamente. Para obtener más información, consulte Reinicio de una instancia de base de datos.

Paso 3: acceder a EM Express a través del navegador

Cuando se accede a EM Express desde un navegador web, aparece una ventana de inicio de sesión que solicita un nombre de usuario y una contraseña.

Acceso a EM Express a través del navegador

1. Identifique el punto de conexión y el puerto de EM Express de su instancia de base de datos de Amazon RDS. Para obtener información acerca de cómo encontrar el punto de enlace de su instancia de base de datos de Amazon RDS, consulte Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle.

2. Introduzca una URL en la barra de localización del navegador con el siguiente formato.

```
https://endpoint.rds.amazonaws.com:port/em
```

Por ejemplo, si el punto de conexión de la instancia de base de datos de Amazon RDS es `mydb.a1bcde234fgh.us-east-1.rds.amazonaws.com` y el puerto de EM Express es `1158`, use la siguiente URL para acceder a EM Express.

```
https://mydb.f9rbfa893tft.us-east-1.rds.amazonaws.com:1158/em
```

3. Cuando se le pida la información de inicio de sesión, lleve a cabo alguna de las siguientes acciones, dependiendo de la arquitectura de la base de datos:

La base de datos no es de CDB.

Escriba el nombre de usuario maestro y la contraseña maestra para la instancia de base de datos.

La base de datos es de CDB.

Introduzca `DBSNMP` como usuario y la contraseña de `DBSNMP`. Deje vacío el campo `Container`.

Modificación de la configuración de OEM Database

Después de activar OEM Database, puede modificar la configuración de grupos de seguridad de la opción.

No se puede modificar el número de puerto de OEM después de asociar el grupo de opciones una instancia de base de datos. Para cambiar el número de puerto de OEM de una instancia de base de datos, haga lo siguiente:

1. Cree un nuevo grupo de opciones.
2. Añada la opción OEM con el nuevo número de puerto al grupo de opciones.
3. Elimine el grupo de opciones existente de la instancia de base de datos.
4. Añada el grupo de opciones nuevo a la instancia de base de datos.

Para obtener más información acerca de cómo modificar la configuración de las opciones, consulte Modificación de una configuración de opciones. Para obtener más información acerca de cada opción, consulte Configuración de la opción OEM.

Ejecución de tareas OEM Database Express

Puede utilizar los procedimientos de Amazon RDS para ejecutar determinadas tareas de OEM Database Express. Al ejecutar estos procedimientos, puede hacer las tareas que se enumeran a continuación.

> **Note**
>
> Las tareas de OEM Database Express se ejecutan de forma asíncrona.

Tareas

- Cambio del front-end del sitio web para OEM Database Express a Adobe Flash
- Cambio del front-end del sitio web para OEM Database Express a Oracle JET

Cambio del front-end del sitio web para OEM Database Express a Adobe Flash

> **Note**
>
> Esta tarea solo está disponible para Oracle Database 19c no CDB.

A partir de Oracle Database 19c, Oracle ha dado de baja la antigua interfaz de usuario de OEM Database Express, que se basaba en Adobe Flash. En su lugar, OEM Database Express utiliza ahora una interfaz creada con Oracle JET. Si tiene dificultades con la nueva interfaz, puede volver a la interfaz basada en Flash obsoleta. Las dificultades que puede tener con la nueva interfaz incluyen quedarse atascado en una pantalla `Loading` después de iniciar sesión en OEM Database Express. También puede perder ciertas características que estaban presentes en la versión basada en Flash de OEM Database Express.

Para cambiar el front-end del sitio web de OEM Database Express a Adobe Flash, ejecute el procedimiento `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash` de Amazon RDS. Este procedimiento es equivalente al comando `execemx emx` de SQL.

Las prácticas recomendadas de seguridad desalientan el uso de Adobe Flash. Aunque puede volver a OEM Database Express basado en Flash, se recomienda el uso de los sitios web de OEM Database Express basados en JET si es posible. Si vuelve a utilizar Adobe Flash y desea volver a Oracle JET, utilice el procedimiento `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet`. Después de una actualización de la base de datos Oracle, una versión más reciente de Oracle JET podría resolver problemas relacionados con JET en OEM Database Express. Para obtener más información sobre cómo cambiar a Oracle JET, consulte Cambio del front-end del sitio web para OEM Database Express a Oracle JET.

> **Note**
>
> La ejecución de esta tarea desde la instancia de base de datos de origen para una réplica de lectura también hace que la réplica de lectura cambie sus front-ends del sitio web de OEM Database Express a Adobe Flash.

La siguiente invocación del procedimiento crea una tarea para cambiar el sitio web de OEM Database Express a Adobe Flash y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash() as TASK_ID from DUAL;
```

Para ver el resultado, visualice el archivo de salida de la tarea.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-id.log'));
```

Reemplace *`task-id`* con el ID de tarea devuelto por el procedimiento. Si necesita más información sobre el procedimiento `rdsadmin.rds_file_util.read_text_file` de Amazon RDS, consulte Lectura de archivos de un directorio de instancia de base de datos

También puede ver el contenido del archivo de salida de la tarea en la AWS Management Console buscando las entradas de registro en las sección Logs & events (Registros y eventos) de la `task-id`.

Cambio del front-end del sitio web para OEM Database Express a Oracle JET

> **Note**
>
> Esta tarea solo está disponible para Oracle Database 19c no CDB.

Para cambiar el front-end del sitio web de OEM Database Express a Oracle JET, ejecute el procedimiento `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet` de Amazon RDS. Este procedimiento es equivalente al comando `execemx omx` de SQL.

De forma predeterminada, los sitios web de OEM Database Express para instancias de base de datos Oracle que ejecutan 19c o versiones posteriores utilizan Oracle JET. Si ha utilizado el procedimiento `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_flash` para cambiar el front-end del sitio web de OEM Database Express a Adobe Flash, puede cambiar de nuevo a Oracle JET. Para hacer esto, utilice el procedimiento `rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet`. Para obtener más información sobre cómo cambiar a Adobe Flash, consulte Cambio del front-end del sitio web para OEM Database Express a Adobe Flash.

> **Note**
>
> La ejecución de esta tarea desde la instancia de base de datos de origen para una réplica de lectura también hace que la réplica de lectura cambie sus front-ends del sitio web de OEM Database Express a Oracle JET.

La siguiente invocación del procedimiento crea una tarea para cambiar el sitio web de OEM Database Express a Oracle JET y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_tasks.em_express_frontend_to_jet() as TASK_ID from DUAL;
```

Para ver el resultado, visualice el archivo de salida de la tarea.

```
SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-task-
id.log'));
```

Reemplace *task-id* con el ID de tarea devuelto por el procedimiento. Si necesita más información sobre el procedimiento `rdsadmin.rds_file_util.read_text_file` de Amazon RDS, consulte Lectura de archivos de un directorio de instancia de base de datos

También puede ver el contenido del archivo de salida de la tarea en la AWS Management Console buscando las entradas de registro en las sección Logs & events (Registros y eventos) de la `task-id`.

Eliminación de la opción OEM Database

Puede eliminar la opción OEM de una instancia de base de datos. Cuando se elimina las opción OEM, se produce una breve interrupción mientras la instancia se reinicia automáticamente. Por lo tanto, después de eliminar la opción OEM, no es necesario reiniciar la instancia de base de datos.

Para eliminar la opción OEM de una instancia de base de datos, realice una de las siguientes operaciones:

- Elimine la opción OEM del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
- Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción OEM. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle Management Agent para Enterprise Manager Cloud Control

Oracle Enterprise Manager (OEM) Management Agent es un componente de software que monitoriza destinos que se ejecutan en hosts y comunica esa información al nivel intermedio de Oracle Management Service (OMS). Amazon RDS es compatible con Management Agent mediante el uso de la opción `OEM_AGENT`.

Para obtener más información, consulte Overview of Oracle Enterprise Manager Cloud Control 12c y Overview of Oracle Enterprise Manager Cloud Control 13c en la documentación de Oracle.

Temas

- Requisitos de Management Agent
- Requisitos previos de comunicación del host de OMS
- Limitaciones de Management Agent
- Configuración de opción de Management Agent
- Habilitación de la opción del agente de gestión a la instancia de base de datos
- Eliminar la opción de Management Agent
- Realización de tareas de base de datos con Management Agent

Requisitos de Management Agent

A continuación, se indican los requisitos generales para utilizar Management Agent:

- Su instancia de base de datos debe ejecutar Oracle Database 19c (19.0.0.0). Puede utilizar la arquitectura de CDB o no CDB.
- Debe utilizar un Oracle Management Service (OMS) configurado para conectarse a su instancia de base de datos. Tenga en cuenta los siguientes requisitos de OMS:
  - Las versiones 13.5.0.0.v2 y 13.5.0.0.v3 del agente de gestión requieren la versión 13.5.0.23 o 24.1 de OMS.
  - La versión 13.5.0.0.v1 del agente de gestión requiere la versión 13.5.0.0 o 24.1 de OMS.
  - Las versiones 13.4.0.9.v1 y 13.4.0.9.v2 del agente de gestiones requieren la versión 13.4.0.9 o posterior de OMS y el parche 32198287.
- En la mayoría de los casos, debe configurar la VPC para permitir conexiones desde OMS a su instancia de base de datos. Si no está familiarizado con Amazon Virtual Private Cloud (Amazon VPC), le recomendamos que antes de seguir realice los pasos que aparecen en Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).

- Puede utilizar Management Agent con Oracle Enterprise Manager Cloud Control para 12c y 13c. Asegúrese de que dispone de suficiente espacio de almacenamiento para su versión de OEM:
  - Al menos 8,5 GiB para OEM 13c versión 5
  - Al menos 8,5 GiB para OEM 13c versión 4
  - Al menos 8,5 GiB para OEM 13c versión 3
  - Al menos 5,5 GiB para OEM 13c versión 2
  - Al menos 4,5 GiB para OEM 13c versión 1
  - Al menos 2,5 GiB para OEM 12c
- Si utiliza las versiones `OEM_AGENT 13.2.0.0.v3` y `13.3.0.0.v2` de Management Agent y desea utilizar la conectividad de TCPS, siga las instrucciones de Configuración de certificados de entidades de certificación externas para la comunicación con las bases de datos de destino que figura en la documentación de Oracle. Además, actualice el JDK en su OMS siguiendo las instrucciones en el documento de Oracle con el Doc ID 2241358.1 de Oracle. Este paso garantiza que OMS sea compatible con todos los conjuntos de cifrado compatibles con la base de datos.

> **Note**
>
> La conectividad TCPS entre Management Agent y la instancia de base de datos solo es compatible para las versiones `OEM_AGENT 13.2.0.0.v3`, `13.3.0.0.v2`, `13.4.0.9.v1` y posteriores de Management Agent.

Requisitos previos de comunicación del host de OMS

Asegúrese de que su host de OMS y su instancia de base de datos de Amazon RDS puedan comunicarse. Haga lo siguiente:

- Para conectarse desde Management Agent al host de OMS cuando este se encuentre detrás de un firewall, agregue las direcciones IP de las instancias de base de datos al firewall. Asegúrese de que el firewall del OMS permita el siguiente tráfico de red:

  Desde el host de OMS a la instancia de base de datos

  Configure una regla de firewall unidireccional que permita el tráfico del host de OMS al puerto del oyente de base de datos (valor predeterminado 1521) y el puerto de OEM Agent (valor predeterminado 3872).

Desde la instancia de base de datos al host de OMS

Configure una regla de firewall unidireccional que permita el tráfico desde la instancia de base de datos al puerto HTTP de OMS (el valor predeterminado es 4903).

- Para conectarse desde OMS a Management Agent, si OMS tiene un nombre de host que se pueda resolver públicamente, debe agregar la dirección de OMS a un grupo de seguridad. El grupo de seguridad debe tener reglas de entrada que permitan el acceso al puerto del agente de escucha de base de datos y al puerto de Management Agent. Para ver un ejemplo de cómo crear una regla de seguridad y agregar reglas de entrada, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).
- Para conectarse desde OMS a Management Agent, si OMS no tiene un nombre de host que se pueda resolver públicamente, utilice uno de los siguientes:
  - Si OMS se hospeda en una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en una VPC privada, puede configurar la interconexión de VPC para conectarse desde OMS a Management Agent. Para obtener más información, consulte Acceso a una instancia de base de datos en una VPC desde una instancia EC2 de otra VPC.
  - Si OMS se hospeda localmente, puede configurar una conexión de VPN para permitir el acceso desde OMS a Management Agent. Para obtener más información, consulte Acceso a una instancia de base de datos en una VPC desde una aplicación cliente a través de internet o Conexiones de VPN.
- Para conectar la versión 13.5.0.0 (v1-v3) del agente de gestión de OEM a un host de OMS 24.1, configure `MINIMUM_TLS_VERSION` para usar el protocolo de TLS 1.2 `TLSv1.2` en las opciones de configuración.

Limitaciones de Management Agent

A continuación se indican algunas limitaciones al utilizar Management Agent:

- No puede proporcionar imágenes personalizadas de Oracle Management Agent.
- No se admiten las tareas administrativas, como la ejecución de tareas y la aplicación de parches a la base de datos, que requieren credenciales de host.
- No se garantiza que las métricas de host y la lista de procesos reflejen el estado real del sistema. Por lo tanto, no debe utilizar OEM para monitorear el sistema de archivos raíz o el sistema de archivos de punto de montaje. Para obtener más información acerca de cómo monitorear el sistema operativo, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

- La detección automática es incompatible. Los destinos de base de datos deben agregarse manualmente.
- La disponibilidad del módulo OMS depende de la edición de su base de datos. Por ejemplo, el módulo de ajuste y diagnóstico de desempeño de la base de datos solo está disponible para Oracle Database Enterprise Edition.
- Management Agent consume memoria adicional y recursos informáticos. Si tiene problemas de rendimiento después de habilitar la opción `OEM_AGENT`, recomendamos que realice una ampliación a una clase de instancia de base de datos más grande. Para obtener más información, consulte Clases de instancia de base de datos de y Modificación de una instancia de base de datos de Amazon RDS.
- El usuario que ejecuta `OEM_AGENT` en el host de Amazon RDS no tiene acceso de sistema operativo al registro de alertas. Por lo tanto, no puede recopilar métricas para `DB Alert Log` y `DB Alert Log Error Status` en OEM.

Configuración de opción de Management Agent

Amazon RDS admite la siguiente configuración para la opción de Management Agent.

Ajuste de la opción	Obligatorio	Valores válidos	Descripción

Version (`AGENT_VERSION`)	Sí	`13.5.0.0.v3`
		`13.5.0.0.v2`
		`13.5.0.0.v1`
		`13.4.0.9.v2`
		`13.4.0.9.v1`
		`13.3.0.0.v2`
			La versión del software Management Agent. La versión mínima compatible es `13.1.0.0.v1` .
			El nombre de la opción de la AWS CLI es `OptionVersion` .
			Note
			En las regiones AWS GovCloud (US), las versiones 13.1 no están disponibles.

Ajuste de la opción	Obligatorio	Valores válidos	Descripción

		`13.3.0.0.v1`
		`13.2.0.0.v3`
		`13.2.0.0.v2`
		`13.2.0.0.v1`
		`13.1.0.0.v1`	

Port (`AGENT_PORT`)	Sí	Un valor entero	El puerto en la instancia de base de datos que escucha el host de OMS. El valor predeterminado es 3872. El host de OMS debe pertenecer a un grupo de seguridad que tenga acceso a este puerto. El nombre de la opción de la AWS CLI es `Port`.
Grupos de seguridad	Sí	Grupos de seguridad existentes	Un grupo de seguridad que tiene acceso a Port. El host de OMS debe pertenecer a este grupo de seguridad. El nombre de la opción de la AWS CLI es `VpcSecurityGroupMemberships` o `DBSecurityGroupMemberships`.

Ajuste de la opción	Obligatorio	Valores válidos	Descripción
OMS_HOST	Sí	Un valor de cadena, por ejemplo *my.example.oms*	El nombre de host accesible públicamente o la dirección IP de OMS. El nombre de la opción de la AWS CLI es `OMS_HOST`.
OMS_PORT	Sí	Un valor entero	El puerto de carga HTTPS en el host de OMS que escucha el Management Agent. Para determinar el puerto de carga HTTPS, conéctese al host de OMS y ejecute el siguiente comando (que requiere la contraseña de `SYSMAN`): `emctl status oms -details` El nombre de la opción de la AWS CLI es `OMS_PORT`.
AGENT_REGISTRATION_PASSWORD	Sí	Un valor de cadena	La contraseña que Management Agent utiliza para autenticarse en OMS. Recomendamos que cree una contraseña persistente en OMS antes de habilitar la opción `OEM_AGENT` . Con una contraseña persistente puede compartir un grupo de opción de Management Agent individual entre múltiples bases de datos de Amazon RDS. El nombre de la opción de la AWS CLI es `AGENT_REGISTRATION_PASSWORD` .

Ajuste de la opción	Obligatorio	Valores válidos	Descripción
ALLOW_TLS_ONLY	No	`true`, `false` (predeterminado)	Un valor que configura el agente de OEM para que solo admita el protocolo `TLSv1` mientras el agente escucha como un servidor. Este ajuste ya no es compatible. Las versiones 13.1.0.0.v1 y superiores de Management Agent admiten seguridad de la capa de transporte (TLS) de forma predeterminada.
MINIMUM_TLS_VERSION	No	`TLSv1` (predeterminado), `TLSv1.2`	Un valor que especifica la versión mínima de TLS admitida por el agente de OEM mientras el agente escucha como un servidor. Las versiones que ya no son compatibles del agente solo admiten la configuración `TLSv1`. Para conectar la versión 13.5.0.0 (v1-v3) a un host de OMS 24.1, configúrelo en `TLSv1.2`.
TLS_CIPHER_SUITE	No	Consulte Configuración de opción de Management Agent.	Un valor que especifica el conjunto de cifrado TLS utilizado por el agente de OEM mientras el agente escucha como un servidor.

La siguiente tabla muestra los conjuntos de cifrado TLS que admite la opción Management Agent.

Conjunto de cifrado	Versión del agente admitida	Conforme con FedRAMP
TLS_RSA_WITH_AES_128_CBC_SHA	Todos	No
TLS_RSA_WITH_AES_128_CBC_SHA256	13.1.0.0.v1 y versiones posteriores	No
TLS_RSA_WITH_AES_256_CBC_SHA	13.2.0.0.v3 y versiones posteriores	No
TLS_RSA_WITH_AES_256_CBC_SHA256	13.2.0.0.v3 y versiones posteriores	No
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	13.2.0.0.v3 y versiones posteriores	Sí
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	13.2.0.0.v3 y versiones posteriores	Sí
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	13.2.0.0.v3 y versiones posteriores	Sí
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	13.2.0.0.v3 y versiones posteriores	Sí

Habilitación de la opción del agente de gestión a la instancia de base de datos

Para habilitar la opción del agente de gestión, utilice los pasos siguientes:

Temas

- Paso 1: agregar la opción de agente de gestión a la instancia de base de datos
- Paso 2: desbloquear la cuenta de usuario de DBSNMP
- Paso 3: añadir los destinos a la consola de Management Agent

Paso 1: agregar la opción de agente de gestión a la instancia de base de datos

Para añadir la opción Management Agent a una instancia de base de datos, haga lo siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Si se produce algún error, consulte los documentos de My Oracle Support para obtener información sobre cómo solucionar determinados problemas.

Después de agregar la opción de Management Agent, no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, OEM Agent también lo estará.

Si el host OMS usa un certificado de terceros que no es de confianza, Amazon RDS devolverá el error siguiente.

```
You successfully installed the OEM_AGENT option. Your OMS host is using an untrusted
 third party certificate.
Configure your OMS host with the trusted certificates from your third party.
```

Si se devuelve este error, la opción de Management Agent no se habilitará hasta que se haya solucionado el problema. Para obtener información acerca de cómo corregir el problema, consulte el documento de soporte de My Oracle 2202569.1.

Consola

Adición de la opción Management Agent a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine, elija la edición de Oracle que corresponda a la instancia de base de datos.
   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.
2. Agregue la opción OEM_AGENT al grupo de opciones y establezca la configuración de opción. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción

a un grupo de opciones. Para obtener más información acerca de cada opción, consulte Configuración de opción de Management Agent.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

En el ejemplo siguiente se usa el comando de la AWS CLI add-option-to-option-group para añadir la opción `OEM_AGENT` a un grupo de opciones llamado `myoptiongroup`.

Para Linux, macOS o Unix:

```
aws rds add-option-to-option-group \
    --option-group-name "myoptiongroup" \
    --options
 OptionName=OEM_AGENT,OptionVersion=13.1.0.0.v1,Port=3872,VpcSecurityGroupMemberships=sg-123456
{Name=OMS_PORT,Value=4903},{Name=AGENT_REGISTRATION_PASSWORD,Value=password}] \
    --apply-immediately
```

Para Windows:

```
aws rds add-option-to-option-group ^
    --option-group-name "myoptiongroup" ^
    --options
 OptionName=OEM_AGENT,OptionVersion=13.1.0.0.v1,Port=3872,VpcSecurityGroupMemberships=sg-123456
{Name=OMS_PORT,Value=4903},{Name=AGENT_REGISTRATION_PASSWORD,Value=password}] ^
    --apply-immediately
```

Paso 2: desbloquear la cuenta de usuario de DBSNMP

Management Agent utiliza la cuenta de usuario de `DBSNMP` para conectarse a la base de datos y notificar los problemas a Oracle Enterprise Manager. En una CDB, `DBSNMP` es un usuario común. Esta cuenta de usuario es necesaria tanto para Management Agent como para OEM Database

Express. De forma predeterminada, esta cuenta está bloqueada. El procedimiento para desbloquear esta cuenta varía en función de si la base de datos utiliza una arquitectura de CDB o no de CDB.

Para desbloquear la cuenta de usuario de DBSNMP

1. En SQL*Plus u otra aplicación de Oracle SQL, inicie sesión como usuario maestro en su instancia de base de datos.
2. Lleve a cabo una de las siguientes acciones, dependiendo de la arquitectura de base de datos:

   La base de datos no es de CDB.

   Ejecute la siguiente instrucción de SQL:

   ```
   ALTER USER dbsnmp IDENTIFIED BY new_password ACCOUNT UNLOCK;
   ```

   La base de datos es de CDB.

   Ejecute el siguiente procedimiento almacenado para desbloquear la cuenta de DBSNMP:

   ```
   EXEC rdsadmin.rdsadmin_util.reset_oem_agent_password('new_password');
   ```

   Si recibe un error que indica que el procedimiento no existe, reinicie la instancia de CDB para instalarla automáticamente. Para obtener más información, consulte Reinicio de una instancia de base de datos.

Paso 3: añadir los destinos a la consola de Management Agent

Para añadir una instancia de base de datos como destino, debe conocer el punto de conexión y el puerto. Para obtener información acerca de cómo encontrar el punto de enlace de su instancia de base de datos de Amazon RDS, consulte Búsqueda del punto de conexión de la instancia de base de datos de RDS para Oracle. Si su base de datos utiliza la arquitectura de CDB, añada el contenedor CDB$ROOT por separado como destino.

Adición de destinos a la consola de Management Agent

1. En consola de OMS, elija Setup, Add Target y, a continuación, Add Targets Manually.
2. Elija Add Targets Declaratively by Specifying Target Monitoring Properties.
3. En Target Type, elija Target Type.

4. En Monitoring Agent (Monitorización del agente), elija el agente con el mismo identificador que su identificador de instancia de base de datos de RDS.
5. Elija Add Manually.
6. Introduzca el punto de conexión de la instancia de base de datos de Amazon RDS o selecciónelo en la lista de nombres de host. Asegúrese de que el nombre de host especificado coincide con el punto de enlace de la instancia de base de datos de Amazon RDS.
7. Especifique las siguientes propiedades para la base de datos:
   - En Target name (Nombre de destino), escriba un nombre.
   - En Database system name (Nombre de sistema de base de datos), escriba un nombre.
   - En Monitor username (Nombre de usuario de monitor), escriba **`dbsnmp`**.
   - En Monitor password, escriba la contraseña de Paso 2: desbloquear la cuenta de usuario de DBSNMP.
   - En Role (Rol), escriba normal.
   - En Oracle home path (Ruta de inicio de Oracle), escriba **`/oracle`**.
   - En Listener Machine name, el identificador del agente ya aparece.
   - En Port (Puerto), escriba el puerto de base de datos. El puerto predeterminado de RDS es 1521.
   - En Database name (Nombre de base de datos), escriba el nombre de la base de datos. Si la base de datos es de CDB, este nombre es `RDSCDB`.
8. Elija Test Connection.
9. Elija Siguiente. La base de datos de destino aparece en su lista de recursos monitorizados.

Eliminar la opción de Management Agent

Puede eliminar OEM Agent de una instancia de base de datos. Después de eliminar OEM Agent, no es necesario reiniciar la instancia de base de datos.

Para eliminar OEM Agent de una instancia de base de datos, realice una de las siguientes operaciones:

- Elimine la opción de OEM Agent del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.

- Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción de OEM Agent. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Realización de tareas de base de datos con Management Agent

Puede utilizar procedimientos de Amazon RDS para ejecutar determinados comandos de EMCTL en Management Agent. Al ejecutar estos procedimientos, puede hacer las tareas que se enumeran a continuación.

> **Note**
>
> Las tareas se ejecutan de forma asíncrona.

Tareas

- Protección del agente de gestión
- Obtención del estado del agente de administración
- Reinicio del Management Agent
- Descripción de los objetivos monitoreados por el Management Agent
- Descripción de los subprocesos de recopilación monitoreados por Management Agent
- Borrado del estado de Management Agent
- Hacer que Management Agent cargue su OMS
- Hacer ping al OMS
- Visualización del estado de una tarea en curso

Protección del agente de gestión

Para proteger el agente de gestión, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.secure_oem_agent` de Amazon RDS. Este procedimiento es equivalente a ejecutar el comando `emctl secure agent`.

El siguiente procedimiento crea una tarea para proteger el agente de gestión y devuelve el ID de la tarea:

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.secure_oem_agent as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Obtención del estado del agente de administración

Para obtener el estado del agente de administración, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent` de Amazon RDS. Este procedimiento es equivalente al comando `emctl status agent`.

El siguiente procedimiento crea una tarea para obtener el estado del agente de gestión y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.get_status_oem_agent() as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Reinicio del Management Agent

Para reiniciar el Management Agent, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.restart_oem_agent` de Amazon RDS. Este procedimiento es equivalente a ejecutar los comandos `emctl stop agent` y `emctl start agent`.

El siguiente procedimiento crea una tarea para reiniciar Management Agent y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.restart_oem_agent as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Descripción de los objetivos monitoreados por el Management Agent

Para enumerar los objetivos monitorizados por el Management Agent, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.list_targets_oem_agent` de Amazon RDS. Este procedimiento es equivalente a ejecutar el comando `emctl config agent listtargets`.

El siguiente procedimiento crea una tarea para mostrar los destinos monitoreados por Management Agent y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.list_targets_oem_agent as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Descripción de los subprocesos de recopilación monitoreados por Management Agent

Para mostrar todos los subprocesos de recopilación en ejecución, listos y programados monitoreados por Management Agent, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.list_clxn_threads_oem_agent` de Amazon RDS. Este procedimiento es equivalente al comando `emctl status agent scheduler`.

El siguiente procedimiento crea una tarea para enumerar los subprocesos de recopilación y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.list_clxn_threads_oem_agent() as TASK_ID from
 DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Borrado del estado de Management Agent

Para borrar el estado de Management Agent, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.clearstate_oem_agent` de Amazon RDS. Este procedimiento es equivalente a ejecutar el comando `emctl clearstate agent`.

El siguiente procedimiento crea una tarea que borra el estado de Management Agent y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.clearstate_oem_agent() as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Hacer que Management Agent cargue su OMS

Para que Management Agent cargue el Oracle Management Server (OMS) asociado al mismo, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.upload_oem_agent` de Amazon RDS. Este procedimiento es equivalente a ejecutar el comando `emclt upload agent`.

El procedimiento siguiente crea una tarea que hace que Management Agent cargue su OMS asociado y devuelva el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.upload_oem_agent() as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Hacer ping al OMS

Para hacer ping al OMS del Management Agent, ejecute el procedimiento `rdsadmin.rdsadmin_oem_agent_tasks.ping_oms_oem_agent` de Amazon RDS. Este procedimiento es equivalente a ejecutar el comando `emctl pingOMS`.

El siguiente procedimiento crea una tarea que realiza ping al OMS de Management Agent y devuelve el ID de la tarea.

```
SELECT rdsadmin.rdsadmin_oem_agent_tasks.ping_oms_oem_agent() as TASK_ID from DUAL;
```

Para mostrar el archivo de salida de la tarea y ver el resultado, consulte Visualización del estado de una tarea en curso.

Visualización del estado de una tarea en curso

Puede ver el estado de una tarea continua en un archivo bdump. Los archivos bdump están ubicados en el directorio `/rdsdbdata/log/trace`. El nombre del archivo bdump está en el siguiente formato.

```
dbtask-task-id.log
```

Si desea monitorizar una tarea, reemplace *`task-id`* por el ID de la tarea que desea monitorizar.

Para ver el contenido de los archivos bdump, ejecute el procedimiento de Amazon RDS `rdsadmin.rds_file_util.read_text_file`. Por ejemplo, la siguiente consulta devuelve el contenido del archivo bdump `dbtask-1546988886389-2444.log`.

```
SELECT text FROM
 table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-1546988886389-2444.log'));
```

Si necesita más información sobre el procedimiento `rdsadmin.rds_file_util.read_text_file` de Amazon RDS, consulte Lectura de archivos de un directorio de instancia de base de datos.

Oracle Label Security

Amazon RDS es compatible con Oracle Label Security para Enterprise Edition de Oracle Database con la opción OLS.

La mayoría de los sistemas de seguridad de bases de datos controlan el acceso en el nivel de objeto. Oracle Label Security proporciona un control de acceso muy preciso a cada una de las filas de las tablas. Por ejemplo, puede utilizar Label Security para imponer el cumplimiento de las normativas mediante un modelo de administración basado en políticas. Puede utilizar las políticas de Label Security para controlar el acceso a la información confidencial y restringirlo únicamente a los usuarios con el nivel adecuado. Para obtener más información, consulte Introduction to Oracle Label Security en la documentación de Oracle.

Temas

- Requisitos de Oracle Label Security
- Factores importantes al utilizar Oracle Label Security
- Adición de la opción Oracle Label Security
- Resolución de problemas

Requisitos de Oracle Label Security

Familiarícese con los siguientes requisitos para Oracle Label Security:

- La instancia de base de datos debe utilizar el modelo Bring Your Own License (BYOL, "Traiga su propia licencia"). Para obtener más información, consulte Opciones de licencias de RDS para Oracle.
- Debe tener una licencia válida de Oracle Enterprise Edition con Software Update License and Support.
- La licencia de Oracle debe incluir la opción Label Security.

Factores importantes al utilizar Oracle Label Security

Para utilizar Oracle Label Security, debe crear políticas que controlen el acceso a determinadas filas de las tablas. Para obtener más información, consulte Creating an Oracle Label Security Policy en la documentación de Oracle.

Considere lo siguiente:

- Oracle Label Security es una opción permanente y persistente. Puesto que la opción es permanente no se puede quitar de un grupo de opciones. Si agrega Oracle Label Security a un grupo de opciones y lo asocia a su instancia de base de datos, más adelante podrá asociar un grupo de opciones diferente a su instancia de base de datos, pero este grupo también deberá contener la opción Oracle Label Security.
- Cuando se utiliza Label Security, todas las acciones se realizan con el rol `LBAC_DBA`. Al usuario maestro de la instancia de base de datos se le concede el rol `LBAC_DBA`. Es posible conceder el rol `LBAC_DBA` a otros usuarios para que puedan administrar las políticas de Label Security.
- Asegúrese de conceder acceso al paquete `OLS_ENFORCEMENT` a cualquier usuario nuevo que requiera acceso a Oracle Label Security. Para conceder acceso al paquete `OLS_ENFORCEMENT`, conéctese a la instancia de base de datos como usuario maestro y ejecute la siguiente instrucción SQL:

```
GRANT ALL ON LBACSYS.OLS_ENFORCEMENT TO username;
```

- Puede configurar Label Security a través de Oracle Enterprise Manager (OEM) Cloud Control. Amazon RDS es compatible con OEM Cloud Control mediante la opción Management Agent. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.

Adición de la opción Oracle Label Security

El proceso general para añadir la opción Oracle Label Security a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.

> **Important**
>
> Oracle Label Security es una opción permanente y persistente.

3. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir la opción Label Security, esta se activará en cuanto se active el grupo de opciones.

Para agregar la opción Label Security a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine, elija oracle-ee.

   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada la opción OLS al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

   > **Important**
   >
   > Si añade Label Security a un grupo de opciones existente que ya está asociado a una o varias instancias de bases de datos, se reinician todas las instancias de bases de datos.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Cuando se añade la opción Label Security a una instancia de base de datos existente, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Resolución de problemas

A continuación se muestran los problemas que pueden presentarse al utilizar Oracle Label Security.

Problema	Sugerencias para la solución de problemas
Al intentar crear una política, ve un mensaje de error similar al siguiente: `insufficient authorization for the SYSDBA package`.	Un problema conocido de la característica Oracle Label Security impide que los usuarios cuyos nombres tienen 16 o 24 caracteres ejecuten comandos de Label Security. Puede crear otro usuario con un número de caracteres distinto, conceder el rol LBAC_DBA a dicho usuario, iniciar sesión con las credenciales de ese usuario y ejecutar los comandos de OLS con ellas. Para obtener más información, póngase en contacto con el servicio de soporte de Oracle.

Oracle Locator

Amazon RDS admite Oracle Locator a través del uso de la opción `LOCATOR`. Oracle Locator proporciona capacidades que suelen ser necesarias para admitir aplicaciones basadas en servicio de Internet e inalámbricas y soluciones de Sistemas de información geográfica (SIG) basadas en el partner. Oracle Locator es una subred limitada de Oracle Spatial. Para obtener más información, consulte Oracle Locator en la documentación de Oracle.

> **Important**
>
> Si usa Oracle Locator, Amazon RDS actualiza automáticamente su instancia de base de datos a la versión más reciente de Oracle PSU si hay vulnerabilidades de seguridad con una puntuación del Common Vulnerability Scoring System (CVSS) superior a 9 u otras vulnerabilidades de seguridad anunciadas.

Versiones de bases de datos compatibles con Oracle Locator

RDS para Oracle es compatible con Oracle Locator para Oracle Database 19c. Oracle Locator no es compatible con Oracle Database 21c, pero su funcionalidad está disponible en la opción Oracle Spatial. Antes, la opción Spatial requería licencias adicionales. Oracle Locator representaba un subconjunto de funciones de Oracle Spatial y no requería licencias adicionales. En 2019 Oracle anunció que todas las características de Oracle Spatial se incluían en las licencias Enterprise Edition y Standard Edition 2 sin costo adicional. En consecuencia, la opción Oracle Spatial ya no requiere licencias adicionales. Para obtener más información, consulte el tema sobre Machine Learning, Spacial y Graph, sin licencia necesaria en el blog de Oracle Database Insider.

Requisitos previos para Oracle Locator

A continuación, se indican los requisitos previos para utilizar Oracle Locator:

- Su instancia de base de datos debe ser de clase suficiente. No se admite Oracle Locator para las clases de instancia de base de datos db.t3.small. Para obtener más información, consulte Clases de instancias de base de datos de RDS para Oracle.
- Su instancia de base de datos debe tener Auto Minor Version Upgrade habilitada. Esta opción permite que la instancia de base de datos reciba actualizaciones de la versión secundaria del motor de base de datos automáticamente cuando estén disponibles y es necesaria para cualquier opción que instale la máquina virtual Java (JVM) de Oracle Amazon RDS utiliza esta opción para

actualizar su instancia de base de datos a la PSU (Patch Set Update) de Oracle más reciente o actualización de la versión (RU). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Prácticas recomendadas para Oracle Locator

A continuación, se indican las prácticas recomendadas para utilizar Oracle Locator:

- Para que la seguridad sea máxima, use la opción `LOCATOR` con Capa de conexión segura (SSL). Para obtener más información, consulte Capa de conexión segura de Oracle.
- Configure su instancia de base de datos para restringir el acceso a la misma. Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC y Uso de una instancia de base de datos en una VPC.

Adición de la opción Oracle Locator

A continuación se muestra el proceso general para añadir la opción `LOCATOR` a una instancia de base de datos:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Si la máquina virtual Java (JVM) de Oracle no está instalada en la instancia de base de datos, se produce una breve interrupción mientras se agrega la opción `LOCATOR`. No hay interrupción si la máquina virtual Java (JVM) de Oracle ya está instalada en la instancia de base de datos. Después de añadir la opción , no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, Oracle Locator estará disponible.

> **Note**
>
> Durante esta interrupción, las funciones de verificación de contraseña se deshabilitan brevemente. También puede esperar ver eventos relacionados con las funciones de verificación de contraseña durante la interrupción. Las funciones de verificación de contraseña se vuelven a habilitar antes de que la instancia de base de datos de Oracle esté disponible.

Para añadir la opción **LOCATOR** a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine, elija la edición de Oracle que corresponda a la instancia de base de datos.

   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada la opción LOCATOR al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Uso de Oracle Locator

Una vez que habilite la opción Oracle Locator, podrá empezar a usarla. Solo debe usar características de Oracle Locator. No use ninguna característica de Oracle Spatial a menos que tenga una licencia para Oracle Spatial.

Para obtener una lista de características compatibles con Oracle Locator, consulte Features Included with Locator en la documentación de Oracle.

Para obtener una lista de características no compatibles con Oracle Locator, consulte Features Not Included with Locator en la documentación de Oracle.

Eliminación de la opción Oracle Locator

Después de eliminar todos los objetos que utilizan los tipos de datos proporcionados por la opción LOCATOR, puede quitar la opción de una instancia de base de datos. Si la máquina virtual Java (JVM) de Oracle no está instalada en la instancia de base de datos, se produce una breve interrupción mientras se elimina la opción LOCATOR. No hay interrupción si la máquina virtual Java (JVM) de Oracle ya está instalada en la instancia de base de datos. Después de quitar la opción LOCATOR, no es necesario reiniciar la instancia de base de datos.

Para eliminar la opción **LOCATOR**

1. Haga una copia de seguridad de sus datos.

   > **Warning**
   >
   > Si la instancia utiliza tipos de datos habilitados como parte de la opción y si elimina la opción LOCATOR, puede perder datos. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

2. Compruebe si los objetos existentes hacen referencia a los tipos de datos o a las características de la opción LOCATOR.

   Si existen opciones LOCATOR, la instancia puede quedarse atascada al aplicar el nuevo grupo de opciones que no tiene la opción LOCATOR. Puede identificar los objetos mediante las siguientes consultas:

```
SELECT OWNER, SEGMENT_NAME, TABLESPACE_NAME, BYTES/1024/1024 mbytes
FROM   DBA_SEGMENTS
WHERE  SEGMENT_TYPE LIKE '%TABLE%'
AND    (OWNER, SEGMENT_NAME) IN
       (SELECT DISTINCT OWNER, TABLE_NAME
        FROM   DBA_TAB_COLUMNS
        WHERE  DATA_TYPE='SDO_GEOMETRY'
        AND    OWNER <> 'MDSYS')
ORDER BY 1,2,3,4;

SELECT OWNER, TABLE_NAME, COLUMN_NAME
FROM   DBA_TAB_COLUMNS
WHERE  DATA_TYPE = 'SDO_GEOMETRY'
AND    OWNER <> 'MDSYS'
```

```
ORDER BY 1,2,3;
```

3. Suelte los objetos que hagan referencia a los tipos de datos o a las características de la opción LOCATOR.
4. Aplique alguna de las siguientes acciones:

   - Quite la opción LOCATOR del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
   - Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción LOCATOR. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle Native Network Encryption

Amazon RDS es compatible con el cifrado de red nativo (NNE, Native Network Encryption) de Oracle. Con la opción `NATIVE_NETWORK_ENCRYPTION`, puede cifrar datos durante su tránsito hacia y desde una instancia de base de datos. Amazon RDS es compatible con NNE para todas las ediciones de Oracle Database.

Esta guía no tiene el propósito de ofrecerle una descripción detallada del cifrado de red nativo de Oracle, pero sí que debe comprender los puntos fuertes y los puntos débiles de cada algoritmo y cada clave antes de decidirse por una solución para su implementación. Para obtener información acerca de los algoritmos y las claves disponibles a través del cifrado de red nativo de Oracle, consulte Configuring Network Data Encryption en la documentación de Oracle. Para obtener más información sobre la seguridad de AWS, consulte el centro de seguridad de AWS.

> **Note**
>
> Es posible utilizar Native Network Encryption o Secure Sockets Layer, pero no ambas opciones. Para obtener más información, consulte Capa de conexión segura de Oracle.

Temas

- Configuración de la opción NATIVE_NETWORK_ENCRYPTION
- Adición de la opción NATIVE_NETWORK_ENCRYPTION
- Establecimiento de valores de NNE en sqlnet.ora
- Modificación de la configuración de la opción NATIVE_NETWORK_ENCRYPTION
- Eliminación de la opción NATIVE_NETWORK_ENCRYPTION

Configuración de la opción NATIVE_NETWORK_ENCRYPTION

Puede especificar requisitos de cifrado tanto en el servidor como en el cliente. La instancia de base de datos puede actuar como cliente cuando, por ejemplo, utiliza un vínculo de base de datos para conectarse a otra base de datos. Es posible que desee evitar forzar el cifrado en el lado del servidor. Por ejemplo, es posible que no desee forzar todas las comunicaciones del cliente para que utilicen el cifrado porque el servidor lo requiera. En este caso, puede forzar el cifrado en el lado del cliente mediante las opciones de `SQLNET.*CLIENT`.

Amazon RDS admite las siguientes configuraciones para la opción `NATIVE_NETWORK_ENCRYPTION`.

> **Note**
>
> Cuando utilice comas para separar valores para una configuración de opción, no coloque un espacio después de la coma.

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
`SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS`	`TRUE`, `FALSE`	`TRUE`	El comportamiento del servidor cuando un cliente que utiliza un cifrado que no está protegido intenta conectarse a la base de datos. Si es `TRUE`, los clientes pueden conectarse incluso si no cuentan con revisiones de PSU de julio de 2021. Si el ajuste es `FALSE`, los clientes pueden conectarse a la base de datos solo cuando cuenten con las revisiones de PSU de julio de 2021. Antes de configurar `SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS` a `FALSE`, asegúrese de que se cumplan las siguientes condiciones: • `SQLNET.ENCRYPTION_TYPES_SERVER` y `SQLNET.ENCRYPTION_TYPES_CLIENT` deben tener un método de cifrado coincidente que no sea `DES`, `3DES`, o bien `RC4` (todas las longitudes de clave).

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
			• `SQLNET.CHECKSUM_TYPES_SERVER` y `SQLNET.CHECKSUM_TYPES_CLIENT` deben tener un método de suma de comprobación seguro coincidente que no sea `MD5`. • El cliente cuenta con la revisión de PSU de julio de 2021. Si el cliente no cuenta con la revisión, el cliente pierde la conexión y recibe el erorr `ORA-12269` .

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
SQLNET.ALLOW_WEAK_CRYPTO	TRUE, FALSE	TRUE	El comportamiento del servidor cuando un cliente que utiliza un cifrado que no está protegido intenta conectarse a la base de datos. Los siguientes cifrados no se consideran seguros: • Método de cifrado DES (todas las longitudes de clave) • Método de cifrado 3DES (todas las longitudes de clave) • Método de cifrado RC4 (todas las longitudes de clave) • Método de sumas de comprobación MD5 Si la configuración es TRUE, los clientes pueden conectarse cuando utilizan los cifrados anteriores que no estén protegidos. Si la configuración es FALSE, la base de datos evita que los clientes se conecten cuando utilizan los cifrados anteriores que no estén protegidos. Antes de configurar SQLNET.ALLOW_WEAK_CRYPTO a FALSE, asegúrese de que se cumplan las siguientes condiciones: • SQLNET.ENCRYPTION_TYPES_SERVER y SQLNET.ENCRYPTION_TYPES_CLIENT

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
			deben tener un método de cifrado coincidente que no sea DES, 3DES, o bien RC4 (todas las longitudes de clave). • SQLNET.CHECKSUM_TYPES_SERVER y SQLNET.CHECKSUM_TYPES_CLIENT deben tener un método de suma de comprobación seguro coincidente que no sea MD5. • El cliente cuenta con la revisión de PSU de julio de 2021. Si el cliente no cuenta con la revisión, el cliente pierde la conexión y recibe el erorr ORA-12269 .
SQLNET.CRYPTO_CHECKSUM_CLIENT	Accepted Rejected Requested , Required	Requested	Comportamiento de integridad de datos cuando una instancia de base de datos se conecta al cliente o cuando un servidor actúa como un cliente. Cuando una instancia de base de datos utiliza un enlace de base de datos, esta actúa como cliente. Requested indica que el cliente no requiere que la instancia de base de datos haga la suma de comprobación.

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
SQLNET.CRYPTO_CHECKSUM_SERVER	Accepted Rejected Requested , Required	Requested	Comportamiento de integridad de datos cuando un cliente o un servidor que actúa como cliente se conecta a la instancia de base de datos. Cuando una instancia de base de datos utiliza un enlace de base de datos, esta actúa como cliente. Requested indica que la instancia de base de datos no requiere que el cliente haga la suma de comprobación.
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT	SHA256, SHA384, SHA512, SHA1, MD5	SHA256, SHA384, SHA512	Una lista de algoritmos de suma de comprobación. Puede especificar un valor o una lista de valores separada por comas. Si utiliza una coma, no inserte un espacio después de la coma; de lo contrario, recibirá un error InvalidParameterValue . Este parámetro y SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER deben tener un cifrado común.

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER	SHA256, SHA384, SHA512, SHA1, MD5	SHA256, SHA384, SHA512, SHA1, MD5	Una lista de algoritmos de suma de comprobación. Puede especificar un valor o una lista de valores separada por comas. Si utiliza una coma, no inserte un espacio después de la coma; de lo contrario, recibirá un error InvalidParameterValue . Este parámetro y SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT deben tener un cifrado común.
SQLNET.ENCRYPTION_CLIENT	Accepted Rejected Requested , Required	Requested	Comportamiento de cifrado del cliente cuando un cliente o un servidor que actúa como cliente se conecta a la instancia de base de datos. Cuando una instancia de base de datos utiliza un enlace de base de datos, esta actúa como cliente. Requested indica que el cliente no requiere que el tráfico del servidor esté cifrado.

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
SQLNET.ENCRYPTION_SERVER	Accepted Rejected Requested , Required	Requested	Comportamiento de cifrado del servidor cuando un cliente o un servidor que actúa como cliente se conecta a la instancia de base de datos. Cuando una instancia de base de datos utiliza un enlace de base de datos, esta actúa como cliente. Requested indica que la instancia de base de datos no requiere que el tráfico del cliente esté cifrado.

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
SQLNET.ENCRYPTION_TYPES_CLIENT	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	Lista de algoritmos de cifrado utilizados por el cliente. El cliente utiliza cada algoritmo, por orden, para intentar descifrar la entrada del servidor hasta que un algoritmo tenga éxito o hasta que se llegue al final de la lista. Amazon RDS utiliza la siguiente lista predeterminada de Oracle. RDS comienza con RC4_256 y continúa con la lista por orden. Es posible cambiar el orden o limitar los algoritmos que aceptará la instancia de base de datos. 1. RC4_256: RSA RC4 (tamaño de clave de 256 bits) 2. AES256: AES (tamaño de clave de 256 bits) 3. AES192: AES (tamaño de clave de 192 bits) 4. 3DES168: 3 claves Triple-DES (tamaño de clave efectivo de 112 bits) 5. RC4_128: RSA RC4 (tamaño de clave de 128 bits) 6. AES128: AES (tamaño de clave de 128 bits) 7. 3DES112: 2 claves Triple-DES (tamaño de clave efectivo de 80 bits) 8. RC4_56: RSA RC4 (tamaño de clave de 56 bits)

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
			9. `DES`: DES estándar (tamaño de clave de 56 bits) 10. `RC4_40`: RSA RC4 (tamaño de clave de 40 bits) 11. `DES40`: DES40 (tamaño de clave de 40 bits) Puede especificar un valor o una lista de valores separada por comas. Si utiliza una coma, no inserte un espacio después de la coma; de lo contrario, recibirá un error `InvalidParameterValue` . Este parámetro y `SQLNET.SQLNET.ENCRYPTION_TYPES_SERVER` deben tener un cifrado común.

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
SQLNET.ENCRYPTION_TYPES_SERVER	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	RC4_256, AES256, AES192, 3DES168, RC4_128, AES128, 3DES112, RC4_56, DES, RC4_40, DES40	Lista de algoritmos de cifrado utilizados por la instancia de base de datos. La instancia de base de datos utiliza cada algoritmo, por orden, para intentar descifrar la entrada del cliente hasta que un algoritmo tenga éxito o hasta que se llegue al final de la lista. Amazon RDS utiliza la siguiente lista predeterminada de Oracle. Es posible cambiar el orden o limitar los algoritmos que aceptará el cliente. 1. RC4_256: RSA RC4 (tamaño de clave de 256 bits) 2. AES256: AES (tamaño de clave de 256 bits) 3. AES192: AES (tamaño de clave de 192 bits) 4. 3DES168: 3 claves Triple-DES (tamaño de clave efectivo de 112 bits) 5. RC4_128: RSA RC4 (tamaño de clave de 128 bits) 6. AES128: AES (tamaño de clave de 128 bits) 7. 3DES112: 2 claves Triple-DES (tamaño de clave efectivo de 80 bits) 8. RC4_56: RSA RC4 (tamaño de clave de 56 bits)

Ajuste de la opción	Valores válidos	Valores predeterminados	Descripción
			9. `DES`: DES estándar (tamaño de clave de 56 bits) 10 `RC4_40`: RSA RC4 (tamaño de clave de 40 bits) 11 `DES40`: DES40 (tamaño de clave de 40 bits) Puede especificar un valor o una lista de valores separada por comas. Si utiliza una coma, no inserte un espacio después de la coma; de lo contrario, recibirá un error `InvalidParameterValue` . Este parámetro y `SQLNET.SQLNET.ENCRYPTION_TYPES_SERVER` deben tener un cifrado común.

Adición de la opción NATIVE_NETWORK_ENCRYPTION

El proceso general para agregar la opción `NATIVE_NETWORK_ENCRYPTION` a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

En cuanto esté activo el grupo de opciones, NNE también estará activo.

Adición de la opción NATIVE_NETWORK_ENCRYPTION a una instancia de base de datos mediante la AWS Management Console

1. En Engine, elija la edición de Oracle que desea utilizar. NNE se admite en todas las ediciones.
2. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.
3. Agregue la opción NATIVE_NETWORK_ENCRYPTION al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

   > **Note**
   >
   > Después de agregar la opción NATIVE_NETWORK_ENCRYPTION, no es necesario reiniciar las instancias de base de datos. En cuanto esté activo el grupo de opciones, NNE también lo estará.
4. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Después de agregar la opción NATIVE_NETWORK_ENCRYPTION, no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, NNE también lo estará. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Establecimiento de valores de NNE en sqlnet.ora

Con el cifrado de red nativo de Oracle, también puede especificar el cifrado de red en lado del cliente y el lado del servidor. El cliente es el ordenador que se utiliza para conectarse a la instancia de base de datos. Puede especificar la siguiente configuración del cliente en el archivo sqlnet.ora:

- `SQLNET.ALLOW_WEAK_CRYPTO`
- `SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS`

- SQLNET.CRYPTO_CHECKSUM_CLIENT
- SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT
- SQLNET.ENCRYPTION_CLIENT
- SQLNET.ENCRYPTION_TYPES_CLIENT

Para obtener más información, consulte Configuring Network Data Encryption and Integrity for Oracle Servers and Clients en la documentación de Oracle.

A veces, la instancia de base de datos rechaza una solicitud de conexión de una aplicación. Por ejemplo, puede producirse un rechazo cuando los algoritmos de cifrado en el cliente y en el servidor no coinciden. Para probar el cifrado de red nativo de Oracle, agregue las siguientes líneas al archivo sqlnet.ora en el cliente:

```
DIAG_ADR_ENABLED=off
TRACE_DIRECTORY_CLIENT=/tmp
TRACE_FILE_CLIENT=nettrace
TRACE_LEVEL_CLIENT=16
```

Cuando se intenta establecer la conexión, estas líneas generan un archivo de seguimiento en el cliente denominado `/tmp/nettrace*`. El archivo de seguimiento contiene información sobre la conexión. Para obtener más información sobre problemas relacionados con la conexión cuando utiliza el cifrado de red nativo de Oracle, consulteAcerca de la negociación del cifrado y la integridad en la documentación de la base de datos de Oracle.

Modificación de la configuración de la opción NATIVE_NETWORK_ENCRYPTION

Después de habilitar la opción `NATIVE_NETWORK_ENCRYPTION`, puede modificar su configuración. Actualmente, solo puede modificar la configuración de las opciones de `NATIVE_NETWORK_ENCRYPTION` con la AWS CLI o la API de RDS. No puede utilizar la consola. En el siguiente ejemplo, se modifican dos ajustes de la opción.

```
aws rds add-option-to-option-group \
    --option-group-name my-option-group \
    --options
 "OptionName=NATIVE_NETWORK_ENCRYPTION,OptionSettings=[{Name=SQLNET.CRYPTO_CHECKSUM_TYPES_SERVE
{Name=SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER,Value=SHA256}]" \
    --apply-immediately
```

Para obtener más información acerca de cómo modificar la configuración de las opciones con la CLI, consulte AWS CLI. Para obtener más información acerca de cada opción, consulte Configuración de la opción NATIVE_NETWORK_ENCRYPTION.

Temas

- Modificación de los valores CRYPTO_CHECKSUM_*
- Modificación de la configuración ALLOW_WEAK_CRYPTO*

Modificación de los valores CRYPTO_CHECKSUM_*

Si modifica la configuración de la opción de NATIVE_NETWORK_ENCRYPTION, asegúrese de que la siguiente configuración de la opción tenga al menos un cifrado común:

- `SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER`
- `SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT`

En el siguiente ejemplo, se muestra un escenario en el que se modifica `SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER`. La configuración es válida porque tanto `CRYPTO_CHECKSUM_TYPES_CLIENT` y `CRYPTO_CHECKSUM_TYPES_SERVER` usan `SHA256`.

Ajuste de la opción	Valores antes de la modificación	Valores tras la modificación
`SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT`	**`SHA256`**, `SHA384`, `SHA512`	Sin cambios
`SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER`	**`SHA256`**, `SHA384`, `SHA512`, `SHA1`, `MD5`	`SHA1,MD5,` **`SHA256`**

Por otro ejemplo, suponga que desea modificar `SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER` de su configuración predeterminada a `SHA1,MD5`. En este caso, asegúrese de establecer uno de estos valores para `SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT`: `SHA1` o `MD5`. Estos algoritmos no se incluyen en los valores predeterminados para `SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT`.

Modificación de la configuración ALLOW_WEAK_CRYPTO*

Para configurar las opciones SQLNET.ALLOW_WEAK_CRYPTO* del valor predeterminado a FALSE, asegúrese de que se cumplan las siguientes condiciones:

- SQLNET.ENCRYPTION_TYPES_SERVER y SQLNET.ENCRYPTION_TYPES_CLIENT deben tener un método de cifrado seguro coincidente. Un método se considera seguro si no es DES, 3DES, o bien RC4 (todas las longitudes de clave).
- SQLNET.CHECKSUM_TYPES_SERVER y SQLNET.CHECKSUM_TYPES_CLIENT deben tener un método de suma de comprobación seguro coincidente. Un método se considera seguro si no es MD5.
- El cliente cuenta con la revisión de PSU de julio de 2021. Si el cliente no cuenta con la revisión, el cliente pierde la conexión y recibe el erorr ORA-12269.

El siguiente ejemplo muestra configuraciones NNE de muestra. Supongamos que desea configurar SQLNET.ENCRYPTION_TYPES_SERVER y SQLNET.ENCRYPTION_TYPES_CLIENT a FALSE, bloqueando así las conexiones no seguras. La configuración de la opción de suma de comprobación cumple los requisitos previos porque ambos tienen SHA256. Sin embargo, SQLNET.ENCRYPTION_TYPES_CLIENT y SQLNET.ENCRYPTION_TYPES_SERVER usan los métodos de cifrado no seguro DES, 3DES, y RC4. Por lo tanto, para establecer las opciones SQLNET.ALLOW_WEAK_CRYPTO* en FALSE, primero establezca SQLNET.ENCRYPTION_TYPES_SERVER y SQLNET.ENCRYPTION_TYPES_CLIENT en un método de cifrado seguro como AES256.

Ajuste de la opción	Valores
SQLNET.CRYPTO_CHECKSUM_TYPES_CLIENT	SHA256, SHA384, SHA512
SQLNET.CRYPTO_CHECKSUM_TYPES_SERVER	SHA1,MD5,SHA256
SQLNET.ENCRYPTION_TYPES_CLIENT	RC4_256, 3DES168, DES40
SQLNET.ENCRYPTION_TYPES_SERVER	RC4_256, 3DES168, DES40

Eliminación de la opción NATIVE_NETWORK_ENCRYPTION

Puede eliminar NNE de una instancia de base de datos.

Para quitar la opción `NATIVE_NETWORK_ENCRYPTION` de una instancia de base de datos, realice una de las siguientes operaciones:

- Para eliminar la opción de varias instancias de bases de datos, elimine la opción `NATIVE_NETWORK_ENCRYPTION` del grupo de opciones al que pertenecen. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Después de eliminar la opción `NATIVE_NETWORK_ENCRYPTION`, no es necesario reiniciar las instancias de base de datos. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
- Para eliminar la opción de una sola instancia de base de datos, modifique la instancia y especifique otro grupo de opciones que no incluya la opción `NATIVE_NETWORK_ENCRYPTION`. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Después de quitar la opción `NATIVE_NETWORK_ENCRYPTION`, no es necesario reiniciar la instancia de base de datos. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle OLAP

Amazon RDS admite Oracle OLAP mediante el uso de la opción OLAP. Esta opción proporciona procesamiento analítico en línea (OLAP) para las instancias de base de datos de Oracle. Puede utilizar Oracle OLAP para analizar grandes cantidades de datos mediante la creación de cubos y objetos dimensionales de acuerdo con el estándar OLAP. Para obtener más información, consulte la documentación de Oracle.

> **Important**
>
> Si usa Oracle OLAP, Amazon RDS actualiza automáticamente la instancia de base de datos a la versión más reciente de Oracle PSU si hay vulnerabilidades de seguridad con una puntuación CVSS (Common Vulnerability Scoring System) superior a 9 u otras vulnerabilidades de seguridad anunciadas.

Amazon RDS admite Oracle OLAP en Enterprise Edition de Oracle Database 19c y versiones posteriores.

Requisitos previos para Oracle OLAP

A continuación se indican los requisitos previos para utilizar Oracle OLAP:

- Debe tener una licencia de Oracle OLAP. Para obtener más información, consulte la información sobre licencias en la documentación de Oracle.
- Su instancia de base de datos debe ser de una clase de instancia suficiente. Oracle OLAP no es compatible con la clase de instancia de base de datos db.t3.small. Para obtener más información, consulte Clases de instancias de base de datos de RDS para Oracle.
- Su instancia de base de datos debe tener Auto Minor Version Upgrade habilitada. Esta opción permite que la instancia de base de datos reciba actualizaciones de la versión secundaria del motor de base de datos automáticamente cuando estén disponibles y es necesaria para cualquier opción que instale la máquina virtual Java (JVM) de Oracle Amazon RDS utiliza esta opción para actualizar su instancia de base de datos a la PSU (Patch Set Update) de Oracle más reciente o actualización de la versión (RU). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
- La instancia de base de datos no debe tener un usuario llamado OLAPSYS. Si lo hace, se produce un error en la instalación de la opción OLAP.

Prácticas recomendadas para Oracle OLAP

A continuación, se indican las prácticas recomendadas para utilizar Oracle OLAP:

- Para que la seguridad sea máxima, use la opción `OLAP` con Capa de conexión segura (SSL). Para obtener más información, consulte Capa de conexión segura de Oracle.
- Configure su instancia de base de datos para restringir el acceso a la misma. Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC y Uso de una instancia de base de datos en una VPC.

Adición de la opción Oracle OLAP

A continuación se muestra el proceso general para añadir la opción `OLAP` a una instancia de base de datos:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Si la máquina virtual Java (JVM) de Oracle no está instalada en la instancia de base de datos, se produce una breve interrupción mientras se agrega la opción `OLAP`. No hay interrupción si la máquina virtual Java (JVM) de Oracle ya está instalada en la instancia de base de datos. Después de añadir la opción , no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, Oracle OLAP estará disponible.

Para agregar la opción OLAP a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   - En Engine (Motor), elija la edición de Oracle que corresponda a la instancia de base de datos.
   - En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.

2. Agregue la opción OLAP al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:
   - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Uso de Oracle OLAP

Una vez que habilite la opción Oracle OLAP, podrá empezar a usarla. Para obtener una lista de características compatibles con Oracle OLAP, consulte la documentación de Oracle.

Eliminación de la opción Oracle OLAP

Después de eliminar todos los objetos que utilizan los tipos de datos proporcionados por la opción OLAP, puede quitar la opción de una instancia de base de datos. Si la máquina virtual Java (JVM) de Oracle no está instalada en la instancia de base de datos, se produce una breve interrupción mientras se elimina la opción OLAP. No hay interrupción si la máquina virtual Java (JVM) de Oracle ya está instalada en la instancia de base de datos. Después de quitar la opción OLAP, no es necesario reiniciar la instancia de base de datos.

Para eliminar la opción **OLAP**

1. Haga una copia de seguridad de sus datos.

   > **Warning**
   >
   > Si la instancia utiliza tipos de datos habilitados como parte de la opción y si elimina la opción OLAP, puede perder datos. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

2. Compruebe si los objetos existentes hacen referencia a los tipos de datos o a las características de la opción OLAP.

3. Suelte los objetos que hagan referencia a los tipos de datos o a las características de la opción `OLAP`.
4. Aplique alguna de las siguientes acciones:

   - Quite la opción `OLAP` del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
   - Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción `OLAP`. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Capa de conexión segura de Oracle

A fin de habilitar el cifrado SSL para una instancia de base de datos de RDS para Oracle, añada la opción Oracle SSL al grupo de opciones asociado a la instancia de base de datos. Amazon RDS utiliza un segundo puerto, según lo requiera Oracle, para las conexiones SSL. Este enfoque permite que se produzca la comunicación cifrada de SSL y de texto sin cifrar al mismo tiempo entre una instancia de base de datos y SQL*Plus. Por ejemplo, es posible utilizar el puerto con la comunicación de texto sin cifrar para ponerse en contacto con otros recursos dentro de una VPC mientras se utiliza el puerto con comunicación cifrada SSL para ponerse en contacto con recursos situados fuera de la VPC.

> **Note**
>
> Se puede utilizar SSL o Native Network Encryption (NNE) en la misma instancia de base de datos de RDS para Oracle, pero no ambos. Si se utiliza el cifrado SSL, se debe desactivar cualquier otro cifrado de conexión. Para obtener más información, consulte Oracle Native Network Encryption.

SSL/TLS y NNE ya no forman parte de Oracle Advanced Security. En RDS para Oracle, el cifrado SSL puede utilizarse con las ediciones con licencia de las siguientes versiones:

- Oracle Database 21c (21.0.0)
- Oracle Database 19c (19.0.0)

Temas

- Versiones de TLS para la opción Oracle SSL
- Conjuntos de cifrado para la opción Oracle SSL
- Compatibilidad FIPS
- Adición de la opción SSL
- Configuración de SQL*Plus para utilizar SSL con una instancia de base de datos de RDS para Oracle
- Conexión a una instancia de base de datos de RDS para Oracle mediante SSL
- Configuración de una conexión SSL a través de JDBC
- Obligatoriedad de la coincidencia del DN con una conexión SSL

- Solución de problemas de las conexiones SSL

Versiones de TLS para la opción Oracle SSL

Amazon RDS para Oracle supports Transport Layer Security (TLS) versiones 1.0 y 1.2. Cuando añada una nueva opción Oracle SSL, establezca `SQLNET.SSL_VERSION` explícitamente en un valor válido. Los siguientes valores están permitidos para esta continuación de opciones:

- `"1.0"`: los clientes pueden conectarse a la instancia de base de datos utilizando TLS versión 1.0 solo. Para las opciones de Oracle SSL existentes, `SQLNET.SSL_VERSION` se establece en `"1.0"` automáticamente. Puede cambiar la configuración si es necesario.
- `"1.2"`: los clientes pueden conectarse a la instancia de base de datos utilizando TLS 1.2 solo.
- `"1.2 or 1.0"`: los clientes pueden conectarse a la instancia de base de datos utilizando TLS 1.2 o 1.0.

Conjuntos de cifrado para la opción Oracle SSL

Amazon RDS para Oracle es compatible con múltiples conjuntos de cifrado SSL. De manera predeterminada, la opción Oracle SSL está configurada para utilizar el conjunto de cifrado `SSL_RSA_WITH_AES_256_CBC_SHA`. Para especificar un conjunto de cifrado diferente para utilizarlo en las conexiones SSL, utilice la configuración de opciones `SQLNET.CIPHER_SUITE`.

Puede especificar varios valores para `SQLNET.CIPHER_SUITE`. Esta técnica resulta útil si tiene enlaces de bases de datos entre sus instancias de base de datos y decide actualizar los conjuntos de cifrado.

En la siguiente tabla se resume la compatibilidad de SSL para RDS para Oracle en todas las ediciones de Oracle Database 19c y 21c.

Conjunto de cifrado (SQLNET.CIPHER_SUITE)	Compatibilidad de la versión de TLS (SQLNET.SSL_VERSION)	Compatibilidad FIPS	Conforme con FedRAMP
SSL_RSA_WITH_AES_256_CBC_SHA (predeterminado)	1.0 y 1.2	Sí	No

Conjunto de cifrado (SQLNET.CIPHER_SUITE)	Compatibilidad de la versión de TLS (SQLNET.SSL_VERSION)	Compatibilidad FIPS	Conforme con FedRAMP
SSL_RSA_WITH_AES_256_CBC_SHA256	1.2	Sí	No
SSL_RSA_WITH_AES_256_GCM_SHA384	1.2	Sí	No
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	1.2	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1.2	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	1.2	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	1.2	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	1.2	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	1.2	Sí	Sí

Compatibilidad FIPS

RDS para Oracle le permite usar el estándar federal de procesamiento de la información (FIPS) para 140-2. FIPS 140-2 es un estándar del gobierno estadounidense que define los requisitos de seguridad de los módulos criptográficos. Para activar el estándar FIPS, establezca el valor `FIPS.SSLFIPS_140` en `TRUE` para la opción SSL de Oracle. Cuando FIPS 140-2 se configura para SSL, las bibliotecas criptográficas cifran los datos entre el cliente y la instancia de base de datos de RDS para Oracle.

Los clientes deben usar el conjunto de cifrado compatible con FIPS. Al establecer una conexión, el cliente y la instancia de base de datos de RDS para Oracle negocian qué conjunto de cifrado utilizar al transmitir mensajes entre ellos. La tabla en Conjuntos de cifrado para la opción Oracle

SSL muestra los conjuntos de cifrado SSL compatibles con FIPS para cada versión de TLS. Para obtener más información, consulte Oracle Database FIPS 140-2 Settings en la documentación de Oracle.

Adición de la opción SSL

Para usar SSL, su instancia de base de datos de RDS para Oracle debe estar asociada a un grupo de opciones que incluya la opción `SSL`.

Consola

Para agregar la opción SSL a un grupo de opciones, realice el siguiente procedimiento:

1. Cree un nuevo grupo de opciones o identifique uno ya existente al que pueda añadir la opción `SSL`.

   Para obtener información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.
2. Agregue la opción `SSL` al grupo de opciones.

   Si solo desea utilizar conjuntos de cifrado verificados por FIPS para las conexiones SSL, establezca la opción `FIPS.SSLFIPS_140` en `TRUE`. Para obtener información sobre el estándar FIPS, consulte Compatibilidad FIPS.

   Para obtener información acerca de cómo añadir una opción a un grupo de opciones, consulte Agregar una opción a un grupo de opciones.
3. Cree una nueva instancia de base de datos de RDS para Oracle y asocie el grupo de opciones a ella, o bien modifique una instancia de base de datos de RDS para Oracle para asociarla al grupo de opciones.

   Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

   Para obtener información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

Para agregar la opción SSL a un grupo de opciones, realice el siguiente procedimiento:

1. Cree un nuevo grupo de opciones o identifique uno ya existente al que pueda añadir la opción SSL.

   Para obtener información acerca de cómo crear un grupo de opciones, consulte Creación de un grupo de opciones.

2. Añada la opción SSL al grupo de opciones.

   Especifique las siguientes opciones de configuración:

   - Port: el número de puerto SSL.
   - VpcSecurityGroupMemberships: el grupo de seguridad de VPC para el que se ha habilitado la opción.
   - SQLNET.SSL_VERSION: la versión TLS que el cliente puede utilizar para conectarse a la instancia de base de datos.

   Por ejemplo, el siguiente comando de la AWS CLI añade la opción SSL a un grupo de opciones denominado ora-option-group.

   Example

   Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group --option-group-name ora-option-group \
  --options
 'OptionName=SSL,Port=2484,VpcSecurityGroupMemberships="sg-68184619",OptionSettings=[{Name=
```

   En:Windows

```
aws rds add-option-to-option-group --option-group-name ora-option-group ^
  --options
 'OptionName=SSL,Port=2484,VpcSecurityGroupMemberships="sg-68184619",OptionSettings=[{Name=
```

3. Cree una nueva instancia de base de datos de RDS para Oracle y asocie el grupo de opciones a ella, o bien modifique una instancia de base de datos de RDS para Oracle para asociarla al grupo de opciones.

   Para obtener información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

   Para obtener información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Configuración de SQL*Plus para utilizar SSL con una instancia de base de datos de RDS para Oracle

Para poder conectarse a una instancia de base de datos de RDS para Oracle que utilice la opción Oracle SSL, deberá configurar SQL*Plus antes de conectarse.

> **Note**
>
> Para permitir el acceso a la instancia de base de los clientes adecuados, asegúrese de que configuren los grupos de seguridad correctamente. Para obtener más información, consulte Control de acceso con grupos de seguridad. Estas instrucciones también son para SQL*Plus y otros clientes que usan directamente un sistema interno de Oracle. Para las conexiones JDBC, consulte Configuración de una conexión SSL a través de JDBC.

Para configurar SQL*Plus para que use SSL para conectarse a una instancia de base de datos de RDS para Oracle

1. Establezca la variable de entorno `ORACLE_HOME` en la ubicación del directorio principal de Oracle.

   La ruta al directorio principal de Oracle depende de cada instalación. En el ejemplo siguiente, se establece la variable de entorno `ORACLE_HOME`.

   ```
   prompt>export ORACLE_HOME=/home/user/app/user/product/19.0.0/dbhome_1
   ```

Para obtener más información sobre cómo establecer variables de entorno de Oracle, consulte SQL*Plus Environment Variables en la documentación de Oracle y vea además la guía de instalación de Oracle correspondiente a su sistema operativo.

2. Agregue `$ORACLE_HOME/lib` a la variable de entorno `LD_LIBRARY_PATH`.

   En el ejemplo siguiente, se establece la variable de entorno LD_LIBRARY_PATH.

   ```
   prompt>export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   ```

3. Cree un directorio para el wallet de Oracle en `$ORACLE_HOME/ssl_wallet`.

   En el ejemplo siguiente, se crea el directorio del wallet de Oracle.

   ```
   prompt>mkdir $ORACLE_HOME/ssl_wallet
   ```

4. Descargue el archivo de paquete de certificados .pem que funciona con todas las Regiones de AWS y coloque el archivo en el directorio ssl_wallet. Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

5. En el directorio `$ORACLE_HOME/network/admin`, modifique o cree el archivo `tnsnames.ora` e incluya la siguiente entrada.

   ```
   net_service_name =
     (DESCRIPTION =
       (ADDRESS_LIST =
         (ADDRESS =
           (PROTOCOL = TCPS)
           (HOST = endpoint)
           (PORT = ssl_port_number)
         )
       )
       (CONNECT_DATA =
         (SID = database_name)
       )
       (SECURITY =
         (SSL_SERVER_CERT_DN =
    "C=US,ST=Washington,L=Seattle,O=Amazon.com,OU=RDS,CN=endpoint")
       )
     )
   ```

6. En el mismo directorio, modifique o cree el archivo sqlnet.ora e incluya los siguientes parámetros.

> **Note**
>
> Para comunicarse con entidades a través de una conexión segura TLS, Oracle requiere un wallet con los certificados necesarios para la autenticación. Puede usar la utilidad ORAPKI de Oracle para crear y mantener los wallets de Oracle, tal y como se muestra en el paso 7. Para obtener más información, consulte Setting Up Oracle Wallet Using ORAPKI (Configuración de wallet de Oracle mediante ORAPKI) en la documentación de Oracle.

```
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY =
 $ORACLE_HOME/ssl_wallet)))
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 1.0
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA)
SSL_SERVER_DN_MATCH = ON
```

> **Note**
>
> Puede establecer `SSL_VERSION` en un valor superior si su instancia de base de datos es compatible.

7. Ejecute el siguiente comando para crear el wallet de Oracle.

```
prompt>orapki wallet create -wallet $ORACLE_HOME/ssl_wallet -auto_login_only
```

8. Extraiga cada certificado del archivo de paquete .pem en un archivo .pem independiente mediante una utilidad del sistema operativo.
9. Agregue cada certificado a su wallet mediante comandos `orapki` independientes y sustituya *`certificate-pem-file`* por el nombre absoluto del archivo .pem.

```
prompt>orapki wallet add -wallet $ORACLE_HOME/ssl_wallet -trusted_cert -cert
      certificate-pem-file -auto_login_only
```

Para obtener más información, consulte Rotar certificados SSL/TLS.

Conexión a una instancia de base de datos de RDS para Oracle mediante SSL

Después de configurar SQL*Plus para utilizar SSL tal como se ha descrito anteriormente, puede conectarse a la instancia de base de datos de RDS para Oracle con la opción SSL. Opcionalmente, puede primero exportar el valor `TNS_ADMIN` que apunta al directorio que contiene los archivos tnsnames.ora y sqlnet.ora. Si realiza este procedimiento, se asegurará de que SQL*Plus puede detectar estos archivos sistemáticamente. En el siguiente ejemplo se exporta el valor `TNS_ADMIN`.

```
export TNS_ADMIN = ${ORACLE_HOME}/network/admin
```

Conéctese a la instancia de base de datos. Por ejemplo, puede conectarse utilizando SQL*Plus y un *<net_service_name>* en un archivo tnsnames.ora.

```
sqlplus mydbuser@net_service_name
```

También puede conectar a la instancia de base de datos mediante SQL*Plus sin utilizar un archivo tnsnames.ora utilizando el siguiente comando.

```
sqlplus 'mydbuser@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCPS)(HOST = endpoint) (PORT
 = ssl_port_number))(CONNECT_DATA = (SID = database_name)))'
```

También puede conectarse a la instancia de base de datos de RDS para Oracle sin utilizar SSL. Por ejemplo, el siguiente comando se conecta a la instancia de base de datos a través del puerto de texto sin cifrar que no utiliza el cifrado SSL.

```
sqlplus 'mydbuser@(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = endpoint) (PORT
 = port_number))(CONNECT_DATA = (SID = database_name)))'
```

Si desea cerrar el acceso al puerto TCP (Protocolo de control de transmisión), cree un grupo de seguridad sin entradas de dirección IP y añádalo a la instancia. Esta adición cierra las conexiones a través del puerto TCP, pero permite las conexiones a través del puerto SSL que se realizan desde las direcciones IP incluidas en el rango permitido por el grupo de seguridad de la opción SSL.

Configuración de una conexión SSL a través de JDBC

Para utilizar una conexión SSL a través de JDBC, debe crear un almacén de claves, confiar en el certificado de CA raíz de Amazon RDS y utilizar el siguiente fragmento de código especificado.

Para crear el almacén de claves con formato JKS, puede utilizar el siguiente comando. Para obtener más información acerca de la creación del almacén de claves, consulte Creating a keystore en la documentación de Oracle. Para obtener información de referencia, consulte keytool en la Referencia de herramientas de la plataforma Java, edición estándar.

```
keytool -genkey -alias client -validity 365 -keyalg RSA -keystore clientkeystore
```

Siga estos pasos para confiar en el certificado de CA raíz de Amazon RDS.

Para confiar en el certificado de CA raíz de Amazon RDS

1. Descargue el archivo de paquete de certificados .pem que funciona con todas las Regiones de AWS y coloque el archivo en el directorio ssl_wallet.

   Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
2. Extraiga cada certificado del archivo .pem en un archivo independiente mediante una utilidad del sistema operativo.
3. Convierta cada certificado al formato .der mediante un comando `openssl` independiente y sustituya *`certificate-pem-file`* por el nombre del archivo .pem del certificado (sin la extensión .pem).

   ```
   openssl x509 -outform der -in certificate-pem-file.pem -out certificate-pem-file.der
   ```
4. Importe cada certificado al almacén de claves utilizando el siguiente comando.

   ```
   keytool -import -alias rds-root -keystore clientkeystore.jks -file certificate-pem-file.der
   ```

   Para obtener más información, consulte Rotar certificados SSL/TLS.
5. Confirme que el almacén de claves se haya creado correctamente.

   ```
   keytool -list -v -keystore clientkeystore.jks
   ```

   Especifique la contraseña del almacén de claves cuando se le solicite.

El siguiente ejemplo de código muestra cómo configurar la conexión SSL mediante JDBC.

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;
import java.util.Properties;

public class OracleSslConnectionTest {
    private static final String DB_SERVER_NAME = "dns-name-provided-by-amazon-rds";
    private static final Integer SSL_PORT = "ssl-option-port-configured-in-option-
group";
    private static final String DB_SID = "oracle-sid";
    private static final String DB_USER = "user-name";
    private static final String DB_PASSWORD = "password";
    // This key store has only the prod root ca.
    private static final String KEY_STORE_FILE_PATH = "file-path-to-keystore";
    private static final String KEY_STORE_PASS = "keystore-password";

    public static void main(String[] args) throws SQLException {
        final Properties properties = new Properties();
        final String connectionString = String.format(
                "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=%s)(PORT=
%d))(CONNECT_DATA=(SID=%s)))",
                DB_SERVER_NAME, SSL_PORT, DB_SID);
        properties.put("user", DB_USER);
        properties.put("password", DB_PASSWORD);
        properties.put("oracle.jdbc.J2EE13Compliant", "true");
        properties.put("javax.net.ssl.trustStore", KEY_STORE_FILE_PATH);
        properties.put("javax.net.ssl.trustStoreType", "JKS");
        properties.put("javax.net.ssl.trustStorePassword", KEY_STORE_PASS);
        final Connection connection = DriverManager.getConnection(connectionString,
 properties);
        // If no exception, that means handshake has passed, and an SSL connection can
 be opened
    }
}
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Obligatoriedad de la coincidencia del DN con una conexión SSL

Puede utilizar el parámetro de Oracle `SSL_SERVER_DN_MATCH` para hacer que sea obligatorio que el nombre distinguido (DN) del servidor de bases de datos coincida con su nombre de servicio. Si la verificación de coincidencia es obligatoria, SSL se asegura de que el certificado sea el del servidor. Si la verificación de coincidencia no es obligatoria, SSL realiza la comprobación, pero permite la conexión, independientemente de que haya o no una coincidencia. Si no se hace obligatoria la coincidencia, el servidor podría falsificar su identidad.

Para hacer obligatoria la coincidencia del DN, añada la propiedad de coincidencia del DN y utilice la cadena de conexión especificada a continuación.

Añada la propiedad a la conexión del cliente para hacer obligatoria la coincidencia del DN.

```
properties.put("oracle.net.ssl_server_dn_match", "TRUE");
```

Utilice la siguiente cadena de conexión para hacer obligatoria la coincidencia del DN al utilizar SSL.

```
final String connectionString = String.format(
    "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS)(HOST=%s)(PORT=%d))" +
    "(CONNECT_DATA=(SID=%s))" +
    "(SECURITY = (SSL_SERVER_CERT_DN =
\"C=US,ST=Washington,L=Seattle,O=Amazon.com,OU=RDS,CN=%s\")))",
    DB_SERVER_NAME, SSL_PORT, DB_SID, DB_SERVER_NAME);
```

Solución de problemas de las conexiones SSL

Puede consultar la base de datos y recibir el error `ORA-28860`.

```
ORA-28860: Fatal SSL error
28860. 00000 - "Fatal SSL error"
*Cause: An error occurred during the SSL connection to the peer. It is likely that this
 side sent data which the peer rejected.
*Action: Enable tracing to determine the exact cause of this error.
```

Este error se produce cuando el cliente intenta conectarse mediante una versión de TLS que el servidor no admite. Para evitar este error, edite sqlnet.ora y establezca `SSL_VERSION` en la versión de TLS correcta. Para obtener más información, consulte el documento de soporte de Oracle 2748438.1 en My Oracle Support.

Oracle Spatial

Amazon RDS admite Oracle Spatial mediante el uso de la opción `SPATIAL`. Oracle Spatial proporciona un esquema y funciones SQL que facilitan el almacenamiento, la recuperación, la actualización y la consulta de colecciones de datos espaciales en una base de datos de Oracle. Para obtener más información, consulte Spatial Concepts en la documentación de Oracle. Amazon RDS admite Oracle Spatial en todas las ediciones de todas las versiones compatibles.

Cómo funcionan las agrupaciones de revisiones espaciales (SPB)

Cada trimestre, RDS para Oracle lanza nuevas versiones de motor secundarias para cada motor principal compatible. Una versión de motor de actualización de revisión (RU) incorpora correcciones de errores de Oracle al incluir las revisiones de RU para el trimestre especificado. Una versión de motor de agrupación de revisiones espaciales (SPB) contiene revisiones de RU más revisiones específicas de Oracle Spatial. Por ejemplo, 19.0.0.0.ru-2025-01.spb-1.r1 es una versión de motor secundaria que contiene las revisiones RU en la versión de motor 19.0.0.0.ru-2025-01.rur-2025-01.r1 más revisiones espaciales. Las SPB solo son compatibles con Oracle Database 19c.

Las SPB funcionan de la misma manera que las RU, aunque se llaman de manera diferente. Una RU utiliza el formato de nomenclatura 19.0.0.0.ru-2025-01.rur-2025-01.r1. Un nombre de SPB incluye el texto “spb”, como en 19.0.0.0.ru-2025-01.spb-1.r1. Por lo general, una SPB se publica entre dos y tres semanas después de la RU trimestral correspondiente. Por ejemplo, 19.0.0.0.ru-2025-01.spb-1.r1 se publica después de 19.0.0.0.ru-2025-01.rur-2025-01.r1.

RDS para Oracle tiene rutas separadas para actualizaciones automáticas de versiones secundarias de las RU y SPB. Si la instancia de base de datos utiliza una RU, RDS la actualiza automáticamente a una RU. Si la instancia de base de datos utiliza una SPB, RDS la actualiza a una SPB. Cuando agrega la opción Oracle Spatial a la instancia de base de datos y habilita las actualizaciones automáticas, RDS coloca la instancia en la ruta de actualización para SPB.

Para obtener más información acerca de las RU y SPB, consulte Actualizaciones de la versión secundaria de Oracle. Para obtener una lista de las RU y SPB compatibles con Oracle Database 19c, consulte Amazon RDS para Oracle Database 19c (19.0.0.0) en Notas de la versión de Amazon RDS para Oracle.

Requisitos previos de Oracle Spatial

A continuación, se indican los requisitos previos para utilizar Oracle Spatial:

- Asegúrese de que su instancia de base de datos sea de una clase de instancia suficiente. Oracle Spatial no es compatible con las clases de instancia de base de datos db.t3.small. Para obtener más información, consulte Clases de instancias de base de datos de RDS para Oracle.
- Asegúrese de que su instancia de base de datos tiene habilitada la Actualización automática de la versión menor. Esta opción permite que la instancia de base de datos reciba actualizaciones de la versión secundaria del motor de base de datos automáticamente cuando estén disponibles y es necesaria para cualquier opción que instale la máquina virtual Java (JVM) de Oracle Amazon RDS utiliza esta opción para actualizar su instancia de base de datos a la PSU (Patch Set Update) de Oracle más reciente o actualización de la versión (RU). Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Prácticas recomendadas de Oracle Spatial

A continuación, se indican las prácticas recomendadas para utilizar Oracle Spatial:

- Para que la seguridad sea máxima, use la opción `SPATIAL` con Capa de conexión segura (SSL). Para obtener más información, consulte Capa de conexión segura de Oracle.
- Configure su instancia de base de datos para restringir el acceso a la misma. Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC y Uso de una instancia de base de datos en una VPC.

Adición de la opción Oracle Spatial

A continuación se muestra el proceso general para añadir la opción `SPATIAL` a una instancia de base de datos:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Si la máquina virtual Java (JVM) de Oracle no está instalada en la instancia de base de datos, se produce una breve interrupción mientras se agrega la opción `SPATIAL`. No hay interrupción si la máquina virtual Java (JVM) de Oracle ya está instalada en la instancia de base de datos. Después de añadir la opción , no es necesario reiniciar la instancia de base de datos. En cuanto esté activo el grupo de opciones, Oracle Spatial estará disponible.

> **Note**
>
> Durante esta interrupción, las funciones de verificación de contraseña se deshabilitan brevemente. También puede esperar ver eventos relacionados con las funciones de verificación de contraseña durante la interrupción. Las funciones de verificación de contraseña se vuelven a habilitar antes de que la instancia de base de datos de Oracle esté disponible.

Para añadir la opción **`SPATIAL`** a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine (Motor), elija la edición de Oracle que corresponda a la instancia de base de datos.

   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada la opción SPATIAL al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Eliminación de la opción Oracle Spatial

Después de eliminar todos los objetos que utilizan los tipos de datos proporcionados por la opción SPATIAL, puede eliminar la opción de una instancia de base de datos. Si la máquina virtual Java (JVM) de Oracle no está instalada en la instancia de base de datos, se produce una breve interrupción mientras se elimina la opción SPATIAL. No hay interrupción si la máquina virtual Java (JVM) de Oracle ya está instalada en la instancia de base de datos. Después de quitar la opción SPATIAL, no es necesario reiniciar la instancia de base de datos.

Para eliminar la opción **SPATIAL**

1. Haga una copia de seguridad de sus datos.

   > **Warning**
   >
   > Si la instancia utiliza tipos de datos habilitados como parte de la opción y si elimina la opción SPATIAL, puede perder datos. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

2. Compruebe si los objetos existentes hacen referencia a los tipos de datos o a las características de la opción SPATIAL.

   Si existen opciones SPATIAL, la instancia puede quedarse atascada al aplicar el nuevo grupo de opciones que no tiene la opción SPATIAL. Puede identificar los objetos mediante las siguientes consultas:

```
SELECT OWNER, SEGMENT_NAME, TABLESPACE_NAME, BYTES/1024/1024 mbytes
FROM   DBA_SEGMENTS
WHERE  SEGMENT_TYPE LIKE '%TABLE%'
AND    (OWNER, SEGMENT_NAME) IN
       (SELECT DISTINCT OWNER, TABLE_NAME
        FROM   DBA_TAB_COLUMNS
        WHERE  DATA_TYPE='SDO_GEOMETRY'
        AND    OWNER <> 'MDSYS')
ORDER BY 1,2,3,4;

SELECT OWNER, TABLE_NAME, COLUMN_NAME
FROM   DBA_TAB_COLUMNS
WHERE  DATA_TYPE = 'SDO_GEOMETRY'
AND    OWNER <> 'MDSYS'
```

```
ORDER BY 1,2,3;
```

3. Suelte los objetos que hagan referencia a los tipos de datos o a las características de la opción `SPATIAL`.
4. Aplique alguna de las siguientes acciones:

   - Quite la opción `SPATIAL` del grupo de opciones al que pertenece. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.
   - Modifique la instancia de base de datos y especifique otro grupo de opciones que no incluya la opción `SPATIAL`. Este cambio afecta a una única instancia de base de datos. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle SQLT

Amazon RDS admite Oracle SQLTXPLAIN (SQLT) mediante el uso de la opción SQLT. Puede utilizar SQLT con cualquier edición de Oracle Database 19c y versiones posteriores.

El enunciado `EXPLAIN PLAN` de Oracle puede determinar el plan de ejecución de una instrucción SQL. Puede verificar si el optimizador de Oracle elige un plan de ejecución determinado, como una combinación de bucles anidados. También le ayuda a comprender las decisiones del optimizador, p. ej. por qué elige una combinación de bucles anidados sobre una combinación hash. Así pues, `EXPLAIN PLAN` le ayuda a comprender el desempeño de la instrucción.

SQLT es una utilidad de Oracle que produce un informe. En el informe se incluyen estadísticas de objetos, metadatos de objetos, parámetros de inicialización relacionados con el optimizador y otra información que puede usar un administrador de base de datos para ajustar una instrucción SQL y obtener un desempeño óptimo. SQLT produce un informe HTML con hipervínculos a todas las secciones del informe.

A diferencia de los informes de Automatic Workload Repository o Statspack, SQLT funciona en instrucciones SQL individuales. SQLT es un conjunto de archivos SQL, PL/SQL y SQL*Plus que recopilan, almacenan y muestran datos de desempeño.

A continuación se encuentran las versiones compatibles de Oracle para cada versión de SQLT.

Versión de SQLT	Oracle Database 21c	Oracle Database 19c
2018-07-25.v1	Soportado	Soportado
2018-03-31.v1	No admitido	No admitido
2016-04-29.v1	No admitido	No admitido

Para descargar SQLT y acceder a sus instrucciones de uso, haga lo siguiente:

- Inicie sesión en su cuenta de My Oracle Support y abra los siguientes documentos:
- Para descargar SQLT: documento 215187.1
- Para obtener instrucciones de uso de SQLT: documento 1614107.1
- Para consultar las preguntas frecuentes acerca de SQLT: documento 1454160.1

- Para obtener información acerca de la lectura de la salida SQLT: documento 1456176.1
- Para interpretar el informe principal: documento 1922234.1

Amazon RDS no admite los siguientes métodos SQLT:

- `XPLORE`
- `XHUME`

Requisitos previos para SQLT

A continuación se indican los requisitos previos para utilizar SQLT:

- Debe quitar los usuarios y funciones requeridos por SQLT, si existen.

  La opción SQLT crea los siguientes usuarios y funciones en una instancia de base de datos:

  - `SQLTXPLAIN` usuario
  - `SQLTXADMIN` usuario
  - `SQLT_USER_ROLE` rol

  Si su instancia de base de datos tiene cualquiera de estos usuarios o funciones, inicie sesión en la instancia de base de datos mediante un cliente SQL y suéltelos mediante las siguientes instrucciones:

```
DROP USER SQLTXPLAIN CASCADE;
DROP USER SQLTXADMIN CASCADE;
DROP ROLE SQLT_USER_ROLE CASCADE;
```

- Debe quitar los espacios de tablas requeridos por SQLT, si existen.

  La opción SQLT crea los siguientes espacios de tablas en una instancia de base de datos:

  - `RDS_SQLT_TS`
  - `RDS_TEMP_SQLT_TS`

  Si su instancia de base de datos tiene estos espacios de tablas, inicie sesión en la instancia de base de datos mediante un cliente SQL y suéltelos.

Configuración de la opción SQLT

SQLT puede trabajar con características con licencia proporcionadas por los paquetes Oracle Tuning Pack y Oracle Diagnostics Pack. El paquete Oracle Tuning Pack incluye SQL Tuning Advisor, mientras que Oracle Diagnostics Pack incluye Automatic Workload Repository. La configuración de SQLT habilita o deshabilita el acceso a estas características desde SQLT.

Amazon RDS admite los siguientes valores para las opciones de SQLT.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
`LICENSE_PACK`	`T`, `D`, `N`	`N`	Los paquetes Oracle Management Pack a los que desea obtener acceso con SQLT. Escriba uno de los siguientes valores: • `T` indica que tiene una licencia de los paquetes Oracle Tuning Pack y Oracle Diagnostics Pack y que desea obtener acceso a SQL Tuning Advisor y Automatic Workload Repository desde SQLT. • `D` indica que tiene una licencia del paquete Oracle Diagnostics Pack y que desea obtener acceso a Automatic Workload Repository desde SQLT. • `N` indica que no tiene ninguna licencia de los paquetes Oracle Tuning Pack y Oracle Diagnostics Pack, o bien que tiene una licencia de uno de ellos o de ambos, pero que no desea que SQLT obtenga acceso a los mismos.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
			Note Amazon RDS no proporciona licencias para estos paquetes Oracle Management Pack. Si indica que desea usar un paquete que no se incluye en su instancia de base de datos, puede usar SQLT con la instancia de base de datos. Sin embargo, SQLT no puede obtener acceso al paquete y en el informe de SQLT no se incluyen los datos del mismo. Por ejemplo, si especifica T, pero la instancia de base de datos no incluye el paquete Oracle Tuning Pack, SQLT trabaja en la instancia de base de datos, pero el informe que genera no contiene datos relacionados con el paquete Oracle Tuning Pack.

Ajuste de la opción	Valores válidos	Valor predeterminado	Descripción
VERSION	2016-04-29.v1 2018-03-31.v1 2018-07-25.v1	2016-04-29.v1	La versión de SQLT que desea instalar. **Note** Para la base de datos Oracle 19c y 21c, la única versión compatible es 2018-07-25.v1 . Esta versión es la predeterminada para estas versiones.

Adición de la opción SQLT

A continuación se muestra el proceso general para añadir la opción SQLT a una instancia de base de datos:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción SQLT al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir la opción SQLT, esta se activará en cuanto se active el grupo de opciones.

Para añadir la opción SQLT a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:
   a. En Engine, elija la edición de Oracle que desea utilizar. La opción SQLT se admite en todas las ediciones.

b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

Para obtener más información, consulte Creación de un grupo de opciones.

2. Añada la opción SQLT al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

   - Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
4. (Opcional) Verifique la instalación de SQLT en cada instancia de base de datos con la opción SQLT.

   a. Use un cliente SQL para conectarse a la instancia de base de datos como usuario maestro.

   Para obtener información acerca de la conexión a su base de datos Oracle mediante un cliente SQL, consulte Conexión a una instancia de base de datos de Oracle.

   b. Ejecute la siguiente consulta:

```
SELECT sqltxplain.sqlt$a.get_param('tool_version') sqlt_version FROM DUAL;
```

   La consulta devuelve la versión actual de la opción SQLT en Amazon RDS. `12.1.160429` es un ejemplo de una versión de SQLT que está disponible en Amazon RDS.
5. Cambie las contraseñas de los usuarios que crea la opción SQLT.

   a. Use un cliente SQL para conectarse a la instancia de base de datos como usuario maestro.

   b. Ejecute la siguiente instrucción SQL para cambiar la contraseña del usuario `SQLTXADMIN`:

```
ALTER USER SQLTXADMIN IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

c. Ejecute la siguiente instrucción SQL para cambiar la contraseña del usuario `SQLTXPLAIN`:

```
ALTER USER SQLTXPLAIN IDENTIFIED BY new_password ACCOUNT UNLOCK;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

> **Note**
>
> La actualización de SQLT requiere la desinstalación de una versión anterior de SQLT para, a continuación, instalar la versión nueva. Así pues, todos los metadatos SQLT se pueden perder al actualizar SQLT. Una actualización de versión principal de una base de datos también desinstala y vuelve a instalar SQLT. Un ejemplo de una actualización de versión principal es una actualización de Oracle Database 19c a Oracle Database 21c.

Uso de SQLT

SQLT funciona con la utilidad Oracle SQL*Plus.

Para usar SQLT

1. Descargue el archivo .zip SQLT en el documento 215187.1 del sitio de My Oracle Support.

> **Note**
>
> No se puede descargar SQLT 12.1.160429 del sitio de My Oracle Support. Oracle ha retirado esta versión antigua.

2. Descomprima el archivo .zip SQLT.
3. En un símbolo del sistema, cambie al directorio `sqlt/run` de su sistema de archivos.
4. En el símbolo del sistema, abra SQL*Plus y conéctese a la instancia de base de datos como usuario maestro.

   Para obtener más información acerca de la conexión a una instancia de base de datos mediante SQL*Plus, consulte Conexión a una instancia de base de datos de Oracle.
5. Obtenga el ID de SQL de una instrucción SQL:

   ```
   SELECT SQL_ID FROM V$SQL WHERE SQL_TEXT='sql_statement';
   ```

   Su resultado es similar al siguiente:

   ```
   SQL_ID
   -------------
   chvsmttqjzjkn
   ```
6. Analice una instrucción SQL con SQLT:

   ```
   START sqltxtract.sql sql_id sqltxplain_user_password
   ```

   Por ejemplo, para el ID de SQL `chvsmttqjzjkn`, escriba lo siguiente:

   ```
   START sqltxtract.sql chvsmttqjzjkn sqltxplain_user_password
   ```

SQLT genera el informe HTML y recursos relacionados como un archivo .zip del directorio de ejecución del comando SQLT.

7. (Opcional) Para permitir a los usuarios de la aplicación diagnosticar instrucciones SQL con SQLT, conceda `SQLT_USER_ROLE` a cada usuario de la aplicación con la siguiente instrucción:

```
GRANT SQLT_USER_ROLE TO application_user_name;
```

> **Note**
>
> Oracle no recomienda ejecutar SQLT con el usuario `SYS` o con usuarios que tienen la función `DBA`. Es una práctica recomendada ejecutar SQLT Diagnostics mediante la cuenta del usuario de la aplicación, concediendo `SQLT_USER_ROLE` a este.

Actualización de la opción de SQLT

Con Amazon RDS for Oracle, puede actualizar la opción de SQLT de su versión existente a una versión superior. Para actualizar la opción de SQLT, complete los pasos 1–3 de Uso de SQLT para obtener la nueva versión de SQLT. Además, si concedió privilegios para la versión anterior de SQLT en el paso 7 de esa sección, vuelva a conceder los privilegios para la nueva versión de SQLT.

La actualización de la opción de SQLT da lugar a la pérdida de los metadatos de la versión más antigua de SQLT. El esquema y los objetos relacionados con la versión más antigua de SQLT se borran y se instala la versión más reciente de SQLT. Para obtener más información acerca de los cambios en la última versión de SQLT, consulte el documento 1614201.1 en el sitio de My Oracle Support.

> **Note**
>
> No se admiten las versiones de nivel inferior.

Modificación de la configuración de SQLT

Después de habilitar SQLT, puede modificar la configuración de `LICENSE_PACK` y `VERSION` de la opción.

Para obtener más información acerca de cómo modificar la configuración de las opciones, consulte Modificación de una configuración de opciones. Para obtener más información acerca de cada opción, consulte Configuración de la opción SQLT.

Eliminación de la opción de SQLT

Puede eliminar SQLT de una instancia de base de datos.

Para quitar SQLT de una instancia de base de datos, realice una de las siguientes operaciones:

- Para quitar SQLT de varias instancias de base de datos, quite la opción SQLT del grupo de opciones al que pertenecen las instancias de base de datos. Este cambio afecta a todas las instancias de base de datos que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.

- Para quitar SQLT de una única instancia de base de datos, modifique la instancia y especifique un grupo de opciones distinto que no incluya la opción SQLT. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Oracle Statspack

La opción Oracle Statspack instala y activa la característica de estadísticas de desempeño Oracle Statspack. Oracle Statspack es un conjunto de scripts SQL, PL/SQL y SQL*Plus que recopilan, almacenan y muestran datos de desempeño. Para obtener información acerca del uso de Oracle Statspack, consulte Oracle Statspack en la documentación de Oracle.

> **Note**
>
> Oracle ha dejado de dar soporte para Oracle Statspack y lo ha reemplazado por una característica más avanzada: Automatic Workload Repository (AWR). AWR solo está disponible para los clientes de Oracle Enterprise Edition que han adquirido el paquete de diagnósticos. Puede utilizar Oracle Statspack con cualquier motor de base de datos de Oracle en Amazon RDS. No puede ejecutar Oracle Statspack en réplicas de lectura de Amazon RDS.

Configuración de Oracle Statspack

Para ejecutar scripts Statspack, debe agregar la opción Statspack.

Para configurar Oracle Statspack

1. En un cliente SQL, inicie sesión en Oracle DB con una cuenta administrativa.
2. Realice una de las siguientes acciones, dependiendo de si Statspack está instalado:
   - Si Statspack está instalado y la cuenta `PERFSTAT` está asociada con Statspack, vaya al Paso 4.
   - Si Statspack no está instalado y la cuenta `PERFSTAT` existe, elimínela de la siguiente manera:

     ```
     DROP USER PERFSTAT CASCADE;
     ```

     De lo contrario, al intentar agregar la opción Statspack se genera un error y `RDS-Event-0058`.
3. Agregue la opción Statspack a un grupo de opciones. Consulte Agregar una opción a un grupo de opciones.

Amazon RDS instala de forma automática los scripts de Statspack en la instancia de base de datos y luego configura la cuenta PERFSTAT.

4. Restablezca la contraseña usando la siguiente instrucción SQL, reemplazando pwd por su nueva contraseña:

```
ALTER USER PERFSTAT IDENTIFIED BY pwd ACCOUNT UNLOCK;
```

Puede iniciar sesión con la cuenta de usuario PERFSTAT y ejecutar los scripts de Statspack.

5. Otorgue el privilegio CREATE JOB a la cuenta PERFSTAT mediante la siguiente instrucción:

```
GRANT CREATE JOB TO PERFSTAT;
```

6. Asegúrese de que los eventos de espera inactiva de la tabla PERFSTAT.STATS$IDLE_EVENT se rellenan.

Debido al error de Oracle 28523746, es posible que los eventos de espera inactiva en PERFSTAT.STATS$IDLE_EVENT no se rellenen. Para asegurarse de que todos los eventos inactivos están disponibles, ejecute la siguiente instrucción:

```
INSERT INTO PERFSTAT.STATS$IDLE_EVENT (EVENT)
SELECT NAME FROM V$EVENT_NAME WHERE WAIT_CLASS='Idle'
MINUS
SELECT EVENT FROM PERFSTAT.STATS$IDLE_EVENT;
COMMIT;
```

Generación de informes de Statspack

Un informe Statspack compara dos instantáneas.

Para generar informes de Statspack

1. En un cliente SQL, inicie sesión en Oracle DB con la cuenta de PERFSTAT.
2. Cree una instantánea utilizando cualquiera de las siguientes técnicas:
   - Cree manualmente una instantánea de Statspack.
   - Cree un trabajo que tome una instantánea de Statspack después de un intervalo de tiempo determinado. Por ejemplo, el trabajo siguiente crea una instantánea de Statspack cada hora:

```
VARIABLE jn NUMBER;
exec dbms_job.submit(:jn, 'statspack.snap;',SYSDATE,'TRUNC(SYSDATE
+1/24,''HH24'')');
COMMIT;
```

3. Vea las instantáneas mediante la siguiente consulta:

```
SELECT SNAP_ID, SNAP_TIME FROM STATS$SNAPSHOT ORDER BY 1;
```

4. Ejecute el procedimiento de Amazon RDS `rdsadmin.rds_run_spreport`, reemplazando begin_snap y end_snap por los ID de instantánea:

```
exec rdsadmin.rds_run_spreport(begin_snap,end_snap);
```

   Por ejemplo, el siguiente comando crea un informe basado en el intervalo entre las instantáneas 1 y 2 de Statspack:

```
exec rdsadmin.rds_run_spreport(1,2);
```

   El nombre de archivo del informe de Statspack incluye el número de las dos instantáneas. Por ejemplo, un archivo de informe creado con las instantáneas 1 y 2 de Statspack se llamaría `ORCL_spreport_1_2.lst`.

5. Monitorice la salida en busca de errores.

   Oracle Statspack realiza comprobaciones antes de ejecutar el informe. Por lo tanto, también puede ver mensajes de error en la salida del comando. Por ejemplo, puede intentar generar un informe basado en un rango no válido, donde el valor de instantánea de Statspack inicial es mayor que el valor final. En este caso, la salida muestra el mensaje de error, pero el motor de base de datos no genera un archivo de error.

```
exec rdsadmin.rds_run_spreport(2,1);
*
ERROR at line 1:
ORA-20000: Invalid snapshot IDs. Find valid ones in perfstat.stats$snapshot.
```

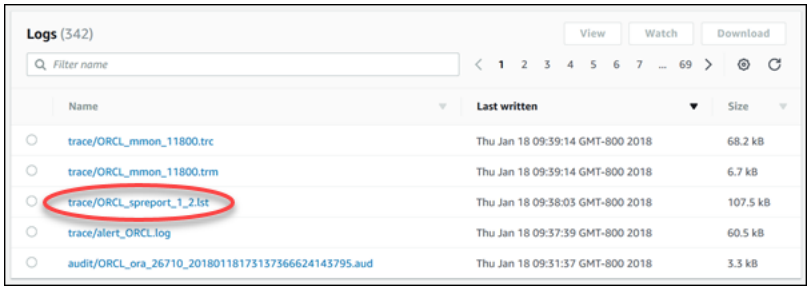
   Si utiliza un número no válido de instantánea de Statspack, la salida muestra un error. Por ejemplo, si intenta generar un informe para las instantáneas 1 y 50, pero la instantánea 50 no existe, el resultado muestra un error.

```
exec rdsadmin.rds_run_spreport(1,50);
*
ERROR at line 1:
ORA-20000: Could not find both snapshot IDs
```

6. (Opcional)

   Para recuperar el informe, llame a los procedimientos del archivo de seguimiento, como se explica en Uso de los archivos de seguimiento de Oracle.

   También puede descargar el informe de Statspack desde la consola de RDS. Vaya a la sección Registro de los detalles de la instancia de base de datos y elija Descargar: El siguiente ejemplo muestra `trace/ORCL_spreport_1_2.lst`



   Si hay un error al generar un informe, el motor de base de datos utiliza las mismas convenciones de nomenclatura que para un informe, pero con una extensión `.err`. Por ejemplo, si se produce un error al crear un informe con las instantáneas 1 y 7 de Statspack, el archivo de informe se denominaría `ORCL_spreport_1_7.err`. Puede descargar el informe de errores mediante las mismas técnicas que para un informe de instantáneas estándar.

Eliminación de instantáneas de Statspack

Para eliminar una variedad de instantáneas de Oracle Statspack, utilice el siguiente comando:

```
exec statspack.purge(begin snap, end snap);
```

Zona horaria Oracle

Puede usar la opción de zona horaria para cambiar la zona horaria del sistema empleada por la instancia de base de datos Oracle. Por ejemplo, puede cambiar la zona horaria de una instancia de base de datos para que sea compatible con un entorno on-premises o con una aplicación heredada. Esta opción cambia la zona horaria al nivel del host. El cambio de la zona horaria afecta a todas las columnas y valores de fecha, como `SYSDATE` y `SYSTIMESTAMP`.

La opción de zona horaria es distinta del comando `rdsadmin_util.alter_db_time_zone`. El comando `alter_db_time_zone` solo cambia la zona horaria para determinados tipos de datos. La opción de zona horaria afecta a todas las columnas y valores de fecha. Para obtener más información acerca de `alter_db_time_zone`, consulte Configuración de la zona horaria de la base de datos. Para obtener información acerca de las consideraciones de actualización, consulte Consideraciones sobre la zona horaria.

Restricciones para configurar la zona horaria

La opción de zona horaria es permanente y persistente. Por lo tanto, no puede hacer lo siguiente:

- Elimine la opción de un grupo de opciones después de agregar la opción de zona horaria.
- eliminar el grupo de opciones de una instancia de base de datos después de agregarlo
- cambiar el ajuste de zona horaria en la opción por una zona horaria distinta

Recomendaciones para configurar la zona horaria

Antes de añadir la opción de zona horaria a una base de datos de producción, le recomendamos que haga lo siguiente:

- Cree una instantánea de su instancia de base de datos. Si configura por accidente la zona horaria de forma incorrecta, debe devolver la instancia de base de datos a su configuración de zona horaria anterior. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
- Añada la opción de zona horaria a una instancia de base de datos de prueba. Al añadir la opción de zona horaria, puede haber problemas en las tablas que utilizan la fecha del sistema para sumar fechas u horas. Le recomendamos que analice sus datos y aplicaciones en la instancia de prueba. De esta forma, puede evaluar el impacto que puede tener cambiar la zona horaria en la instancia de producción.

Si su instancia de base de datos usa el grupo de opciones predeterminado, siga estos pasos:

1. Cree una instantánea de su instancia de base de datos.
2. Añada la opción de zona horaria a una instancia de base de datos.

Si su instancia de base de datos usa un grupo de opciones no predeterminado, siga estos pasos:

1. Cree una instantánea de su instancia de base de datos.
2. Cree un nuevo grupo de opciones.
3. Añada la opción de zona horaria junto con todas las demás opciones que estén asociadas actualmente al grupo de opciones existente.

   Esto evita que se desinstalen las opciones existentes y, al mismo tiempo, se habilita la opción de zona horaria.
4. Añada el grupo de opciones a la instancia de base de datos.

Configuración de la opción de zona horaria

Amazon RDS admite los siguientes valores para las opciones de zona horaria.

Ajuste de la opción	Valores válidos	Descripción
`TIME_ZONE`	Una de las zonas horarias disponibles. Puede consultar la lista completa e Zonas horarias disponibles.	Nueva zona horaria para la instancia de base de datos.

Adición de la opción de zona horaria

Siga los pasos indicados a continuación para agregar la opción de zona horaria a su instancia de base de datos:

1. (Recomendado) Cree una instantánea de su instancia de base de datos.
2. Realice una de las siguientes tareas siguientes:
   - Cree un nuevo grupo de opciones desde cero. Para obtener más información, consulte Creación de un grupo de opciones.

- Copie un grupo de opciones existente con la AWS CLI o la API. Para obtener más información, consulte Copia de un grupo de opciones.
- Reutilice un grupo de opciones existente que no sea predeterminado. Se recomienda utilizar un grupo de opciones que no esté asociado actualmente a ninguna instancia de base de datos o instantánea.

3. Agregue la nueva opción al grupo de opciones del paso anterior.
4. Si el grupo de opciones que está actualmente asociado a la instancia de base de datos tiene opciones habilitadas, agregue estas opciones al nuevo grupo de opciones. Esta estrategia evita que se desinstalen las opciones existentes y, al mismo tiempo, se habilita la nueva opción.
5. Añada el nuevo grupo de opciones a la instancia de base de datos.

Cuando se añade la opción de zona horaria, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente.

Consola

Adición de la opción de zona horaria a un grupo de opciones y asociarla a una instancia de base de datos

1. En la consola de RDS, elija Grupos de opciones.
2. Elija el nombre del grupo de opciones al que desea agregar la opción.
3. Elija Agregar opción.
4. En Nombre de la opción, elija Zona horaria y, a continuación, configure los ajustes de la opción.
5. Asocie el grupo de opciones a una instancia de base de datos nueva o ya existente:

   - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Cuando se agrega la nueva opción a una instancia de base de datos existente, se produce una breve interrupción mientras la instancia de base de datos se reinicia automáticamente. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

En el ejemplo siguiente, se usa el comando add-option-to-option-group de la AWS CLI para añadir la opción `Timezone` y la opción de configuración `TIME_ZONE` a un grupo de opciones denominado `myoptiongroup`. La zona horaria establecida es `Africa/Cairo`.

Para Linux, macOS o Unix:

```
aws rds add-option-to-option-group \
    --option-group-name "myoptiongroup" \
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=Africa/
Cairo}]" \
    --apply-immediately
```

Para Windows:

```
aws rds add-option-to-option-group ^
    --option-group-name "myoptiongroup" ^
    --options "OptionName=Timezone,OptionSettings=[{Name=TIME_ZONE,Value=Africa/
Cairo}]" ^
    --apply-immediately
```

Modificación de la configuración de la zona horaria

La opción de zona horaria es permanente y persistente. Una vez agregada a un grupo de opciones, no es posible retirarla de nuevo. Una vez agregado el grupo de opciones a una instancia de base de datos, no es posible retirarlo de nuevo. El valor de zona horaria de la opción no puede cambiarse por una zona horaria distinta. Si establece una zona horaria incorrecta, restaure una instantánea de la instancia de base de datos obtenida antes de añadir la opción de zona horaria.

Eliminación de la opción de zona horaria

La opción de zona horaria es permanente y persistente. Una vez agregada a un grupo de opciones, no es posible retirarla de nuevo. Una vez agregado el grupo de opciones a una instancia de base de datos, no es posible retirarlo de nuevo. Para eliminar la opción de zona horaria, restaure una instantánea de la instancia de base de datos obtenida antes de añadir la opción de zona horaria.

Zonas horarias disponibles

Los siguientes son los valores que pueden elegirse para la opción de zona horaria.

Zona	Time zone (Zona horarioa)
África	África/Casablanca, África/El Cairo, África/Harare, África/Lagos, África/Luanda, África/Monrovia, África/Nairobi, África/Trípoli, África/Windhoek
América	América/Araguaína, América/Argentina/Buenos_Aires, América/Asunción, América/Bogotá, América/Caracas, América/Chicago, América/Chihuahua, América/Cuiaba, América/Denver, América/Detroit, América/Fortaleza, América/Godthab, América/Guatemala, América/Halifax, América/Lima, América/Los_Ángeles, América/Manaos, América/Matamoros, América/Ciudad_de_México, América/Monterrey, América/Montevideo, América/Nueva_York, América/Phoenix, América/Santiago, América/São_Paulo, América/Tijuana, América/Toronto
Asia	Asia/Amán, Asia/Asjabad, Asia/Bagdad, Asia/Bakú, Asia/Bangkok, Asia/Beirut, Asia/Calcuta, Asia/Daca, Asia/Damasco, Asia/Ereván, Asia/Hong_Kong, Asia/Irkutsk, Asia/Jerusalén, Asia/Kabul, Asia/Karachi, Asia/Katmandú, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Magadán, Asia/Manila, Asia/Mascate, Asia/Novosibirsk, Asia/Rangún, Asia/Riad, Asia/Seúl, Asia/Shanghái, Asia/Singapur, Asia/Taipéi, Asia/Teherán, Asia/Tokio, Asia/Ulán_Bator, Asia/Vladivostok, Asia/Yakarta, Asia/Yakutsk
Atlántico	Atlántico/Azores, Atlántico/Cabo_Verde
Australia	Australia/Adelaida, Australia/Brisbane, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/Lord_Howe, Australia/Perth, Australia/Sídney
Brasil	Brasil/DeNoronha, Brasil/Este
Canadá	Canadá/Terranova, Canadá/Saskatchewan
etc	Etc/GMT-3
Europa	Europa/Ámsterdam, Europa/Atenas, Europa/Berlín, Europa/Dublín, Europa/Helsinki, Europa/Kaliningrado, Europa/Londres, Europa/Madrid, Europa/Moscú, Europa/París, Europa/Praga, Europa/Roma, Europa/Sarajevo

Zona	Time zone (Zona horarioa)
Pacífico	Pacífico/Apia, Pacífico/Auckland, Pacífico/Chatham, Pacífico/Fiyi, Pacífico/Guam, Pacífico/Honolulu, Pacífico/Kiritimati, Pacífico/Marquesas, Pacífico/Samoa, Pacífico/Tongatapu, Pacífico/Wake
EE. UU.	EE. UU./Alaska, EE. UU./Central, EE. UU./Indiana-Este, EE. UU./Este, EE. UU./Pacífico
UTC	UTC

Actualización automática del archivo de zona horaria de Oracle

Con la opción `TIMEZONE_FILE_AUTOUPGRADE`, puede actualizar el archivo de zona horaria actual a la versión más reciente de su instancia de base de datos de RDS for Oracle.

Temas

- Información general sobre los archivos de zona horaria de Oracle
- Estrategias para actualizar el archivo de zona horaria
- Tiempo de inactividad durante la actualización del archivo de zona horaria
- Preparación para actualizar el archivo de zona horaria
- Adición de la opción de actualización automática del archivo de zona horaria
- Verificación de los datos después de la actualización del archivo de zona horaria

Información general sobre los archivos de zona horaria de Oracle

Un archivo de zona horaria de Oracle Database almacena la siguiente información:

- Desfase con respecto a la hora universal coordinada (UTC)
- Horas de transición para el horario de verano (DST)
- Abreviaturas de hora estándar y DST

Oracle Database proporciona varias versiones de los archivos de zonas horarias. Cuando se crea una base de datos Oracle en un entorno local, se elige la versión del archivo de zona horaria. Para obtener más información, consulte Choosing a Time Zone File (Selección de un archivo de zona horaria) en la Oracle Database Globalization Support Guide (Guía de soporte de globalización de Oracle Database).

Si las reglas cambian en lo referente al DST, Oracle publica nuevos archivos de zona horaria. Oracle publica estos nuevos archivos de zona horaria con independencia del calendario de actualizaciones de versiones (RU) y revisiones de actualizaciones de versiones (RUR). Los archivos de zona horaria residen en el host de la base de datos en el directorio `$ORACLE_HOME/oracore/zoneinfo/`. Los nombres de archivo de zona horaria utilizan el formato DSTv *`version`*, como en DSTv35.

Cómo afecta el archivo de zona horaria a la transferencia de datos

En Oracle Database, el tipo de datos `TIMESTAMP WITH TIME ZONE` almacena datos de marca temporal y zona horaria. Datos con el tipo de datos `TIMESTAMP WITH TIME ZONE` utiliza las reglas

de la versión del archivo de zona horaria asociada. Por lo tanto, cuando se actualiza el archivo de zona horaria, eso afecta a los datos `TIMESTAMP WITH TIME ZONE` existentes.

Se pueden producir problemas al transferir datos entre bases de datos que utilizan diferentes versiones del archivo de zona horaria. Por ejemplo, si importa datos de una base de datos de origen con una versión de archivo de zona horaria más alta que la base de datos de destino, la base de datos devuelve el error `ORA-39405`. Anteriormente, tenía que evitar el error utilizando cualquiera de las siguientes técnicas:

- Crear una instancia de RDS para Oracle DB con el archivo de zona horaria deseado, exportar datos de la base de datos de origen y, a continuación, importarlos a la nueva base de datos.
- Usar AWS DMS o replicación lógica para migrar los datos.

Actualizaciones automáticas mediante la opción TIMEZONE_FILE_AUTOUPGRADE

Cuando el grupo de opciones adjunto a su instancia de base de datos de RDS para Oracle incluye la opción `TIMEZONE_FILE_AUTOUPGRADE`, RDS actualiza los archivos de zona horaria de manera automática. Al garantizar que las bases de datos de Oracle utilicen la misma versión del archivo de zona horaria, evita tener que recurrir a técnicas manuales que consumen mucho tiempo para mover datos entre diferentes entornos. Tanto las bases de datos de contenedores (CDB) como las que no lo son admiten la opción `TIMEZONE_FILE_AUTOUPGRADE`.

Al añadir la opción `TIMEZONE_FILE_AUTOUPGRADE` al grupo de opciones, puede elegir si desea añadir la opción inmediatamente o durante el período de mantenimiento. Una vez que la instancia de base de datos aplique la nueva opción, RDS comprueba si puede instalar un archivo de *`versión`* DSTv más reciente. La *`versión`* de DStv de destino depende de lo siguiente:

- La versión secundaria del motor que su instancia de base de datos está ejecutando actualmente
- La versión secundaria del motor a la que desea actualizar la instancia de base de datos

Por ejemplo, la versión actual del archivo de zona horaria podría ser DSTv33. Cuando RDS aplique la actualización al grupo de opciones, podría determinar que DSTv34 ya está disponible en su sistema de archivos de la instancia de base de datos. RDS actualizará entonces su archivo de zona horaria a DSTv34 de manera automática.

Para buscar las versiones de DST disponibles en las actualizaciones de las versiones de RDS compatibles, consulte las revisiones en Release notes for Amazon Relational Database Service (Amazon RDS) for Oracle (Notas de versión de Amazon Relational Database Service [Amazon

RDS] para Oracle). Por ejemplo, la versión 19.0.0.0.ru-2022-10.rur-2022-10.r1 incluye la revisión 34533061: RDBMS - DSTV39 UPDATE - TZDATA2022C.

Estrategias para actualizar el archivo de zona horaria

La actualización del motor de base de datos y la adición de la opción `TIMEZONE_FILE_AUTOUPGRADE` a un grupo de opciones son operaciones independientes. Al agregar la opción `TIMEZONE_FILE_AUTOUPGRADE`, se inicia la actualización del archivo de zona horaria si hay uno más actual disponible. Ejecute los siguientes comandos (solo se muestran las opciones relevantes) inmediatamente o en el siguiente período de mantenimiento:

- Actualice el motor de base de datos únicamente mediante el siguiente comando de la CLI de RDS:

```
modify-db-instance --engine-version name ...
```

- Para ello, agregue la opción `TIMEZONE_FILE_AUTOUPGRADE` únicamente mediante el siguiente comando de la CLI:

```
add-option-to-option-group --option-group-name name --options
 OptionName=TIMEZONE_FILE_AUTOUPGRADE ...
```

- Actualice el motor de base de datos y agregue un nuevo grupo de opciones a la instancia mediante el siguiente comando de la CLI:

```
modify-db-instance --engine-version name --option-group-name name ...
```

La estrategia de actualización depende de si desea actualizar la base de datos y el archivo de zona horaria de manera conjunta o realizar solo una de estas operaciones. Tenga en cuenta que si actualiza el grupo de opciones y, a continuación, el motor de base de datos en operaciones de API independientes, es posible que se esté realizando una actualización del archivo de zona horaria cuando actualice el motor de base de datos.

Los ejemplos de esta sección suponen lo siguiente:

- Aún no ha agregado `TIMEZONE_FILE_AUTOUPGRADE` al grupo de opciones asociado actualmente a su instancia de base de datos.
- Su instancia de base de datos utiliza la versión de base de datos 19.0.0.0.ru-2019-07.rur-2019-07.r1 y el archivo de zona horaria DSTv33.

- Su sistema de archivos de instancia de base de datos incluye el archivo DSTv34.
- La actualización de la versión 19.0.0.0.ru-2022-10.rur-2022-10.r1 incluye DSTv35.

Para actualizar el archivo de zona horaria, utilice las siguientes estrategias.

Temas

- Actualice el archivo de zona horaria sin actualizar el motor
- Actualice el archivo de zona horaria y la versión del motor de base de datos
- Actualice la versión del motor de base de datos sin actualizar el archivo de zona horaria.

Actualice el archivo de zona horaria sin actualizar el motor

En este escenario, la base de datos utiliza DSTv33, pero el sistema de archivos de instancias de base de datos dispone de DSTv34. Desea actualizar el archivo de zona horaria que utiliza la instancia de base de datos de DSTv33 a DSTv34, pero no desea actualizar el motor a una versión nueva secundaria, que incluye DSTv35.

En un comando `add-option-to-option-group`, agregue `TIMEZONE_FILE_AUTOUPGRADE` al grupo de opciones que utiliza su instancia de base de datos. Especifique si desea añadir la opción inmediatamente o aplazarlo hasta el período de mantenimiento. Tras aplicar la opción `TIMEZONE_FILE_AUTOUPGRADE`, RDS hace lo siguiente:

1. Comprueba si hay una nueva versión de DST.
2. Determina que el DSTv34 está disponible en el sistema de archivos.
3. Actualiza el archivo de zona horaria inmediatamente.

Actualice el archivo de zona horaria y la versión del motor de base de datos

En este escenario, la base de datos utiliza DSTv33, pero el sistema de archivos de instancias de base de datos dispone de DSTv34. Desea actualizar su motor de base de datos a la versión secundaria 19.0.0.0.ru-2022-10.rur-2022-10.r1, que incluye DSTv35, y actualizar su archivo de zona horaria a DSTv35 durante la actualización del motor. Por lo tanto, su objetivo es omitir DSTv34 y actualizar sus archivos de zona horaria directamente a DSTv35.

Para actualizar el motor y el archivo de zona horaria al mismo tiempo, ejecute `modify-db-instance` con las opciones `--option-group-name` y `--engine-version`. Puede ejecutar el comando inmediatamente o aplazarlo hasta el período de mantenimiento. `In --option-group-`

name, especifique un grupo de opciones que incluya la opción TIMEZONE_FILE_AUTOUPGRADE. Por ejemplo:

```
aws rds modify-db-instance
    --db-instance-identifier my-instance \
    --engine-version new-version \
    ----option-group-name og-with-timezone-file-autoupgrade \
    --apply-immediately
```

RDS comienza a actualizar su motor a 19.0.0.0.ru-2022-10.rur-2022-10.r1. Una vez aplicada la opción TIMEZONE_FILE_AUTOUPGRADE, RDS comprueba si hay una nueva versión de DST, ve que DSTv35 está disponible en 19.0.0.0.ru-2022-10.rur-2022-10.r1 e inicia inmediatamente la actualización a DSTv35.

Para actualizar el motor inmediatamente y, a continuación, actualizar el archivo de zona horaria, lleve a cabo las siguientes operaciones en esta secuencia:

1. Actualice el motor de base de datos únicamente mediante el siguiente comando de la CLI:

   ```
   aws rds modify-db-instance \
       --db-instance-identifier my-instance \
       --engine-version new-version \
       --apply-immediately
   ```

2. Agregue la opción TIMEZONE_FILE_AUTOUPGRADE al grupo de opciones adjunto a su instancia mediante el siguiente comando de la CLI:

   ```
   aws rds add-option-to-option-group \
       --option-group-name og-in-use-by-your-instance \
       --options OptionName=TIMEZONE_FILE_AUTOUPGRADE \
       --apply-immediately
   ```

Actualice la versión del motor de base de datos sin actualizar el archivo de zona horaria.

En este escenario, la base de datos utiliza DSTv33, pero el sistema de archivos de instancias de base de datos dispone de DSTv34. Desea actualizar su motor de base de datos a la versión 19.0.0.0.ru-2022-10.rur-2022-10.r1, que incluye DSTv35, pero retener el archivo de zona horaria DSTv33. Puede elegir esta estrategia por las razones siguientes:

- Sus datos no utilizan el tipo de datos TIMESTAMP WITH TIME ZONE.

- Sus datos utilizan el tipo de datos `TIMESTAMP WITH TIME ZONE`, pero los datos no se ven afectados por los cambios de zona horaria.
- Desea posponer la actualización del archivo de zona horaria porque no puede tolerar el tiempo de inactividad adicional.

La estrategia depende de cuál de las siguientes posibilidades se dé:

- Su instancia de base de datos no está asociada a un grupo de opciones que incluya `TIMEZONE_FILE_AUTOUPGRADE`. En su comando `modify-db-instance`, no especifique un nuevo grupo de opciones para que RDS no actualice el archivo de zona horaria.
- Su instancia de base de datos está asociada actualmente a un grupo de opciones que incluye `TIMEZONE_FILE_AUTOUPGRADE`. Dentro de un único comando `modify-db-instance`, asocie su instancia de base de datos a un grupo de opciones que no incluya `TIMEZONE_FILE_AUTOUPGRADE` y, a continuación, actualice su motor de base de datos a 19.0.0.0.ru-2022-10.rur-2022-10.r1.

Tiempo de inactividad durante la actualización del archivo de zona horaria

Cuando RDS actualiza el archivo de zona horaria, los datos que utiliza `TIMESTAMP WITH TIME ZONE` podrían cambiar. En este caso, su principal preocupación es el tiempo de inactividad.

> **Warning**
>
> Si añade la opción `TIMEZONE_FILE_AUTOUPGRADE`, la actualización del motor podría haber prolongado el tiempo de inactividad. La actualización de datos de zona horaria para una base de datos grande puede tardar horas o incluso días.

La duración de la actualización del archivo de zona horaria depende de factores como los siguientes:

- La cantidad de datos de `TIMESTAMP WITH TIME ZONE` de la base de datos
- La configuración de la instancia de la base de datos
- La clase de instancia de base de datos
- La configuración de almacenamiento
- La configuración de las bases de datos
- La configuración de parámetros de base de datos

Se puede producir un tiempo de inactividad adicional cuando hace lo siguiente:

- Añada la opción al grupo de opciones si la instancia de base de datos utiliza un archivo de zona horaria obsoleto
- Actualice el motor de base de datos Oracle cuando la nueva versión del motor contiene una nueva versión del archivo de zona horaria

> **Note**
>
> Durante la actualización del archivo de zona horaria, RDS para Oracle llama a `PURGE DBA_RECYCLEBIN`.

Preparación para actualizar el archivo de zona horaria

Una actualización de archivos de zona horaria tiene dos fases separadas: preparación y actualización. Si bien no es necesario, recomendamos encarecidamente que realice el paso de preparación. En este paso, descubrirá qué datos se verán afectados al ejecutar el procedimiento PL/SQL `DBMS_DST.FIND_AFFECTED_TABLES`. Para obtener más información sobre la ventana de preparación, consulte Actualización del archivo de zona horaria y la marca de hora con datos de zona horaria en la Documentación de la base de datos de Oracle.

Para preparar la actualización del archivo de zona horaria

1. Conecte el cliente SQL a la base de datos de Oracle utilizando el cliente SQL.
2. Determine la versión actual del archivo de zona horaria utilizada.

   ```
   SELECT * FROM V$TIMEZONE_FILE;
   ```

3. Determine la última versión del archivo de zona horaria disponible en su instancia de base de datos.

   ```
   SELECT DBMS_DST.GET_LATEST_TIMEZONE_VERSION FROM DUAL;
   ```

4. Determine el tamaño total de las tablas que tienen columnas de tipo `TIMESTAMP WITH LOCAL TIME ZONE` o `TIMESTAMP WITH TIME ZONE`.

   ```
   SELECT SUM(BYTES)/1024/1024/1024 "Total_size_w_TSTZ_columns_GB"
   ```

```
FROM   DBA_SEGMENTS
WHERE  SEGMENT_TYPE LIKE 'TABLE%'
AND    (OWNER, SEGMENT_NAME) IN
         (SELECT OWNER, TABLE_NAME
          FROM   DBA_TAB_COLUMNS
          WHERE  DATA_TYPE LIKE 'TIMESTAMP%TIME ZONE');
```

5. Determine los nombres y tamaños de los segmentos que tienen columnas de tipo `TIMESTAMP WITH LOCAL TIME ZONE` o `TIMESTAMP WITH TIME ZONE`.

```
SELECT OWNER, SEGMENT_NAME, SUM(BYTES)/1024/1024/1024
 "SEGMENT_SIZE_W_TSTZ_COLUMNS_GB"
FROM   DBA_SEGMENTS
WHERE  SEGMENT_TYPE LIKE 'TABLE%'
AND    (OWNER, SEGMENT_NAME) IN
         (SELECT OWNER, TABLE_NAME
          FROM   DBA_TAB_COLUMNS
          WHERE  DATA_TYPE LIKE 'TIMESTAMP%TIME ZONE')
GROUP BY OWNER, SEGMENT_NAME;
```

6. Ejecute el paso de preparación.

   - El procedimiento `DBMS_DST.CREATE_AFFECTED_TABLE` crea una tabla para almacenar cualquier dato afectado. Se pasa el nombre de esta tabla al procedimiento `DBMS_DST.FIND_AFFECTED_TABLES`. Para obtener más información, consulte el Procedimiento CREATE_AFFECTED_TABLE en la Documentación de la base de datos de Oracle.
   - Este procedimiento `CREATE_ERROR_TABLE` crea una tabla para registrar errores. Para obtener más información, consulte el Procedimiento CREATE_ERROR_TABLE en la Documentación de la base de datos de Oracle.

   En el siguiente ejemplo se crean los datos afectados y las tablas de errores, y se buscan todas las tablas afectadas.

```
EXEC DBMS_DST.CREATE_ERROR_TABLE('my_error_table')
EXEC DBMS_DST.CREATE_AFFECTED_TABLE('my_affected_table')

EXEC DBMS_DST.BEGIN_PREPARE(new_version);
EXEC DBMS_DST.FIND_AFFECTED_TABLES('my_affected_table', TRUE, 'my_error_table');
EXEC DBMS_DST.END_PREPARE;
```

```
SELECT * FROM my_affected_table;
SELECT * FROM my_error_table;
```

7. Consulte las tablas afectadas y de error.

```
SELECT * FROM my_affected_table;
SELECT * FROM my_error_table;
```

Adición de la opción de actualización automática del archivo de zona horaria

Al añadir la opción a un grupo de opciones, este se encuentra en uno de los siguientes estados:

- Actualmente hay un grupo de opciones asociado al menos a una instancia de base de datos. Al añadir la opción, todas las instancias de base de datos que utilizan este grupo de opciones se reinician automáticamente. Esto provoca una breve interrupción.
- No hay ningún grupo de opciones asociado a ninguna instancia de base de datos. Tiene previsto añadir la opción y, a continuación, asociar el grupo de opciones existente a las instancias de base de datos existentes o a una instancia de base de datos nueva.
- Crea un nuevo grupo de opciones y luego añade la opción. Tiene previsto asociar el nuevo grupo de opciones a instancias de base de datos ya existentes o a una nueva.

Consola

Para agregar la opción de actualización del archivo de zona horaria a una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Option groups (Grupos de opciones).
3. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

    a. En Engine (Motor), elija la edición de Oracle Database que corresponda a la instancia de base de datos.

    b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

Para obtener más información, consulte Creación de un grupo de opciones.

4. Elija el grupo de opciones que desea modificar y, a continuación, elija Add option (Agregar opción).
5. En la ventana Add option (Añadir opción), haga lo siguiente:
   a. Elija TIMEZONE_FILE_AUTOUPGRADE.
   b. Para habilitar la opción en todas las instancias de base de datos asociadas en cuanto la agregue, en Apply Immediately, elija Yes. Si elige No (valor predeterminado), la opción se habilita para cada instancia de base de datos asociada durante su siguiente período de mantenimiento.
6. Cuando los ajustes sean los deseados, elija Add Option (Agregar opción).

AWS CLI

En el ejemplo siguiente se usa el comando de la AWS CLI add-option-to-option-group para añadir la opción `TIMEZONE_FILE_AUTOUPGRADE` a un grupo de opciones llamado `myoptiongroup`.

Para Linux, macOS o:Unix

```
aws rds add-option-to-option-group \
    --option-group-name "myoptiongroup" \
    --options "OptionName=TIMEZONE_FILE_AUTOUPGRADE" \
    --apply-immediately
```

En:Windows

```
aws rds add-option-to-option-group ^
    --option-group-name "myoptiongroup" ^
    --options "OptionName=TIMEZONE_FILE_AUTOUPGRADE" ^
    --apply-immediately
```

Verificación de los datos después de la actualización del archivo de zona horaria

Le recomendamos que verifique los datos después de actualizar el archivo de zona horaria. Durante el paso de preparación, RDS para Oracle crea automáticamente las siguientes tablas:

- `rdsadmin.rds_dst_affected_tables`: enumera las tablas que contienen datos afectados por la actualización
- `rdsadmin.rds_dst_error_table`: muestra los errores generados durante la actualización

Estas tablas son independientes de las tablas que se crean en la ventana de preparación. Para ver los resultados de la actualización, consulte las tablas de la siguiente manera.

```
SELECT * FROM rdsadmin.rds_dst_affected_tables;
SELECT * FROM rdsadmin.rds_dst_error_table;
```

Para obtener más información sobre el esquema de los datos afectados y las tablas de errores, consulte el Procedimiento FIND_AFFECTED_TABLES en la documentación de Oracle.

Cifrado de datos transparente de Oracle

Amazon RDS es compatible con el cifrado de datos transparente (TDE) de Oracle, una característica de la opción Oracle Advanced Security disponible en Oracle Enterprise Edition. Esta característica cifra automáticamente los datos antes de que se escriban en el sistema de almacenamiento y los descifra automáticamente cuando se leen. Esta opción solo se admite el modelo “traiga su propia licencia” (BYOL).

El TDE es útil en situaciones en las que es necesario cifrar información confidencial por si un tercero obtiene los archivos de datos y las copias de seguridad. El TDE también es útil cuando se necesita cumplir con las normas relacionadas con la seguridad.

Esta guía no tiene el propósito de ofrecerle una descripción detallada del TDE en Oracle Database. Para obtener información, consulte los siguientes recursos de Oracle Database:

- Introducción al cifrado de datos transparente en la documentación de Oracle Database
- Oracle advanced security en la documentación de Oracle Database
- Oracle advanced security Transparent Data Encryption best practices, que es un documento técnico de Oracle

Para obtener más información acerca del uso del TDE con RDS para Oracle, consulte los siguientes blogs:

- Opciones de cifrado de bases de datos Oracle en Amazon RDS
- Migre una instancia de base de datos de Amazon RDS para Oracle multicuenta con TDE y reduzca el tiempo de inactividad mediante AWS DMS

Modos de cifrado de TDE

El cifrado de datos transparente de Oracle admite dos modos de cifrado: el cifrado de espacios de tabla de TDE y el cifrado de columnas de TDE. El cifrado de espacios de tabla de TDE se utiliza para cifrar tablas de aplicaciones completas. El cifrado de columnas de TDE se utiliza para cifrar elementos de datos individuales que contienen información confidencial. También es posible aplicar una solución de cifrado híbrida que utilice tanto el cifrado de espacios de tabla como el cifrado de columnas de TDE.

> **Note**
>
> Amazon RDS administra la clave maestra de TDE y de Oracle Wallet para la instancia de base de datos. No es necesario configurar la clave de cifrado con el comando `ALTER SYSTEM set encryption key`.

Una vez activada la opción `TDE`, puede comprobar el estado del wallet de Oracle mediante el siguiente comando:

```
SELECT * FROM v$encryption_wallet;
```

Para crear un espacio de tabla cifrado, utilice el siguiente comando:

```
CREATE TABLESPACE encrypt_ts ENCRYPTION DEFAULT STORAGE (ENCRYPT);
```

Para especificar el algoritmo de cifrado, utilice el comando siguiente:

```
CREATE TABLESPACE encrypt_ts ENCRYPTION USING 'AES256' DEFAULT STORAGE (ENCRYPT);
```

Las instrucciones anteriores para cifrar un espacio de tablas son las mismas que se utilizarían en una base de datos de Oracle en las instalaciones.

Restricciones para la opción TDE

La opción TDE es persistente y permanente. Después de asociar su instancia de base de datos con un grupo de opciones que tiene la opción TDE habilitada, no puede realizar las siguientes acciones:

- Deshabilitar la opción `TDE` en el grupo de opciones actualmente asociado.
- Asociar la instancia de base de datos a un grupo de opciones diferente que no incluya la opción `TDE`.
- Compartir una instantánea de base de datos que utilice la opción `TDE`. Para obtener más información sobre el uso compartido de instantáneas de base de datos, consulte Uso compartido de una instantánea manual de base de datos de Amazon RDS.

Para obtener más información sobre las opciones persistentes y permanentes, consulte Opciones permanentes y persistentes.

Determinación de si su instancia de base de datos utiliza TDE

Puede que quiera determinar si la instancia de base de datos está asociada a un grupo de opciones que tenga la opción TDE habilitada. Para ver el grupo de opciones al que está asociada una instancia de base de datos, utilice la consola de RDS, el comando describe-db-instance de la AWS CLI o la operación DescribeDBInstances de la API.

Adición de la opción TDE

Para agregar la opción TDE a su instancia de base de datos, siga los pasos que se describen a continuación:

1. (Recomendado) Cree una instantánea de su instancia de base de datos.
2. Realice una de las siguientes tareas siguientes:
   - Cree un nuevo grupo de opciones desde cero. Para obtener más información, consulte Creación de un grupo de opciones.
   - Copie un grupo de opciones existente con la AWS CLI o la API. Para obtener más información, consulte Copia de un grupo de opciones.
   - Reutilice un grupo de opciones existente que no sea predeterminado. Se recomienda utilizar un grupo de opciones que no esté asociado actualmente a ninguna instancia de base de datos o instantánea.
3. Agregue la nueva opción al grupo de opciones del paso anterior.
4. Si el grupo de opciones que está actualmente asociado a la instancia de base de datos tiene opciones habilitadas, agregue estas opciones al nuevo grupo de opciones. Esta estrategia evita que se desinstalen las opciones existentes y, al mismo tiempo, se habilita la nueva opción.
5. Añada el nuevo grupo de opciones a la instancia de base de datos.

Consola

Añadido de la opción TDE a un grupo de opciones y asociarla a su instancia de base de datos

1. En la consola de RDS, elija Grupos de opciones.
2. Elija el nombre del grupo de opciones al que desea agregar la opción.
3. Elija Agregar opción.
4. En Nombre de la opción, elija TDE y, a continuación, configure los ajustes de la opción.
5. Elija Agregar opción.

> **Important**
>
> Si agrega la opción TDE a un grupo de opciones existente que ya se ha adjuntado a una o varias instancias de base de datos, se producirá una breve interrupción mientras se reinician todas las instancias de base de datos.

Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.

6. Asocie el grupo de opciones a una instancia de base de datos nueva o ya existente:

   - Si se trata de una instancia de base de datos nueva, aplique el grupo de opciones al lanzar la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
   - Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. La instancia de base de datos no se reinicia como parte de esta operación. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

AWS CLI

En el ejemplo siguiente, se usa el comando de la AWS CLI add-option-to-option-group para añadir la opción TDE a un grupo de opciones llamado `myoptiongroup`. Para obtener más información, consulte Introducción: Flink 1.13.2 .

Para Linux, macOS o Unix:

```
aws rds add-option-to-option-group \
    --option-group-name "myoptiongroup" \
    --options "OptionName=TDE" \
    --apply-immediately
```

Para Windows:

```
aws rds add-option-to-option-group ^
    --option-group-name "myoptiongroup" ^
    --options "OptionName=TDE" ^
```

```
    --apply-immediately
```

Copia de los datos a una instancia de base de datos que no incluye la opción TDE

No puede eliminar la opción de TDE de una instancia de base de datos ni asociarla a un grupo de opciones que no incluya la opción de TDE. Para migrar los datos a una instancia que no incluya la opción de TDE, haga lo siguiente:

1. Descifre los datos en la instancia de base de datos.
2. Copie los datos en una nueva instancia de base de datos que no esté asociada a un grupo de opciones con la opción `TDE` habilitada.
3. Elimine la instancia de base de datos original.

Puede usar para la instancia nueva el mismo nombre que la instancia de base de datos anterior.

Consideraciones al usar TDE con Oracle Data Pump

Puede utilizar Oracle Data Pump para importar o exportar archivos de volcado cifrados. Amazon RDS admite el modo de cifrado de contraseñas (`ENCRYPTION_MODE=PASSWORD`) para Oracle Data Pump. Amazon RDS no admite el modo de cifrado transparente (`ENCRYPTION_MODE=TRANSPARENT`) para Oracle Data Pump. Para obtener más información, consulte Importación mediante Oracle Data Pump.

Oracle UTL_MAIL

Amazon RDS es compatible con Oracle UTL_MAIL mediante el uso de la opción UTL_MAIL y de servidores SMTP. Puede enviar un email directamente desde su base de datos mediante el paquete UTL_MAIL. Amazon RDS admite UTL_MAIL para las siguientes versiones de Oracle:

- Oracle Database 21c (21.0.0.0), todas las versiones
- Oracle Database 19c (19.0.0.0), todas las versiones

A continuación se indican algunas limitaciones que afectan al uso de UTL_MAIL:

- UTL_MAIL no es compatible con Transport Layer Security (TLS) y, por lo tanto, los mensajes de correo electrónico se cifran.

  Para conectarse de forma segura a recursos SSL/TLS remotos creando y cargando wallets de Oracle personalizados, siga las instrucciones que se proporcionan en Configuración del acceso UTL_HTTP mediante certificados y un wallet de Oracle..

  Los certificados específicos que se requieren para el wallet varían en función del servicio. Para los servicios de AWS, estos se puedan encontrar normalmente en el repositorio de Amazon Trust Services.
- UTL_MAIL no admite la autenticación con servidores SMTP.
- Solo se puede enviar un único archivo adjunto en un correo electrónico.
- No se pueden enviar archivos adjuntos de más de 32 K.
- Solo se pueden utilizar las codificaciones de caracteres ASCII y Extended Binary Coded Decimal Interchange Code (EBCDIC).
- El puerto SMTP (25) se limita en base a las políticas del propietario de la interfaz de red elástica.

Cuando se activa UTL_MAIL, solo se le concede el privilegio execute al usuario maestro de la instancia de base de datos. Si es necesario, el usuario maestro puede conceder el privilegio execute a otros usuarios para que puedan utilizar UTL_MAIL.

> **Important**
>
> Recomendamos que active la característica de auditoría integrada de Oracle para realizar un seguimiento del uso de los procedimientos de UTL_MAIL.

Requisitos previos para Oracle UTL_MAIL

A continuación se indican los requisitos previos para utilizar Oracle UTL_MAIL:

- Uno o varios servidores SMTP, con sus correspondientes direcciones IP o nombres de servidores de nombres de dominio (DNS) públicos o privados. Para obtener más información acerca de los nombres de DNS privados resueltos a través de un servidor DNS personalizado, consulte Configuración de un servidor DNS personalizado.

Adición de la opción Oracle UTL_MAIL

El proceso general para añadir la opción Oracle UTL_MAIL a una instancia de base de datos es el siguiente:

1. Cree un grupo de opciones nuevo o copie o modifique un grupo de opciones existente.
2. Añada la opción al grupo de opciones.
3. Asocie el grupo de opciones a la instancia de base de datos.

Después de añadir la opción UTL_MAIL, esta se activará en cuanto se active el grupo de opciones.

Para añadir la opción UTL_MAIL a una instancia de base de datos

1. Determine el grupo de opciones que desea utilizar. Puede crear un grupo de opciones o utilizar uno existente. Si desea utilizar un grupo de opciones existente, vaya al siguiente paso. De lo contrario, cree un grupo de opciones de base de datos personalizado con las siguientes opciones:

   a. En Engine, elija la edición de Oracle que desea utilizar.

   b. En Major engine version (Versión principal del motor), elija la versión de su instancia de base de datos.

   Para obtener más información, consulte Creación de un grupo de opciones.
2. Añada la opción UTL_MAIL al grupo de opciones. Para obtener más información acerca de la adición de opciones, consulte Agregar una opción a un grupo de opciones.
3. Aplique el grupo de opciones a una instancia de base de datos nueva o existente:

- Si se trata de una instancia de base de datos nueva, el grupo de opciones se aplica cuando se lanza la instancia. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para una instancia de base de datos existente, el grupo de opciones se aplica modificando la instancia y asociando el grupo de opciones nuevo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Uso de Oracle UTL_MAIL

Después de activar la opción UTL_MAIL, debe configurar el servidor SMTP para poder empezar a utilizarlo.

Puede configurar el servidor SMTP estableciendo el parámetro SMTP_OUT_SERVER como una dirección IP o como un nombre de DNS público válido. Para el parámetro SMTP_OUT_SERVER, puede especificar una lista separada por comas con las direcciones de varios servidores. Si el primer servidor no está disponible, UTL_MAIL intenta usar el servidor siguiente, y así sucesivamente.

Puede configurar el servidor SMTP predeterminado SMTP_OUT_SERVER para una instancia de base de datos mediante un grupo de parámetros de base de datos. Puede establecer el parámetro SMTP_OUT_SERVER para una sesión ejecutando el siguiente código en la base de datos mediante la instancia de base de datos.

```
ALTER SESSION SET smtp_out_server = mailserver.domain.com:25;
```

Después de activar la opción UTL_MAIL y configurar SMTP_OUT_SERVER, puede enviar un correo electrónico utilizando el procedimiento SEND. Para obtener más información, consulte UTL_MAIL en la documentación de Oracle.

Eliminación de la opción Oracle UTL_MAIL

Puede eliminar Oracle UTL_MAIL de una instancia de base de datos.

Para eliminar UTL_MAIL de una instancia de base de datos, realice una de las siguientes operaciones:

- Para eliminar UTL_MAIL de varias instancias de bases de datos, elimine la opción UTL_MAIL del grupo de opciones al que pertenecen. Este cambio afecta a todas las instancias de base de datos

que utilizan el grupo de opciones. Para obtener más información, consulte Quitar una opción de un grupo de opciones.

- Para eliminar UTL_MAIL de una única instancia de base de datos, modifique la instancia y especifique un grupo de opciones distinto que no incluya la opción UTL_MAIL. Puede especificar el grupo de opciones predeterminado (vacío) u otro grupo de opciones personalizado. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Solución de problemas

A continuación se indican los problemas que se puede encontrar al utilizar UTL_MAIL con Amazon RDS.

- Limitación controlada. El puerto SMTP (25) se limita en base a las políticas del propietario de la interfaz de red elástica. Si puede enviar correo electrónico correctamente utilizando UTL_MAIL y se muestra el error `ORA-29278: SMTP transient error: 421 Service not available`, es posible que esté aplicándose una limitación controlada. Si experimenta una limitación controlada en la entrega de correo electrónico, recomendamos implementar un algoritmo de retardo. Para obtener más información sobre los algoritmos de retroceso, consulte Reintentos de error y retroceso exponencial en AWS y la publicación sobre cómo manejar un error "throttling Maximum sending rate exceeded" (velocidad de envío de limitación controlada excedida).

  Puede solicitar que se elimine dicho límite. Para obtener más información, consulte ¿Cómo quito el límite en el puerto 25 de mi instancia EC2?

Oracle XML DB

Oracle XML DB añade soporte XML nativo a una instancia de base de datos. Con XML DB, puede almacenar y recuperar XML estructurado o no estructurado y datos relacionales. El protocolo de servidores de XML DB no se admite en RDS para Oracle.

XML DB está preinstalado en Oracle Database 12c y versiones posteriores. Por lo tanto, no es necesario utilizar un grupo de opciones para instalar explícitamente XML DB como característica adicional.

Para obtener información sobre cómo configurar y utilizar XML DB, consulte Oracle XML DB Developer's Guide en la documentación de Oracle Database.

Actualización del motor de base de datos de RDS para Oracle

Cuando Amazon RDS admite una nueva versión de Oracle Database, es posible actualizar sus instancias de bases de datos a la nueva versión. Para obtener información acerca de las versiones de Oracle disponibles en Amazon RDS, consulte las notas de la versión de Amazon RDS for Oracle.

> **Important**
>
> Ya no se admite RDS para Oracle Databases 11g, 12c y 18c. Si mantiene instantáneas de Oracle Database 11g, 12c o 18c, puede actualizarlas a una versión posterior. Para obtener más información, consulte Actualización de una instantánea de base de datos de Oracle.

Temas

- Información general sobre las actualizaciones del motor de RDS para Oracle
- Actualizaciones principales de versiones de Oracle
- Actualizaciones de la versión secundaria de Oracle
- Consideraciones de las actualizaciones de base de datos de Oracle
- Prueba de una actualización de base de datos de Oracle
- Actualización de la versión de una instancia de base de datos de RDS para Oracle
- Actualización de una instantánea de base de datos de Oracle

Información general sobre las actualizaciones del motor de RDS para Oracle

Antes de actualizar una instancia de base de datos de RDS para Oracle, es necesario familiarizarse con los siguientes conceptos clave.

Temas

- Actualizaciones de versiones principales y secundarias
- Fechas de soporte y actualizaciones obligatorias para RDS para Oracle
- Administración de versiones del motor de base de datos Oracle
- Instantáneas automáticas durante las actualizaciones de motor

- Actualizaciones de Oracle en una implementación Multi-AZ
- Actualizaciones de réplicas de lectura de Oracle

Actualizaciones de versiones principales y secundarias

Las versiones principales son las principales versiones de Oracle Database que se publican cada 1 o 2 años. Oracle Database 19c y Oracle 21c son versiones principales.

Cada trimestre, RDS para Oracle lanza nuevas versiones de motor secundarias para cada motor principal compatible. Una versión de motor de actualización de revisión (RU) incorpora correcciones de errores de Oracle al incluir las revisiones de RU para el trimestre especificado. Por ejemplo, 21.0.0.0.ru-2024-10.rur-2024-10.r1 es una versión secundaria de Oracle Database 21c que incorpora la RU de octubre de 2024.

Una versión de motor de agrupación de revisiones espaciales (SPB) contiene revisiones de RU y revisiones específicas de Oracle Spatial. Por ejemplo, 19.0.0.0.ru-2025-01.spb-1.r1 es una versión de motor secundaria que contiene las revisiones RU en la versión de motor 19.0.0.0.ru-2025-01.rur-2025-01.r1 más revisiones espaciales. Normalmente, RDS para Oracle lanza las SPB dos o tres semanas después de la RU correspondiente. Para obtener una explicación de las diferencias entre las RU y las SPB, consulte Actualizaciones de versión (RU) y agrupaciones de revisiones espaciales (SPB). Para obtener información sobre las RU y las SPB admitidas, consulte Notas de la versión de Amazon Relational Database Service (Amazon RDS) para Oracle.

RDS para Oracle admite las siguientes actualizaciones de una instancia de base de datos.

Tipo de actualización	Compatibilidad de las aplicaciones	Métodos de actualización	Ruta de actualización de ejemplo
Versión principal	Una actualización de versión principal puede introducir cambios que no sean compatibles con las aplicaciones existentes.	Solo manual	De Oracle Database 19c a Oracle Database 21c
Versión secundaria	Una actualización de una versión secundaria solo incluye cambios	Automática o manual	De 21.0.0.0.ru-2023-07.rur-2022-07.r1 a

Tipo de actualización	Compatibilidad de las aplicaciones	Métodos de actualización	Ruta de actualización de ejemplo
	compatibles con las versiones anteriores de las aplicaciones existentes.		21.0.0.0.ru-2023-10.rur-2022-10.r1

> **Important**
>
> Cuando actualiza el motor de base de datos, se produce una interrupción. La duración de la interrupción depende de la versión del motor y del tamaño de la instancia de la base de datos.
>
> Pruebe exhaustivamente cualquier actualización para comprobar que las aplicaciones funcionen correctamente antes de aplicar la actualización a sus bases de datos de producción. Para obtener más información, consulte Prueba de una actualización de base de datos de Oracle.

Fechas de soporte y actualizaciones obligatorias para RDS para Oracle

Las versiones de base de datos de RDS para Oracle tienen fechas de soporte previstas. Cuando una versión principal o secundaria de un motor de base de datos de RDS para Oracle se acerca a su fecha de fin de soporte, RDS inicia las actualizaciones obligatorias, también conocidas como actualizaciones forzadas. RDS publica la siguiente información:

- Una recomendación para que comience a actualizar manualmente las instancias de las versiones obsoletas a las versiones compatibles
- Una fecha a partir de la cual ya no se pueden crear instancias en las versiones no compatibles
- Una fecha en la que RDS comienza a actualizar automáticamente las instancias a las versiones compatibles durante los periodos de mantenimiento
- Una fecha en la que RDS comienza a actualizar automáticamente las instancias a las versiones compatibles fuera de los periodos de mantenimiento

> **Important**
>
> Las actualizaciones forzadas pueden tener consecuencias inesperadas para las pilas de AWS CloudFormation. Si confía en RDS para actualizar automáticamente las instancias de base de datos, es posible que encuentre problemas con AWS CloudFormation.

Esta sección contiene los siguientes temas:

Temas

- Fechas de soporte de las versiones principales de RDS para Oracle
- Fechas de soporte para versiones secundarias de RDS para Oracle

Fechas de soporte de las versiones principales de RDS para Oracle

Las versiones principales de RDS para Oracle seguirán estando disponibles al menos hasta la fecha de final de soporte para la versión correspondiente de Oracle Database. Puede utilizar las siguientes fechas para planificar sus ciclos de prueba y actualización. Estas fechas representan la fecha más temprana en la que podría requerirse una actualización a una versión más reciente. Si Amazon amplía la compatibilidad con una versión de RDS para Oracle durante más tiempo de lo previsto originalmente, esta tabla se actualizará para reflejar la fecha posterior.

> **Note**
>
> Puede ver las versiones principales de las bases de datos de Oracle ejecutando el comando describe-db-major-engine-versions de la AWS CLI o mediante la operación de la API de RDS DescribeDBMajorEngineVersions.

Versión principal de Oracle Database	Fecha prevista para la actualización a una versión más reciente
Oracle Database 19c	31 de diciembre de 2029 con soporte de BYOL Premier (no se aplican cargos para el soporte extendido) 31 de diciembre de 2032 con soporte extendido de BYOL (coste adicional) o un acuerdo de licencia ilimitada

Versión principal de Oracle Database	Fecha prevista para la actualización a una versión más reciente
	31 de diciembre de 2029 con licencia incluida (LI)
Oracle Database 21c	31 de julio de 2027 (no disponible para soporte extendido)

RDS le notifica al menos 12 meses antes de que necesite actualizar a una versión principal más reciente. La notificación describe el proceso de actualización, incluido el calendario de hitos importantes, el efecto en las instancias de base de datos y las acciones recomendadas. Le recomendamos que pruebe minuciosamente las aplicaciones con las nuevas versiones de RDS for Oracle antes de actualizar la base de datos a una versión principal.

Después de este período de notificación previa, podría aplicarse una actualización automática de la versión principal posterior a cualquier instancia base de datos de RDS para Oracle que aún esté ejecutando la versión anterior. Si es así, la actualización se inicia durante las ventanas de mantenimiento programadas.

Para obtener más información, consulte Release Schedule of Current Database Releases en My Oracle Support.

Fechas de soporte para versiones secundarias de RDS para Oracle

Las siguientes versiones secundarias de Oracle Database 19c se acercan a su fecha de fin de soporte:

- 19.0.0.0.ru-2019-07.rur-2019-07.r1
- 19.0.0.0.ru-2019-10.rur-2019-10.r1
- 19.0.0.0.ru-2020-01.rur-2020-01.r1

Las siguientes versiones secundarias de Oracle Database 21c se acercan a su fecha de fin de soporte:

- 21.0.0.0.ru-2022-01.rur-2022-01.r1
- 21.0.0.0.ru-2022-04.rur-2022-04.r1
- 21.0.0.0.ru-2022-07.rur-2022-07.r1
- 21.0.0.0.ru-2022-10.rur-2022-10.r1

- 21.0.0.0.ru-2023-01.rur-2023-01.r1
- 21.0.0.0.ru-2023-01.rur-2023-01.r2

La siguiente tabla muestra un cronograma de las actualizaciones obligatorias de las versiones secundarias anteriores que han quedado obsoletas.

Date	Acción para versiones obsoletas
02/07/2025	Ya no podrá crear instancias de base de datos que ejecuten versiones obsoletas. Actualice las instancias de base de datos manualmente a la última actualización de versión (RU) o espere a que RDS las actualice automátic amente.
01/08/25 – 15/09/25	RDS actualiza de forma forzada las instancias de base de datos en el periodo de mantenimiento programado a la última RU. RDS también actualiza las instancias restauradas a partir de instantáneas de las versiones obsoletas.
15/09/2025	RDS comienza a forzar la actualización de las instancias de base de datos a la última RU, independientemente de la ventana de mantenimiento programada. Las actualizaciones forzosas continúan hasta que todas las instancias ejecuten versiones secundarias compatibles.

Si no desea que RDS actualice automáticamente las instancias que ejecutan versiones obsoletas, haga lo siguiente:

- Actualice manualmente las versiones secundarias de Oracle Database 19c y 21c a la última RU o a cualquier RU que no esté programada para actualizaciones obligatorias. Por ejemplo, puede actualizar 21.0.0.0.ru-2023-01.rur-2023-01.r2 a 21.0.0.0.ru-2023-04.rur-2023-04.r2 o actualizar 19.0.0.0.ru-2019-07.rur-2019-07.r1 a 19.0.0.0.ru-2025-01.rur-2025-01.r2.
- Actualice las instantáneas de base de datos que utilizan versiones secundarias obsoletas y, a continuación, restaure las instantáneas.

Para obtener más información sobre versiones secundarias, consulte Notas de la versión de Amazon Relational Database Service (Amazon RDS) para Oracle.

Administración de versiones del motor de base de datos Oracle

Con la administración de versiones del motor de base de datos, se controla cuándo y cómo se parchea y actualiza el motor de base de datos. De esta manera, se obtiene la flexibilidad necesaria para mantener la compatibilidad con las versiones de parche del motor de base de datos. También puede probar nuevas versiones de parches de RDS para Oracle para asegurarse de que funcionan eficazmente con la aplicación antes de implementarlas en producción. Además, se actualizan las versiones según los términos y plazos de cada usuario.

> **Note**
>
> Amazon RDS agrega periódicamente los parches oficiales de Oracle Database utilizando una versión específica del motor de base de datos para Amazon RDS. Para ver una lista de los parches de Oracle incluidos en una versión específica del motor de base de datos de Amazon RDS Oracle, vaya a Notas de la versión de Amazon RDS for Oracle.

Instantáneas automáticas durante las actualizaciones de motor

Cuando se actualiza una instancia de base de datos de Oracle, las instantáneas ofrecen protección contra problemas de actualización. Si el período de retención de copia de seguridad de la instancia de base de datos es mayor que 0, Amazon RDS toma las siguientes instantáneas de base de datos durante la actualización:

1. Una instantánea de la instancia de base de datos antes de que se haya llevado a cabo ningún cambio. Si la actualización falla, puede restaurar esta instantánea para crear una instancia de base de datos que ejecute la versión anterior.
2. Una instantánea de la instancia de base de datos una vez finalizada la actualización.

> **Note**
>
> Para cambiar el periodo de retención de copia de seguridad, consulte Modificación de una instancia de base de datos de Amazon RDS.

Después de una actualización, no se puede volver a la versión anterior del motor. Sin embargo, se puede crear una nueva instancia de base de datos de Oracle restaurando la instantánea previa a la actualización.

Actualizaciones de Oracle en una implementación Multi-AZ

Si la instancia de base de datos está en una implementación Multi-AZ, Amazon RDS actualiza las réplicas principal y de reserva. Si no se requieren actualizaciones del sistema operativo, las actualizaciones principal y en espera se producen simultáneamente. Las instancias no estarán disponibles hasta que se complete la actualización.

Si se requieren actualizaciones del sistema operativo en una implementación Multi-AZ, Amazon RDS aplica las actualizaciones cuando solicite la actualización de la base de datos. Amazon RDS realiza los siguientes pasos:

1. Actualiza el sistema operativo en la instancia de base de datos de reserva actual.
2. Conmuta por error la instancia de base de datos principal a la instancia de base de datos de reserva.
3. Actualiza la versión de la base de datos en la nueva instancia principal de la base de datos, que antes era la instancia de reserva. La base de datos principal no está disponible durante la actualización.
4. Actualiza el sistema operativo en la nueva instancia de base de datos de reserva, que anteriormente era la instancia de base de datos principal.
5. Actualiza la versión de base de datos de la nueva instancia de base de datos de reserva.
6. Realiza una conmutación por error de la nueva instancia de base de datos principal a la instancia de base de datos principal original, y de la nueva instancia de base de datos de reserva a la instancia de base de datos de reserva original. Por lo tanto, Amazon RDS devuelve la configuración de réplica a su estado original.

Actualizaciones de réplicas de lectura de Oracle

La versión del motor de base de datos Oracle de la instancia de base de datos de origen y todas sus réplicas de lectura deben ser iguales. Amazon RDS realiza la actualización en las siguientes etapas:

1. Actualiza la instancia de base de datos de origen. Las réplicas de lectura están disponibles durante esta etapa.
2. Actualiza las réplicas de lectura en paralelo, independientemente del período de mantenimiento de las réplicas. La base de datos de origen está disponible durante esta etapa.

Para las actualizaciones de la versión principal de réplicas de lectura entre regiones, Amazon RDS realiza acciones adicionales:

- Genera automáticamente un grupo de opciones para la versión de destino
- Copia todas las opciones y configuraciones de opciones del grupo de opciones original al nuevo grupo de opciones
- Asocia la réplica de lectura entre regiones actualizada con el nuevo grupo de opciones

Actualizaciones principales de versiones de Oracle

Para realizar una actualización de versión principal, modifique la instancia de base de datos a mano. Las actualizaciones de la versión principal no se realizan automáticamente.

> **Important**
>
> Pruebe exhaustivamente cualquier actualización para comprobar que las aplicaciones funcionen correctamente antes de aplicar la actualización a sus bases de datos de producción. Para obtener más información, consulte Prueba de una actualización de base de datos de Oracle.

Temas

- Versiones compatibles para actualizaciones principales
- Clases de instancias admitidas para actualizaciones principales
- Recopilación de estadísticas antes de las actualizaciones principales
- Permiso para actualizaciones principales

Versiones compatibles para actualizaciones principales

Amazon RDS es compatible con las siguientes actualizaciones de versión principal.

Versión actual	Actualización compatible
19.0.0.0 con arquitectura CDB	21.0.0.0

La actualización de una versión principal de Oracle Database debe ser una actualización de versión (RU) publicada el mismo mes o posterior. No se puede actualizar a versiones inferiores de ninguna versión de Oracle Database.

Clases de instancias admitidas para actualizaciones principales

Su instancia de base de datos Oracle actual podría estar ejecutándose en una clase de instancia de base de datos no compatible con la versión a la que está actualizando. En este caso, antes de actualizar, migre la instancia de base de datos a una clase de instancia de base de datos compatible. Para obtener más información sobre las clases de instancias de base de datos compatibles para cada versión y edición de Amazon RDS for Oracle, consulte Clases de instancia de base de datos de .

Recopilación de estadísticas antes de las actualizaciones principales

Antes de realizar una actualización de versión principal, Oracle recomienda que recopile estadísticas del optimizador en la instancia de base de datos que esté actualizando. Esta acción puede reducir el tiempo de inactividad de la instancia de base de datos durante la actualización.

Para recopilar estadísticas del optimizador, conéctese a la instancia de base de datos como usuario maestro y ejecute el procedimiento `DBMS_STATS.GATHER_DICTIONARY_STATS`, como se muestra en el siguiente ejemplo.

```
EXEC DBMS_STATS.GATHER_DICTIONARY_STATS;
```

Para obtener más información, consulte GATHER_DICTIONARY_STATS Procedure en la documentación de Oracle.

Permiso para actualizaciones principales

Una actualización principal de la versión del motor es posible que sea incompatible con la aplicación. La actualización es irreversible. Si especifica una versión principal para el parámetro EngineVersion que sea diferente de la versión principal actual, debe permitir actualizaciones de versiones principales.

Si actualiza una versión principal mediante el comando de la interfaz de línea de comandos (CLI) modify-db-instance, especifique `--allow-major-version-upgrade`. Esta configuración no es persistente, por lo que debe especificar `--allow-major-version-upgrade` cada vez que realice una actualización principal. Este parámetro no afecta a las actualizaciones de versiones secundarias

del motor. Para obtener más información, consulte Actualización de una versión del motor de una instancia de base de datos.

Si actualiza una versión principal mediante la consola, no es necesario que elija una opción para permitir la actualización. En su lugar, la consola muestra una advertencia de que las actualizaciones principales son irreversibles.

Actualizaciones de la versión secundaria de Oracle

En RDS para Oracle, una actualización de versión secundaria es una actualización a una versión principal del motor de base de datos. En RDS, una versión secundaria del motor es una actualización de versión (RU) o una agrupación de revisiones espaciales (SPB). Por ejemplo, si la instancia de base de datos ejecuta la versión principal Oracle Database 21c y la versión secundaria 21.0.0.0.ru-2024-10.rur-2024-10.r1, puede actualizar el motor de base de datos a la versión secundaria 21.0.0.0.ru-2025-01.rur-2025-01.r1. RDS para Oracle no admite versiones secundarias de nivel inferior.

Puede actualizar su motor de base de datos a una versión secundaria de forma manual o automática. Para obtener información sobre cómo realizar la actualización de forma manual, consulte Actualización manual de la versión del motor. Para obtener información sobre cómo configurar las actualizaciones automáticas, consulte Actualización automática de la versión secundaria del motor. Tanto en la actualización manual o automática, la actualización de la versión secundaria implica un tiempo de inactividad. Tenga en cuenta este tiempo de inactividad cuando planifique las actualizaciones.

> **Important**
>
> Pruebe exhaustivamente cualquier actualización para comprobar que las aplicaciones funcionen correctamente antes de aplicar la actualización a sus bases de datos de producción. Para obtener más información, consulte Prueba de una actualización de base de datos de Oracle.

Temas

- Actualizaciones de versión (RU) y agrupaciones de revisiones espaciales (SPB)
- Activación de las actualizaciones automáticas de versiones secundarias para Oracle
- Notificación de actualizaciones de versiones secundarias automáticas en RDS para Oracle

- Cuando RDS programa actualizaciones automáticas de versiones secundarias en RDS para Oracle
- Administración de una actualización de versión secundaria automática en RDS para Oracle

Actualizaciones de versión (RU) y agrupaciones de revisiones espaciales (SPB)

En RDS, la actualización de versión (RU) es una versión de motor secundaria trimestral que incluye correcciones de seguridad, correcciones de errores y nuevas características para Oracle Database. Una agrupación de revisiones espaciales (SPB) es una versión de motor de RU que incluye revisiones diseñadas para la opción Oracle Spatial. Por ejemplo, la SPB denominada 19.0.0.0.ru-2025-01.spb-1.r1 incluye todas las revisiones de la RU correspondiente 19.0.0.0.ru-2025-01.rur-2025-01.r1, además de las revisiones específicas de Spatial. Las SPB solo son compatibles con Oracle Database 19c.

Cuando la instancia está configurada para actualizaciones automáticas de versiones secundarias, las RU y las SPB se encuentran en rutas de actualización separadas. Por lo general, una SPB se publica entre dos y tres semanas después de la RU correspondiente. En la siguiente tabla se muestra un ejemplo de versiones secundarias para Oracle Database 19c.

Ruta de actualización de RU estándar	Ruta de actualización de SPB
19.0.0.0.ru-2025-01.rur-2025-01.r1	19.0.0.0.ru-2025-01.spb-1.r1
19.0.0.0.ru-2025-04.rur-2025-04.r1	19.0.0.0.ru-2025-04.spb-1.r1
19.0.0.0.ru-2025-07.rur-2025-07.r1	19.0.0.0.ru-2025-07.spb-1.r1
19.0.0.0.ru-2025-10.rur-2025-10.r1	19.0.0.0.ru-2025-10.spb-1.r1

Si la instancia de base de datos está configurada para actualizaciones automáticas, la instancia se encuentra en la ruta de actualización correspondiente a la versión actual. Por ejemplo, si la instancia de base de datos ejecuta la versión 19.0.0.0.ru-2025-01.rur-2025-01.r1, cuando se publique la versión 19.0.0.0.ru-2025-04.rur-2025-04.r1, la instancia se actualizará automáticamente a esta RU. Del mismo modo, si la instancia de base de datos ejecuta 19.0.0.0.ru-2025-01.spb-1.r1, cuando se publique 19.0.0.0.ru-2025-04.spb-1.r1, la instancia se actualizará automáticamente a esta SPB. Una instancia que ejecute 19.0.0.0.ru-2025-01.rur-2025-01.r1, que es una RU, no se actualizará

automáticamente a 19.0.0.0.ru-2025-04.spb-1.r1, que es una SPB en una ruta de actualización independiente.

Puede actualizar la instancia de base de datos a las SPB incluso si la instancia no utiliza Spatial, pero las revisiones de Spatial se aplican solo a Oracle Spatial. Puede actualizar manualmente de una RU a una SPB con la misma versión de motor o superior. Por ejemplo, puede actualizar la instancia de 19.0.0.0.ru-2025-01.rur-2025-01.r1 a cualquiera de las siguientes versiones de motor:

- 19.0.0.0.ru-2025-01.spb-1.r1
- 19.0.0.0.ru-2025-04.spb-1.r1

Puede actualizar la instancia de SPB a RU solo si la RU es una versión de motor superior. Por ejemplo, puede actualizar de la SPB versión 19.0.0.0.ru-2025-04. spb-1.r1 a una versión de RU superior 19.0.0.0.ru-2025-07.rur-2025-07.r1, pero no a la misma versión de RU 19.0.0.0.ru-2025-04.rur-2025-04.r1.

Si la instancia de base de datos está configurada para actualizaciones automáticas de versiones secundarias y actualiza manualmente de una RU a una SPB o de una SPB a una RU, la ruta de actualización automática cambia. Suponga que actualiza manualmente de la RU versión 19.0.0.0.ru-2025-01.rur-2025-01.r1 a la SPB versión 19.0.0.0.ru-2025-01.spb-1.r1. La próxima actualización automática de versión secundaria será a la SPB versión 19.0.0.0.ru-2025-04.spb-1.r1.

Debido a que las SPB funcionan como las RU, las API de RDS para actualizar la instancia a las RU y SPB son idénticas. Los siguientes comandos muestran cómo actualizar a una RU y a una SPB.

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --engine-version 19.0.0.0.ru-2025-01.rur-2025-01.r1

aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --engine-version 19.0.0.0.ru-2025-01.spb-1.r1
```

Para obtener más información sobre la opción Oracle Spatial, consulte Cómo funcionan las agrupaciones de revisiones espaciales (SPB). Para obtener información sobre las RU y SPB compatibles con Oracle Database 19c, consulte Amazon RDS para Oracle Database 19c (19.0.0.0).

Activación de las actualizaciones automáticas de versiones secundarias para Oracle

En una actualización automática de la versión secundaria, RDS aplica la última versión secundaria disponible a la base de datos Oracle sin intervención manual. Una instancia de base de datos de Amazon RDS para Oracle programa la actualización durante el siguiente periodo de mantenimiento en las siguientes circunstancias:

- La instancia de base de datos tiene activada la opción Actualización automática de versión secundaria.
- La instancia de base de datos no está ejecutando ya la última versión secundaria del motor de base de datos.
- La instancia de base de datos no tiene programada ya una actualización pendiente.

Para obtener información sobre cómo activar las actualizaciones automáticas, consulte Actualización automática de la versión secundaria del motor.

Notificación de actualizaciones de versiones secundarias automáticas en RDS para Oracle

RDS publica una notificación anticipada antes de empezar a programar las actualizaciones automáticas. Encontrará la notificación en la pestaña Mantenimiento y copias de seguridad de la página de detalles de la base de datos. El mensaje tiene el siguiente formato:

```
An automatic minor version upgrade to engine version will become available
 on availability-date and will be applied during a subsequent maintenance window.
```

La *fecha de disponibilidad* del aviso anterior es la fecha en que RDS comienza a programar las actualizaciones de las instancias de base de datos de la Región de AWS. No es la fecha en la que está programada la actualización de la instancia de base de datos. Por ejemplo, si la *fecha de disponibilidad* es el 1 de marzo, en esa fecha RDS podría programar la actualización para el 14 de abril.

También puede obtener la fecha de disponibilidad de la actualización mediante el comando `describe-pending-maintenance-actions` de la AWS CLI, tal y como se muestra en el siguiente ejemplo:

```
aws rds describe-pending-maintenance-actions
```

```
{
    "PendingMaintenanceActions": [
        {
            "ResourceIdentifier": "arn:aws:rds:us-east-1:123456789012:db:orclinst1",
            "PendingMaintenanceActionDetails": [
                {
                    "Action": "db-upgrade",
                    "Description": "Automatic minor version upgrade to
 21.0.0.0.ru-2024-07.rur-2024-07.r1",
                    "CurrentApplyDate": "2024-12-02T08:10:00Z",
                    "OptInStatus": "next-maintenance"
                }
            ]
        }, ...
```

En la siguiente tabla se describen las opciones para cada tipo de mensaje de acción de mantenimiento pendiente.

Mensaje de acción de mantenimiento pendiente	Cuando aparece un mensaje	¿Cumple los requisitos para aplicarse al próximo período de mantenimiento?	¿Cumple los requisitos para aplicarse de forma inmediata?	¿Cumple con los requisitos para que se anule?
La actualización automática de la versión secundaria a la *versión del motor* estará disponible en la *fecha de disponibilidad* y deberá aplicarse durante un período de mantenimiento posterior.	De 4 a 6 semanas antes de que se programen las actualizaciones automáticas.	Sí	Sí	Sí
Actualización automática de la versión secundaria a la *versión del motor*	En la *fecha de disponibilidad* o	Sí	Sí	No

Mensaje de acción de mantenimiento pendiente	Cuando aparece un mensaje	¿Cumple los requisitos para aplicarse al próximo período de mantenimiento?	¿Cumple los requisitos para aplicarse de forma inmediata?	¿Cumple con los requisitos para que se anule?
	después. RDS aplica automáticamente esta actualización en el siguiente período de mantenimiento de la instancia de base de datos.			

Para obtener más información sobre describe-pending-maintenance-actions, consulte AWS CLI Command Reference (Referencia de comandos de la CLI).

Cuando RDS programa actualizaciones automáticas de versiones secundarias en RDS para Oracle

Cuando llegue la fecha de disponibilidad de las actualizaciones automáticas, RDS comenzará a programar las actualizaciones. En la mayoría de las Regiones de AWS, RDS programa su actualización a la última RU trimestral aproximadamente entre cuatro y seis semanas después de la fecha de disponibilidad. La fecha programada varía según la Región de AWS y otros factores. Para obtener más información sobre RU y RUR, consulte las notas de la versión de Amazon RDS para Oracle.

Cuando RDS programa la actualización, aparece la siguiente notificación en la pestaña Mantenimiento y copias de seguridad de la página de detalles de la base de datos:

```
Automatic minor version upgrade to engine-version
```

El mensaje anterior indica que RDS ha programado la actualización del motor de base de datos en el siguiente periodo de mantenimiento.

A veces, aparece una nueva versión secundaria antes de que RDS aplique una versión secundaria anterior. Por ejemplo, la instancia ejecuta la *versión secundaria 1* cuando la *versión secundaria 2* y la *versión secundaria 3* están disponibles como destinos de actualización. En esta situación, para evitar tiempos de inactividad innecesarios para las instancias de base de datos, RDS programa la actualización automática de la versión secundaria a la versión más reciente y omite la actualización a la versión anterior. En este ejemplo, RDS actualiza la instancia de la *versión secundaria 1* directamente a la *versión secundaria 3*.

Para garantizar una cierta frecuencia de actualizaciones de versiones secundarias, puede actualizar las instancias manualmente en lugar de utilizar el mecanismo de actualización automática. Para programar una actualización para el siguiente periodo de mantenimiento, especifique `--no-apply-immediately` cuando actualice a una versión secundaria mediante `modify-db-instance`. Para actualizar inmediatamente, especifique `--apply-immediately` en su lugar. Para obtener más información, consulte Actualización manual de la versión del motor.

Administración de una actualización de versión secundaria automática en RDS para Oracle

Cuando está disponible una nueva versión secundaria, puede actualizar su instancia de base de datos a esta versión manualmente. En el ejemplo siguiente, se actualiza inmediatamente la instancia de base de datos con el nombre `orclinst1`:

```
aws rds apply-pending-maintenance-action \
    --resource-identifier arn:aws:rds:us-east-1:123456789012:db:orclinst1 \
    --apply-action db-upgrade \
    --opt-in-type immediate
```

Para excluirse de una actualización automática de una versión secundaria que aún no se haya programado, configure `--opt-in-type` en `undo-opt-in` como en el siguiente ejemplo:

```
aws rds apply-pending-maintenance-action \
    --resource-identifier arn:aws:rds:us-east-1:123456789012:db:orclinst1 \
    --apply-action db-upgrade \
    --opt-in-type undo-opt-in
```

Si RDS ya ha programado una actualización de su instancia de base de datos, no puede utilizar `apply-pending-maintenance-action` para cancelarla. Sin embargo, puede modificar la instancia de base de datos y desactivar la característica de actualización secundaria automática, que cancela la programación de la actualización.

Para obtener información sobre cómo desactivar las actualizaciones automáticas, consulte Actualización automática de la versión secundaria del motor. Para obtener más información sobre apply-pending-maintenance-action, consulte AWS CLI Command Reference (Referencia de comandos de la CLI).

Consideraciones de las actualizaciones de base de datos de Oracle

Antes de actualizar la instancia de Oracle, lea la siguiente información.

Temas

- Consideraciones sobre Oracle Multitenant
- Consideraciones relativas al grupo de opciones
- Consideraciones relativas al grupo de parámetros
- Consideraciones sobre la zona horaria
- Consideraciones sobre la agrupación de revisiones espaciales (SPB)

Consideraciones sobre Oracle Multitenant

En la tabla siguiente se describen las arquitecturas de Oracle Database admitidas en las distintas versiones.

Versión de Oracle Database	Estado de compatibilidad de RDS	Arquitectura
Oracle Database 21c	Compatible	CDB solamente
Oracle Database 19c	Compatible	CDB o no CDB

En la tabla siguiente se describen las rutas de actualización admitidas y no admitidas.

Ruta de actualización	¿Se admite?
De CDB a CDB	Sí
De no CDB a CDB	No, pero se puede convertir de una que no sea CDB a una CDB y, a continuación, actualizarla

Ruta de actualización	¿Se admite?
De CDB a no CDB	No

Para obtener más información acerca de Oracle Multitenant en RDS para Oracle, consulte Configuración de un solo inquilino de la arquitectura CDB.

Consideraciones relativas al grupo de opciones

Si su instancia de base de datos utiliza un grupo de opciones personalizado, a veces, Amazon RDS no puede asignar automáticamente un nuevo grupo de opciones. Por ejemplo, esta situación ocurre cuando se actualiza a una nueva versión principal. En tales casos, especifique un nuevo grupo de opciones al actualizar. Recomendamos que cree un grupo de opciones nuevo y que le añada las mismas opciones que tiene el grupo de opciones personalizado existente.

Para obtener más información, consulte Creación de un grupo de opciones o Copia de un grupo de opciones.

Si la instancia de base de datos utiliza un grupo de opciones personalizado que contiene las opciones de `APEX` y `APEX-DEV`, a veces puede reducir el tiempo de actualización. Para ello, actualice la versión de Oracle APEX al mismo tiempo que la instancia de base de datos. Para obtener más información, consulte Actualización de la versión de Oracle APEX.

Consideraciones relativas al grupo de parámetros

Si la instancia de base de datos utiliza un grupo de parámetros personalizado, en algunos casos Amazon RDS no puede asignar a su instancia de base de datos un grupo de parámetros nuevo. Por ejemplo, esta situación ocurre cuando se actualiza a una nueva versión principal. En estos casos, asegúrese de especificar un nuevo grupo de parámetros al actualizar. Recomendamos que cree un grupo de parámetros nuevo y que configure en él los mismos parámetros que tiene el grupo de parámetros personalizado existente.

Para obtener más información, consulte Creación de un grupo de parámetros de base de datos en Amazon RDS o Copia de un grupo de parámetros de base de datos en Amazon RDS.

Consideraciones sobre la zona horaria

Puede usar la opción de zona horaria para cambiar la zona horaria del sistema empleada por la instancia de base de datos Oracle. Por ejemplo, puede cambiar la zona horaria de una instancia de

base de datos para que sea compatible con un entorno on-premises o con una aplicación heredada. Esta opción cambia la zona horaria al nivel del host. Amazon RDS for Oracle actualiza la zona horaria del sistema automáticamente durante el año. Para obtener más información sobre la zona horaria del sistema, consulte Zona horaria Oracle.

Al crear una instancia de base de datos de Oracle, la base de datos establece automáticamente la zona horaria de la base de datos. La zona horaria de la base de datos también se conoce como la zona horaria de horario de verano (DST). La zona horaria de la base de datos es distinta de la zona horaria del sistema.

Entre versiones de Oracle Database, juegos de parches o parches individuales pueden incluir nuevas versiones de DST. Estos parches reflejan los cambios en las reglas de transición para diversas regiones de zona horaria. Por ejemplo, un gobierno podría cambiar cuando entra en vigor el horario de verano. Los cambios en las reglas de DST pueden afectar a los datos existentes del tipo de datos `TIMESTAMP WITH TIME ZONE`.

Si actualiza una instancia de RDS for Oracle, Amazon RDS no actualiza automáticamente el archivo de zona horaria de la base de datos. Para actualizar automáticamente el archivo de zona horaria, puede incluir la opción `TIMEZONE_FILE_AUTOUPGRADE` en el grupo de opciones asociado a su instancia de base de datos durante o después de la actualización de la versión del motor. Para obtener más información, consulte Actualización automática del archivo de zona horaria de Oracle.

Alternativamente, para actualizar manualmente el archivo de zona horaria de la base de datos, cree una nueva instancia de base de datos de Oracle que tenga el parche de DST deseado. Sin embargo, le recomendamos que actualice el archivo de zona horaria de la base de datos con la opción `TIMEZONE_FILE_AUTOUPGRADE`.

Después de actualizar el archivo de zona horaria, migre los datos de la instancia actual a la nueva instancia. Puede migrar los datos mediante varias técnicas, entre las que se incluyen las siguientes:

- AWS Database Migration Service
- Oracle GoldenGate
- Oracle Data Pump
- Exportación e importación originales (no compatible para uso general)

> **Note**
>
> Al migrar datos mediante Oracle Data Pump, la utilidad genera el error ORA-39405 cuando la versión de zona horaria de destino es inferior a la versión de zona horaria de origen.

Para obtener más información, consulte TIMESTAMP WITH TIMEZONE Restrictions en la documentación de Oracle.

Consideraciones sobre la agrupación de revisiones espaciales (SPB)

En RDS para Oracle, la actualización de versión (RU) es una versión de motor secundaria que incluye correcciones de seguridad, correcciones de errores y nuevas características para Oracle Database. Una agrupación de revisiones espaciales (SPB) es una versión de motor secundaria que también incluye revisiones diseñadas para la opción Oracle Spatial. Por ejemplo, 19.0.0.0.ru-2025-01.spb-1.r1 es una versión de motor secundaria que contiene las revisiones RU en la versión de motor 19.0.0.0.ru-2025-01.rur-2025-01.r1 más revisiones espaciales.

Cuando actualice la base de datos a SPB, tenga en cuenta lo siguiente:

- Las SPB solo son compatibles con Oracle Database 19c.
- Por lo general, una SPB se publica entre dos y tres semanas después de la RU trimestral correspondiente.
- Puede actualizar la instancia de base de datos a una SPB incluso si la instancia no utiliza la opción Oracle Spatial, pero las revisiones espaciales de la versión de motor se aplican solo a Oracle Spatial. Puede crear una nueva instancia en una SPB e instalar la opción Oracle Spatial más adelante.
- Si habilita la actualización automática de la versión secundaria para la instancia de base de datos, la ruta de actualización dependerá de si la instancia utiliza actualmente una SPB o una RU. Si la instancia utiliza una SPB, RDS la actualiza automáticamente a la SPB más reciente. Si la instancia utiliza una RU, RDS la actualiza automáticamente a la RU más reciente.
- Puede actualizar manualmente la instancia de base de datos de una RU a una SPB solo si la SPB tiene la misma versión de motor o una superior a la de la RU actual.
- Puede actualizar manualmente la instancia de base de datos de SPB a RU solo si la RU es una versión superior.

Prueba de una actualización de base de datos de Oracle

Antes de realizar una actualización de versión principal en su instancia de base de datos, realice una comprobación exhaustiva de su base de datos y de todas las aplicaciones que tienen acceso a ella, para determinar la compatibilidad con la versión nueva. Le recomendamos que utilice el siguiente procedimiento.

Para probar una actualización de versión principal

1. Lea la documentación de actualización de Oracle de la nueva versión del motor de base de datos para ver si existen problemas de compatibilidad que pudieran afectar a su base de datos o sus aplicaciones. Para obtener más información, consulte la Database Upgrade Guide en la documentación de Oracle.
2. Si la instancia de base de datos utiliza un grupo de opciones personalizado, cree un grupo de opciones nuevo compatible con la versión nueva a la que va a actualizar. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.
3. Si la instancia de base de datos utiliza un grupo de parámetros personalizado, cree un grupo de parámetros nuevo compatible con la versión nueva a la que va a actualizar. Para obtener más información, consulte Consideraciones relativas al grupo de parámetros.
4. Cree una instantánea de base de datos de la instancia de base de datos que se va a actualizar. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.
5. Restaure la instantánea de base de datos para crear una nueva instancia de base de datos de prueba. Para obtener más información, consulte Restauración a una instancia de base de datos.
6. Modifique esta instancia de base de datos de prueba nueva para actualizarla a la nueva versión, utilizando uno de los siguientes métodos:

   - Consola
   - AWS CLI
   - API de RDS
7. Haga pruebas:

   - Ejecute tantas pruebas de control de calidad en la instancia de base de datos actualizada como necesite para asegurarse de que la base de datos y la aplicación funcionan correctamente con la versión nueva.

- Implemente las pruebas nuevas que sean necesarias para evaluar el impacto de cualquier problema de compatibilidad que haya identificado en el paso 1.
- Pruebe todos los procedimientos, las funciones y los disparadores.
- Dirija las versiones de prueba de sus aplicaciones a la instancia de base de datos actualizada. Compruebe que las aplicaciones funcionan correctamente con la versión nueva.
- Evalúe el almacenamiento utilizado por la instancia actualizada para determinar si la actualización necesita almacenamiento adicional. Es posible que deba cambiar a una clase de instancia más grande para admitir la nueva versión de producción. Para obtener más información, consulte Clases de instancia de base de datos de .

8. Si se superan todas las pruebas, actualice su instancia de base de datos de producción. Se recomienda que confirme que la instancia de base de datos funciona correctamente antes de permitir operaciones de escritura en la instancia de base de datos.

Actualización de la versión de una instancia de base de datos de RDS para Oracle

Para actualizar manualmente la versión del motor de base de datos de una instancia de base de datos de RDS para Oracle, puede utilizar la AWS Management Console, la AWS CLI o la API de RDS. Para obtener información general acerca de las actualizaciones de bases de datos, consulte Actualización de la versión de una instancia de base de datos de RDS para Oracle. Para obtener objetivos de actualización válidos, utilice el comando describe-db-engine-versions de la AWS CLI.

Consola

Actualización de la versión del motor de una instancia de base de datos de RDS para Oracle con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, elija la instancia de base de datos que desea actualizar.
3. Elija Modify.
4. Para la versión del motor de base de datos, elija una versión de base de datos superior.
5. Elija Continue (Continuar) y consulte el resumen de las modificaciones. Asegúrese de entender las implicaciones de actualizar una versión de base de datos. No puede convertir una instancia

de base de datos actualizada a la versión anterior. Asegúrese de haber probado la base de datos y la aplicación con la nueva versión antes de continuar.

6. Decida cuándo programar la actualización de la instancia de base de datos. Para aplicar los cambios inmediatamente, elija Apply immediately. Si se selecciona esta opción, puede producirse una interrupción en algunos casos. Para obtener más información, consulte Uso de la configuración de la programación de modificaciones.
7. En la página de confirmación, revise los cambios. Si son correctos, elija Modify DB instance (Modificar instancia de base de datos) para guardar los cambios.

   O bien, elija Back para editar los cambios o Cancel para cancelarlos.

AWS CLI

Para actualizar la versión del motor de una instancia de base de datos de RDS para Oracle, puede utilizar el comando modify-db-instance de la CLI. Especifique los siguientes parámetros:

- `--db-instance-identifier`: el nombre de la instancia de base de datos de RDS para Oracle.
- `--engine-version`: número de versión del motor de base de datos al que se va a actualizar.

  Para obtener información sobre versiones de motores válidas, utilice el comando describe-db-engine-versions de la AWS CLI.
- `--allow-major-version-upgrade`: para actualizar la versión del motor de base de datos.
- `--no-apply-immediately`–: para aplicar los cambios en el siguiente periodo de mantenimiento. Para aplicar los cambios inmediatamente, use `--apply-immediately`.

Example

En el siguiente ejemplo, se actualiza una instancia de CDB nombrada `myorainst` de su versión actual de `19.0.0.0.ru-2024-01.rur-2024-01.r1` a la versión `21.0.0.0.ru-2024-04.rur-2024-04.r1`.

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier myorainst \
    --engine-version 21.0.0.0.ru-2024-04.rur-2024-04.r1 \
    --allow-major-version-upgrade \
```

```
    --no-apply-immediately
```

En:Windows

```
aws rds modify-db-instance ^
    --db-instance-identifier myorainst ^
    --engine-version 21.0.0.0.ru-2024-04.rur-2024-04.r1 ^
    --allow-major-version-upgrade ^
    --no-apply-immediately
```

API de RDS

Para actualizar una instancia de base de datos de RDS para Oracle, utilice la acción ModifyDBInstance. Especifique los siguientes parámetros:

- `DBInstanceIdentifier` – nombre de la instancia de base de datos, por ejemplo *`myorainst`*.
- `EngineVersion`: número de versión del motor de base de datos al que se va a actualizar. Para obtener información sobre versiones de motores válidas, utilice la operación DescribeDBEngineVersions.
- `AllowMajorVersionUpgrade`: si se permite una actualización de versión principal. Para ello, defina el valor en `true`.
- `ApplyImmediately`: indica si se deben aplicar los cambios inmediatamente o en la siguiente ventana de mantenimiento. Para aplicar los cambios inmediatamente, establezca el valor en `true`. Para aplicar los cambios en el siguiente periodo de mantenimiento, establezca el valor en `false`.

Actualización de una instantánea de base de datos de Oracle

La actualización de las instantáneas de base de datos de Oracle en Amazon RDS garantiza que la base de datos siga siendo segura y totalmente compatible. A medida que las versiones anteriores de Oracle vayan dejando de recibir soporte de parches, podrá actualizar cualquier instantánea de base de datos manual vinculada a estas versiones para evitar posibles vulnerabilidades o limitaciones del servicio. Para obtener más información, consulte Administración de versiones del motor de base de datos Oracle.

Amazon RDS es compatible con la actualización de instancias en todas las Regiones de AWS.

Consola

Para actualizar una instantánea de base de datos de Oracle

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Snapshots y, a continuación, seleccione la instantánea de base de datos que desea actualizar.
3. En Actions (Acciones), seleccione Upgrade Snapshot (Actualizar instantánea). Aparece la página Upgrade snapshot.
4. Elija la Nueva versión del motor a la que actualizar la instantánea.
5. (Opcional) En Option group, elija el grupo de opciones para la instantánea de base de datos actualizada. Las mismas consideraciones del grupo de opciones se aplican al actualizar una instantánea de base de datos que al actualizar una instancia de base de datos. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.
6. Para guardar los cambios, elija Guardar cambios.

   Durante el proceso de actualización, todas las acciones están deshabilitadas para esta instantánea de base de datos. Además, el estado de la instantánea de base de datos cambia de available a upgrading y después cambia a active al completarse. Si la instantánea de base de datos no se puede actualizar porque se ha dañado, el estado cambia a unavailable. No puede recuperar el snapshot desde este estado.

   > **Note**
   >
   > Si la actualización de la base de datos falla, la instantánea se revierte al estado original con la versión original.

AWS CLI

Para actualizar una instantánea de base de datos de Oracle con la AWS CLI, llame al comando modify-db-snapshot con los siguientes parámetros:

- `--db-snapshot-identifier`: nombre de la instantánea de base de datos.
- `--engine-version`: versión a la que se va a actualizar la instantánea.

También puede ser necesario incluir el siguiente parámetro. Las mismas consideraciones del grupo de opciones se aplican al actualizar una instantánea de base de datos que al actualizar una instancia de base de datos. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.

- `--option-group-name`: grupo de opciones de la instantánea de base de datos actualizada.

Example

En el siguiente ejemplo se actualiza una instantánea de base de datos.

Para Linux, macOS o:Unix

```
aws rds modify-db-snapshot \
    --db-snapshot-identifier mydbsnapshot \
    --engine-version 19.0.0.0.ru-2020-10.rur-2020-10.r1 \
    --option-group-name default:oracle-se2-19
```

En:Windows

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier mydbsnapshot ^
    --engine-version 19.0.0.0.ru-2020-10.rur-2020-10.r1 ^
    --option-group-name default:oracle-se2-19
```

API de RDS

Para actualizar una instantánea de base de datos de Oracle con la API de Amazon RDS , llame a la operación ModifyDBSnapshot con los siguientes parámetros:

- `DBSnapshotIdentifier`: nombre de la instantánea de base de datos.
- `EngineVersion`: versión a la que se va a actualizar la instantánea.

Es posible que también deba incluir el parámetro `OptionGroupName`. Las mismas consideraciones del grupo de opciones se aplican al actualizar una instantánea de base de datos que al actualizar una instancia de base de datos. Para obtener más información, consulte Consideraciones relativas al grupo de opciones.

Uso de software de terceros con la instancia de base de datos de RDS for Oracle

Puede alojar una instancia de base de datos de RDS para Oracle que sea compatible con herramientas y software de terceros.

Temas

- Uso de Oracle GoldenGate con Amazon RDS para Oracle
- Uso de Oracle Repository Creation Utility en RDS para Oracle
- Configuración de Oracle Connection Manager en una instancia de Amazon EC2
- Instalación de una base de datos de Siebel en Oracle en Amazon RDS

Uso de Oracle GoldenGate con Amazon RDS para Oracle

Oracle GoldenGate recopila, replica y administra datos transaccionales entre bases de datos. Se trata de un paquete de software de replicación y de captura de datos de cambios (CDC, por sus siglas en inglés) basada en registros que se utiliza con bases de datos para sistemas de procesamiento de transacciones online (OLTP, por sus siglas en inglés). Oracle GoldenGate crea archivos de seguimiento que contienen los datos cambiados más recientes de la base de datos de origen. A continuación, envía estos archivos al servidor, donde un proceso convierte el archivo de seguimiento en SQL estándar para aplicarlo a la base de datos de destino.

Oracle GoldenGate con RDS para Oracle admite las siguientes características:

- Reproducción de bases de datos activa a activa
- Recuperación de desastres
- Protección de los datos
- Replicación dentro y fuera de la región
- Migración y actualizaciones sin tiempo de inactividad
- Replicación de datos entre una instancia de base de datos de RDS para Oracle y una base de datos que no es de Oracle

> **Note**
>
> Para obtener una lista de baSes de datos compatibles, consulte Oracle Fusion Middleware Supported System Configurations (Configuraciones de sistemas compatibles con Oracle Fusion Middleware) en la documentación de Oracle.

Puede usar Oracle GoldenGate con RDS para Oracle para actualizar a las principales versiones de base de datos de Oracle. Por ejemplo, puede usar Oracle GoldenGate para actualizar una base de datos Oracle Database 11g en las instalaciones a Oracle Database 19c en una instancia de base de datos de Amazon RDS.

Temas

- Versiones y opciones de licencia compatibles con Oracle GoldenGate
- Requisitos y limitaciones de Oracle GoldenGate
- Arquitectura de Oracle GoldenGate

- Configuración de Oracle GoldenGate
- Uso de las utilidades EXTRACT y REPLICAT de Oracle GoldenGate
- Supervisión de Oracle GoldenGate
- Solución de problemas de Oracle GoldenGate

Versiones y opciones de licencia compatibles con Oracle GoldenGate

Puede utilizar Standard Edition 2 (SE2) o Enterprise Edition (EE) de RDS para Oracle con Oracle GoldenGate versión 12c y posteriores. Puede utilizar las siguientes características de Oracle GoldenGate:

- Se admite la captura remota (extracción) de Oracle GoldenGate.
- Las instancias de base de datos de RDS para Oracle que utilizan la arquitectura de base de datos tradicional que no es de CDB admiten la captura (extracción). La captura de PDB remota de Oracle GoldenGate es compatible con las CDB que ejecuten Oracle Database 21c u Oracle Database 19c versión 19.0.0.0.ru-2024-04.rur-2024-04.r1 o superior.
- La entrega remota (replicación) de Oracle GoldenGate es compatible con instancias de bases de datos de RDS para Oracle que utilizan arquitecturas de CDB o que no son de CDB. La entrega remota admite las funciones Replicación integrada, Replicación paralela, Replicación coordenada y Replicación clásica.
- RDS para Oracle es compatible con las arquitecturas clásica y de microservicios de Oracle GoldenGate.
- Se admite la replicación de valores de Oracle GoldenGate DDL y Sequence cuando se utiliza el modo de captura integrado.

El usuario es responsable de administrar las licencias de GoldenGate (BYOL) para usarlas con Amazon RDS en todas las Regiones de AWS. Para obtener más información, consulte Opciones de licencias de RDS para Oracle.

Requisitos y limitaciones de Oracle GoldenGate

Cuando trabaje con Oracle GoldenGate y RDS para Oracle, tenga en cuenta los siguientes requisitos y limitaciones:

- Es responsable de configurar y administrar Oracle GoldenGate para usarlo con RDS para Oracle.

- Es responsable de configurar una versión de Oracle GoldenGate que esté certificada con las bases de datos de origen y destino. Para obtener más información, consulte Oracle Fusion Middleware Supported System Configurations (Configuraciones de sistemas compatibles con Oracle Fusion Middleware) en la documentación de Oracle.
- Puede utilizar Oracle GoldenGate en muchos entornos diferentes de AWS para muchos casos de uso diferentes. Si tiene algún problema relacionado con el soporte de Oracle GoldenGate, póngase en contacto con los servicios de soporte de Oracle.
- Puede utilizar Oracle GoldenGate en RDS para Oracle para instancias de base de datos de Oracle que utilicen el cifrado de datos transparente (TDE, por sus siglas en inglés) de Oracle. Para mantener la integridad de los datos replicados, configure el cifrado en el centro de Oracle GoldenGate con volúmenes cifrados de Amazon EBS o el cifrado de archivos de trazado. Configure también el cifrado de los datos enviados entre el centro de Oracle GoldenGate y las instancias de base de datos de origen y destino. Las instancias de base de datos de RDS for Oracle admiten el cifrado con Capa de conexión segura de Oracle o Oracle Native Network Encryption.

Arquitectura de Oracle GoldenGate

La arquitectura de Oracle GoldenGate para su uso con Amazon RDS consta de los siguientes módulos desacoplados:

Base de datos de origen

La base de datos de origen puede ser una base de datos de Oracle en las instalaciones, una base de datos de Oracle en una instancia de Amazon EC2 o una base de datos de Oracle en una instancia de base de datos de Amazon RDS.

Hub de Oracle GoldenGate

Un hub de Oracle GoldenGate mueve la información de las transacciones desde la base de datos de origen a la base de datos de destino. El hub puede ser cualquiera de los siguientes:

- Una instancia de Amazon EC2 con la base de datos de Oracle y con Oracle GoldenGate instalado
- Una instalación de Oracle en las instalaciones

Puede tener más de un hub de Amazon EC2. Le recomendamos que use dos hubs si utiliza Oracle GoldenGate para la replicación entre regiones.

Bases de datos de destino

La base de datos de destino puede residir en una instancia de base de datos de Amazon RDS, en una instancia Amazon EC2 o en una ubicación en las instalaciones.

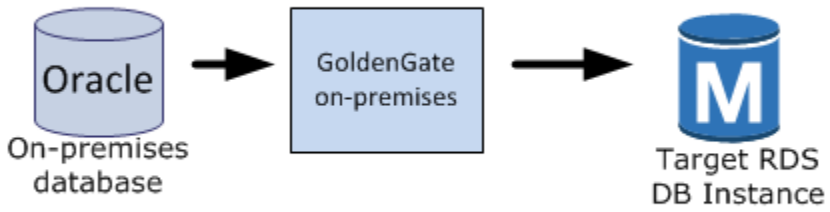
Las siguientes secciones describen escenarios comunes de Oracle GoldenGate en Amazon RDS.

Temas

- Base de datos de origen en las instalaciones y hub de Oracle GoldenGate
- Base de datos de origen en las instalaciones y hub de Amazon EC2
- Base de datos de origen de Amazon RDS y hub de Amazon EC2
- Base de datos de origen de Amazon EC2 y hub de Amazon EC2
- Hubs de Amazon EC2 en diferentes regiones de AWS

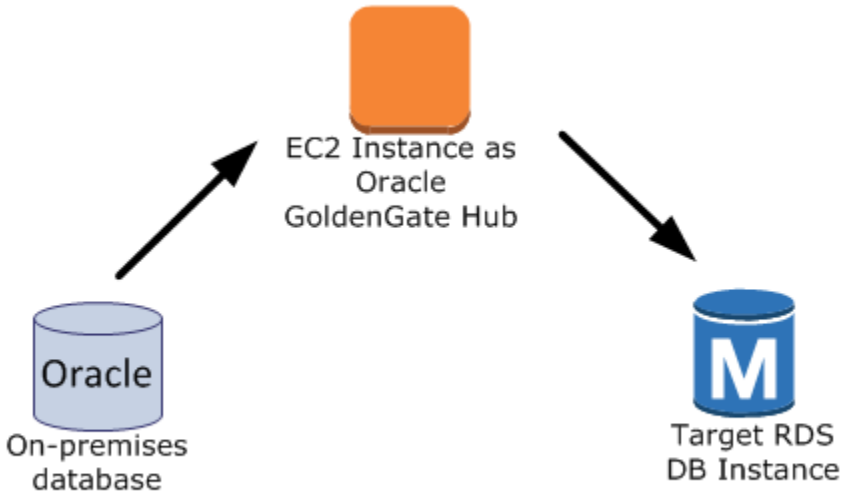
Base de datos de origen en las instalaciones y hub de Oracle GoldenGate

En este escenario, una base de datos de origen Oracle en las instalaciones y un hub de Oracle GoldenGate en las instalaciones proporcionan datos a una instancia de base de datos de Amazon RDS de destino.



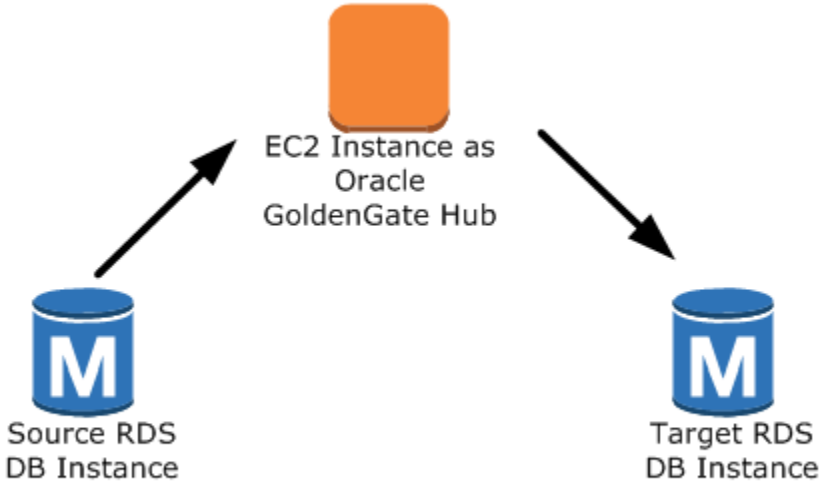
Base de datos de origen en las instalaciones y hub de Amazon EC2

En este escenario, una base de datos Oracle local actúa como base de datos de origen. Está conectada a un hub de instancias de Amazon EC2. Este hub proporciona datos a una instancia de base de datos RDS for Oracle de destino.



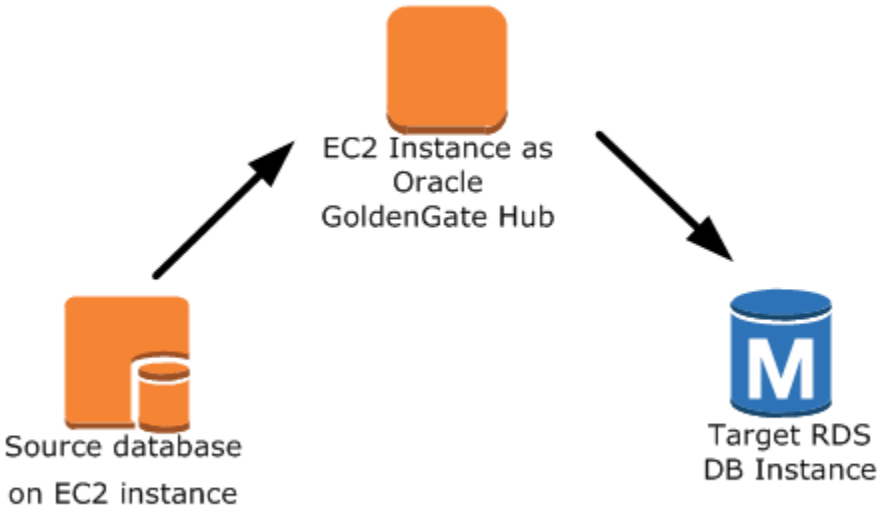
Base de datos de origen de Amazon RDS y hub de Amazon EC2

En este escenario, una instancia de base de datos RDS for Oracle actúa como base de datos de origen. Está conectada a un hub de instancia de Amazon EC2. Este hub proporciona datos a una instancia de base de datos RDS for Oracle de destino.



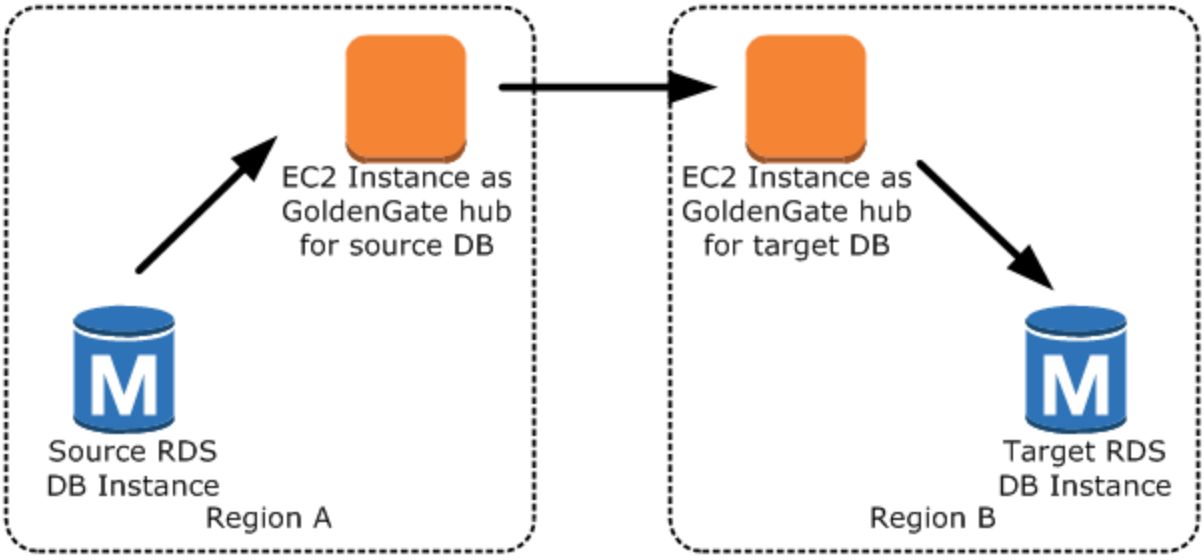
Base de datos de origen de Amazon EC2 y hub de Amazon EC2

En este escenario, una base de datos Oracle en una instancia de Amazon EC2 actúa como base de datos de origen. Está conectada a un hub de instancia de Amazon EC2. Este hub proporciona datos a una instancia de base de datos RDS for Oracle de destino.



Hubs de Amazon EC2 en diferentes regiones de AWS

En este escenario, una base de datos Oracle en una instancia de base de datos de Amazon RDS está conectada a un hub de instancias de Amazon EC2 en la misma región de AWS. El hub está conectado a un hub de instancias de Amazon EC2 en una región de AWS diferente. Este segundo hub proporciona datos a la instancia de base de datos de RDS for Oracle de destino en la misma región de AWS que el segundo hub de instancias de Amazon EC2.



> **Note**
>
> Cualquier problema que afecte a la ejecución de Oracle GoldenGate en un entorno en las instalaciones también afecta a la ejecución de Oracle GoldenGate en AWS. Le recomendamos que supervise el hub de Oracle GoldenGate para asegurarse de que `EXTRACT` y `REPLICAT` se reanudan si se produce una conmutación por error. Dado que el hub de Oracle GoldenGate se ejecuta en una instancia de Amazon EC2, Amazon RDS no administra el hub de Oracle GoldenGate y no puede garantizar que se esté ejecutando.

Configuración de Oracle GoldenGate

Para configurar Oracle GoldenGate mediante Amazon RDS, tiene que configurar el hub en la instancia de Amazon EC2 y, a continuación, configurar las bases de datos de origen y de destino. Las siguientes secciones muestran un ejemplo de cómo configurar Oracle GoldenGate para usarlo con Amazon RDS para Oracle.

Temas

- Configuración de un hub de Oracle GoldenGate en Amazon EC2
- Configuración de una base de datos de origen para usarla con Oracle GoldenGate en Amazon RDS
- Configuración de una base de datos de destino para Oracle GoldenGate en Amazon RDS

Configuración de un hub de Oracle GoldenGate en Amazon EC2

Para crear un hub de Oracle GoldenGate en una instancia de Amazon EC2, cree en primer lugar una instancia de Amazon EC2 con una instalación completa de cliente de Oracle DBMS. La instancia de Amazon EC2 también debe tener instalado el software GoldenGate de Oracle. Las versiones del software de Oracle GoldenGate dependen de las versiones de la base de datos de origen y destino. Para obtener más información acerca de la instalación de Oracle GoldenGate, consulte la documentación de Oracle GolgenGate.

La instancia de Amazon EC2 que actúa de hub de Oracle GoldenGate almacena y procesa la información de las transacciones de la base de datos de origen a los archivos de trazado. Para admitir este proceso, asegúrese de que cumpla los siguientes requisitos:

- Haber asignado suficiente espacio de almacenamiento para los archivos de seguimiento.

- La instancia de Amazon EC2 tiene suficiente potencia de procesamiento para administrar la cantidad de datos.
- La instancia EC2 tiene suficiente memoria para almacenar la información de transacción antes de que se escriba en el archivo de seguimiento.

Para configurar un hub de arquitectura clásica de Oracle GoldenGate en una instancia Amazon EC2

1. Cree los subdirectorios en el directorio de Oracle GoldenGate.

   En el shell de la línea de comandos de Amazon EC2, lance `ggsci`, el intérprete del comando de Oracle GoldenGate. El comando `CREATE SUBDIRS` crea subdirectorios bajo el directorio `/gg` para los archivos de parámetros, informes y puntos de comprobación.

   ```
   prompt$ cd /gg
   prompt$ ./ggsci

   GGSCI> CREATE SUBDIRS
   ```

2. Configure el archivo `mgr.prm`.

   El siguiente ejemplo añade líneas al archivo `$GGHOME/dirprm/mgr.prm`.

   ```
   PORT 8199
   PurgeOldExtracts ./dirdat/*, UseCheckpoints, MINKEEPDAYS 5
   ```

3. Inicie el administrador.

   En el siguiente ejemplo se lanza `ggsci` y se ejecuta el comando `start mgr`.

   ```
   GGSCI> start mgr
   ```

El hub de Oracle GoldenGate ya se puede utilizar.

Configuración de una base de datos de origen para usarla con Oracle GoldenGate en Amazon RDS

Complete las siguientes tareas para configurar una base de datos de origen con el fin de utilizarla con Oracle GoldenGate.

Pasos de configuración

- Paso 1: activar el registro suplementario en la base de datos de origen
- Paso 2: establecer el parámetro de inicialización ENABLE_GOLDENGATE_REPLICATION en verdadero
- Paso 3: establecer el período de retención del registro en la base de datos de origen
- Paso 4: crear una cuenta de usuario de Oracle GoldenGate en la base de datos de origen
- Paso 5: conceder privilegios al usuario en la base de datos de origen
- Paso 6: agregar un alias de TNS para la base de datos de origen

Paso 1: activar el registro suplementario en la base de datos de origen

Para activar el registro suplementario mínimo en el nivel de la base de datos, ejecute el siguiente procedimiento PL/SQL:

```
EXEC rdsadmin.rdsadmin_util.alter_supplemental_logging(p_action => 'ADD')
```

Paso 2: establecer el parámetro de inicialización ENABLE_GOLDENGATE_REPLICATION en verdadero

Al establecer el parámetro de inicialización `ENABLE_GOLDENGATE_REPLICATION` en `true`, permite que los servicios de bases de datos admitan la replicación lógica. Si la base de datos de origen está en una instancia de base de datos de Amazon RDS, asegúrese de asignar un grupo de parámetros a dicha instancia de base de datos con el parámetro de inicialización `ENABLE_GOLDENGATE_REPLICATION` establecido en `true`. Para obtener más información acerca del parámetro de inicialización `ENABLE_GOLDENGATE_REPLICATION`, consulte la documentación de la base de datos de Oracle.

Paso 3: establecer el período de retención del registro en la base de datos de origen

Asegúrese de configurar la base de datos de origen para retener los registros redo archivados. Tenga en cuenta estas directrices:

- Especifique la duración de la retención de registros en horas. El valor mínimo es una hora.
- Establezca la duración de manera que supere cualquier posible periodo de inactividad de la instancia de base de datos de origen, cualquier posible periodo de comunicación y cualquier posible periodo de problemas de red para dicha instancia de origen. Dicha duración permite a Oracle GoldenGate recuperar registros de la instancia de origen según sea necesario.
- Asegúrese de que dispone de suficiente almacenamiento en la instancia para los archivos.

Por ejemplo, establezca el período de retención para los registros REDO archivados en 24 horas.

```
EXEC rdsadmin.rdsadmin_util.set_configuration('archivelog retention hours',24)
```

Si no tiene la retención de registros habilitada, o bien si el valor de retención es demasiado pequeño, recibirá un mensaje de error similar al siguiente.

```
2022-03-06 06:17:27  ERROR   OGG-00446  error 2 (No such file or directory)
opening redo log /rdsdbdata/db/GGTEST3_A/onlinelog/o1_mf_2_9k4bp1n6_.log for sequence
 1306
Not able to establish initial position for begin time 2022-03-06 06:16:55.
```

Dado que la instancia de base de datos conserva los registros redo archivados, asegúrese de tener suficiente espacio para los archivos. Para ver cuánto espacio ha utilizado en las últimas *num_hours* horas, utilice la siguiente consulta, sustituyendo *num_hours* por el número de horas.

```
SELECT SUM(BLOCKS * BLOCK_SIZE) BYTES FROM V$ARCHIVED_LOG
   WHERE NEXT_TIME>=SYSDATE-num_hours/24 AND DEST_ID=1;
```

Paso 4: crear una cuenta de usuario de Oracle GoldenGate en la base de datos de origen

Oracle GoldenGate se ejecuta como usuario de base de datos y requiere los privilegios de base de datos apropiados para obtener acceso a los registros redo y redo archivados para la base de datos de origen. Para proporcionarlos, cree una cuenta de usuario en la base de datos de origen. Para obtener más información sobre los permisos para una cuenta de usuario de Oracle GoldenGate, consulte la documentación de Oracle.

Las siguientes instrucciones crean una cuenta de usuario llamada `oggadm1`.

```
CREATE TABLESPACE administrator;
CREATE USER oggadm1  IDENTIFIED BY "password"
   DEFAULT TABLESPACE ADMINISTRATOR TEMPORARY TABLESPACE TEMP;
ALTER USER oggadm1 QUOTA UNLIMITED ON administrator;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Paso 5: conceder privilegios al usuario en la base de datos de origen

En esta tarea, concederá los privilegios de cuenta necesarios a los usuarios de la base de datos de la base de datos de origen.

Para conceder privilegios a la cuenta en la base de datos de origen

1. Conceda los privilegios necesarios a la cuenta de usuario de Oracle GoldenGate mediante el comando SQL `grant` y el procedimiento `grant_sys_object` de `rdsadmin.rdsadmin_util`. Las siguientes instrucciones conceden privilegios a un usuario llamado `oggadm1`.

```
GRANT CREATE SESSION, ALTER SESSION TO oggadm1;
GRANT RESOURCE TO oggadm1;
GRANT SELECT ANY DICTIONARY TO oggadm1;
GRANT FLASHBACK ANY TABLE TO oggadm1;
GRANT SELECT ANY TABLE TO oggadm1;
GRANT SELECT_CATALOG_ROLE TO rds_master_user_name WITH ADMIN OPTION;
EXEC rdsadmin.rdsadmin_util.grant_sys_object ('DBA_CLUSTERS', 'OGGADM1');
GRANT EXECUTE ON DBMS_FLASHBACK TO oggadm1;
GRANT SELECT ON SYS.V_$DATABASE TO oggadm1;
GRANT ALTER ANY TABLE TO oggadm1;
```

2. Otorgue los privilegios necesarios para que una cuenta de usuario sea administrador de Oracle GoldenGate. Ejecute el siguiente programa PL/SQL.

```
EXEC rdsadmin.rdsadmin_dbms_goldengate_auth.grant_admin_privilege (
    grantee                 => 'OGGADM1',
    privilege_type          => 'capture',
    grant_select_privileges => true,
    do_grants               => TRUE);
```

   Para revocar privilegios, utilice el procedimiento `revoke_admin_privilege` en el mismo paquete.

Paso 6: agregar un alias de TNS para la base de datos de origen

Agregue la siguiente entrada a `$ORACLE_HOME/network/admin/tnsnames.ora` en el directorio raíz de Oracle que utilizará el proceso `EXTRACT`. Para obtener más información sobre el archivo `tnsnames.ora`, consulte la documentación de Oracle.

```
OGGSOURCE=
   (DESCRIPTION=
        (ENABLE=BROKEN)
        (ADDRESS_LIST=
            (ADDRESS=(PROTOCOL=TCP)(HOST=goldengate-source.abcdef12345.us-
west-2.rds.amazonaws.com)(PORT=8200)))
        (CONNECT_DATA=(SERVICE_NAME=ORCL))
    )
```

Configuración de una base de datos de destino para Oracle GoldenGate en Amazon RDS

En esta tarea, debe configurar una instancia de base de datos de destino para usarla con Oracle GoldenGate.

Pasos de configuración

- Paso 2: establecer el parámetro de inicialización ENABLE_GOLDENGATE_REPLICATION en verdadero
- Paso 2: crear una cuenta de usuario de Oracle GoldenGate en la base de datos de destino
- Paso 3: otorgar privilegios de cuenta en la base de datos de destino
- Paso 4: agregar un alias de TNS para la base de datos de destino

Paso 2: establecer el parámetro de inicialización ENABLE_GOLDENGATE_REPLICATION en verdadero

Al establecer el parámetro de inicialización `ENABLE_GOLDENGATE_REPLICATION` en `true`, permite que los servicios de bases de datos admitan la replicación lógica. Si la base de datos de origen está en una instancia de base de datos de Amazon RDS, asegúrese de asignar un grupo de parámetros a dicha instancia de base de datos con el parámetro de inicialización `ENABLE_GOLDENGATE_REPLICATION` establecido en `true`. Para obtener más información acerca del parámetro de inicialización `ENABLE_GOLDENGATE_REPLICATION`, consulte la documentación de la base de datos de Oracle.

Paso 2: crear una cuenta de usuario de Oracle GoldenGate en la base de datos de destino

Oracle GoldenGate se ejecuta como usuario de base de datos y requiere los privilegios de base de datos apropiados. Para asegurarse de que los tiene, cree una cuenta de usuario en la base de datos de destino.

La siguiente instrucción crea una cuenta de usuario llamada `oggadm1`.

```
CREATE TABLESPSACE administrator;
CREATE USER oggadm1  IDENTIFIED BY "password"
   DEFAULT TABLESPACE administrator
   TEMPORARY TABLESPACE temp;
ALTER USER oggadm1 QUOTA UNLIMITED ON administrator;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Paso 3: otorgar privilegios de cuenta en la base de datos de destino

En esta tarea, concederá los privilegios de cuenta necesarios a los usuarios de la base de datos en la base de datos de destino.

Para otorgar privilegios de cuenta en la base de datos de destino

1. Otorgue los privilegios necesarios a la cuenta de usuario de Oracle GoldenGate en la base de datos de destino. En el siguiente ejemplo, otorgará privilegios a `oggadm1`.

```
GRANT CREATE SESSION        TO oggadm1;
GRANT ALTER SESSION         TO oggadm1;
GRANT CREATE CLUSTER        TO oggadm1;
GRANT CREATE INDEXTYPE      TO oggadm1;
GRANT CREATE OPERATOR       TO oggadm1;
GRANT CREATE PROCEDURE      TO oggadm1;
GRANT CREATE SEQUENCE       TO oggadm1;
GRANT CREATE TABLE          TO oggadm1;
GRANT CREATE TRIGGER        TO oggadm1;
GRANT CREATE TYPE           TO oggadm1;
GRANT SELECT ANY DICTIONARY TO oggadm1;
GRANT CREATE ANY TABLE      TO oggadm1;
GRANT ALTER ANY TABLE       TO oggadm1;
GRANT LOCK ANY TABLE        TO oggadm1;
GRANT SELECT ANY TABLE      TO oggadm1;
GRANT INSERT ANY TABLE      TO oggadm1;
GRANT UPDATE ANY TABLE      TO oggadm1;
GRANT DELETE ANY TABLE      TO oggadm1;
```

2. Otorgue los privilegios necesarios para que una cuenta de usuario sea administrador de Oracle GoldenGate. Ejecute el siguiente programa PL/SQL.

```
EXEC rdsadmin.rdsadmin_dbms_goldengate_auth.grant_admin_privilege (
    grantee                 => 'OGGADM1',
    privilege_type          => 'apply',
    grant_select_privileges => true,
    do_grants               => TRUE);
```

   Para revocar privilegios, utilice el procedimiento `revoke_admin_privilege` en el mismo paquete.

Paso 4: agregar un alias de TNS para la base de datos de destino

Agregue la siguiente entrada a `$ORACLE_HOME/network/admin/tnsnames.ora` en el directorio raíz de Oracle que utilizará el proceso `REPLICAT`. Para las bases de datos Oracle Multitenant, asegúrese de que el alias TNS apunte hacia el nombre del servicio de la PDB. Para obtener más información sobre el archivo `tnsnames.ora`, consulte la documentación de Oracle.

```
OGGTARGET=
    (DESCRIPTION=
        (ENABLE=BROKEN)
        (ADDRESS_LIST=
            (ADDRESS=(PROTOCOL=TCP)(HOST=goldengate-target.abcdef12345.us-
west-2.rds.amazonaws.com)(PORT=8200)))
        (CONNECT_DATA=(SERVICE_NAME=ORCL))
    )
```

Uso de las utilidades EXTRACT y REPLICAT de Oracle GoldenGate

Las utilidades de Oracle GoldenGate `EXTRACT` y `REPLICAT` trabajan juntas para mantener las bases de datos de origen y de destino sincronizadas mediante la replicación incremental de transacciones utilizando archivos de seguimiento. Todos los cambios que se producen en la base de datos de origen son detectados automáticamente por `EXTRACT` y, a continuación, se formatean y transfieren a los archivos de seguimiento en el hub de instancias de EC2 o en Oracle GoldenGate en las instalaciones. Una vez finalizada la carga inicial, se leen los datos de estos archivos y se replican en la base de datos de destino mediante la utilidad `REPLICAT`.

Ejecución de la utilidad EXTRACT de Oracle GoldenGate

La utilidad `EXTRACT` recupera, convierte y devuelve datos de la base de datos de origen a los archivos de seguimiento. El procedimiento básico es el siguiente:

1. `EXTRACT` pone en cola detalles de la transacción en la memoria o en el almacenamiento del disco temporal.
2. La base de datos de origen confirma la transacción.
3. `EXTRACT` escribe los detalles de la transacción en un archivo de seguimiento.
4. El archivo de seguimiento dirige estos detalles hacia el hub de instancias de EC2 o en las instalaciones de Oracle GoldenGate y, a continuación, hacia la base de datos de destino.

Los siguientes pasos inician la utilidad `EXTRACT`, capturan los datos de `EXAMPLE.TABLE` en la base de datos `OGGSOURCE` de origen y crean los archivos de seguimiento.

Para ejecutar la utilidad EXTRACT

1. Configure el archivo de parámetros `EXTRACT` en el hub de Oracle GoldenGate (instancia en las instalaciones o de Amazon EC2). El siguiente listado muestra un archivo de parámetros `EXTRACT` de ejemplo denominado `$GGHOME/dirprm/eabc.prm`.

   ```
   EXTRACT EABC

   USERID oggadm1@OGGSOURCE, PASSWORD "my-password"
   EXTTRAIL /path/to/goldengate/dirdat/ab

   IGNOREREPLICATES
   GETAPPLOPS
   TRANLOGOPTIONS EXCLUDEUSER OGGADM1

   TABLE EXAMPLE.TABLE;
   ```

2. En el hub de Oracle GoldenGate, inicie sesión en la base de datos de origen y lance la interfaz de la línea de comandos de Oracle GoldenGate `ggsci`. En el siguiente ejemplo, se muestra el formato para iniciar sesión.

   ```
   dblogin oggadm1@OGGSOURCE
   ```

3. Agregue datos transaccionales para activar el registro complementario para la tabla de base de datos.

```
add trandata EXAMPLE.TABLE
```

4. Con la línea de comandos `ggsci`, habilite la utilidad `EXTRACT` mediante los siguientes comandos.

```
add extract EABC tranlog, INTEGRATED tranlog, begin now
add exttrail /path/to/goldengate/dirdat/ab
   extract EABC,
   MEGABYTES 100
```

5. Registre la utilidad `EXTRACT` con la base de datos de manera que no se eliminen los archivos de registro. Esta tarea le permite recuperar, si fuera necesario, transacciones antiguas sin confirmar. Para registrar la utilidad `EXTRACT` en la base de datos, utilice el siguiente comando.

```
register EXTRACT EABC, DATABASE
```

6. Inicie la utilidad `EXTRACT` con el siguiente comando.

```
start EABC
```

Ejecución de la utilidad REPLICAT de Oracle GoldenGate

La utilidad `REPLICAT` "inserta" información sobre transacciones de los archivos de seguimiento en la base de datos de destino.

Los siguientes pasos habilitan e inician la utilidad `REPLICAT` para que pueda replicar los datos capturados en la tabla `EXAMPLE.TABLE` de la base de datos de destino `OGGTARGET`.

Para ejecutar la utilidad REPLICATE

1. Configure el archivo de parámetros `REPLICAT` en el hub de Oracle GoldenGate (instancia local o de EC2). El siguiente listado muestra un archivo de parámetros `REPLICAT` de ejemplo denominado `$GGHOME/dirprm/rabc.prm`.

```
REPLICAT RABC

USERID oggadm1@OGGTARGET, password "my-password"
```

```
ASSUMETARGETDEFS
MAP EXAMPLE.TABLE, TARGET EXAMPLE.TABLE;
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

2. Inicie sesión en la base de datos de destino y lance la interfaz de la línea de comandos de Oracle GoldenGate (`ggsci`). En el siguiente ejemplo, se muestra el formato para iniciar sesión.

```
dblogin userid oggadm1@OGGTARGET
```

3. Con la línea de comandos `ggsci`, agregue una tabla de punto de comprobación. El usuario indicado debe ser la cuenta de usuario de Oracle GoldenGate, no el propietario del esquema de la tabla de destino. En el siguiente ejemplo, se crea una tabla de punto de comprobación llamada `gg_checkpoint`.

```
add checkpointtable oggadm1.oggchkpt
```

4. Para habilitar la utilidad `REPLICAT`, utilice el siguiente comando.

```
add replicat RABC EXTTRAIL /path/to/goldengate/dirdat/ab CHECKPOINTTABLE
 oggadm1.oggchkpt
```

5. Inicie la utilidad `REPLICAT` con el siguiente comando.

```
start RABC
```

Supervisión de Oracle GoldenGate

Cuando utilice Oracle GoldenGate para la replicación, asegúrese de que el proceso de Oracle GoldenGate esté activo y en ejecución y que las bases de datos de origen y destino estén sincronizadas. Puede utilizar las siguientes herramientas de supervisión:

- Amazon CloudWatch es un servicio de supervisión que se utiliza en este patrón para supervisar los registros de errores de GoldenGate.

- Amazon SNS es un servicio de notificación de mensajes que se utiliza en este patrón para enviar notificaciones por correo electrónico.

Para obtener instrucciones detalladas, consulte Monitor Oracle GoldenGate logs by using Amazon CloudWatch (Supervisión de los registros de Oracle GoldenGate mediante Amazon CloudWatch).

Solución de problemas de Oracle GoldenGate

Esta sección explica los problemas más habituales al usar Oracle GoldenGate con Amazon RDS para Oracle.

Temas

- Error al abrir un registro redo en línea
- Oracle GoldenGate parece estar configurado correctamente, pero la replicación no está funcionando
- La REPLICAT integrada es lenta debido a la consulta en SYS."_DBA_APPLY_CDR_INFO"

Error al abrir un registro redo en línea

Asegúrese de configurar las bases de datos para que retengan los registros redo archivados. Tenga en cuenta estas directrices:

- Especifique la duración de la retención de registros en horas. El valor mínimo es una hora.
- Establezca la duración de manera que supere cualquier posible periodo de inactividad de la instancia de base de datos de origen, cualquier posible periodo de comunicación y cualquier posible periodo de problemas de red para la instancia de base de datos de origen. Dicha duración permite a Oracle GoldenGate recuperar registros de la instancia de base de datos de origen según sea necesario.
- Asegúrese de que dispone de suficiente almacenamiento en la instancia para los archivos.

Si no tiene la retención de registros habilitada, o bien si el valor de retención es demasiado pequeño, recibirá un mensaje de error similar al siguiente.

```
2022-03-06 06:17:27  ERROR   OGG-00446  error 2 (No such file or directory)
opening redo log /rdsdbdata/db/GGTEST3_A/onlinelog/o1_mf_2_9k4bp1n6_.log for sequence
 1306
Not able to establish initial position for begin time 2022-03-06 06:16:55.
```

Oracle GoldenGate parece estar configurado correctamente, pero la replicación no está funcionando

Para tablas preexistentes, debe especificar el SCN desde el que trabaja Oracle GoldenGate.

Para solucionar este problema

1. Inicie sesión en la base de datos de origen y lance la interfaz de la línea de comandos de Oracle GoldenGate (`ggsci`). En el siguiente ejemplo, se muestra el formato para iniciar sesión.

   ```
   dblogin userid oggadm1@OGGSOURCE
   ```

2. Con la línea de comandos `ggsci`, configure el SCN de inicio para el proceso `EXTRACT`. En el siguiente ejemplo, se establece el SCN en 223274 para `EXTRACT`.

   ```
   ALTER EXTRACT EABC SCN 223274
   start EABC
   ```

3. Inicie sesión en la base de datos de destino. En el siguiente ejemplo, se muestra el formato para iniciar sesión.

   ```
   dblogin userid oggadm1@OGGTARGET
   ```

4. Con la línea de comandos `ggsci`, configure el SCN de inicio para el proceso `REPLICAT`. En el siguiente ejemplo, se establece el SCN en 223274 para `REPLICAT`.

   ```
   start RABC atcsn 223274
   ```

La REPLICAT integrada es lenta debido a la consulta en SYS."_DBA_APPLY_CDR_INFO"

Con la detección y resolución de conflictos (CDR) de Oracle GoldenGate se ofrecen rutinas básicas de resolución de conflictos. Por ejemplo, con la CDR se puede resolver un conflicto distintivo de una instrucción `INSERT`.

Cuando la CDR resuelve una colisión, puede insertar registros en la tabla de excepciones `_DBA_APPLY_CDR_INFO` temporalmente. La `REPLICAT` integrada elimina estos registros después. En un escenario raro, la `REPLICAT` integrada puede procesar un gran número de colisiones, pero una `REPLICAT` integrada nueva no la reemplaza. En lugar de eliminarse, las filas que ya están en `_DBA_APPLY_CDR_INFO` quedan huérfanas. Los procesos `REPLICAT` integrados nuevos se ralentizan, pues están consultando filas huérfanas en `_DBA_APPLY_CDR_INFO`.

Para eliminar todas las filas de `_DBA_APPLY_CDR_INFO`, utilice el procedimiento `rdsadmin.rdsadmin_util.truncate_apply$_cdr_info` de Amazon RDS. Este procedimiento se publica como parte de la versión y actualización de parche de octubre de 2020. El procedimiento está disponible en las siguientes versiones de base de datos:

- Versión 21.0.0.0.ru-2022-01.rur-2022-01.r1 y posteriores
- Versión 19.0.0.0.ru-2020-10.rur-2020-10.r1 y posteriores

En el ejemplo siguiente se trunca la tabla `_DBA_APPLY_CDR_INFO`.

```
SET SERVEROUTPUT ON SIZE 2000
EXEC rdsadmin.rdsadmin_util.truncate_apply$_cdr_info;
```

Uso de Oracle Repository Creation Utility en RDS para Oracle

Puede usar Amazon RDS para alojar una instancia de base de datos RDS for Oracle que contenga los esquemas para admitir los componentes de Oracle Fusion Middleware. Antes de poder utilizar los componentes de Fusion Middleware, cree y rellene los esquemas para ellos en su base de datos. Los esquemas se crean y se rellenan con Oracle Repository Creation Utility (RCU).

Versiones y opciones de licencia compatibles con la RCU

Amazon RDS solo es compatible con Oracle Repository Creation Utility (RCU) versión 12c. Puede usar RCU en las siguientes configuraciones:

- RCU 12c con Oracle Database 21c
- RCU 12c con Oracle Database 19c

Para poder usar RCU, asegúrese de que hace lo siguiente:

- Obtenga una licencia de Oracle Fusion Middleware.
- Siga las directrices sobre licencias de Oracle para la base de datos de Oracle que aloja el repositorio. Para obtener más información, consulte el Manual del usuario de información de licencias de Oracle Fusion Middleware en la documentación de Oracle.

Fusion MiddleWare admite los repositorios de Oracle Database Enterprise Edition y Standard Edition 2. Oracle recomienda usar Enterprise Edition para las instalaciones de producción que requieren particiones y las instalaciones en las que es necesario reconstruir índices online.

Antes de crear su instancia de base de datos de RDS for Oracle, confirme la versión de Oracle Database que necesita para usar los componentes que desea implementar. Para encontrar los requisitos de los componentes y versiones de Fusion Middleware que desea desplegar, utilice la matriz de certificación. Para obtener más información, consulte Oracle Fusion Middleware Supported System Configurations (Configuraciones de sistemas compatibles con Oracle Fusion Middleware) en la documentación de Oracle.

Amazon RDS admite actualizaciones de las versiones de Oracle Database cuando sean necesarias. Para obtener más información, consulte Actualización de una versión del motor de una instancia de base de datos.

Requisitos y limitaciones de la RCU

Para usar la RCU, necesita una Amazon VPC. Su instancia de base de datos de Amazon RDS debe estar disponible únicamente para los componentes de Fusion Middleware y no para la Internet pública. Por lo tanto, aloje la instancia de base de datos de Amazon RDS en una subred privada, que proporciona mayor seguridad. También necesita una instancia de base de datos de RDS for Oracle. Para obtener más información, consulte Creación y conexión a una instancia de base de datos de Oracle.

Puede almacenar los esquemas de cualquier componente de Fusion Middleware en su instancia de base de datos de Amazon RDS. Se verificó que los siguientes esquemas se instalan correctamente:

- Analytics (ACTIVITIES)
- Audit Services (IAU)
- Audit Services Append (IAU_APPEND)
- Audit Services Viewer (IAU_VIEWER)
- Discussions (DISCUSSIONS)
- Metadata Services (MDS)
- Oracle Business Intelligence (BIPLATFORM)
- Oracle Platform Security Services (OPSS)
- Portal and Services (WEBCENTER)
- Portlet Producers (PORTLET)
- Service Table (STB)
- SOA Infrastructure (SOAINFRA)
- User Messaging Service (UCSUMS)
- WebLogic Services (WLS)

Pautas para el uso de la RCU

A continuación se detallan algunas recomendaciones para trabajar con una instancia de base de datos en esta situación:

- Es recomendable usar Multi-AZ para las cargas de trabajo de producción. Para obtener más información acerca del uso de varias zonas de disponibilidad, consulte Regiones, zonas de disponibilidad y Local Zones.

- Para mayor seguridad, Oracle recomienda usar Cifrado de datos transparente (TDE) para cifrar los datos en reposo. Si tiene una licencia de Enterprise Edition que incluye Advanced Security Option, puede habilitar el cifrado en reposo usando la opción TDE. Para obtener más información, consulte Cifrado de datos transparente de Oracle.

  Amazon RDS también proporciona una opción de cifrado en reposo para todas las ediciones de la base de datos. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
- Configure sus grupos de seguridad de VPC para permitir la comunicación entre los servidores de su aplicación y su instancia de base de datos de Amazon RDS. Los servidores de aplicación que alojan los componentes de Fusion Middleware pueden estar en Amazon EC2 o instalados localmente.

Ejecución de la RCU

Para crear y rellenar los esquemas que admiten los componentes de Fusion Middleware, use la utilidad de creación de repositorios de Oracle (RCU). Puede ejecutar la RCU de distintas formas.

Temas

- Ejecución de RCU a través de la línea de comando en un paso
- Ejecución de RCU a través de la línea de comando en varios pasos
- Ejecución de RCU en modo interactivo

Ejecución de RCU a través de la línea de comando en un paso

Si no necesita editar ninguno de sus esquemas antes de rellenarlos, puede ejecutar RCU en un solo paso. De lo contrario, consulte la siguiente sección para ejecutar RCU en varios pasos.

Puede ejecutar RCU en modo silencioso usando el parámetro de línea de comando `-silent`. Cuando se ejecuta la RCU en modo silencioso, se puede evitar introducir contraseñas en la línea de comandos mediante la creación de un archivo de texto que contiene las contraseñas. Cree un archivo de texto con la contraseña de `dbUser` en la primera línea y la contraseña de cada componente en las líneas siguientes. Debe especificar el nombre del archivo de contraseñas como último parámetro del comando de RCU.

Example

En el siguiente ejemplo se crean y se rellenan esquemas para el componente SOA Infrastructure (y sus dependencias) en un solo paso.

Para Linux, macOS o:Unix

```
export ORACLE_HOME=/u01/app/oracle/product/12.2.1.0/fmw
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-silent \
-createRepository \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal \
-honorOMF \
-schemaPrefix ${SCHEMA_PREFIX} \
-component MDS \
-component STB \
-component OPSS \
-component IAU \
-component IAU_APPEND \
-component IAU_VIEWER \
-component UCSUMS \
-component WLS \
-component SOAINFRA \
-f < /tmp/passwordfile.txt
```

Para obtener más información, consulte Running Repository Creation Utility from the Command Line en la documentación de Oracle.

Ejecución de RCU a través de la línea de comando en varios pasos

Para editar de forma manual los scripts de sus esquemas, ejecute la RCU en varios pasos:

1. Ejecute RCU en el modo Prepare Scripts for System Load usando el parámetro de línea de comando `-generateScript` para crear los scripts de sus esquemas.
2. Edite y ejecute manualmente el script generad `script_systemLoad.sql`.
3. Ejecute RCU de nuevo en el modo Perform Product Load usando el parámetro de línea de comando `-dataLoad` para rellenar los esquemas.
4. Ejecute el script de limpieza creado `script_postDataLoad.sql`.

Para ejecutar la RCU en modo silencioso, especifique el parámetro de línea de comandos `-silent`. Cuando se ejecuta la RCU en modo silencioso, se puede evitar escribir contraseñas en la línea de comandos mediante la creación de un archivo de texto que contiene las contraseñas. Cree

un archivo de texto con la contraseña de `dbUser` en la primera línea y la contraseña de cada componente en las líneas siguientes. Especifique el nombre del archivo de contraseñas como último parámetro del comando de la RCU.

Example

El siguiente ejemplo crea scripts de esquema para el componente SOA Infrastructure y sus dependencias.

Para Linux, macOS o:Unix

```
export ORACLE_HOME=/u01/app/oracle/product/12.2.1.0/fmw
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-silent \
-generateScript \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal \
-honorOMF \
[-encryptTablespace true] \
-schemaPrefix ${SCHEMA_PREFIX} \
-component MDS \
-component STB \
-component OPSS \
-component IAU \
-component IAU_APPEND \
-component IAU_VIEWER \
-component UCSUMS \
-component WLS \
-component SOAINFRA \
-scriptLocation /tmp/rcuscripts \
-f < /tmp/passwordfile.txt
```

Ahora puede editar el script generado, conectarse a su instancia de base de datos de Oracle y ejecutar el script. El script generado se llama `script_systemLoad.sql`. Para obtener información acerca de la conexión a su instancia de base de datos de Oracle, consulte Paso 3: conectar el cliente de SQL a una instancia de base de datos de Oracle.

En el siguiente ejemplo se rellenan los esquemas para el componente SOA Infrastructure (y sus dependencias).

Para Linux, macOS o:Unix

```
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
-silent \
-dataLoad \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal \
-honorOMF \
-schemaPrefix ${SCHEMA_PREFIX} \
-component MDS \
-component STB \
-component OPSS \
-component IAU \
-component IAU_APPEND \
-component IAU_VIEWER \
-component UCSUMS \
-component WLS \
-component SOAINFRA \
-f < /tmp/passwordfile.txt
```

Para terminar, conéctese a su instancia de base de datos de Oracle y ejecute el script de limpieza. El script se llama `script_postDataLoad.sql`.

Para obtener más información, consulte Running Repository Creation Utility from the Command Line en la documentación de Oracle.

Ejecución de RCU en modo interactivo

Para usar la interfaz gráfica de usuario de la RCU, ejecute la RCU en modo interactivo. Incluya el parámetro `-interactive` y omita el parámetro `-silent`. Para obtener más información, consulte Understanding Repository Creation Utility Screens en la documentación de Oracle.

Example

En el siguiente ejemplo, RCU se inicia en modo interactivo y la información de la conexión se rellena automáticamente.

Para Linux, macOS o:Unix

```
export ORACLE_HOME=/u01/app/oracle/product/12.2.1.0/fmw
export JAVA_HOME=/usr/java/jdk1.8.0_65
${ORACLE_HOME}/oracle_common/bin/rcu \
```

```
-interactive \
-createRepository \
-connectString ${dbhost}:${dbport}:${dbname} \
-dbUser ${dbuser} \
-dbRole Normal
```

Solución de problemas de la RCU

Tenga en cuenta los siguientes problemas.

Temas

- Oracle Managed Files (OMF)
- Privilegios de objeto
- Enterprise Scheduler Service

Oracle Managed Files (OMF)

Amazon RDS usa archivos de datos de OMF para simplificar la administración del almacenamiento. Puede personalizar los atributos del espacio de tabla, como la administración del tamaño y la extensión. Sin embargo, si se especifica un nombre de archivo de datos cuando se ejecuta RCU, el código del espacio de tabla falla con `ORA-20900`. Puede utilizar RCU con OMF de las siguientes formas:

- En RCU 12.2.1.0 y versiones posteriores, use el parámetro de línea de comando `-honorOMF`.
- En RCU 12.1.0.3 y versiones posteriores, use varios pasos y edite el script generado. Para obtener más información, consulte Ejecución de RCU a través de la línea de comando en varios pasos.

Privilegios de objeto

Dado que Amazon RDS es un servicio administrado, no tiene acceso `SYSDBA` completo a la instancia de base de datos de RDS for Oracle. Sin embargo, RCU 12c admite usuarios con privilegios más bajos. En la mayoría de los casos, el privilegio de usuario maestro es suficiente para crear repositorios.

La cuenta maestra puede conceder directamente los privilegios que ya se le han concedido a `WITH GRANT OPTION`. En algunos casos, RCU puede generar el error con `ORA-01031` cuando se intenta conceder a `SYS` privilegios de objeto. Puede volver a intentar ejecutar el procedimiento almacenado `rdsadmin_util.grant_sys_object`, como se muestra en el ejemplo siguiente:

```
BEGIN
  rdsadmin.rdsadmin_util.grant_sys_object('GV_$SESSION','MY_DBA','SELECT');
END;
/
```

Si intenta conceder privilegios SYS en el objeto SCHEMA_VERSION_REGISTRY, la operación podría fallar con `ORA-20199: Error in rdsadmin_util.grant_sys_object`. Puede calificar la tabla SCHEMA_VERSION_REGISTRY$ y la vista SCHEMA_VERSION_REGISTRY con el nombre del propietario del esquema, que es SYSTEM, y volver a intentar la operación. O bien, puede crear un sinónimo. Inicie sesión como usuario maestro y ejecute las siguientes instrucciones:

```
CREATE OR REPLACE VIEW SYSTEM.SCHEMA_VERSION_REGISTRY
  AS SELECT * FROM SYSTEM.SCHEMA_VERSION_REGISTRY$;
CREATE OR REPLACE PUBLIC SYNONYM SCHEMA_VERSION_REGISTRY FOR
 SYSTEM.SCHEMA_VERSION_REGISTRY;
CREATE OR REPLACE PUBLIC SYNONYM SCHEMA_VERSION_REGISTRY$ FOR SCHEMA_VERSION_REGISTRY;
```

Enterprise Scheduler Service

Cuando se usa la RCU para eliminar un repositorio de Enterprise Scheduler Service, la RCU puede fallar con `Error: Component drop check failed`.

Configuración de Oracle Connection Manager en una instancia de Amazon EC2

Oracle Connection Manager (CMAN) es un servidor proxy que reenvía las peticiones de conexión a los servidores de bases de datos o a otros servidores proxy. Puede utilizar CMAN para configurar lo siguiente:

Control de acceso

Puede crear reglas que filtren las solicitudes de los clientes especificadas por el usuario y acepten otras.

Multiplexación de sesiones

Puede canalizar varias sesiones de cliente a través de una conexión de red a un destino de servidor compartido.

Normalmente, CMAN reside en un host separado del servidor de la base de datos y de los hosts de los clientes. Para más información, consulte Configuring Oracle Connection Manager (Configuración de Oracle Connection Manager) en la documentación de Oracle Database.

Temas

- Versiones y opciones de licencia compatibles con CMAN
- Requisitos y limitaciones para CMAN
- Configuración de CMAN

Versiones y opciones de licencia compatibles con CMAN

CMAN es compatible con la edición Enterprise de todas las versiones de Oracle Database que admite Amazon RDS. Para obtener más información, consulte Versiones de RDS para Oracle.

Puede instalar Oracle Connection Manager en un host distinto del host donde está instalada Oracle Database. No necesita una licencia independiente para el host que ejecuta CMAN.

Requisitos y limitaciones para CMAN

Para proporcionar una experiencia completamente administrada, Amazon RDS restringe el acceso al sistema operativo. No se pueden modificar los parámetros de la base de datos que requieren acceso

al sistema operativo. Por lo tanto, Amazon RDS no es compatible con las características de CMAN que requieren que inicie sesión en el sistema operativo.

Configuración de CMAN

Cuando se configura CMAN, se realiza la mayor parte del trabajo fuera de la base de datos de RDS for Oracle.

Temas

- Paso 1: configurar CMAN en una instancia de Amazon EC2 en la misma VPC que la instancia de RDS for Oracle
- Paso 2: configurar los parámetros de la base de datos para CMAN
- Paso 3: asociar la instancia de base de datos con el grupo de parámetros

Paso 1: configurar CMAN en una instancia de Amazon EC2 en la misma VPC que la instancia de RDS for Oracle

Para saber cómo configurar CMAN, siga las instrucciones detalladas en la publicación del blog Configuring and using Oracle Connection Manager on Amazon EC2 for Amazon RDS for Oracle (Configurar y utilizar Oracle Connection Manager en Amazon EC2 para Amazon RDS for Oracle).

Paso 2: configurar los parámetros de la base de datos para CMAN

Para las funciones de CMAN, como el modo de director de tráfico y la multiplexación de sesiones, establezca el parámetro `REMOTE_LISTENER` en la dirección de la instancia de CMAN en un grupo de parámetros de base de datos. Veamos la siguiente situación:

- La instancia CMAN reside en un host con la dirección IP `10.0.159.100` y utiliza el puerto `1521`.
- Las bases de datos `orcla`, `orclb` y `orclc` residen en instancias de base de datos de RDS for Oracle separadas.

La siguiente tabla muestra cómo establecer el valor de `REMOTE_LISTENER`. El valor de `LOCAL_LISTENER` lo establece automáticamente Amazon RDS.

Nombre de instancia de base de datos	IP de la instancia de la base de datos	Valor del oyente local (establecido automáticamente)	Valor de la escucha remota (establecida por el usuario)
orcla	10.0.159.200	`( address= (protocol=tcp) (host=10.0.159.200) (port=1521) )`	10.0.159.100:1521
orclb	10.0.159.300	`( address= (protocol=tcp) (host=10.0.159.300) (port=1521) )`	10.0.159.100:1521
orclc	10.0.159.400	`( address= (protocol=tcp) (host=10.0.159.400) (port=1521) )`	10.0.159.100:1521

Paso 3: asociar la instancia de base de datos con el grupo de parámetros

Cree o modifique la instancia de base de datos para utilizar el grupo de parámetros que configuró en Paso 2: configurar los parámetros de la base de datos para CMAN. Para obtener más información, consulte Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS.

Instalación de una base de datos de Siebel en Oracle en Amazon RDS

Puede utilizar Amazon RDS para alojar una base de datos de Siebel en una instancia de base de datos de Oracle. La base de datos de Siebel forma parte de la arquitectura de aplicaciones Siebel Customer Relationship Management (CRM). Para ver una ilustración, consulte Generic Architecture of Siebel Business Application.

Utilice el siguiente tema para configurar una base de datos de Siebel en una instancia de base de datos de Oracle en Amazon RDS. También puede aprender cómo utilizar Amazon Web Services con los demás componentes que requiere la arquitectura de aplicaciones Siebel CRM.

> **Note**
>
> Para instalar una base de datos de Siebel en Oracle en Amazon RDS, debe utilizar la cuenta de usuario maestro. No necesita el privilegio SYSDBA, ya que el privilegio de usuario maestro es suficiente. Para obtener más información, consulte Privilegios de la cuenta de usuario maestro.

Licencias y versiones

Para instalar una base de datos de Siebel en Amazon RDS, debe utilizar su propia licencia de Oracle Database y su propia licencia de Siebel. Debe tener la licencia de Oracle Database adecuada (con Software Update License and Support) para la clase de instancia de base de datos y la edición de Oracle Database. Para obtener más información, consulte Opciones de licencias de RDS para Oracle.

Oracle Database Enterprise Edition es la única edición certificada por Siebel para esta situación. Amazon RDS es compatible con las versiones 15.0 o 16.0 de Siebel CRM.

Amazon RDS admite actualizaciones de las versiones de los motores de bases de datos. Para obtener más información, consulte Actualización de una versión del motor de una instancia de base de datos.

Antes de empezar

Antes de comenzar, necesita una Amazon VPC. Como la instancia de base de datos de Amazon RDS únicamente debe estar disponible para Siebel Enterprise Server y no para la red pública de

Internet, la instancia de base de datos de Amazon RDS se aloja en una subred privada, lo que proporciona mayor seguridad. Para obtener información acerca de cómo crear una Amazon VPC para usarla con Siebel CRM, consulte Creación y conexión a una instancia de base de datos de Oracle.

Antes de comenzar, necesitará también una instancia de base de datos de Oracle. Para obtener información acerca de cómo crear una instancia de base de datos de Oracle para utilizarla con Siebel CRM, consulte Creación de una instancia de base de datos de Amazon RDS.

Instalación y configuración de una base de datos de Siebel

Una vez que haya creado la instancia de base de datos de Oracle, puede instalar la base de datos de Siebel. La base de datos se instala creando las cuentas del propietario y del administrador de tablas, instalando las funciones y los procedimientos almacenados, y ejecutando el asistente para la configuración de bases de datos de Siebel. Para obtener más información, consulte Installing the Siebel Database on the RDBMS.

Para ejecutar el asistente para la configuración de bases de datos de Siebel, debe utilizar la cuenta de usuario maestro. No necesita el privilegio `SYSDBA`, ya que el privilegio de usuario maestro es suficiente. Para obtener más información, consulte Privilegios de la cuenta de usuario maestro.

Uso de otras características de Amazon RDS con una base de datos de Siebel

Una vez que haya creado la instancia de base de datos de Oracle, puede utilizar características adicionales de Amazon RDS que le ayudarán a personalizar la base de datos de Siebel.

Recopilación de estadísticas con la opción Oracle Statspack

Puede añadir características a la instancia de base de datos utilizando opciones en los grupos de opciones de base de datos. Cuando creó la instancia de base de datos de Oracle, utilizó el grupo de opciones de base de datos predeterminado. Si desea añadir características a la base de datos, puede crear un grupo de opciones nuevo para la instancia de base de datos.

Si desea recopilar estadísticas de desempeño de la base de datos de Siebel, puede añadir la característica Oracle Statspack. Para obtener más información, consulte Oracle Statspack.

Algunos cambios realizados en las opciones se aplican inmediatamente, mientras que otros se aplican durante el siguiente periodo de mantenimiento de la instancia de base de datos. Para obtener más información, consulte Trabajo con grupos de opciones. Una vez que haya creado un grupo de

opciones personalizado, modifique la instancia de base de datos para adjuntarlo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Ajuste del rendimiento mediante parámetros

Puede administrar la configuración del motor de base de datos mediante el uso de los parámetros de un grupo de parámetros de base de datos. Cuando creó la instancia de base de datos de Oracle, utilizó el grupo de parámetros de base de datos predeterminado. Si desea personalizar la configuración de la base de datos, puede crear un grupo de parámetros nuevo para la instancia de base de datos.

Al cambiar un parámetro, dependiendo del tipo de parámetro, los cambios se aplican inmediatamente o después de reiniciar manualmente la instancia de base de datos. Para obtener más información, consulte Grupos de parámetros para Amazon RDS. Una vez que haya creado un grupo de parámetros personalizado, modifique la instancia de base de datos para adjuntarlo. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Para optimizar la instancia de base de datos de Oracle para Siebel CRM, puede personalizar determinados parámetros. En la siguiente tabla se muestran algunos valores de parámetros recomendados. Si quiere obtener más información para ajustar el rendimiento de Siebel CRM, consulte la guía de ajuste de rendimiento de Siebel CRM.

Nombre del parámetro	Valor predeterminado	Valor aconsejado para optimizar el rendimiento de Siebel CRM
`_always_semi_join`	`CHOOSE`	`OFF`
`_b_tree_bitmap_plans`	`TRUE`	`FALSE`
`_like_with_bind_as_equality`	`FALSE`	`TRUE`
`_no_or_expansion`	`FALSE`	`FALSE`

Nombre del parámetro	Valor predeterminado	Valor aconsejado para optimizar el rendimiento de Siebel CRM
`_optimizer_join_sel_sanity_check`	`TRUE`	`TRUE`
`_optimizer_max_permutations`	2000	100
`_optimizer_sortmerge_join_enabled`	`TRUE`	`FALSE`
`_partition_view_enabled`	`TRUE`	`FALSE`
`open_cursors`	`300`	Como mínimo **`2000`**.

Creación de instantáneas

Una vez que haya creado la base de datos de Siebel, puede copiarla utilizando las características de instantáneas de Amazon RDS. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS y Restauración a una instancia de base de datos.

Otros componentes compatibles de Siebel CRM

Además de la base de datos de Siebel, también puede utilizar Amazon Web Services con los demás componentes de la arquitectura de aplicaciones Siebel CRM. Puede encontrar más información acerca de la compatibilidad de Amazon AWS con componentes adicionales de Siebel CRM en la siguiente tabla.

Componente de Siebel CRM	Soporte de Amazon AWS
Siebel Enterprise (con uno o varios servidores Siebel)	Puede alojar los servidores Siebel en instancias de Amazon Elastic Compute Cloud (Amazon EC2). Puede utilizar Amazon EC2 para lanzar tantos servidores virtuales como necesite. Utilizando Amazon EC2, puede escalar hacia arriba o hacia abajo fácilmente para afrontar los cambios que se produzcan en los requisitos. Para obtener más información, consulte ¿Qué es Amazon EC2? Puede colocar los servidores en la misma VPC que la instancia de base de datos y utilizar el grupo de seguridad de VPC para obtener acceso a la base de datos. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.
Servidores web (con Siebel Web Server Extensions)	Puede instalar varios servidores web en varias instancias EC2. A continuación, puede utilizar Elastic Load Balancing para distribuir el tráfico entrante entre las instancias. Para obtener más información, consulte ¿Qué es Elastic Load Balancing?
Siebel Gateway Name Server	Puede alojar el servidor de nombres Siebel Gateway Name Server en una instancia EC2. A continuación, puede colocar el servidor en la misma VPC que la instancia de base de datos y utilizar el grupo de seguridad de VPC para obtener acceso a la base de datos. Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.

Notas de la versión del motor de Oracle Database

Las actualizaciones en sus instancias de base de datos de Amazon RDS for Oracle las mantienen al día. Si aplica actualizaciones, tendrá la seguridad de que su instancia de base de datos está ejecutando una versión del software de la base de datos que han probado tanto Oracle como Amazon. No se permite aplicar parches únicos a instancias de base de datos de RDS para Oracle.

Puede especificar cualquier versión de Oracle Database compatible actualmente al crear una nueva instancia de base de datos. Puede especificar las versiones principales, como Oracle Database 19c y cualquier versión secundaria admitida para la versión principal especificada. Si no se especifica ninguna versión, Amazon RDS cambia de forma predeterminada a una versión admitida, normalmente la más reciente. Si se especifica una versión principal pero no una versión secundaria, Amazon RDS usa de manera predeterminada una versión reciente de la versión principal especificada. Para ver una lista de las versiones admitidas y de las versiones predeterminadas para instancias de bases de datos recién creadas, utilice el comando `describe-db-engine-versions` de la AWS CLI.

Para obtener más información sobre las versiones de Oracle Database compatibles con Amazon RDS, consulte las notas de la versión de Amazon RDS para Oracle.

Amazon RDS para PostgreSQL

Amazon RDS admite instancias de base de datos que ejecutan varias versiones de PostgreSQL. Para obtener una lista de las versiones disponibles, consulte Versiones de base de datos de PostgreSQL disponibles.

Puede crear instancias de base de datos e instantáneas de base de datos, restauraciones de un momento dado y backups. Las instancias de base de datos en las que se ejecuta PostgreSQL admiten implementaciones Multi-AZ, réplicas de lectura, IOPS aprovisionadas y se pueden crear dentro de una nube virtual privada (VPC). También puede utilizar la Capa de conexión segura (SSL) para conectarse a una instancia de base de datos en la que se ejecuta PostgreSQL.

Antes de crear una instancia de base de datos, debe completar los pasos que se describen en Configuración del entorno para Amazon RDS.

Puede usar cualquier aplicación cliente de SQL estándar para ejecutar comandos para la instancia desde su equipo cliente. Entre estas aplicaciones se incluyen pgAdmin, una conocida herramienta de administración y desarrollo de código abierto para PostgreSQL, o psql, una utilidad de línea de comando que forma parte de una instalación de PostgreSQL. Para ofrecer una experiencia de servicio administrado, Amazon RDS no proporciona acceso de host a las instancias de base de datos. También restringe el acceso a ciertos procedimientos y tablas del sistema que requieren privilegios avanzados. Amazon RDS permite el acceso a las bases de datos de una instancia de base de datos usando cualquier aplicación cliente de SQL estándar. Amazon RDS no permite el acceso directo de anfitrión a una instancia de base de datos mediante Telnet o Secure Shell (SSH).

Amazon RDS para PostgreSQL cumple muchos estándares del sector. Por ejemplo, puede utilizar las bases de datos de Amazon RDS para PostgreSQL para crear aplicaciones conformes con HIPAA y para almacenar información relacionada con la sanidad. Esto incluye el almacenamiento de información sanitaria protegida (PHI) en virtud de un Contrato de asociación empresarial (BAA) completado con AWS. Amazon RDS para PostgreSQL también cumple con los requisitos de seguridad del Programa federal de administración de riesgos y autorizaciones (FedRAMP). Amazon RDS para PostgreSQL ha recibido una autorización provisional para operar (P-ATO) de la Junta de Autorización Conjunta (JAB) de FedRAMP en la referencia FedRAMP HIGH dentro de las regiones de AWS GovCloud (US). Para obtener más información acerca de los estándares de conformidad admitidos, consulte Conformidad en la nube de AWS.

Para importar los datos de PostgreSQL en una instancia de base de datos, siga el procedimiento que se describe en la sección Importación de datos en PostgreSQL en Amazon RDS.

Important

Si detecta algún problema con la instancia de la de base de datos de RDS para PostgreSQL, es posible que el agente de asistencia de AWS necesite más información sobre el estado de las bases de datos. El objetivo es asegurarnos de que la asistencia de AWS recibe la información requerida en el menor tiempo posible.
Puede utilizar PG Collector para recopilar información valiosa sobre la base de datos en un archivo HTML consolidado. Para obtener más información sobre PG Collector, cómo ejecutarlo y cómo descargar el informe HTML, consulte PG Collector.
Una vez finalizado correctamente, y a menos que se indique lo contrario, el script devuelve el resultado en un formato HTML legible. El script está diseñado para excluir cualquier dato o detalle de seguridad del HTML que pueda comprometer el negocio. Además, no realiza modificaciones en la base de datos ni en el entorno. Sin embargo, si encuentra alguna información en el HTML que no le resulte cómodo compartir, no dude en eliminar la información problemática antes de cargar el HTML. Cuando el HTML sea aceptable, cárguelo utilizando la sección de archivos adjuntos en los detalles del caso de su caso de asistencia.

Temas

- Tareas de administración comunes de Amazon RDS para PostgreSQL
- Trabajo con el entorno de vista previa de bases de datos
- Versiones de base de datos de PostgreSQL disponibles
- Descripción del proceso de lanzamiento incremental de RDS para PostgreSQL
- Versiones de extensiones de PostgreSQL compatibles
- Uso de las características de PostgreSQL admitidas por Amazon RDS para PostgreSQL
- Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL
- Protección de conexiones a RDS for PostgreSQL con SSL/TLS
- Uso de la autenticación Kerberos con Amazon RDS para PostgreSQL
- Uso de un servidor de DNS personalizado para el acceso a la red de salida.
- Actualizaciones del motor de base de datos de RDS para PostgreSQL
- Actualización de una versión del motor de instantáneas de base de datos de PostgreSQL
- Uso de réplicas de lectura para Amazon RDS para PostgreSQL
- Mejora del rendimiento de las consultas de RDS para PostgreSQL con lecturas optimizadas para Amazon RDS

- Importación de datos en PostgreSQL en Amazon RDS
- Exportación de datos de una de Amazon S3
- Invocación de una función de AWS Lambda desde una instancia de base de datos de RDS for PostgreSQL
- Tareas comunes de los administradores de base de datos (DBA) para Amazon RDS para PostgreSQL
- Ajuste con eventos de espera de RDS para PostgreSQL
- Ajuste de RDS para PostgreSQL con información proactiva de Amazon DevOps Guru
- Uso de extensiones PostgreSQL con Amazon RDS para PostgreSQL
- Uso de los contenedores de datos externos compatibles para Amazon RDS for PostgreSQL
- Uso de Extensiones de lenguaje de confianza para PostgreSQL

Tareas de administración comunes de Amazon RDS para PostgreSQL

A continuación se detallan las tareas de administración frecuentes que se realizan para una instancia de base de datos de Amazon RDS para PostgreSQL, con enlaces a la documentación relativa a cada tarea.

Área de la tarea	Documentación relacionada
Configuración de Amazon RDS para el primer uso Debe completar algunos requisitos previos antes de crear su instancia de base de datos. Por ejemplo, las instancias de base de datos se crean de manera predeterminada con un firewall que impide el acceso. Debe crear un grupo de seguridad con las direcciones IP y la configuración de red correctas para tener acceso a la instancia de base de datos.	Configuración del entorno para Amazon RDS
Descripción de las instancias de base de datos de Amazon RDS Si va a crear una instancia de base de datos con fines de producción, debe entender cómo funcionan en Amazon RDS	Clases de instancia de base de datos de Tipos de almacenamiento de Amazon RDS

Área de la tarea	Documentación relacionada
las clases de instancia, los tipos de almacenamiento y las IOPS aprovisionadas.	Almacenamiento de SSD de IOPS aprovisionadas
Búsqueda de versiones disponibles de PostgreSQL Amazon RDS admite varias versiones de PostgreSQL.	Versiones de base de datos de PostgreSQL disponibles
Configuración de la compatibilidad con alta disponibilidad y conmutación por error Una instancia de base de datos de producción debe usar implementaciones Multi-AZ. Las implementaciones Multi-AZ proporcionan unos niveles superiores de disponibilidad, durabilidad de los datos y tolerancia a errores para las instancias de base de datos.	Configuración y administración de una implementación multi-AZ para Amazon RDS
Descripción de la red de Amazon Virtual Private Cloud (VPC) Si su cuenta de AWS tiene una VPC predeterminada, la instancia de base de datos se creará automáticamente dentro de la VPC predeterminada. En algunos casos, su cuenta podría no tener una VPC predeterminada y es posible que quiera la instancia de base de datos en una VPC. En estos casos, cree los grupos de VPC y de subred antes de crear la instancia de base de datos.	Uso de una instancia de base de datos en una VPC
Importación de datos en PostgreSQL en Amazon RDS Puede usar varias herramientas diferentes para importar datos en su instancia de base de datos PostgreSQL en Amazon RDS.	Importación de datos en PostgreSQL en Amazon RDS

Área de la tarea	Documentación relacionada
Configuración de réplicas de solo lectura (principales y en espera) RDS for PostgreSQL admite réplicas de lectura en la misma región de AWS y en una región de AWS distinta a la de la instancia principal.	Trabajo con réplicas de lectura de instancias de base de datos Uso de réplicas de lectura para Amazon RDS para PostgreSQL Creación de una réplica de lectura en una Región de AWS distinta
Descripción de los grupos de seguridad De manera predeterminada, las instancias de base de datos se crean con un firewall que impide el acceso a ellas. Para proporcionar acceso a través de ese firewall, edite las reglas de entrada para el grupo de seguridad asociado a la VPC que aloja la instancia de base de datos.	Control de acceso con grupos de seguridad
Configuración de grupo de parámetros y características Para cambiar los parámetros predeterminados de la instancia de base de datos, cree un grupo de parámetros de base de datos personalizado y cambie la configuración en él. Si lo hace antes de crear la instancia de base de datos, puede elegir su grupo de parámetros de base de datos personalizado cuando crea la instancia.	Grupos de parámetros para Amazon RDS
Conexión a la instancia de base de datos PostgreSQL Después de crear un grupo de seguridad y de asociarlo a una instancia de base de datos, puede conectarse a la instancia de base de datos usando cualquier aplicación cliente estándar de SQL, como `psql` o `pgAdmin`.	Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL Uso de SSL con una instancia de base de datos PostgreSQL

Área de la tarea	Documentación relacionada
Backup y restauración de una instancia de base de datos Puede configurar su instancia de base de datos para que realice backups automatizados o tomar snapshots manuales y restaurar después las instancias a partir de los backups o los snapshots.	Copia de seguridad, restauración y exportación de datos
Monitorización de la actividad y el desempeño de una instancia de base de datos Puede monitorizar una instancia de base de datos PostgreSQL utilizando métricas, eventos y monitorización avanzada de CloudWatch Amazon RDS.	Consulta de métricas en la consola de Amazon RDS Consulta de eventos de Amazon RDS
Actualización de la versión de la base de datos de PostgreSQL Puede realizar actualizaciones principales y secundarias de su instancia de base de datos PostgreSQL.	Actualizaciones del motor de base de datos de RDS para PostgreSQL Elección de una versión principal para una actualización de RDS para PostgreSQL
Trabajo con archivos de registro Puede obtener acceso a los archivos de registro de su instancia de base de datos PostgreSQL.	Archivos de registro de bases de datos de RDS para PostgreSQL
Descripción de las prácticas recomendadas para las instancias de base de datos de PostgreSQL Consulte algunas de las prácticas recomendadas para trabajar con PostgreSQL en Amazon RDS.	Prácticas recomendadas para trabajar con PostgreSQL

A continuación, se presenta una lista de otras secciones de esta guía que pueden ser útiles para comprender y utilizar las características importantes de RDS for PostgreSQL:

- Descripción de los roles y permisos de PostgreSQL
- Control del acceso de los usuarios a la base de datos de PostgreSQL

- Uso de parámetros en su instancia de base de datos de RDS for PostgreSQL
- Comprensión de los mecanismos de registro admitidos por RDS for PostgreSQL
- Uso de autovacuum de PostgreSQL en Amazon RDS para PostgreSQL
- Uso de un servidor de DNS personalizado para el acceso a la red de salida.

Trabajo con el entorno de vista previa de bases de datos

La comunidad de PostgreSQL lanza continuamente nuevas versiones y nuevas extensiones de PostgreSQL, incluso versiones beta. Esto ofrece a los usuarios de PostgreSQL la oportunidad de probar una nueva versión de PostgreSQL con antelación. Para obtener más información sobre el proceso de lanzamiento de la versión beta de la comunidad de PostgreSQL, consulte la información sobre la versión beta en la documentación de PostgreSQL. Del mismo modo, Amazon RDS ofrece algunas versiones beta de PostgreSQL como versiones preliminares. Esto le permite crear instancias de base de datos con la versión de vista previa y probar sus funciones en el entorno de vista previa de la base de datos.

Las instancias de base de datos de RDS para PostgreSQL en el entorno de vista previa de base de datos son funcionalmente similares a otras instancias de RDS para PostgreSQL. Sin embargo, no puede usar una versión de vista previa para la producción.

Tenga en cuenta las siguientes limitaciones importantes:

- Todas las instancias de base de datos se eliminan 60 días después de crearlas, junto con las copias de seguridad e instantáneas.
- Solo puede crear una instancia de base de datos en una Virtual Private Cloud (VPC) en función del servicio de Amazon VPC.
- Solo puede utilizar almacenamiento SSD de uso general y SSD IOPS provisionadas.
- No puede obtener ayuda de AWS Support con instancias de base de datos. En su lugar, puede publicar sus preguntas en la comunidad de preguntas y respuestas administrada de AWS, AWSre:Post.
- No puede copiar una instantánea de una instancia de base de datos en un entorno de producción.

Las siguientes opciones son compatibles con la vista previa:

- Puede crear instancias de base de datos únicamente con los tipos de instancia M6i, R6i, M6g, M5, T3, R6g y R5. Para obtener más información sobre las clases de instancias de RDS, consulte Clases de instancia de base de datos de .
- Puede utilizar implementaciones Single-AZ y Multi-AZ.
- Puede utilizar las funciones estándar de volcado y carga de PostgreSQL para exportar bases de datos desde o importar bases de datos hacia el entorno de la vista previa de base de datos.

Temas

- Características no compatibles en el entorno de vista previa de bases de datos
- Versión 17 de PostgreSQL en el entorno de vista previa de bases de datos
- Creación de una nueva instancia de base de datos en el entorno de vista previa de bases de datos

Características no compatibles en el entorno de vista previa de bases de datos

Las siguientes características no están disponibles en el entorno de vista previa de bases de datos:

- Copia de instantáneas entre regiones
- Réplicas de lectura entre regiones

Versión 17 de PostgreSQL en el entorno de vista previa de bases de datos

> **Note**
>
> Esta es la documentación preliminar de la versión 17 de Amazon RDS PostgreSQL. Está sujeta a cambios.

La versión 17.0 de PostgreSQL ya está disponible en el entorno de vista previa de bases de datos de Amazon RDS. La versión 17.0 de PostgreSQL incluye varias mejoras que se describen en la siguiente documentación de PostgreSQL, PostgreSQL 17 Released!

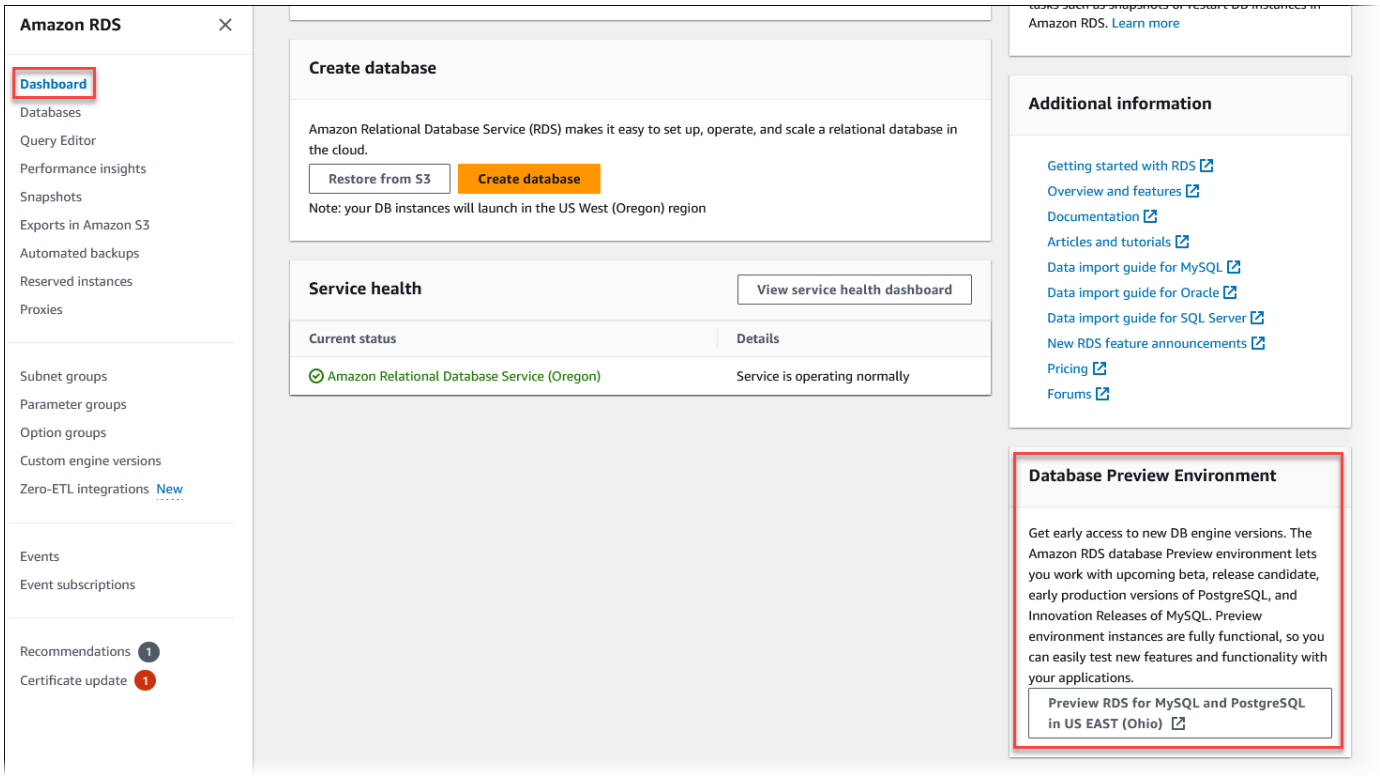
Para obtener información acerca del entorno de vista previa de base de datos, consulte the section called “Trabajo con el entorno de vista previa de bases de datos”. Para acceder al entorno de vista previa desde la consola, seleccione https://console.aws.amazon.com/rds-preview/.

Creación de una nueva instancia de base de datos en el entorno de vista previa de bases de datos

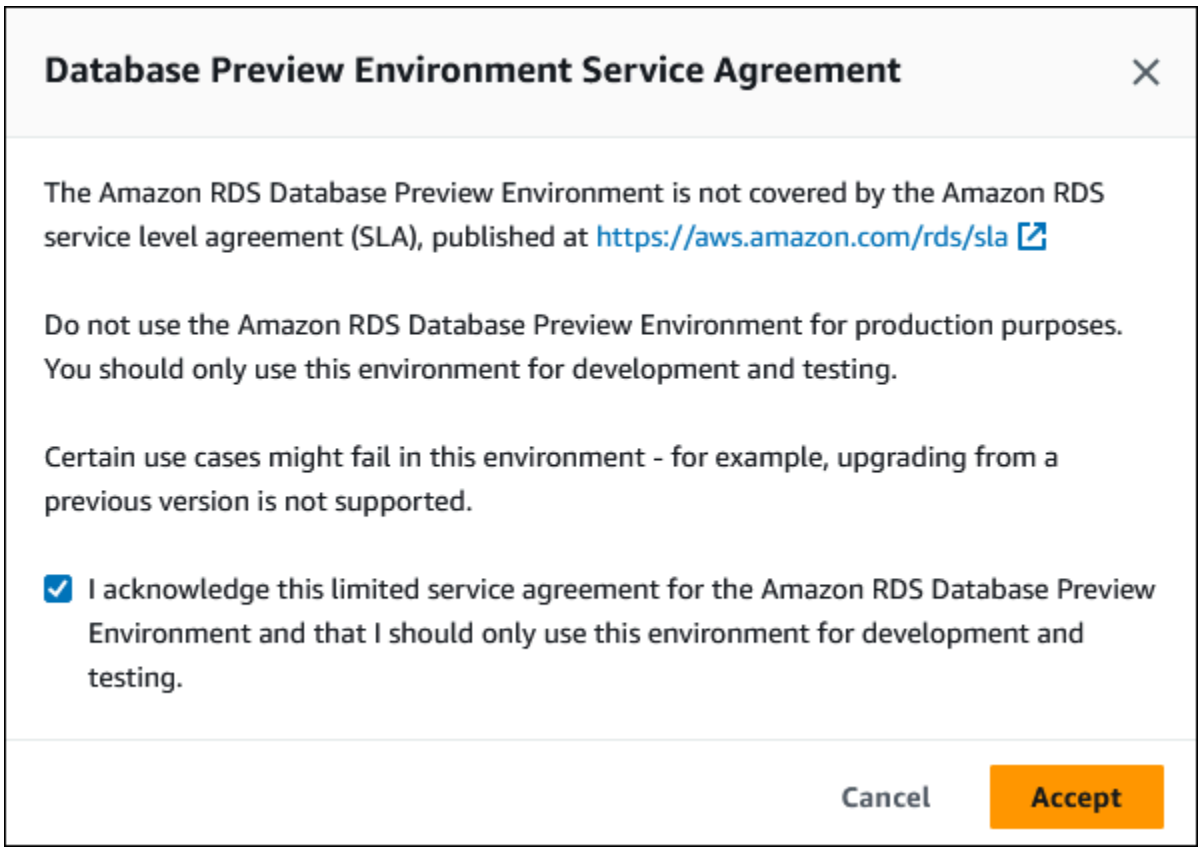
Utilice el procedimiento siguiente para crear una instancia de base de datos en el entorno de vista previa.

Para crear una instancia de base de datos en el entorno de vista previa de bases de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Dashboard (Panel) en el panel de navegación.
3. En la página Dashboard (Panel), busque la sección Database Preview Environment (Entorno de vista previa de base de datos), tal como se muestra en la siguiente imagen.



Puede navegar directamente a Database Preview Environment. Antes de continuar, debe reconocer y aceptar las limitaciones.



4. Para crear la instancia de base de datos de RDS para PostgreSQL, siga el mismo proceso que para crear cualquier instancia de base de datos de Amazon RDS. Para obtener más información, consulte el procedimiento Consola en Creación de una instancia de base de datos.

Para crear una instancia en el entorno de vista previa de base de datos mediante la API de RDS o la AWS CLI, utilice el siguiente punto de conexión.

```
rds-preview.us-east-2.amazonaws.com
```

Versiones de base de datos de PostgreSQL disponibles

Amazon RDS admite instancias de base de datos que ejecutan varias ediciones de PostgreSQL. Puede especificar cualquier versión disponible actualmente de PostgreSQL cuando crea una nueva instancia de base de datos. Puede especificar la versión principal (como PostgreSQL 14) y cualquier versión secundaria disponible para la versión principal especificada. Si no se especifica ninguna versión, Amazon RDS cambia de forma predeterminada a una versión disponible, normalmente la más reciente. Si se especifica una versión principal pero no una versión secundaria, Amazon RDS usa de manera predeterminada una versión reciente de la versión principal especificada.

Para ver una lista de las versiones disponibles, así como de las versiones predeterminadas para instancias de bases de datos recién creadas, utilice el comando `describe-db-engine-versions` de la AWS CLI. Por ejemplo, para mostrar la versión predeterminada del motor PostgreSQL, utilice el siguiente comando:

```
aws rds describe-db-engine-versions --default-only --engine postgres
```

Para obtener más información sobre las versiones de PostgreSQL compatibles con Amazon RDS, consulte las notas de la versión de Amazon RDS para PostgreSQL. También puede ver información sobre las fechas de soporte de las versiones principales del motor ejecutando el comando describe-db-major-engine-versions de la AWS CLI o mediante la operación de la API de RDS DescribeDBMajorEngineVersions.

Si no está preparado para realizar una actualización manual a una nueva versión principal del motor antes de la fecha de finalización del soporte estándar de RDS, Amazon RDS inscribirá automáticamente las bases de datos en el Soporte extendido de Amazon RDS después de la fecha de finalización del soporte estándar de RDS. Luego, puede seguir ejecutando RDS para PostgreSQL (versión 11 y posteriores). Para obtener más información, consulte Soporte extendido de Amazon RDS con Amazon RDS y Precios de Amazon RDS.

Versiones obsoleta para Amazon RDS for PostgreSQL

Tenga en cuenta las siguientes versiones obsoletas:

- RDS para PostgreSQL 10 quedó obsoleto en febrero de 2023.
- RDS para PostgreSQL 9.6 quedó obsoleto en marzo de 2022.
- RDS para PostgreSQL 9.5 quedó obsoleto en marzo de 2021.

Para obtener más información sobre la política de obsolescencia de RDS for PostgreSQL, consulte Preguntas frecuentes de Amazon RDS Para obtener más información sobre las versiones de PostgreSQL, consulte Política de control de versiones en la documentación de PostgreSQL.

Descripción del proceso de lanzamiento incremental de RDS para PostgreSQL

RDS para PostgreSQL ofrece correcciones de seguridad, mejoras de rendimiento y nuevas características mediante versiones incrementales, al tiempo que mantiene la compatibilidad con las versiones menores. Estas versiones se etiquetan como R1, R2, R3, etc.

Convención de nomenclatura de las versiones de lanzamiento

- R1 es la versión inicial de una versión menor. Ocasionalmente, incluye nuevas características, extensiones o actualizaciones de las extensiones existentes.
- Las versiones de lanzamiento posteriores (R2, R3 y posteriores) incluyen:
  - Actualizaciones de seguridad
  - Mejoras en el rendimiento
  - Correcciones de errores
  - Actualizaciones de extensiones

Ventajas del proceso de lanzamiento incremental de RDS para PostgreSQL

El proceso de lanzamiento incremental proporciona las siguientes ventajas:

- Adopción rápida de las nuevas versiones de la comunidad de PostgreSQL, gestionando por separado las mejoras específicas de RDS a través de versiones posteriores. Esto agiliza el proceso de lanzamiento y garantiza una entrega más rápida de las actualizaciones críticas.
- Acceso a correcciones de errores, nuevas características, actualizaciones de seguridad y actualizaciones de extensiones mientras se mantiene la compatibilidad con la versión secundaria de PostgreSQL.

Administración de actualizaciones de versiones

Amazon RDS le notifica sobre las nuevas versiones incrementales mediante acciones de mantenimiento pendientes en la AWS Management Console. Puede actualizar la base de datos mediante uno de estos métodos:

- Habilite las actualizaciones automáticas durante las ventanas de mantenimiento programadas.
- Aplique las actualizaciones manualmente mediante las acciones de mantenimiento pendientes.

- Utilice implementaciones azul/verde con replicación física para minimizar el tiempo de inactividad. Para obtener más información, consulte Las implementaciones azul/verde admiten la actualización de versiones secundarias de RDS para PostgreSQL.

Antes de actualizar la base de datos, tenga en cuenta los siguientes puntos claves:

- Es necesario reiniciar la base de datos para realizar actualizaciones a menos que utilice implementaciones azul/verde con replicación física.
- Algunas versiones incrementales son obligatorias, especialmente las que incluyen correcciones de seguridad.

Para obtener más información sobre la actualización de la instancia de base de datos de Amazon RDS, consulte Extensiones de confianza de PostgreSQL y apply-pending-maintenance-action.

Versiones de extensiones de PostgreSQL compatibles

RDS for PostgreSQL admite muchas extensiones de PostgreSQL. La comunidad de PostgreSQL a veces se refiere a estos como módulos. Las extensiones amplían la funcionalidad proporcionada por el motor PostgreSQL. Puede encontrar una lista de las extensiones admitidas por Amazon RDS en el grupo de parámetros de base de datos predeterminado de esa versión de PostgreSQL. También puede ver la lista de extensiones actuales que usan `psql` mostrando el parámetro `rds.extensions` como en el siguiente ejemplo.

```
SHOW rds.extensions;
```

> **Note**
>
> Los parámetros añadidos en una versión secundaria pueden mostrarse de manera incorrecta cuando se utiliza el parámetro `rds.extensions` en `psql`.

A partir de RDS para PostgreSQL 13, ciertas extensiones pueden instalarlas usuarios de bases de datos que no sean `rds_superuser`. Esto se conoce como extensiones de confianza. Para obtener más información, consulte Extensiones de confianza de PostgreSQL.

Ciertas versiones de RDS para PostgreSQL admiten el parámetro `rds.allowed_extensions`. Este parámetro permite que un `rds_superuser` limite las extensiones que se pueden instalar en la instancia de base de datos de RDS para PostgreSQL. Para obtener más información, consulte Restringir la instalación de extensiones de PostgreSQL.

Para obtener una lista de las extensiones y versiones de PostgreSQL compatibles con cada versión disponible de RDS para PostgreSQL, consulte Extensiones de PostgreSQL admitidas en Amazon RDS en las Notas de la versión de Amazon RDS para PostgreSQL.

Restringir la instalación de extensiones de PostgreSQL

Puede restringir qué extensiones se pueden instalar en una instancia de base de datos de PostgreSQL. De forma predeterminada, este parámetro no está configurado, por lo que se puede agregar cualquier extensión compatible si el usuario tiene permisos para hacerlo. Para ello, establezca el parámetro `rds.allowed_extensions` en una cadena de nombres de extensión separados por comas. Al agregar una lista de extensiones a este parámetro, identifica explícitamente

las extensiones que puede utilizar su instancia de base de datos de RDS para PostgreSQL. Solo estas extensiones se pueden instalar en la instancia de base de datos de PostgreSQL.

La cadena predeterminada para el parámetro `rds.allowed_extensions` es '*', lo que significa que se puede instalar cualquier extensión disponible para la versión del motor. Cambiar el parámetro `rds.allowed_extensions` no requiere un reinicio de la base de datos porque es un parámetro dinámico.

El motor de instancia de base de datos de PostgreSQL debe ser una de las siguientes versiones para que pueda utilizar el parámetro:`rds.allowed_extensions`

- Todas las versiones de PostgreSQL 16
- PostgreSQL 15 y todas las versiones posteriores
- PostgreSQL 14 y todas las versiones posteriores
- PostgreSQL 13.3 y versiones secundarias posteriores
- PostgreSQL 12.7 y versiones secundarias posteriores

Para ver qué instalaciones de extensión están permitidas, utilice el siguiente comando psql.

```
postgres=> SHOW rds.allowed_extensions;
 rds.allowed_extensions
------------------------
 *
```

Si se instaló una extensión antes de dejarla fuera de la lista en el parámetro `rds.allowed_extensions`, la extensión todavía se puede utilizar normalmente y comandos como `ALTER EXTENSION` y `DROP EXTENSION` continuarán funcionando. Sin embargo, una vez restringida una extensión, los comandos `CREATE EXTENSION` de la extensión restringida fallarán.

La instalación de dependencias de extensión con `CREATE EXTENSION CASCADE` también están restringidas. La extensión y sus dependencias deben especificarse en `rds.allowed_extensions`. Si falla una instalación de dependencia de extensión, se producirá un error en toda la instrucción `CREATE EXTENSION CASCADE`.

Si no se incluye una extensión con el parámetro `rds.allowed_extensions`, verá un error como el siguiente si intenta instalarla.

```
ERROR: permission denied to create extension "extension-name"
```

```
HINT: This extension is not specified in "rds.allowed_extensions".
```

Extensiones de confianza de PostgreSQL

Para instalar la mayoría de las extensiones de PostgreSQL requiere privilegios de `rds_superuser`. PostgreSQL 13 presentó extensiones de confianza, que reducen la necesidad de conceder privilegios `rds_superuser` a los usuarios normales. Con esta característica, los usuarios pueden instalar muchas extensiones si tienen el privilegio de `CREATE` en la base de datos actual en lugar de requerir el rol de `rds_superuser`. Para obtener más información, consulte el comando de SQL CREATE EXTENSION en la documentación de PostgreSQL.

A continuación se enumeran las extensiones que puede instalar un usuario que tiene el privilegio de `CREATE` en la base de datos actual y no requieren el rol de:`rds_superuser`

- bool_plperl
- btree_gin
- btree_gist
- citext
- cube
- dict_int
- fuzzystrmatch
- hstore
- intarray
- isn
- jsonb_plperl
- ltree
- pg_trgm
- pgcrypto
- plperl
- plpgsql
- pltcl
- tablefunc
- tsm_system_rows

- tsm_system_time
- unaccent
- uuid-ossp

Para obtener una lista de las extensiones y versiones de PostgreSQL compatibles con cada versión disponible de RDS para PostgreSQL, consulte Extensiones de PostgreSQL admitidas en Amazon RDS en las Notas de la versión de Amazon RDS para PostgreSQL.

Uso de las características de PostgreSQL admitidas por Amazon RDS para PostgreSQL

Amazon RDS para PostgreSQL es compatible con muchas de las características más comunes de PostgreSQL. Por ejemplo, PostgreSQL tiene una característica de autovacuum que realiza un mantenimiento rutinario de la base de datos. La característica autovacuum está activa de forma predeterminada. Aunque puede desactivar esta característica, le recomendamos encarecidamente que la mantenga activada. Comprender esta característica y lo que puede hacer para asegurarse de que funciona como debería es una tarea básica de cualquier DBA. Para obtener más información sobre el autovacuum, consulte Uso de autovacuum de PostgreSQL en Amazon RDS para PostgreSQL. Para obtener más información sobre otras tareas comunes de DBA, consulte Tareas comunes de los administradores de base de datos (DBA) para Amazon RDS para PostgreSQL.

RDS for PostgreSQL también admite extensiones que agregan funcionalidades importantes a la instancia de base de datos. Por ejemplo, puede utilizar la extensión PostGIS para trabajar con datos espaciales o utilizar la extensión pg_cron para programar el mantenimiento desde la instancia. Para obtener más información sobre las extensiones de PostgreSQL, consulte Uso de extensiones PostgreSQL con Amazon RDS para PostgreSQL.

Los contenedores de datos externos son un tipo específico de extensión diseñada para permitir que la instancia de base de datos de RDS for PostgreSQL funcione con otros tipos de datos o bases de datos comerciales. Para obtener más información sobre los contenedores de datos externos admitidos por RDS for PostgreSQL, consulte Uso de los contenedores de datos externos compatibles para Amazon RDS for PostgreSQL.

A continuación, encontrará información sobre algunas otras características admitidas por RDS para PostgreSQL.

Temas

- Tipos de datos personalizados y enumeraciones con RDS for PostgreSQL
- Desencadenadores de eventos para RDS for PostgreSQL
- Páginas enormes para RDS for PostgreSQL
- Replicación lógica para Amazon RDS para PostgreSQL
- Disco RAM para stats_temp_directory
- Espacios de tablas para RDS for PostgreSQL
- Intercalaciones de RDS para PostgreSQL para EBCDIC y otras migraciones de mainframe

- Administración de ranuras lógicas de RDS para PostgreSQL

Tipos de datos personalizados y enumeraciones con RDS for PostgreSQL

PostgreSQL admite la creación de tipos de datos personalizados y el trabajo con enumeraciones. Para obtener más información sobre cómo crear y trabajar con enumeraciones y otros tipos de datos, consulte Tipos enumerados en la documentación de PostgreSQL.

El siguiente es un ejemplo de creación de un tipo como enumeración seguida de la inserción de valores en una tabla.

```
CREATE TYPE rainbow AS ENUM ('red', 'orange', 'yellow', 'green', 'blue', 'purple');
CREATE TYPE
CREATE TABLE t1 (colors rainbow);
CREATE TABLE
INSERT INTO t1 VALUES ('red'), ( 'orange');
INSERT 0 2
SELECT * from t1;
colors
--------
red
orange
(2 rows)
postgres=> ALTER TYPE rainbow RENAME VALUE 'red' TO 'crimson';
ALTER TYPE
postgres=> SELECT * from t1;
colors
---------
crimson
orange
(2 rows)
```

Desencadenadores de eventos para RDS for PostgreSQL

Todas las versiones actuales de PostgreSQL admiten desencadenadores de eventos, al igual que todas las versiones disponibles de RDS for PostgreSQL. Puede utilizar la cuenta de usuario principal (`postgres`, predeterminada) para crear, modificar, renombrar y eliminar desencadenadores de eventos. Los disparadores de eventos están en el nivel de la instancia de base de datos, de modo que se pueden aplicar a todas las bases de datos de una instancia.

Por ejemplo, el siguiente código crea un desencadenador de evento que imprime el usuario actual al final de cada comando de lenguaje de definición de datos (DDL).

```
CREATE OR REPLACE FUNCTION raise_notice_func()
    RETURNS event_trigger
    LANGUAGE plpgsql AS
$$
BEGIN
    RAISE NOTICE 'In trigger function: %', current_user;
END;
$$;

CREATE EVENT TRIGGER event_trigger_1
    ON ddl_command_end
EXECUTE PROCEDURE raise_notice_func();
```

Para obtener más información acerca de los desencadenadores de eventos de PostgreSQL, consulte Desencadenadores de eventos en la documentación de PostgreSQL.

Hay varias limitaciones que afectan al uso de los disparadores de eventos de PostgreSQL en Amazon RDS. Estos incluyen los siguientes:

- No puede crear desencadenadores de eventos en réplicas de lectura. Puede, no obstante, crear desencadenadores de eventos en un origen de réplica de lectura. Los disparadores de eventos se copian a continuación en la réplica de lectura. Los desencadenadores de eventos en la réplica de lectura no se activan en la réplica de lectura cuando los cambios se envían desde el origen. No obstante, si se promueve la réplica de lectura, los disparadores de eventos existentes se activarán cuando se produzcan operaciones en la base de datos.
- Para realizar una actualización de versión principal en una instancia de base de datos de PostgreSQL que use desencadenadores de eventos, debe eliminar los desencadenadores de eventos antes de actualizar la instancia.

Páginas enormes para RDS for PostgreSQL

Las páginas enormes son una característica de administración de la memoria que reduce la sobrecarga cuando una instancia de base de datos trabaja con grandes fragmentos contiguos de memoria, como la utilizada por los búferes compartidos. Esta característica de PostgreSQL es compatible con todas las versiones de RDS for PostgreSQL disponibles actualmente. Las páginas

de gran tamaño se asignan a la aplicación con llamadas a la memoria compartida de `mmap` o `SYSV`. RDS for PostgreSQL admite tamaños de página de 4 KB y 2 MB.

Puede activar o desactivar las páginas enormes cambiando el valor del parámetro `huge_pages`. La característica está habilitada de forma predeterminada para todas las clases de instancias de base de datos que no sean de la clase de instancia de base de datos micro, pequeña y mediana.

RDS for PostgreSQL utiliza páginas enormes en función de la memoria compartida disponible. Si la instancia de base de datos no puede usar páginas de gran tamaño a causa de las restricciones de la memoria compartida, Amazon RDS impide que la instancia de base de datos se inicie. En este caso, Amazon RDS define el estado de la instancia de base de datos en un estado de los parámetros no compatible. En este caso, puede establecer el parámetro `huge_pages` en `off` para permitir que Amazon RDS inicie la instancia de base de datos.

El parámetro `shared_buffers` es esencial para configurar el grupo de memoria compartida que se requiere para usar las páginas enormes. El valor predeterminado del parámetro `shared_buffers` utiliza una macro de parámetros de base de datos. Esta macro define un porcentaje del total de las páginas de 8 KB disponibles para la memoria de la instancia de base de datos. Cuando utiliza páginas de gran tamaño, esas páginas se asignan con las páginas de gran tamaño. Amazon RDS cambia una instancia de base de datos a un estado de parámetros incompatible si los parámetros de memoria compartida se han definido de un modo que requiere más del 90 % de la memoria de la instancia de base de datos.

Para obtener más información sobre la administración de memoria de PostgreSQL, consulte Consumo de recursos en la documentación de PostgreSQL.

Replicación lógica para Amazon RDS para PostgreSQL

A partir de la versión 10.4, RDS para PostgreSQL admite la sintaxis SQL de publicación y suscripción introducida en PostgreSQL 10. Para obtener más información, consulte Replicación lógica en la documentación de PostgreSQL.

> **Note**
>
> Además de la función de replicación lógica nativa de PostgreSQL introducida en PostgreSQL 10, RDS para PostgreSQL también admite la extensión `pglogical`. Para obtener más información, consulte Uso de pglogical para sincronizar datos entre instancias.

A continuación encontrará información sobre la configuración de la replicación lógica para una instancia de base de datos de RDS for PostgreSQL.

Temas

- Comprensión de la replicación lógica y la descodificación lógica
- Trabajo con ranuras de replicación lógica
- Replicación de datos de nivel de tabla mediante replicación lógica

Comprensión de la replicación lógica y la descodificación lógica

RDS for PostgreSQL admite el streaming de los cambios del registro de escritura anticipada (WAL) mediante las ranuras de replicación lógica de PostgreSQL. También admite el uso de decodificación lógica. Puede configurar ranuras de replicación lógica en su instancia y transmitir los cambios de la base de datos a través de estas ranuras a un cliente como `pg_recvlogical`. Las ranuras de replicación lógica se crean a nivel de la base de datos y admiten conexiones de replicación a una única base de datos.

Los clientes más comunes para la replicación lógica de PostgreSQL son AWS Database Migration Service o un host administrado personalizado en una instancia de Amazon EC2. La ranura de replicación lógica no tiene información sobre el receptor de la transmisión. Además, no existe el requisito de que el destino sea una base de datos de réplica. Si configura una ranura de replicación lógica y no lee desde la ranura, los datos podrían escribirse y rellenarse rápidamente en el almacenamiento de la instancia de base de datos.

La replicación y descodificación lógicas de PostgreSQL en Amazon RDS se activan con un parámetro, un tipo de conexión de replicación y un rol de seguridad. El cliente para la descodificación lógica puede ser cualquier cliente que sea capaz de establecer una conexión de replicación con una base de datos en una instancia de base de datos PostgreSQL.

Para activar la descodificación lógica para una instancia de base de datos de RDS for PostgreSQL

1. Asegúrese de que la cuenta de usuario que está utilizando tenga los siguientes roles:
   - El rol `rds_superuser` para poder activar la replicación lógica
   - El rol `rds_replication` para conceder permisos para administrar ranuras lógicas y para transmitir datos mediante ranuras lógicas
2. Establezca el parámetro estático `rds.logical_replication` en 1. Como parte de la aplicación de este parámetro, también defina los parámetros `wal_level`, `max_wal_senders`,

`max_replication_slots` y `max_connections`. Estos cambios de parámetro pueden incrementar la generación de WAL, por lo que el parámetro `rds.logical_replication` se debe configurar solo cuando se utilicen ranuras lógicas.

3. Reinicie la instancia de base de datos para que el parámetro `rds.logical_replication` estático tenga efecto.
4. Cree una ranura de replicación lógica como se indica en la siguiente sección. Este proceso necesita que especifique un complemento de descodificación. Actualmente, RDS for PostgreSQL admite los complementos de salida test_decoding y wal2json que se incluyen con PostgreSQL.

Para obtener más información acerca de la descodificación lógica de PostgreSQL, consulte la documentación de PostgreSQL.

Trabajo con ranuras de replicación lógica

Puede usar comandos de SQL para trabajar con las ranuras lógicas. Por ejemplo, el siguiente comando crea una ranura lógica denominada `test_slot` usando el complemento de salida predeterminado de PostgreSQL `test_decoding`.

```
SELECT * FROM pg_create_logical_replication_slot('test_slot', 'test_decoding');
slot_name    | xlog_position
-----------------+---------------
regression_slot | 0/16B1970
(1 row)
```

Para ver las ranuras lógicas, use el siguiente comando.

```
SELECT * FROM pg_replication_slots;
```

Para eliminar una ranura lógica, use el siguiente comando.

```
SELECT pg_drop_replication_slot('test_slot');
pg_drop_replication_slot
----------------------
(1 row)
```

Para ver más ejemplos del trabajo con ranuras de replicación lógica, consulte Logical Decoding Examples en la documentación de PostgreSQL.

Luego de crear la ranura de replicación lógica, se puede iniciar el streaming. El siguiente ejemplo muestra cómo se controla la decodificación lógica a través del protocolo de replicación del streaming. Este ejemplo utiliza el programa pg_recvlogical, que se incluye en la distribución de PostgreSQL. Esto requiere que la autenticación del cliente se configure para permitir las conexiones de replicación.

```
pg_recvlogical -d postgres --slot test_slot -U postgres
    --host -instance-name.111122223333.aws-region.rds.amazonaws.com
    -f -  --start
```

Para ver el contenido de la vista `pg_replication_origin_status`, consulte la función `pg_show_replication_origin_status`.

```
SELECT * FROM pg_show_replication_origin_status();
local_id | external_id | remote_lsn | local_lsn
----------+-------------+------------+-----------
(0 rows)
```

Replicación de datos de nivel de tabla mediante replicación lógica

Puede utilizar la replicación lógica para replicar los datos de las tablas de origen a las tablas de destino en RDS para PostgreSQL. La replicación lógica primero realiza una carga inicial de los datos existentes de las tablas de origen y, a continuación, continúa replicando los cambios en curso.

1. Creación de las tablas de origen

   Conéctese a la base de datos de origen en la instancia de base de datos de RDS para PostgreSQL:

   ```
   source=> CREATE TABLE testtab (slno int primary key);
   CREATE TABLE
   ```

2. Inserción de datos en las tablas de origen

   ```
   source=> INSERT INTO testtab VALUES (generate_series(1,1000));
   INSERT 0 1000
   ```

3. Creación de una publicación para las tablas de origen

   - Cree una publicación para las tablas de origen:

```
source=> CREATE PUBLICATION testpub FOR TABLE testtab;
CREATE PUBLICATION
```

   - Utilice una consulta SELECT para verificar los detalles de la publicación que se creó:

```
source=> SELECT * FROM pg_publication;
  oid   | pubname | pubowner | puballtables | pubinsert | pubupdate | pubdelete |
 pubtruncate | pubviaroot
--------+---------+----------+--------------+-----------+-----------+-----------
+-------------+------------
 115069 | testpub |    16395 | f            | t         | t         | t         |
 t           | f
(1 row)
```

   - Verifique que las tablas de origen se hayan agregado a la publicación:

```
source=> SELECT * FROM pg_publication_tables;
pubname | schemaname | tablename
---------+------------+-----------
 testpub | public     | testtab
(1 rows)
```

   - Para replicar todas las tablas de una base de datos, utilice:

```
CREATE PUBLICATION testpub FOR ALL TABLES;
```

   - Si la publicación ya está creada para una tabla individual y necesita agregar una tabla nueva, puede ejecutar la siguiente consulta para agregar cualquier tabla nueva a la publicación existente:

```
ALTER PUBLICATION <publication_name> add table <new_table_name>;
```

4. Conéctese a la base de datos de destino y cree tablas de destino

   - Conéctese a la base de datos de destino en la instancia de base de datos de destino. Cree las tablas de destino con los mismos nombres que las tablas de origen:

```
target=> CREATE TABLE testtab (slno int primary key);
CREATE TABLE
```

   - Asegúrese de que no haya datos presentes en las tablas de destino ejecutando una consulta SELECT en las tablas de destino:

```
target=> SELECT count(*) FROM testtab;
 count
-------
     0
(1 row)
```

5. Cree y verifique la suscripción en la base de datos de destino

   - Cree la suscripción en la base de datos de destino:

```
target=> CREATE SUBSCRIPTION testsub
CONNECTION 'host=<source RDS/host endpoint> port=5432 dbname=<source_db_name>
 user=<user> password=<password>'
PUBLICATION testpub;
NOTICE:  Created replication slot "testsub" on publisher
CREATE SUBSCRIPTION
```

   - Utilice una consulta SELECT para verificar que la suscripción esté habilitada:

```
target=> SELECT oid, subname, subenabled, subslotname, subpublications FROM
 pg_subscription;
  oid  | subname | subenabled | subslotname | subpublications
-------+---------+------------+-------------+-----------------
 16434 | testsub | t          | testsub     | {testpub}
(1 row)
```

- Cuando se crea la suscripción, se cargan todos los datos de las tablas de origen en las tablas de destino. Ejecute una consulta SELECT en las tablas de destino para verificar que se cargan los datos iniciales:

```
target=> SELECT count(*) FROM testtab;
 count
-------
  1000
(1 row)
```

6. Verificación de la ranura de replicación en la base de datos de origen

   La creación de una suscripción en la base de datos de destino crea una ranura de replicación en la base de datos de origen. Verifique los detalles de la ranura de replicación ejecutando la siguiente consulta SELECT en la base de datos de origen:

```
source=> SELECT * FROM pg_replication_slots;

slot_name |  plugin  | slot_type | datoid | database | temporary | active |
 active_pid | xmin | catalog_xmin | restart_lsn | confirmed_flush_lsn | wal_status
 | safe_wal_size
----------+----------+-----------+--------+----------+-----------+--------
+------------+------+--------------+-------------+---------------------
+------------+---------------
testsub   | pgoutput | logical   | 115048 | source   | f         | t      |
 846 |      |         6945 | 58/B4000568 | 58/B40005A0         | reserved   |
(1 row)
```

7. prueba de replicación

   - Compruebe si los cambios en los datos de las tablas de origen se están replicando en las tablas de destino insertando filas en las tablas de origen:

```
source=> INSERT INTO testtab VALUES(generate_series(1001,2000));
INSERT 0 1000

source=> SELECT count(*) FROM testtab;
 count
-------
  2000
(1 row)
```

   - Verifique el número de filas en las tablas de destino para confirmar que se están replicando las nuevas inserciones:

```
target=> SELECT count(*) FROM testtab;
 count
-------
  2000
(1 row)
```

8. Actualización de la suscripción después de agregar tablas

   - Cuando se agregan nuevas tablas a una publicación existente, es obligatorio actualizar la suscripción para que los cambios surtan efecto:

```
ALTER SUBSCRIPTION <subscription_name> REFRESH PUBLICATION;
```

   - Este comando obtiene la información de las tablas que faltan del publicador e inicia la replicación de las tablas que se agregaron a las publicaciones suscritas desde que se creó la suscripción o se actualizó por última vez.

Disco RAM para stats_temp_directory

Puede utilizar el parámetro `rds.pg_stat_ramdisk_size` de RDS for PostgreSQL para especificar la memoria del sistema asignada a un disco RAM para almacenar el `stats_temp_directory` de PostgreSQL. El parámetro del disco RAM solo está disponible en RDS para la versión 14 y anteriores de PostgreSQL.

Para algunas cargas de trabajo, configurar este parámetro puede mejorar el rendimiento y reducir los requisitos de E/S. Para obtener más información acerca de `stats_temp_directory`, consulte la documentación de PostgreSQL..

Para configurar un disco RAM para `stats_temp_directory`, configure el parámetro `rds.pg_stat_ramdisk_size` en un valor literal entero en el grupo de parámetros utilizado por la instancia de base de datos. Este parámetro indica MB, por lo que debe utilizar un valor entero. Las expresiones, fórmulas y funciones no son válidas para el parámetro `rds.pg_stat_ramdisk_size`. Asegúrese de reiniciar la instancia de base de datos para que el cambio surta efecto. Para obtener información acerca de cómo configurar los parámetros, consulte Grupos de parámetros para Amazon RDS.

Por ejemplo, el comando de la AWS CLI siguiente establece el parámetro del disco RAM en 256 MB.

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name pg-95-ramdisk-testing \
    --parameters "ParameterName=rds.pg_stat_ramdisk_size, ParameterValue=256,
 ApplyMethod=pending-reboot"
```

Después de reiniciar, ejecute el siguiente comando para ver el estado de `stats_temp_directory`.

```
postgres=> SHOW stats_temp_directory;
```

El comando debe devolver lo siguiente.

```
stats_temp_directory
---------------------------
/rdsdbramdisk/pg_stat_tmp
(1 row)
```

Espacios de tablas para RDS for PostgreSQL

RDS for PostgreSQL es compatible con los espacios de tablas por razones de compatibilidad. Debido a que todo el almacenamiento se encuentra en un único volumen lógico, no puede usar espacios de tabla para la división o el aislamiento de la E/S. Nuestros puntos de referencia y experiencia indican que un único volumen lógico es la mejor configuración para la mayoría de los casos de uso.

Para crear y utilizar espacios de tablas con su instancia de base de datos RDS para PostgreSQL se requiere el rol de `rds_superuser`. La cuenta de usuario principal de su instancia de base de datos RDS para PostgreSQL (nombre predeterminado, `postgres`) es miembro de este rol. Para obtener más información, consulte Descripción de los roles y permisos de PostgreSQL.

Si especifica un nombre de archivo al crear un espacio de tabla, el prefijo de ruta es `/rdsdbdata/db/base/tablespace`. El siguiente ejemplo coloca los archivos de espacio de tabla en `/rdsdbdata/db/base/tablespace/data`. Este ejemplo asume que existe un usuario `dbadmin` (rol) y que se le otorgó el rol `rds_superuser` necesario para trabajar con espacios de tablas.

```
postgres=> CREATE TABLESPACE act_data
  OWNER dbadmin
  LOCATION '/data';
CREATE TABLESPACE
```

Para saber más sobre los espacios de tablas de PostgreSQL, consulte Espacios de tablas en la documentación de PostgreSQL.

Intercalaciones de RDS para PostgreSQL para EBCDIC y otras migraciones de mainframe

Las versiones 10 y posteriores de RDS para PostgreSQL incluyen la versión 60.2 de ICU, que se basa en Unicode 10.0 e incluye intercalaciones del repositorio de datos de configuración regional común de Unicode, CLDR 32. Estas bibliotecas de internacionalización de software garantizan que las codificaciones de caracteres se presenten de forma coherente, independientemente del sistema operativo o la plataforma. Para obtener más información acerca de Unicode CLDR-32, consulte la Nota de la versión de CLDR 32 en el sitio web de CLDR de Unicode. Puede obtener más información sobre los componentes de internacionalización de Unicode (ICU) en el sitio web del Comité Técnico de la UCI (ICU-TC). Para obtener información sobre la ICU-60, consulte Download ICU 60 (Descargar ICU 60).

A partir de la versión 14.3, RDS para PostgreSQL también incluye intercalaciones que ayudan con la integración y conversión de datos desde sistemas basados en EBCDIC. El código de intercambio decimal extendido codificado en binario extendido o EBCDIC se usa comúnmente en los sistemas operativos de mainframe. Estas intercalaciones proporcionadas por Amazon RDS están definidas de forma limitada para ordenar solo los caracteres Unicode que se asignan directamente a las páginas de códigos EBCDIC. Los caracteres se ordenan por puntos de código EBCDIC para permitir la validación de los datos después de la conversión. Estas intercalaciones no incluyen formularios desnormalizados ni caracteres Unicode que no se asignen directamente a un carácter en la página de códigos EBCDIC de origen.

Las asignaciones de caracteres entre las páginas de códigos EBCDIC y los puntos de código Unicode se basan en tablas publicadas por IBM. El conjunto completo está disponible en IBM como un archivo comprimido para descargarlo. RDS para PostgreSQL utilizó estas asignaciones con herramientas proporcionadas por la ICU para crear las intercalaciones que se enumeran en las tablas de esta sección. Los nombres de las intercalaciones incluyen un idioma y un país, según lo requiera la ICU. Sin embargo, en las páginas de códigos EBCDIC no se especifican idiomas y algunas páginas de códigos EBCDIC cubren varios países. Esto significa que la parte del idioma y el país de los nombres de intercalaciones de la tabla es arbitraria y no es necesario que coincidan con la configuración regional actual. En otras palabras, el número de página del código es la parte más importante del nombre de la intercalación en esta tabla. Puede usar cualquiera de las intercalaciones que se enumeran en las siguientes tablas en cualquier base de datos de RDS para PostgreSQL.

- Unicode to EBCDIC collations table: algunas herramientas de migración de datos de mainframe utilizan LATIN1 o LATIN9 internamente para codificar y procesar datos. Estas herramientas utilizan esquemas de ida y vuelta para proteger la integridad de los datos y admitir la conversión inversa. Las herramientas que procesan datos mediante la intercalación LATIN1, que no requiere un tratamiento especial, pueden usar las intercalaciones de esta tabla.
- Unicode to LATIN9 collations table: puede usar estas intercalaciones en cualquier base de datos de RDS para PostgreSQL.

En la siguiente tabla, encontrará intercalaciones disponibles en RDS para PostgreSQL que asignan páginas de códigos EBCDIC a puntos de código Unicode. Le recomendamos que utilice las intercalaciones de esta tabla para desarrollar aplicaciones que requieran una clasificación basada en el orden de las páginas de códigos de IBM.

Nombre de intercalación de PostgreSQL	Descripción de la asignación y el orden de clasificación de páginas de códigos
da-DK-cp277-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 277 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 277 de IBM CP.
de-DE-cp273-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 273 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 273 de IBM CP.
en-GB-cp285-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 285 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 285 de IBM CP.
en-US-cp037-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 037 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 037 de IBM CP.
es-ES-cp284-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 284 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 284 de IBM CP.
fi-FI-cp278-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 278 de IBM EBCDIC (por tablas de conversión) se ordenan

Nombre de intercalación de PostgreSQL	Descripción de la asignación y el orden de clasificación de páginas de códigos
	de acuerdo con la clasificación de puntos de códigos 278 de IBM CP.
fr-FR-cp297-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 297 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 297 de IBM CP.
it-IT-cp280-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 280 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 280 de IBM CP.
nl-BE-cp500-x-icu	Los caracteres Unicode que se asignan directamente a la página de código 500 de IBM EBCDIC (por tablas de conversión) se ordenan de acuerdo con la clasificación de puntos de códigos 500 de IBM CP.

Amazon RDS proporciona un conjunto de intercalaciones adicionales que ordenan los puntos de código Unicode que se asignan a caracteres LATIN9 mediante las tablas publicadas por IBM, en el orden de los puntos de código originales de acuerdo con la página de códigos EBCDIC de los datos de origen.

Nombre de intercalación de PostgreSQL	Descripción de la asignación y el orden de clasificación de páginas de códigos
da-DK-cp1142m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalm ente desde la página de código 1142 de IBM EBCDIC (según las tablas de conversión) se

Nombre de intercalación de PostgreSQL	Descripción de la asignación y el orden de clasificación de páginas de códigos
	clasifican en el orden de los puntos de códigos 1142 de IBM CP.
de-DE-cp1141m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalmente desde la página de código 1141 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1141 de IBM CP.
en-GB-cp1146m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalmente desde la página de código 1146 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1146 de IBM CP.
en-US-cp1140m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalmente desde la página de código 1140 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1140 de IBM CP.
es-ES-cp1145m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalmente desde la página de código 1145 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1145 de IBM CP.

Nombre de intercalación de PostgreSQL	Descripción de la asignación y el orden de clasificación de páginas de códigos
fi-FI-cp1143m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalm ente desde la página de código 1143 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1143 de IBM CP.
fr-FR-cp1147m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalm ente desde la página de código 1147 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1147 de IBM CP.
it-IT-cp1144m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalm ente desde la página de código 1144 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1144 de IBM CP.
nl-BE-cp1148m-x-icu	Los caracteres Unicode que se asignan a los caracteres LATIN9 convertidos originalm ente desde la página de código 1148 de IBM EBCDIC (según las tablas de conversión) se clasifican en el orden de los puntos de códigos 1148 de IBM CP.

A continuación, encontrará un ejemplo de cómo utilizar una intercalación de RDS para PostgreSQL.

```
db1=> SELECT pg_import_system_collations('pg_catalog');
 pg_import_system_collations
-----------------------------
                          36
db1=> SELECT '¤' < 'a' col1;
```

```
 col1
------
 t
db1=> SELECT '¤' < 'a' COLLATE "da-DK-cp277-x-icu" col1;
 col1
------
 f
```

Le recomendamos que utilice las intercalaciones de la Unicode to EBCDIC collations table y en la Unicode to LATIN9 collations table para el desarrollo de aplicaciones que requieran una clasificación basada en el orden de las páginas de códigos de IBM. Las siguientes intercalaciones (sufijo con la letra “b”) también son visibles en `pg_collation`, pero están pensadas para que las utilicen las herramientas de integración y migración de datos del mainframe en AWS que asignan páginas de códigos con cambios de puntos de código específicos y requieren un tratamiento especial en la intercalación. En otras palabras, no se recomienda el uso de las siguientes intercalaciones.

- da-DK-277b-x-icu
- da-DK-1142b-x-icu
- de-DE-cp273b-x-icu
- de-DE-cp1141b-x-icu
- en-GB-cp1146b-x-icu
- en-GB-cp285b-x-icu
- en-US-cp037b-x-icu
- en-US-cp1140b-x-icu
- es-ES-cp1145b-x-icu
- es-ES-cp284b-x-icu
- fi-FI-cp1143b-x-icu
- fr-FR-cp1147b-x-icu
- fr-FR-cp297b-x-icu
- it-IT-cp1144b-x-icu
- it-IT-cp280b-x-icu
- nl-BE-cp1148b-x-icu
- nl-BE-cp500b-x-icu

Para obtener más información sobre la migración de aplicaciones de entornos mainframe a AWS, consulte What is AWS Mainframe Modernization? (¿Qué es Mainframe Modernization?).

Para obtener más información sobre la administración de las intercalaciones en PostgreSQL, consulte Collation Support (Compatibilidad de Soporte de intercalaciones en la documentación de PostgreSQL.

Administración de ranuras lógicas de RDS para PostgreSQL

A partir de la versión 17 de Community PostgreSQL, se ha introducido una nueva característica para sincronizar automáticamente las ranuras de replicación lógica de los servidores principales a los servidores en espera mediante el parámetro `sync_replication_slots` o la función relacionada `pg_sync_replication_slots()`, que sincroniza manualmente las ranuras durante la ejecución.

Estas características están disponibles a partir de la versión 17 de RDS para PostgreSQL. Una configuración típica tendrá una instancia principal y su réplica de lectura, así como un suscriptor de replicación lógica a la principal.

Asegúrese de que la suscripción se cree con la opción de conmutación por error establecida en true:

```
CREATE SUBSCRIPTION subname CONNECTION 'host=...' PUBLICATION pubname WITH (failover =
 true);
```

Esto crea una ranura lógica en el publicador con la conmutación por error habilitada.

```
postgres=> SELECT slot_name, slot_type, failover FROM pg_catalog.pg_replication_slots;
 slot_name | slot_type | failover
-----------+-----------+----------
 subname   | logical   | t
(1 row)
```

Al habilitar la sincronización de ranuras, todas las ranuras de replicación lógica de conmutación por error del servidor principal se crean automáticamente en los servidores físicos y en espera y se sincronizan de forma periódica. Asegúrese de que se hayan establecido los siguientes valores mediante grupos de parámetros:

- `rds.logical_replication` debe ser 1 para habilitar la replicación lógica
- `hot_standby_feedback` debe ser 1 en la instancia en espera
- Debe establecerse `rds.logical_slot_sync_dbname` en la instancia en espera en un nombre válido de base de datos

El valor predeterminado del parámetro es `postgres`. Si la instancia de publicación lógica tiene la base de datos de `postgres`, no es necesario cambiar el parámetro predeterminado.

- Debe establecerse `synchronized_standby_slots` en la instancia principal en la ranura de replicación física de la instancia en espera destinada a sincronizarse
- `sync_replication_slots` debe ser `1` para habilitar la sincronización automática

Con una ranura de suscripción habilitada para la conmutación por error y los valores de parámetros anteriores, cuando se promociona una instancia en espera, el suscriptor puede modificar su suscripción a la instancia recién promovida y continuar con la replicación lógica sin problemas.

Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL

Una vez que Amazon RDS aprovisione su instancia de base de datos, puede usar cualquier aplicación cliente de SQL estándar para conectarse a la instancia. Antes de que pueda conectarse, la instancia de base de datos tiene que estar disponible y accesible. Si puede conectarse a la instancia desde fuera de la VPC depende de cómo haya creado la instancia de base de datos de Amazon RDS:

- Si creó la instancia de base de datos como public (pública), los dispositivos y las instancias de Amazon EC2 fuera de la VPC se pueden conectarse a la base de datos.
- Si creó la instancia de base de datos como private (privada), solo las instancias y dispositivos de Amazon EC2 dentro de Amazon VPC pueden conectarse a la base de datos.

Para verificar si la instancia de base de datos es pública o privada, use la AWS Management Console para ver la pestaña Connectivity & security (Conectividad y seguridad) de la instancia. En Security (Seguridad), puede encontrar el valor “Publicly accessible” (Accesible públicamente), con “No” si es privada, y “Yes” (Sí) si es pública.

Para obtener más información sobre las distintas configuraciones de Amazon RDS y Amazon VPC y cómo afectan a la accesibilidad, consulte Escenarios de acceso a una instancia de base de datos en una VPC.

Contenido

- Instalación del cliente psql
- Búsqueda de información de conexión para una instancia de base de datos RDS para PostgreSQL
- Uso de pgAdmin para conectarse a una instancia de base de datos de RDS for PostgreSQL
- Uso de psql para conectarse a una instancia de base de datos de RDS for PostgreSQL
- Conexión a RDS para PostgreSQL con el controlador JDBC de Amazon Web Services (AWS)
- Conexión a RDS para PostgreSQL con el controlador de Python de Amazon Web Services (AWS)
- Solución de problemas de conexiones a la instancia de RDS for PostgreSQL
  - Error – FATAL: el nombre de la base de datos no existe
  - Error – No se pudo conectar al servidor: se ha agotado el tiempo de espera.
  - Errores con reglas de acceso de grupos de seguridad

Instalación del cliente psql

Para conectarse a la instancia de base de datos desde una instancia de EC2, puede instalar un cliente PostgreSQL en la instancia de EC2. Para instalar la versión más reciente del cliente psql en Amazon Linux 2023, ejecute el siguiente comando:

```
sudo dnf install postgresql<version number>
```

Para instalar la versión más reciente del cliente psql en Amazon Linux 2, ejecute el siguiente comando:

```
sudo yum install -y postgresql
```

Para instalar la versión más reciente del cliente psql en Ubuntu, ejecute el siguiente comando:

```
sudo apt install -y postgresql-client
```

Búsqueda de información de conexión para una instancia de base de datos RDS para PostgreSQL

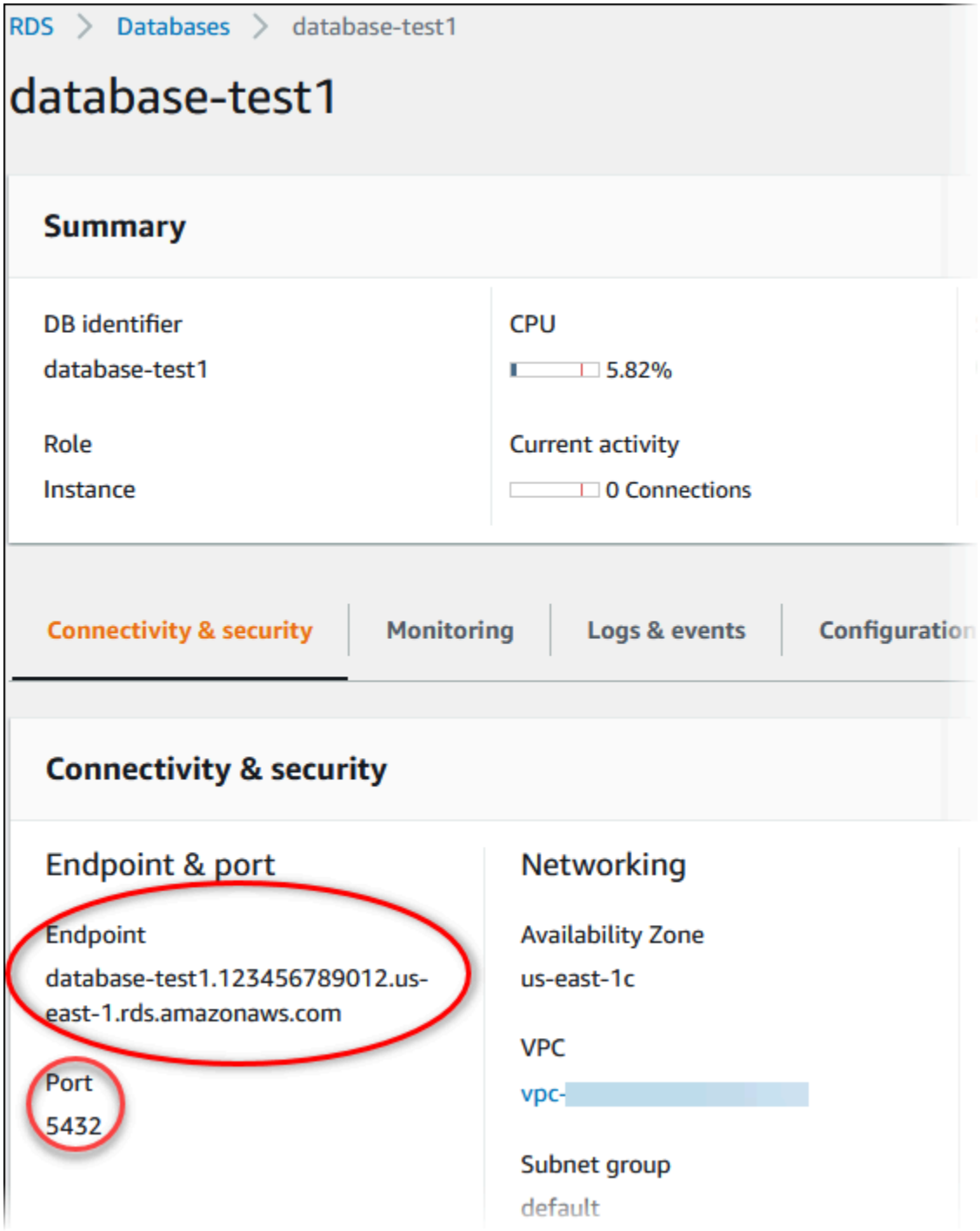
Si la instancia de base de datos está disponible y accesible, puede conectarse si proporciona la siguiente información a la aplicación cliente de SQL:

- El punto de conexión de la instancia de base de datos, que sirve como nombre de host (nombre DNS) de la instancia.
- El puerto en el que la instancia de base de datos está a la escucha. Para PostgreSQL, el puerto predeterminado es el 5432.
- El nombre de usuario y la contraseña de la instancia de base de datos. El “nombre de usuario maestro” predeterminado para PostgreSQL es `postgres`.
- El nombre y contraseña de la base de datos (nombre de base de datos).

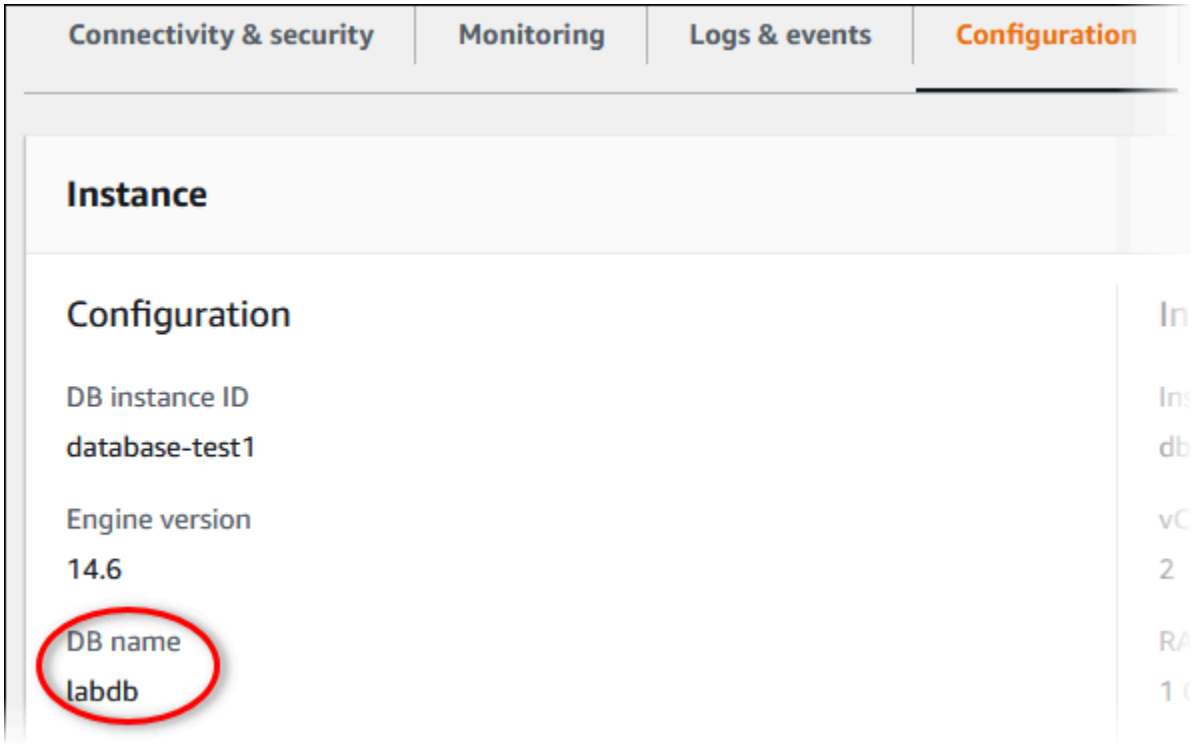
Para obtener estos detalles puede usar la AWS Management Console, el comando describe-db-instances de la AWS CLI o la operación DescribeDBInstances de la API de Amazon RDS.

Para buscar el punto de conexión, el número de puerto y el nombre de la base de datos mediante la AWS Management Console

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Abra la consola de RDS y, a continuación, elija Databases (Bases de datos) para mostrar una lista de las instancias de base de datos.
3. Seleccione el nombre de la instancia de base de datos de PostgreSQL para mostrar sus detalles.
4. En la pestaña Connectivity & security (Conectividad y seguridad), copie el punto de enlace. También anote el número de puerto. Necesita el punto de enlace y el número de puerto para conectarse a la instancia de base de datos.



5. En la pestaña Configuration (Configuración), anote el nombre de la base de datos. Si creó una base de datos al crear la instancia de RDS for PostgreSQL, verá el nombre que aparece en DB name (Nombre de base de datos). Si no ha creado una base de datos, el nombre de la base de datos muestra un guion (-).



A continuación, se muestran dos formas de conectarse a una instancia de base de datos PostgreSQL. En el primer ejemplo, se usa pgAdmin, una conocida herramienta de administración y desarrollo de código abierto para PostgreSQL. En el segundo ejemplo, se usa psql, una utilidad de línea de comandos que forma parte de una instalación de PostgreSQL.

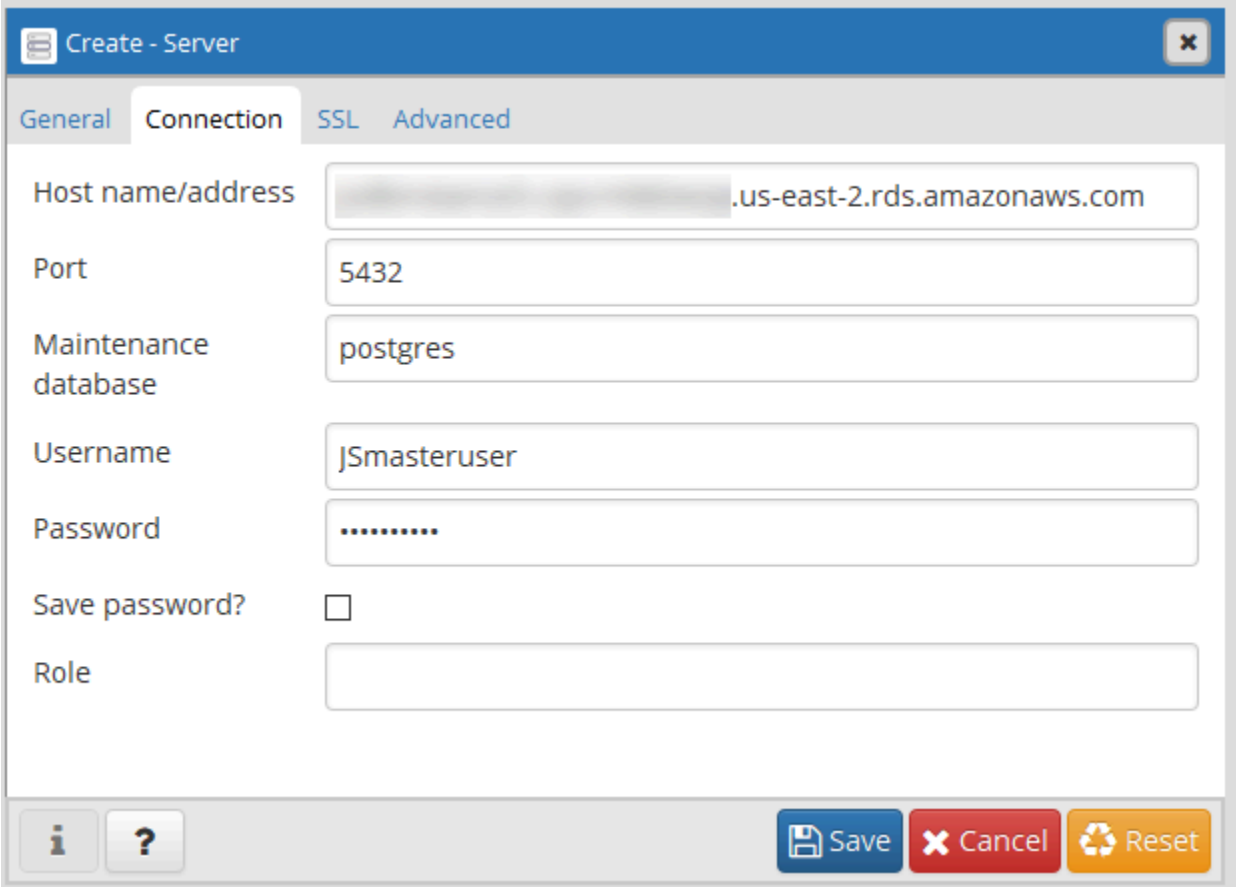
Uso de pgAdmin para conectarse a una instancia de base de datos de RDS for PostgreSQL

Puede usar la herramienta de código abierto pgAdmin para conectarse a una instancia de base de datos de RDS for PostgreSQL. Puede descargar y usar pgAdmin desde http://www.pgadmin.org/ sin tener una instancia local de PostgreSQL en su ordenador cliente.

Para conectarse a una instancia de base de datos de RDS for PostgreSQL mediante pgAdmin

1. Lance la aplicación pgAdmin en su equipo cliente.
2. En la pestaña Dashboard (Panel), elija Add New Server (Añadir nuevo servidor).
3. En el cuadro de diálogo Create - Server (Crear - Servidor), escriba un nombre en la pestaña General para identificar el servidor en pgAdmin.
4. En la pestaña Connection (Conexión), escriba la siguiente información de su instancia de base de datos:

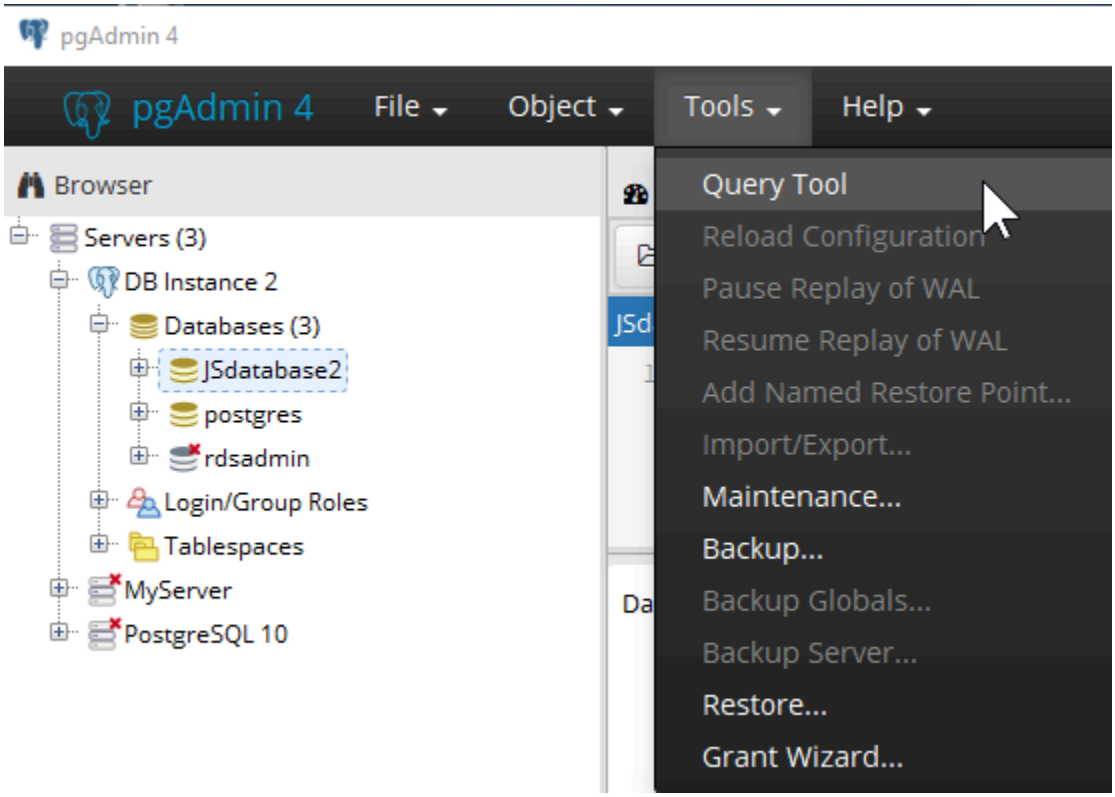
- En Host, especifique el punto de enlace, como `mypostgresql.c6c8dntfzzhgv0.us-east-2.rds.amazonaws.com`.
- En Port (Puerto), escriba el puerto asignado.
- Para Username (Nombre de usuario), escriba el nombre de usuario que especificó cuando creó la instancia de base de datos (si cambió el “nombre de usuario maestro” del predeterminado, `postgres`).
- En Password (Contraseña), escriba la contraseña que especificó cuando creó la instancia de base de datos.



5. Seleccione Guardar.

   Si tiene problemas para conectarse, consulte Solución de problemas de conexiones a la instancia de RDS for PostgreSQL.

6. Para obtener acceso a una base de datos en el navegador de pgAdmin, expanda Servers (Servidores), la instancia de base de datos y Databases (Bases de datos). Elija el nombre de base de datos de la instancia de base de datos.



7. Para abrir un panel en el que puede especificar comandos SQL, elija Tools (Herramientas), Query Tool (Herramienta de consulta).

Uso de psql para conectarse a una instancia de base de datos de RDS for PostgreSQL

Puede usar una instancia local de la utilidad de línea de comandos psql para conectarse a una instancia de base de datos de RDS for PostgreSQL. Necesitará que PostgreSQL o el cliente de psql estén instalados en el equipo cliente.

Puede descargar el cliente de PostgreSQL desde el sitio web de PostgreSQL. Para instalar psql, siga las instrucciones específicas de su sistema operativo.

Para conectarse a la instancia de base de datos de RDS for PostgreSQL mediante psql, debe proporcionar la información del host (DNS) y las credenciales de acceso.

Use uno de los siguientes formatos para conectarse a la instancia de base de datos de RDS for PostgreSQL. Cuando se conecte, se le pedirá una contraseña. En los trabajos por lotes o scripts, use la opción `--no-password`. Esta opción está establecida para toda la sesión.

> **Note**
>
> Un intento de conexión con `--no-password` falla cuando el servidor requiere autenticación de contraseña y una contraseña no está disponible desde otras fuentes. Para obtener más información, consulte la documentación de psql.

Si es la primera vez que se conecta a esta instancia de base de datos o si aún no creó una base de datos para esta instancia de RDS for PostgreSQL, puede conectarse a la base de datos postgres mediante el “nombre de usuario maestro” y la contraseña.

En Unix, utilice el formato siguiente.

```
psql \
   --host=<DB instance endpoint> \
   --port=<port> \
   --username=<master username> \
   --password \
   --dbname=<database name>
```

En Windows, utilice el formato siguiente.

```
psql ^
   --host=<DB instance endpoint> ^
   --port=<port> ^
   --username=<master username> ^
   --password ^
   --dbname=<database name>
```

Por ejemplo, el siguiente comando se conecta a una base de datos denominada `mypgdb` en una instancia de base de datos PostgreSQL denominada `mypostgresql` usando credenciales ficticias.

```
psql --host=mypostgresql.c6c8mwvfdgv0.us-west-2.rds.amazonaws.com --port=5432 --
username=awsuser --password --dbname=mypgdb
```

Conexión a RDS para PostgreSQL con el controlador JDBC de Amazon Web Services (AWS)

El controlador JDBC de Amazon Web Services (AWS) se ha diseñado como un contenedor JDBC avanzado. Este contenedor complementa y amplía la funcionalidad del controlador JDBC existente. El controlador se admite con el controlador pgJDBC de la comunidad.

Para instalar el controlador JDBC de AWS, añada el archivo .jar del controlador JDBC de AWS (ubicado en la aplicación `CLASSPATH`) y conserve las referencias al controlador de la comunidad correspondiente. Actualice el prefijo de la URL de conexión correspondiente de la siguiente manera:

- De `jdbc:postgresql://` a `jdbc:aws-wrapper:postgresql://`

Para obtener más información sobre el controlador JDBC de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador JDBC de Amazon Web Services (AWS).

Conexión a RDS para PostgreSQL con el controlador de Python de Amazon Web Services (AWS)

El controlador de Python de Amazon Web Services (AWS) se ha diseñado como un contenedor de Python avanzado. Este contenedor complementa y amplía la funcionalidad del controlador de Psycopg de código abierto. El controlador de Python de AWS se admite con las versiones 3.8 y posteriores de Python. Puede instalar el paquete de `aws-advanced-python-wrapper` mediante el comando `pip`, junto con los paquetes de código abierto de `psycopg`.

Para obtener más información sobre el controlador de Python de AWS e instrucciones completas para utilizarlo, consulte el repositorio GitHub del controlador de Python de Amazon Web Services (AWS).

Solución de problemas de conexiones a la instancia de RDS for PostgreSQL

Temas

- Error – FATAL: el nombre de la base de datos no existe
- Error – No se pudo conectar al servidor: se ha agotado el tiempo de espera.
- Errores con reglas de acceso de grupos de seguridad

Error – FATAL: el *nombre* de la base de datos no existe

Si al intentar conectarse recibe un error como `FATAL: database name does not exist`, intente utilizar el nombre de base de datos predeterminado postgres para la opción `--dbname`.

Error – No se pudo conectar al servidor: se ha agotado el tiempo de espera.

Si no puede conectarse a la instancia de base de datos, el error más frecuente es `Could not connect to server: Connection timed out.` Si recibe este error, proceda de la siguiente forma:

- Compruebe que el nombre de host usado es el punto de enlace de la instancia de base de datos y que el número de puerto usado es correcto.
- Asegúrese de que la accesibilidad pública de la instancia de base de datos está establecida en Yes (Sí) para permitir conexiones externas. Para modificar la configuración Public access (Acceso público), consulte Modificación de una instancia de base de datos de Amazon RDS.
- Asegúrese de que el usuario que se conecta a la base de datos tenga acceso CONNECT. Puede utilizar la siguiente consulta para proporcionar acceso a la base de datos.

```
GRANT CONNECT ON DATABASE database name TO username;
```

- Compruebe que el grupo de seguridad asignado a la instancia de base de datos cuenta con las reglas necesarias para permitir el acceso de su conexión a través de cualquier firewall. Por ejemplo, si la instancia de base de datos se creó utilizando el puerto predeterminado 5432, es posible que su empresa tenga reglas de firewall que bloquean las conexiones a ese puerto desde los dispositivos externos de la empresa.

  Para solucionar esto, modifique la instancia de base de datos para que use un puerto diferente. Asegúrese también de que el grupo de seguridad aplicado a la instancia de base de datos permite las conexiones en el nuevo puerto. Para modificar la configuración del Database port (Puerto de base de datos), consulte Modificación de una instancia de base de datos de Amazon RDS.
- Compruebe si el puerto que intenta utilizar ya está ocupado por una instancia local de PostgreSQL u otro servicio que se ejecute en el ordenador. Por ejemplo, si tiene una base de datos PostgreSQL local que se ejecuta en el mismo puerto (el valor predeterminado es 5432), podría impedir una conexión correcta a la instancia de base de datos de RDS para PostgreSQL. Asegúrese de que el puerto esté libre o intente conectarse con un número de puerto diferente si es posible.
- Véase también Errores con reglas de acceso de grupos de seguridad.

Errores con reglas de acceso de grupos de seguridad

El problema de conexión más frecuente se suele producir con las reglas de acceso del grupo de seguridad asignado a la instancia de base de datos. Si al crear la instancia de base de datos usó el grupo de seguridad predeterminado, lo más probable es que ese grupo no tuviera las reglas que le permiten obtener acceso a la instancia.

Para que funcione la conexión, el grupo de seguridad que asignó a la instancia de base de datos al crearla debe permitir el acceso a esa instancia de base de datos. Por ejemplo, si la instancia de base de datos se creó en una VPC, debe tener un grupo de seguridad de VPC que autorice las conexiones. Compruebe si la instancia de base de datos se creó utilizando un grupo de seguridad que no autoriza las conexiones desde el dispositivo o la instancia Amazon EC2 en la que se está ejecutando la aplicación.

Puede añadir o editar una regla de entrada en el grupo de seguridad. En Source (Origen), elegir My IP (Mi IP) permite el acceso a la instancia de base de datos desde la dirección IP detectada en su navegador. Para obtener más información, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

Igualmente, si la instancia de base de datos se creó fuera de una VPC, debe tener un grupo de seguridad de base de datos que autorice esas conexiones.

Para obtener más información acerca de los grupos de seguridad de Amazon RDS, consulte Control de acceso con grupos de seguridad.

Protección de conexiones a RDS for PostgreSQL con SSL/TLS

RDS for PostgreSQL admite el cifrado de la capa de sockets seguros (SSL) para las instancias de base de datos de PostgreSQL. Con SSL, puede cifrar una conexión de PostgreSQL entre sus aplicaciones y sus instancias de base de datos de PostgreSQL. También puede obligar a todas las conexiones con su instancia de base de datos PostgreSQL a usar SSL. RDS for PostgreSQL también admite la seguridad de la capa de transporte (TLS), el protocolo sucesor de la SSL.

Para obtener más información sobre Amazon RDS y la protección de datos, incluido el cifrado de conexiones mediante SSL/TLS, consulte Protección de datos en Amazon RDS.

Temas

- Uso de SSL con una instancia de base de datos PostgreSQL
- Actualización de aplicaciones para la conexión a las instancias de base de datos de PostgreSQL con los nuevos certificados SSL/TLS

Uso de SSL con una instancia de base de datos PostgreSQL

Amazon RDS admite el cifrado de la Capa de conexión segura (SSL) para las instancias de base de datos de PostgreSQL. Con SSL, puede cifrar una conexión de PostgreSQL entre sus aplicaciones y sus instancias de base de datos de PostgreSQL. De forma predeterminada, RDS for PostgreSQL utiliza y espera que todos los clientes se conecten mediante SSL/TLS, pero también puede hacer que sea obligatorio. RDS para PostgreSQL admite las versiones 1.1, 1.2 y 1.3 de la seguridad de la capa de transporte (TLS).

Para obtener la información general acerca de la compatibilidad con SSL y las bases de datos de PostgreSQL, consulte Compatibilidad con SSL en la documentación de PostgreSQL. Para obtener información sobre el uso de una conexión SSL a través de JDBC, consulte Configuración del cliente en la documentación de PostgreSQL.

La compatibilidad con SSL está disponible en todas las regiones de AWS para PostgreSQL. Amazon RDS crea un certificado SSL para su instancia de base de datos de PostgreSQL cuando se crea la instancia. Si se habilita la verificación con certificado SSL, el certificado incluye el punto de enlace de la instancia de base de datos como nombre común (CN) que el certificado de SSL debe proteger frente a los ataques de suplantación.

Temas

- Conectar con una instancia de base de datos PostgreSQL a través de SSL
- Requerir una conexión SSL a una instancia de base de datos PostgreSQL
- Determinar el estado de la conexión SSL
- Conjuntos de cifrado SSL en RDS for PostgreSQL

Conectar con una instancia de base de datos PostgreSQL a través de SSL

Para conectar con una instancia de base de datos PostgreSQL a través de SSL

1. Descargue el certificado.

   Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

2. Conecte su instancia de base de datos de PostgreSQL a través de SSL.

   Cuando se conecte utilizando SSL, su cliente podrá elegir si verifica la cadena de certificados. Si sus parámetros de conexión especifican `sslmode=verify-ca` o `sslmode=verify-full`, su cliente precisa que los certificados de CA de RDS estén en su almacén de confianza o se haga referencia a ellos en la URL de conexión. Este requisito es para verificar la cadena de certificados que firma su certificado de base de datos.

   Cuando un cliente, como psql o JDBC, está configurado con soporte de SSL, primero el cliente intenta conectarse a la base de datos con SSL de manera predeterminada. SI el cliente no puede conectarse con SSL, vuelve a la conexión sin SSL. El modo `sslmode` predeterminado utilizado es diferente entre los clientes basados en libpq (como psql) y JDBC. Los clientes basados en libpq y JDBC utilizan de manera predeterminada `prefer`.

   Use el parámetro `sslrootcert` para hacer referencia al certificado, por ejemplo: `sslrootcert=rds-ssl-ca-cert.pem`.

A continuación, se muestra un ejemplo de cómo se utiliza `psql` para conectarse a una instancia de base de datos de PostgreSQL mediante SSL con verificación de certificados.

```
$ psql "host=db-name.555555555555.ap-southeast-1.rds.amazonaws.com
    port=5432 dbname=testDB user=testuser sslrootcert=rds-ca-rsa2048-g1.pem
 sslmode=verify-full"
```

Requerir una conexión SSL a una instancia de base de datos PostgreSQL

Puede exigir que las conexiones a la instancia de base de datos PostgreSQL usen SSL por medio del parámetro `rds.force_ssl`. El valor predeterminado del valor `rds.force_ssl` es 1 (activado) para RDS para PostgreSQL versión 15 y posteriores. Para todas las demás versiones principales de RDS para PostgreSQL 14 y anteriores, el valor predeterminado de este parámetro es 0 (desactivado). Puede definir el parámetro `rds.force_ssl` en 1 (activado) fin de imponer SSL/TLS para las conexiones al clúster de base de datos. Puede definir el parámetro `rds.force_ssl` en 1 (activado) para imponer SSL para las conexiones a la instancia de base de datos.

Para cambiar el valor de este parámetro, debe crear un grupo de parámetros de base de datos personalizado. A continuación, cambie el valor de `rds.force_ssl` en el grupo de parámetros de base de datos personalizado a 1 para activar esta característica. Si prepara el grupo de parámetros de base de datos personalizado antes de crear la instancia de base de datos de RDS for PostgreSQL, puede elegirlo (en lugar de un grupo de parámetros predeterminado) durante el proceso de creación. Si lo hace después de que la instancia de base de datos de RDS for PostgreSQL ya se esté ejecutando, debe reiniciar la instancia para que utilice el grupo de parámetros personalizado. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

Cuando la característica `rds.force_ssl` está activa en la instancia de base de datos, los intentos de conexión que no utilizan SSL se rechazan con el siguiente mensaje:

```
$ psql -h db-name.555555555555.ap-southeast-1.rds.amazonaws.com port=5432 dbname=testDB
 user=testuser
psql: error: FATAL: no pg_hba.conf entry for host "w.x.y.z", user "testuser", database
 "testDB", SSL off
```

Determinar el estado de la conexión SSL

El estado cifrado de su conexión se muestra en el banner de inicio de sesión al establecer conexión con la instancia de base de datos:

```
Password for user master:
psql (10.3)
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.
postgres=>
```

También puede cargar la extensión `sslinfo` y llamar después a la función `ssl_is_used()` para determinar si se está usando SSL. La función devuelve `t` si la conexión usa SSL; de lo contrario, devuelve `f`.

```
postgres=> CREATE EXTENSION sslinfo;
CREATE EXTENSION
postgres=> SELECT ssl_is_used();
ssl_is_used
---------
t
(1 row)
```

Para obtener información más detallada, puede usar la siguiente consulta para obtener información de `pg_settings`:

```
SELECT name as "Parameter name", setting as value, short_desc FROM pg_settings WHERE
 name LIKE '%ssl%';
             Parameter name             |                  value                  |
                  short_desc
----------------------------------------+-----------------------------------------
+-----------------------------------------------------
 ssl                                    | on                                      |
 Enables SSL connections.
 ssl_ca_file                            | /rdsdbdata/rds-metadata/ca-cert.pem     |
 Location of the SSL certificate authority file.
 ssl_cert_file                          | /rdsdbdata/rds-metadata/server-cert.pem |
 Location of the SSL server certificate file.
 ssl_ciphers                            | HIGH:!aNULL:!3DES                       |
 Sets the list of allowed SSL ciphers.
 ssl_crl_file                           |                                         |
 Location of the SSL certificate revocation list file.
 ssl_dh_params_file                     |                                         |
 Location of the SSL DH parameters file.
 ssl_ecdh_curve                         | prime256v1                              |
 Sets the curve to use for ECDH.
 ssl_key_file                           | /rdsdbdata/rds-metadata/server-key.pem  |
 Location of the SSL server private key file.
 ssl_library                            | OpenSSL                                 |
 Name of the SSL library.
 ssl_max_protocol_version               |                                         |
 Sets the maximum SSL/TLS protocol version to use.
```

```
 ssl_min_protocol_version               | TLSv1.2                                  |
 Sets the minimum SSL/TLS protocol version to use.
 ssl_passphrase_command                 |                                          |
 Command to obtain passphrases for SSL.
 ssl_passphrase_command_supports_reload | off                                      |
 Also use ssl_passphrase_command during server reload.
 ssl_prefer_server_ciphers              | on                                       |
 Give priority to server ciphersuite order.
(14 rows)
```

También puede recopilar toda la información sobre el uso de SSL de la instancia de base de datos de RDS for PostgreSQL por proceso, cliente y aplicación mediante la siguiente consulta:

```
SELECT datname as "Database name", usename as "User name", ssl, client_addr,
 application_name, backend_type
   FROM pg_stat_ssl
   JOIN pg_stat_activity
   ON pg_stat_ssl.pid = pg_stat_activity.pid
   ORDER BY ssl;
 Database name | User name | ssl |  client_addr   |    application_name    |
 backend_type
---------------+-----------+-----+----------------+------------------------
+------------------------------
               |           | f   |                |                        | autovacuum
 launcher
               | rdsadmin  | f   |                |                        | logical
 replication launcher
               |           | f   |                |                        | background
 writer
               |           | f   |                |                        |
 checkpointer
               |           | f   |                |                        | walwriter
 rdsadmin      | rdsadmin  | t   | 127.0.0.1      |                        | client
 backend
 rdsadmin      | rdsadmin  | t   | 127.0.0.1      | PostgreSQL JDBC Driver | client
 backend
 postgres      | postgres  | t   | 204.246.162.36 | psql                   | client
 backend
(8 rows)
```

Para identificar el cifrado utilizado para la conexión SSL, puede realizar la consulta de la siguiente manera:

```
postgres=> SELECT ssl_cipher();
ssl_cipher
--------------------
DHE-RSA-AES256-SHA
(1 row)
```

Para obtener información acerca de la opción `sslmode`, consulte Funciones de control de conexión de la base de datos en la documentación de PostgreSQL.

Conjuntos de cifrado SSL en RDS for PostgreSQL

El parámetro de configuración de PostgreSQL ssl_ciphers especifica las categorías de conjuntos de cifrado permitidos para las conexiones SSL a la base de datos al usar TLS 1.2 y anteriores.

En RDS para PostgreSQL 16 y versiones posteriores, puede modificar el parámetro `ssl_ciphers` para usar valores específicos de los conjuntos de cifrado de la lista de permitidos. Este es un parámetro dinámico que no requiere el reinicio de la instancia de base de datos. Para ver los conjuntos de cifrado de la lista de permitidos, utilice la consola de Amazon RDS o el siguiente comando de la CLI de AWS:

```
aws rds describe-db-parameters --db-parameter-group-name <your-parameter-group> --
region <region> --endpoint-url <endpoint-url> --output json | jq '.Parameters[] |
 select(.ParameterName == "ssl_ciphers")'
```

La siguiente tabla muestra los conjuntos de cifrado predeterminados y los conjuntos de cifrado permitidos para las versiones que admiten configuraciones personalizadas.

Versión del motor de PostgreSQL	Valores predeterminados del conjunto ssl_cipher	Valores personalizados del conjunto ssl_cipher de la lista de permitidos

17	`HIGH:!aNULL:!3DES`	`TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
		`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256`
		`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`

Versión del motor de PostgreSQL	Valores predeterminados del conjunto ssl_cipher	Valores personalizados del conjunto ssl_cipher de la lista de permitidos
		TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
16	HIGH:!aNULL:!3DES	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
15	HIGH:!aNULL:!3DES	No se admite ssl_ciphers personalizado
14	HIGH:!aNULL:!3DES	No se admite ssl_ciphers personalizado
13	HIGH:!aNULL:!3DES	No se admite ssl_ciphers personalizado

Versión del motor de PostgreSQL	Valores predeterminados del conjunto ssl_cipher	Valores personalizados del conjunto ssl_cipher de la lista de permitidos
12	`HIGH:!aNULL:!3DES`	No se admite ssl_ciphers personalizado
11.4 y versiones secundarias posteriores	`HIGH:MEDIUM:+3DES:!aNULL:!RC4`	No se admite ssl_ciphers personalizado
11.1, 11.2	`HIGH:MEDIUM:+3DES:!aNULL`	No se admite ssl_ciphers personalizado
10.9 y versiones secundarias posteriores	`HIGH:MEDIUM:+3DES:!aNULL:!RC4`	No se admite ssl_ciphers personalizado
10.7 y versiones menores inferiores	`HIGH:MEDIUM:+3DES:!aNULL`	No se admite ssl_ciphers personalizado

Para configurar todas las conexiones de instancias para que usen el conjunto de cifrado `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`, modifique el grupo de parámetros como se muestra en el siguiente ejemplo:

```
aws rds modify-db-parameter-group --db-parameter-group-name <your-parameter-group> --
parameters
 "ParameterName='ssl_ciphers',ParameterValue='TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384',ApplyMet
```

Este ejemplo utiliza un cifrado ECDSA, que requiere que la instancia use una autoridad de certificación con criptografía de curva elíptica (ECC) para establecer una conexión. Para obtener información sobre las autoridades de certificación proporcionadas por Amazon RDS, consulte Autoridades de certificación.

Puede verificar los cifrados en uso mediante los métodos descritos en Determinación del estado de la conexión SSL.

Los cifrados pueden tener diferentes nombres en función del contexto:

- Los cifrados de la lista de permitidos que puede configurar en el grupo de parámetros se denominan con sus nombres de IANA.

- Los banners de inicio de sesión `sslinfo` y `psql` hacen referencia a los cifrados mediante los nombres de OpenSSL.

De forma predeterminada, el valor de `ssl_max_protocol_version` en RDS para PostgreSQL 16 y versiones posteriores es TLS v1.3. Debe establecer el valor de este parámetro en TLS v1.2, ya que TLS v1.3 no utiliza las configuraciones de cifrado especificadas en el parámetro `ssl_ciphers`. Cuando establece el valor como TLS v1.2, las conexiones utilizan solo los cifrados que usted defina en `ssl_ciphers`.

```
aws rds modify-db-parameter-group --db-parameter-group-name <your-parameter-group> --
parameters
 "ParameterName='ssl_max_protocol_version',ParameterValue='TLSv1.2',ApplyMethod=immediate"
```

Para garantizar que las conexiones a la base de datos utilicen SSL, establezca `rds.force_ssl parameter` en 1 en el grupo de parámetros. Para obtener más información acerca de los parámetros y grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

Actualización de aplicaciones para la conexión a las instancias de base de datos de PostgreSQL con los nuevos certificados SSL/TLS

Los certificados utilizados para capas de sockets seguros o seguridad de la capa de transporte (SSL/TLS) suelen tener una vida útil establecida. Cuando los proveedores de servicios actualizan sus certificados de la autoridad de certificación (CA), los clientes deben actualizar sus aplicaciones para utilizar los certificados nuevos. A continuación, puede encontrar información sobre cómo determinar si sus aplicaciones cliente utilizan SSL/TLS para conectarse a su instancia de base de datos de Amazon RDS for PostgreSQL. También encontrará información sobre cómo comprobar si esas aplicaciones verifican el certificado del servidor cuando se conectan.

> **Note**
>
> Una aplicación cliente configurada para verificar el certificado del servidor antes de la conexión SSL/TLS debe tener un certificado de CA válido en el almacén de confianza del cliente. Actualice el almacén de confianza del cliente cuando sea necesario para acceder a certificados nuevos.

Después actualizar sus certificados de CA en los almacenes de confianza de la aplicación de su cliente, puede rotar los certificados en sus instancias de base de datos. Se recomienda probar estos

procedimientos en un entorno que no sea de producción antes de implementarlos en entornos de producción.

Para obtener más información acerca de la rotación de certificados, consulte Rotar certificados SSL/TLS. Para obtener más información acerca de cómo descargar certificados, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Para obtener información sobre el uso de SSL/TLS con las instancias de base de datos de PostgreSQL, consulte Uso de SSL con una instancia de base de datos PostgreSQL.

Temas

- Determinación de si las aplicaciones se conectan a sus instancias de base de datos de PostfreSQL mediante SSL
- Determinación de si un cliente necesita una verificación de certificados para conectarse
- Actualización del almacén de confianza de su aplicación
- Uso de conexiones SSL/TLS para diferentes tipos de aplicaciones

Determinación de si las aplicaciones se conectan a sus instancias de base de datos de PostfreSQL mediante SSL

Compruebe la configuración de la instancia de base de datos para obtener el valor del parámetro de `rds.force_ssl`. De forma predeterminada, el parámetro `rds.force_ssl` está configurado en `0` (desactivado) para las instancias de base de datos que utilizan versiones de PostgreSQL anteriores a la versión 15. De forma predeterminada, `rds.force_ssl` está configurado en 1 (activado) para las instancias de base de datos que utilizan PostgreSQL versión 15 y versiones principales posteriores. Si el parámetro `rds.force_ssl` está configurado como 1 (activado), se precisa que los clientes utilicen SSL/TLS para las conexiones. Para obtener más información acerca de los grupos de parámetros, consulte Grupos de parámetros para Amazon RDS.

Si utiliza la versión 9.5 o una versión importante anterior de RDS PostgreSQL y `rds.force_ssl` no está configurado como 1 (activado), consulte la vista `pg_stat_ssl` para comprobar las conexiones que utilizan SSL. Por ejemplo, la siguiente consulta devuelve solo las conexiones SSL y la información acerca de los clientes que utilizan SSL.

```
SELECT datname, usename, ssl, client_addr
  FROM pg_stat_ssl INNER JOIN pg_stat_activity ON pg_stat_ssl.pid =
 pg_stat_activity.pid
  WHERE ssl is true and usename<>'rdsadmin';
```

Solo las filas que utilizan conexiones SSL/TLS se muestran con información sobre la conexión. A continuación, se muestra un ejemplo del resultado.

```
 datname  | usename | ssl | client_addr
----------+---------+-----+-------------
 benchdb  | pgadmin | t   | 53.95.6.13
 postgres | pgadmin | t   | 53.95.6.13
(2 rows)
```

Esta consulta solo muestra las conexiones actuales en el momento de la consulta. La ausencia de resultados no indica que no haya ninguna aplicación utilizando conexiones SSL. Se pueden establecer otras conexiones SSL en un momento diferente.

Determinación de si un cliente necesita una verificación de certificados para conectarse

Cuando un cliente, como psql o JDBC, está configurado con soporte de SSL, primero el cliente intenta conectarse a la base de datos con SSL de manera predeterminada. SI el cliente no puede conectarse con SSL, vuelve a la conexión sin SSL. El modo `sslmode` predeterminado utilizado para clientes con libpq (como psql) y JDBC está establecido en `prefer`. El certificado del servidor se verifica solo cuando se proporciona `sslrootcert` con `sslmode` configurado como `verify-ca` o `verify-full`. Se lanza un error si el certificado no es válido.

Utilice `PGSSLROOTCERT` para verificar el certificado con la variable de entorno `PGSSLMODE`, con `PGSSLMODE` establecido como `verify-ca` o `verify-full`.

```
PGSSLMODE=verify-full PGSSLROOTCERT=/fullpath/ssl-cert.pem psql -h
 pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com -U masteruser -d postgres
```

Utilice el argumento `sslrootcert` para verificar el certificado con `sslmode` en el formato de la cadena de conexión, con `sslmode` establecido como `verify-ca` o `verify-full` para verificar el certificado.

```
psql "host=pgdbidentifier.cxxxxxxxx.us-east-2.rds.amazonaws.com sslmode=verify-full
 sslrootcert=/full/path/ssl-cert.pem user=masteruser dbname=postgres"
```

Por ejemplo, en el caso anterior, si utiliza un certificado raíz no válido, observa un error similar a lo siguiente en su cliente.

```
psql: SSL error: certificate verify failed
```

Actualización del almacén de confianza de su aplicación

Para obtener información sobre la actualización del almacén de confianza para las aplicaciones de PostgreSQL, consulte Conexiones TCP/IP seguras con SSL en la documentación de PostgreSQL.

Para obtener información sobre la descarga del certificado raíz, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Para obtener secuencias de comandos de ejemplo que importan certificados, consulte Script de muestra para la importación de certificados en su almacén de confianza.

> **Note**
>
> Cuando actualice el almacén de confianza, puede retener certificados antiguos además de añadir los nuevos certificados.

Uso de conexiones SSL/TLS para diferentes tipos de aplicaciones

Lo siguiente proporciona información acerca del uso de conexiones SSL/TLS para diferentes tipo de aplicaciones:

- psql

  El cliente se ha invocado desde la línea de comandos especificando las opciones como una cadena de conexión o como variables del entorno. Para las conexiones SSL/TLS, las opciones relevantes son `sslmode` (variable de entorno `PGSSLMODE`), `sslrootcert` (variable de entorno `PGSSLROOTCERT`).

  Para obtener la lista completa de opciones, consulte Palabras de clave del parámetro en la documentación de PostgreSQL. Para obtener la lista completa de variables de entorno, consulte Variables de entorno en la documentación de PostgreSQL.

- pgAdmin

  Este cliente basado en el navegador es una interfaz más intuitiva para conectarse a la base de datos de PostgreSQL.

Para obtener información sobre la configuración de las conexiones, consulte la documentación de pgAdmin.

- JDBC

  JDBC habilita las conexiones de base de datos con aplicaciones de Java.

  Para obtener información general sobre la conexión a la base de datos de PostgreSQL con JDBC, consulte Connecting to the database (Conexión con la base de datos) en la documentación del controlador JDBC de PostgreSQL. Para obtener información sobre la conexión con SSL/TLS, consulte Configuring the client (Configuración del cliente) en la documentación del controlador JDBC de PostgreSQL.

- Python

  Una biblioteca de Python popular para la conexión a las bases de datos de PostgreSQL es `psycopg2`.

  Para obtener información acerca del uso de `psycopg2`, consulte la documentación de psycopg2. Para obtener un breve tutorial sobre cómo conectarse a una base de datos de PostgreSQL, consulte Tutorial de psycopg2. Puede encontrar información acerca de las opciones que acepta del comando de conexión en El contenido del módulo psycopg2.

> **Important**
>
> Después de que haya determinado que sus conexiones de base de datos utilizan SSL/TLS y haya actualizado el almacén de confianza de su aplicación, puede actualizar su base de datos para que utilice los certificados de rds-ca-rsa2048-g1. Para obtener instrucciones, consulte el paso 3 en Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos.

Uso de la autenticación Kerberos con Amazon RDS para PostgreSQL

Puede usar Kerberos para autenticar a los usuarios cuando se conecten a su instancia de base de datos en la que se ejecuta PostgreSQL. Para ello, configure la instancia de base de datos para utilizar AWS Directory Service for Microsoft Active Directory para la autenticación Kerberos. AWS Directory Service for Microsoft Active Directory también se denomina AWS Managed Microsoft AD. Es una función disponible con AWS Directory Service. Para obtener más información, consulte ¿Qué esAWS Directory Service? en la Guía de administración de AWS Directory Service.

Para empezar, cree un directorio de AWS Managed Microsoft AD para almacenar las credenciales de usuario. A continuación, proporcione a su instancia de base de datos de PostgreSQL el dominio de Active Directory y otra información. Cuando los usuarios se autentican con la instancia de de base de datos de PostgreSQL, las solicitudes de autenticación se reenvían al directorio AWS Managed Microsoft AD.

Mantener todas las credenciales en el mismo directorio puede ahorrarle tiempo y esfuerzo. Tiene un lugar centralizado para almacenar y administrar credenciales para varias instancias de bases de datos. El uso de un directorio también puede mejorar su perfil de seguridad general.

Además, puede acceder a las credenciales desde su propio Microsoft Active Directory en las instalaciones. Para ello, cree una relación de dominio de confianza para que el directorio de AWS Managed Microsoft AD confíe en su Microsoft Active Directory en las instalaciones. De esta manera, los usuarios pueden acceder a las instancias de los de PostgreSQL con la misma experiencia de inicio de sesión único (SSO) de Windows que cuando acceden a cargas de trabajo en las instalaciones.

Una base de datos puede utilizar la autenticación por contraseña o la autenticación por contraseña con Kerberos o con la autenticación de AWS Identity and Access Management (IAM). Para obtener más información acerca de la autenticación IAM, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

Temas

- Disponibilidad en regiones y versiones
- Información general de la autenticación Kerberos para instancias de base de datos de PostgreSQL
- Configuración de autenticación Kerberos para instancias de base de datos de PostgreSQL

- Administración de una instancia de base de datos de RDS para PostgreSQL en un dominio de Active Directory
- Conexión a PostgreSQL con autenticación Kerberos

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad en versiones y regiones de RDS para PostgreSQL con autenticación Kerberos, consulte Regiones y motores de base de datos admitidos para autenticación de Kerberos en Amazon RDS.

Información general de la autenticación Kerberos para instancias de base de datos de PostgreSQL

Para configurar la autenticación Kerberos para una instancia de base de datos de PostgreSQL, complete los siguientes pasos generales, que se describen con más detalle más adelante:

1. Utilice AWS Managed Microsoft AD para crear un directorio de AWS Managed Microsoft AD. Puede utilizar la AWS Management Console, la AWS CLI o la API de AWS Directory Service para crear el directorio. Asegúrese de abrir los puertos de salida relevantes en el grupo de seguridad del directorio para que el directorio pueda comunicarse con la instancia.
2. Cree un rol que proporcione a Amazon RDS acceso para realizar llamadas a su directorio de AWS Managed Microsoft AD. Para ello, cree un rol de AWS Identity and Access Management (IAM) que utilice la política administrada de IAM `AmazonRDSDirectoryServiceAccess`.

   Para que el rol de IAM permita el acceso, el punto de enlace AWS Security Token Service (AWS STS) debe activarse en la región de AWS correcta para su cuenta de AWS. Los puntos de conexión de AWS STS están activos de forma predeterminada en todas las Regiones de AWS y puede usarlos sin ninguna acción posterior. Para obtener más información, consulte Activación y desactivación de AWS STS en una región de AWS en la Guía del usuario de IAM.
3. Cree y configure usuarios en el directorio de AWS Managed Microsoft AD usando las herramientas de Microsoft Active Directory. Para obtener más información sobre la creación de usuarios en su Active Directory, consulte Administrar usuarios y grupos en AWS Managed Microsoft AD en la Guía de administración de AWS Directory Service.

4. Si piensa localizar el directorio y la instancia de base de datos en diferentes cuentas de AWS o nubes virtuales privadas (VPC), configure la interconexión de VPC. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la Amazon VPC Peering Guide.
5. Cree o modifique una instancia de base de datos de PostgreSQL desde la consola, la CLI o la API de RDS utilizando uno de los siguientes métodos:
   - Creación de una instancia de base de datos de Amazon RDS
   - Modificación de una instancia de base de datos de Amazon RDS
   - Restauración a una instancia de base de datos
   - Restauración de una instancia de base de datos a un momento especificado para Amazon RDS

   Puede localizar la instancia en la misma Amazon Virtual Private Cloud (VPC) que el directorio o en una VPC o cuenta de AWS diferente. Cuando cree o modifique la instancia de base de datos de PostgreSQL, haga lo siguiente:
   - Proporcione el identificador de dominio (identificador `d-*`) que se generó cuando creó el directorio.
   - Proporcione el nombre del rol de IAM que ha creado.
   - Asegúrese de que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico de entrada del grupo de seguridad del directorio.
6. Use las credenciales de usuario maestro de RDS para conectarse a la instancia de base de datos de PostgreSQL. Cree el usuario en PostgreSQL para que sea identificado externamente. Los usuarios identificados externamente pueden iniciar sesión en la instancia de base de datos de PostgreSQL utilizando la autenticación Kerberos.

Configuración de autenticación Kerberos para instancias de base de datos de PostgreSQL

Utilice AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) para configurar la autenticación Kerberos para una instancia de base de datos de PostgreSQL. Para configurar la autenticación Kerberos, siga los pasos que se indican a continuación:

Temas

- Paso 1: crear un directorio con AWS Managed Microsoft AD
- Paso 2: (opcional) crear una relación de confianza entre su Active Directory en las instalaciones y AWS Directory Service

- Paso 3: crear un rol de IAM para que Amazon RDS acceda a AWS Directory Service
- Paso 4: crear y configurar usuarios
- Paso 5: habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos
- Paso 6: crear o modificar una instancia de base de datos de PostgreSQL
- Paso 7: crear usuarios de PostgreSQL para las entidades principales de Kerberos
- Paso 8: configurar un cliente de PostgreSQL

Paso 1: crear un directorio con AWS Managed Microsoft AD

AWS Directory Service crea un directorio de Active Directory completamente administrado en la nube de AWS. Al crear un directorio de AWS Managed Microsoft AD, AWS Directory Service crea dos controladores de dominio y servidores DNS para usted. Los servidores de directorios se crean en diferentes subredes de una VPC. Esta redundancia ayuda a garantizar que su directorio permanezca accesible incluso si ocurre un error.

Cuando se crea un directorio de AWS Managed Microsoft AD, AWS Directory Service realiza las siguientes tareas en su nombre:

- Configura un Active Directory dentro de la VPC.
- Crea una cuenta de administrador del directorio con el nombre de usuario `Admin` y la contraseña especificada. Esta cuenta le permite administrar el directorio.

  > **Important**
  >
  > Asegúrese de guardar esta contraseña. AWS Directory Service no almacena esta contraseña y no se puede recuperar ni restablecer.

- Crea un grupo de seguridad para los controladores del directorio. El grupo de seguridad debe permitir la comunicación con la instancia de base de datos de PostgreSQL.

Al lanzar AWS Directory Service for Microsoft Active Directory, AWS crea una unidad organizativa (OU) que contiene todos los objetos del directorio. Esta unidad organizativa, que tiene el nombre de NetBIOS que introdujo al crear el directorio, se encuentra en la raíz del dominio. La raíz del dominio es propiedad de AWS, que también se encarga de su administración.

La cuenta `Admin` que se creó con el directorio de AWS Managed Microsoft AD dispone de permisos para realizar las actividades administrativas más habituales para la unidad organizativa:

- Crear, actualizar o eliminar usuarios
- Añadir recursos a su dominio, como servidores de archivos o de impresión y, a continuación, asignar permisos para esos recursos a usuarios dentro de la unidad organizativa
- Crear unidades organizativas y contenedores adicionales
- Delegar autoridad
- Restaurar objetos eliminados de la papelera de reciclaje de Active Directory
- Ejecute módulos de Active Directory y Domain Name Service (DNS) para Windows Powershell en el servicio web de Active Directory

La cuenta `Admin` también tiene derechos para realizar las siguientes actividades en todo el dominio:

- Administrar configuraciones DNS (agregar, quitar o actualizar registros, zonas y programas de envío).
- Ver logs de eventos DNS
- Ver logs de eventos de seguridad

Para crear un directorio con AWS Managed Microsoft AD

1. En el panel de navegación de la consola de AWS Directory Service, elija Directories (Directorios) y, a continuación, elija Set up Directory (Configurar directorio).
2. Elija AWS Managed Microsoft AD. AWS Managed Microsoft AD es la única opción que se admite actualmente para usar con Amazon RDS.
3. Elija Siguiente.
4. En la página Enter directory information (Especifique la información del directorio), facilite la siguiente información:

   Edición

   Elija la edición que se adapte a sus necesidades.

   Nombre de DNS del directorio

   El nombre completo del directorio, como por ejemplo **`corp.example.com`**.

   Nombre NetBIOS del directorio

   Un nombre abreviado del directorio opcional, como COR `CORP`.

Descripción del directorio

Descripción opcional del directorio.

Contraseña de administrador

Contraseña del administrador del directorio. Al crear el directorio, se crea también una cuenta de administrador con el nombre de usuario `Admin` y esta contraseña.

La contraseña del administrador del directorio no puede contener la palabra "admin".
La contraseña distingue entre mayúsculas y minúsculas y debe tener un mínimo de 864 caracteres y un máximo de 64. También debe contener al menos un carácter de tres de las siguientes categorías:

- Letras minúsculas (a–z)
- Letras mayúsculas (A–Z)
- Números (0–9)
- Caracteres no alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password

Vuelva a escribir la contraseña de administrador.

> **Important**
>
> Asegúrese de guardar esta contraseña. AWS Directory Service no almacena esta contraseña y no se puede recuperar ni restablecer.

5. Elija Siguiente.
6. En la página Choose VPC and subnets (Elegir la VPC y las subredes), proporcione la información siguiente:

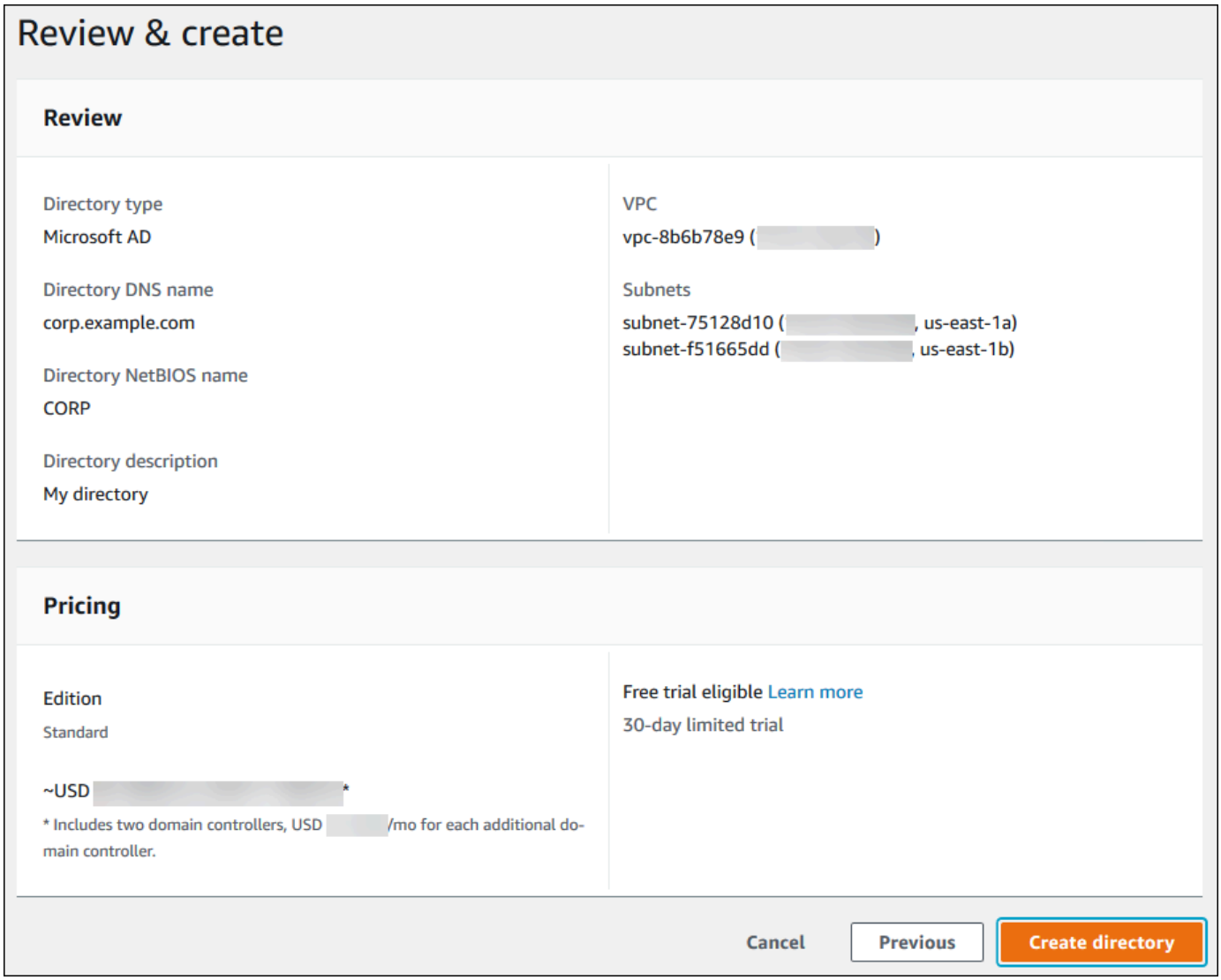
VPC

Elija la VPC del directorio. Puede crear la instancia de base de datos de PostgreSQL en esta misma VPC o en una VPC diferente.

Subredes

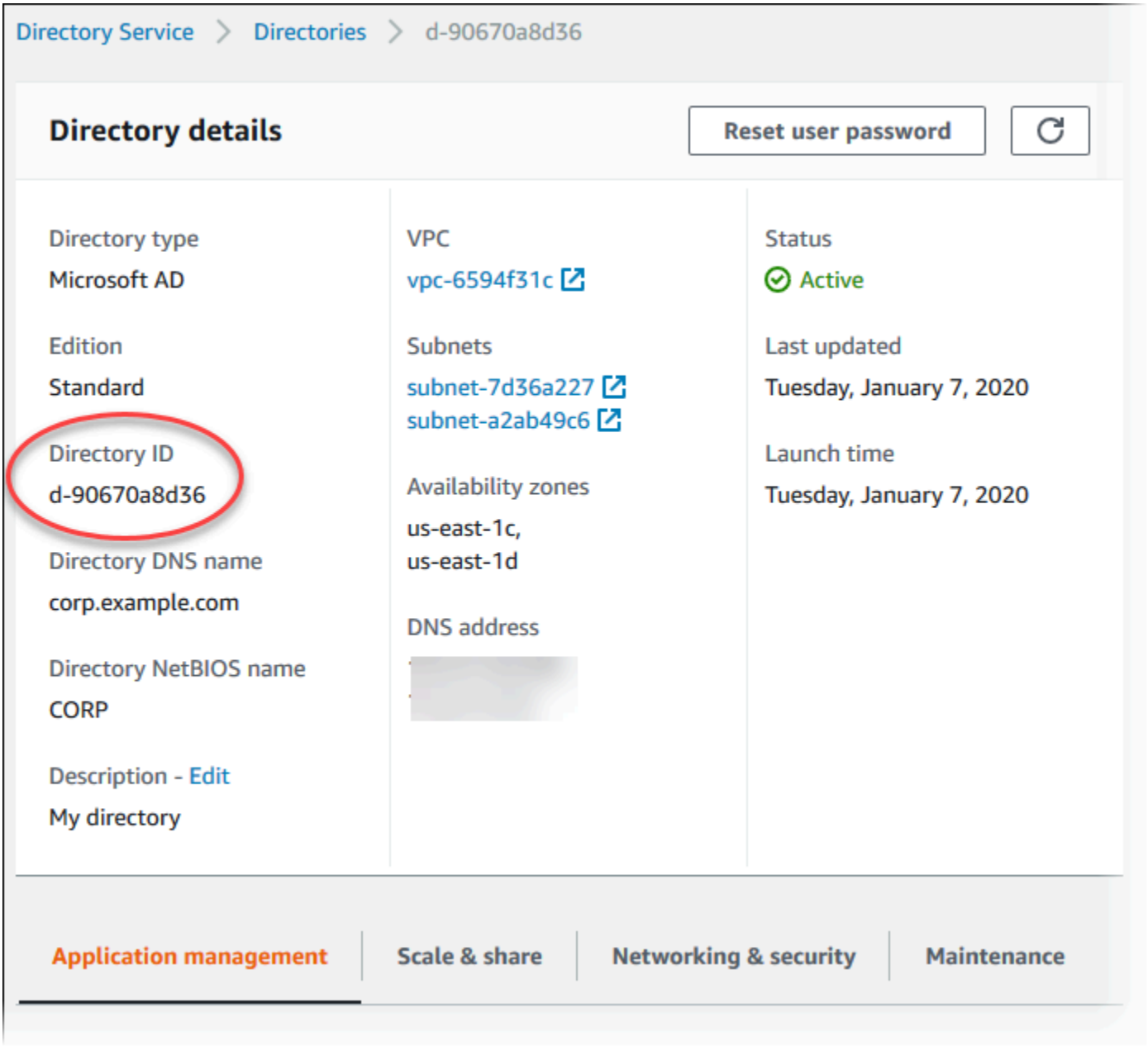
Elija las subredes de los servidores del directorio. Las dos subredes deben estar en diferentes zonas de disponibilidad.

7. Elija Siguiente.
8. Revise la información del directorio. Si es necesario realizar algún cambio, seleccione Previous (Anterior) y realizar los cambios. Cuando la información sea correcta, seleccione Create directory (Crear directorio).



La creación del directorio tarda varios minutos. Cuando se haya creado correctamente, el valor de Status (Estado) cambiará a Active (Activo).

Para ver información acerca de su directorio, seleccione el ID del directorio en la lista de directorios. Anote el valor de Directory ID (ID de directorio). Necesita este valor cuando cree o modifique su instancia de base de datos de PostgreSQL.



Paso 2: (opcional) crear una relación de confianza entre su Active Directory en las instalaciones y AWS Directory Service

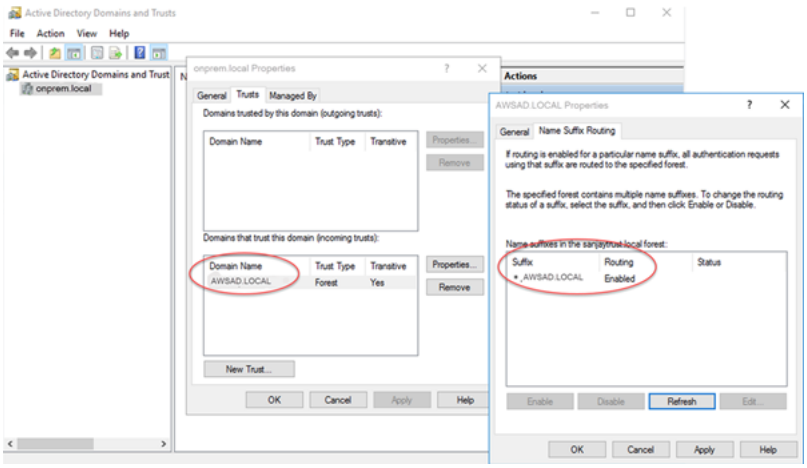
Si no planea usar su propio Microsoft Active Directory local, vaya a Paso 3: crear un rol de IAM para que Amazon RDS acceda a AWS Directory Service.

Para obtener la autenticación Kerberos mediante Active Directory en las instalaciones, debe crear una relación de dominio de confianza entre Microsoft Active Directory en las instalaciones y el directorio AWS Managed Microsoft AD (creado en Paso 1: crear un directorio con AWS Managed Microsoft AD). La confianza puede ser unidireccional, donde el directorio AWS Managed Microsoft

AD confía en Microsoft Active Directory local. La confianza también puede ser bidireccional, donde ambos Active Directories confían entre sí. Para obtener más información acerca de la configuración de relaciones de confianza con AWS Directory Service, consulte Cuándo crear una relación de confianza en la guía de administración de AWS Directory Service.

> **Note**
>
> Si utiliza Microsoft Active Directory en las instalaciones, los clientes de Windows se conectan con el nombre de dominio del AWS Directory Service en el punto de conexión en lugar de con rds.amazonaws.com. Para obtener más información, consulte Conexión a PostgreSQL con autenticación Kerberos.

Asegúrese de que el nombre de dominio local de Microsoft Active Directory incluya un enrutamiento de sufijo DNS que corresponda a la relación de confianza recién creada. En la siguiente captura de pantalla, se muestra un ejemplo.



Paso 3: crear un rol de IAM para que Amazon RDS acceda a AWS Directory Service

Para que Amazon RDS llame a AWS Directory Service en su nombre, su cuenta de AWS se precisa un rol de IAM que utilice la política de IAM administrada `AmazonRDSDirectoryServiceAccess`. Este rol permite que Amazon RDS llame a AWS Directory Service.

Cuando se crea una instancia de base de datos con la AWS Management Console y la cuenta de usuario de la consola tiene el permiso `iam:CreateRole`, la consola crea automáticamente el rol de IAM necesario. En este caso, el nombre del rol es `rds-directoryservice-kerberos-access-role`. De no ser así, debe crear el rol de IAM manualmente. Cuando

cree este rol de IAM, elija `Directory Service` y asocie la política administrada de AWS `AmazonRDSDirectoryServiceAccess` a este.

A fin de obtener más información acerca de la creación de roles de IAM para un servicio, consulte Creación de un rol para delegar permisos a un servicio de AWS en la guía del usuario de IAM.

> **Note**
>
> El rol de IAM utilizado para la autenticación de Windows para RDS para Microsoft SQL Server no puede ser utilizado por Amazon RDS para PostgreSQL.

Como alternativa al uso de la política administrada de `AmazonRDSDirectoryServiceAccess`, puede crear políticas con los permisos necesarios. En este caso, el rol de IAM debe tener la siguiente política de confianza de IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.amazonaws.com",
          "rds.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El rol debe también tener la siguiente política de rol de IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
    "Effect": "Allow",
    "Resource": "*"
    }
  ]
}
```

Para suscribirse a Regiones de AWS, utilice las entidades principales de servicios específicos de la región en las políticas de confianza de roles de IAM. Cuando cree una política de confianza para servicios en estas regiones, especifique el código de región en la entidad principal de servicio.

En el siguiente ejemplo se muestra una política de confianza que incluye entidades principales de servicio específicas de la región:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "directoryservice.rds.REGION-CODE.amazonaws.com",
          "rds.REGION-CODE.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
```

```
    }
  ]
}
```

Reemplace REGION-CODE por el código de la región específica. Por ejemplo, utilice las siguientes entidades principales de servicio para la región Asia-Pacífico (Melbourne):

```
"Service": [
  "directoryservice.rds.ap-southeast-4.amazonaws.com",
  "rds.ap-southeast-4.amazonaws.com"
]
```

Paso 4: crear y configurar usuarios

Puede crear usuarios usando la herramienta Usuarios y equipos de Active Directory. Es una de las herramientas Active Directory Domain Services y Active Directory Lightweight Directory Services. Para obtener más información, consulte Agregar usuarios y equipos al dominio de Active Directory en la documentación de Microsoft. En este caso, los usuarios son individuos u otras entidades, como sus equipos, que forman parte del dominio y cuyas identidades se mantienen en el directorio.

Para crear usuarios en un directorio de AWS Directory Service, debe estar conectado a una instancia de Amazon EC2 con Windows que sea miembro del directorio de AWS Directory Service. Al mismo tiempo, debe iniciar sesión como usuario con privilegios para crear usuarios. Para obtener más información, consulte Crear un usuario en la Guía de administración de AWS Directory Service.

Paso 5: habilitar el tráfico entre VPC entre el directorio y la instancia de base de datos

Si prevé ubicar el directorio y la instancia de base de datos en la misma VPC, omita este paso y continúe con Paso 6: crear o modificar una instancia de base de datos de PostgreSQL.

Si tiene previsto ubicar el directorio y la instancia de base de datos en diferentes VPC, configure el tráfico entre VPC mediante la interconexión de VPC o AWSTransit Gateway.

El siguiente procedimiento permite el tráfico entre VPC mediante la interconexión de VPC. Siga las instrucciones de ¿Qué es una interconexión de VPC? en la Guía de interconexión de Amazon Virtual Private Cloud.

Para habilitar el tráfico entre VPC mediante la interconexión de VPC

1. Configure las reglas de enrutamiento de VPC adecuadas para garantizar que el tráfico de red pueda fluir en ambos sentidos.
2. Asegúrese de que el grupo de seguridad de la instancia de base de datos pueda recibir tráfico de entrada del grupo de seguridad del directorio.
3. Asegúrese de que no haya una regla de lista de control de acceso (ACL) a la red para bloquear el tráfico.

Si una cuenta de AWS distinta es la propietaria del directorio, debe compartirlo.

Para compartir el directorio entre cuentas de AWS

1. Comience a compartir el directorio con la cuenta de AWS en la que se creará la instancia de base de datos mediante las instrucciones de Tutorial: Uso compartido del directorio de AWS Managed Microsoft AD para realizar la unión al dominio de EC2 sin problemas en la Guía de administración de AWS Directory Service.
2. Inicie sesión en la consola de AWS Directory Service utilizando la cuenta para la instancia de base de datos y asegúrese de que el dominio tiene el estado `SHARED` antes de continuar.
3. Una vez iniciada sesión en la consola de AWS Directory Service utilizando la cuenta de la instancia de base de datos, anote el valor de Directory ID (ID de directorio). Utilice este identificador de directorio para unir la instancia de base de datos al dominio.

Paso 6: crear o modificar una instancia de base de datos de PostgreSQL

Cree o modifique una instancia de base de datos de PostgreSQL para usarla con su directorio. Puede utilizar la consola, la CLI o la API de RDS para asociar una instancia de base de datos con un directorio. Puede hacerlo de una de las siguientes formas:

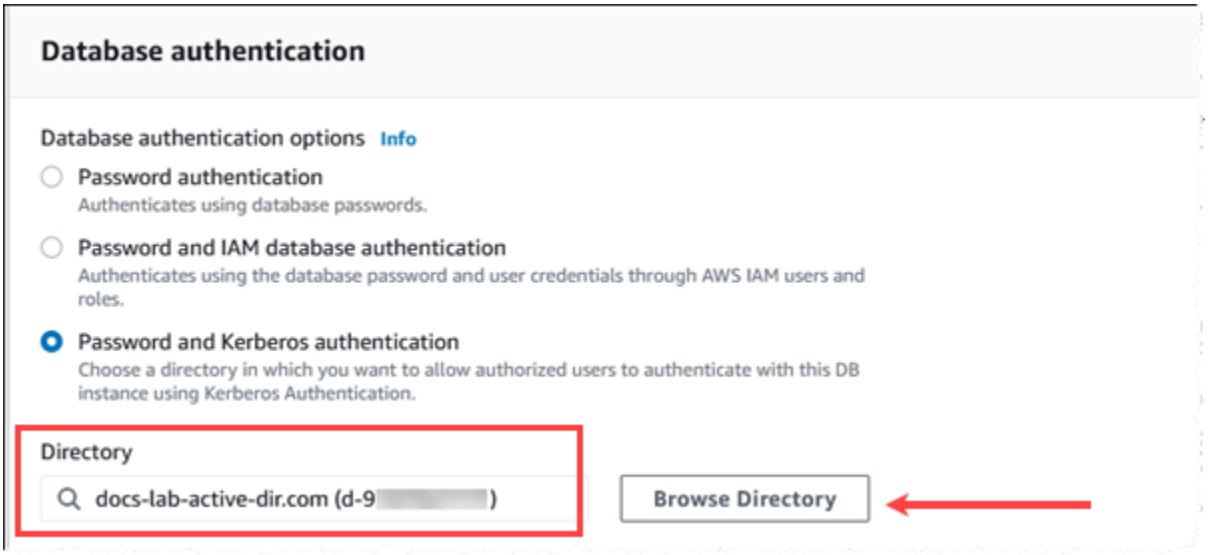
- Cree una nueva instancia de base de datos de PostgreSQL utilizando la consola, el comando de CLI create-db-instance o la operación CreateDBInstance de la API de RDS. Para obtener instrucciones, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de PostgreSQL existente utilizando la consola, el comando de CLI modify-db-instance o la operación ModifyDBInstance de la API de RDS. Para obtener instrucciones, consulte Modificación de una instancia de base de datos de Amazon RDS.

- Restaure una instancia de base de datos de PostgreSQL a partir de una instantánea de base de datos utilizando la consola, el comando de CLI restore-db-instance-from-db-snapshot o la operación RestoreDBInstanceFromDBSnapshot de la API de RDS. Para obtener instrucciones, consulte Restauración a una instancia de base de datos.
- Restaure una instancia de base de datos de PostgreSQL a partir de un punto en el tiempo utilizando la consola, el comando de CLI restore-db-instance-to-point-in-time o la operación RestoreDBInstanceToPointInTime de la API de RDS. Para obtener instrucciones, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

La autenticación de Kerberos solo es compatible con de clústeres de base de datos de PostgreSQL en una VPC. La instancia de DB puede estar en la misma VPC que el directorio o en una VPC diferente. La instancia de base de datos debe usar un grupo de seguridad que permita el ingreso y la salida dentro de la VPC del directorio, de modo que la instancia de base de datos pueda comunicarse con el directorio.

Consola

Si utiliza la consola para crear, modificar o restaurar una instancia de base de datos, elija Password and Kerberos authentication (Contraseña y autenticación de Kerberos) en la sección Database authentication (Autenticación de base de datos). Luego, elija Browse Directory (Examinar directorio). Seleccione el directorio o elija Create a new directory (Crear un nuevo directorio) para utilizar Directory Service.



AWS CLI

Cuando utilice la AWS CLI, se necesitan los siguientes parámetros para que la instancia de base de datos pueda usar el directorio que ha creado:

- Para el parámetro `--domain`, utilice el identificador de dominio (identificador "d-*") que se generó cuando creó el directorio.
- Para el parámetro `--domain-iam-role-name`, utilice el rol que creó que usa la política `AmazonRDSDirectoryServiceAccess` de IAM administrada.

Por ejemplo, el siguiente comando de CLI modifica una instancia de base de datos para que use un directorio.

```
aws rds modify-db-instance --db-instance-identifier mydbinstance --domain d-Directory-ID --domain-iam-role-name role-name
```

> **Important**
>
> Si modifica una instancia de base de datos para habilitar la autenticación de Kerberos, reinicie la instancia de base de datos después de hacer el cambio.

Paso 7: crear usuarios de PostgreSQL para las entidades principales de Kerberos

En este punto, su instancia de base de datos de RDS para PostgreSQL se une al dominio AWS Managed Microsoft AD. Los usuarios que haya creado en el directorio en el Paso 4: crear y configurar usuarios deben configurarse como usuarios de la base de datos de PostgreSQL y tener privilegios para iniciar sesión en la base de datos. Para ello, inicie sesión como usuario de la base de datos con privilegios `rds_superuser`. Por ejemplo, si ha aceptado los valores predeterminados al crear la instancia de base de datos de RDS para PostgreSQL, utiliza `postgres`, tal como se muestra en los pasos siguientes.

Para crear usuarios de la base de datos de PostgreSQL para las entidades principales de Kerberos

1. Use `psql` para conectarse a su punto de conexión de la instancia de base de datos del RDS para PostgreSQL mediante `psql`. En el siguiente ejemplo, se usa la cuenta de `postgres` predeterminada del rol de `rds_superuser`.

```
psql --host=cluster-instance-1.111122223333.aws-region.rds.amazonaws.com --
port=5432 --username=postgres --password
```

2. Cree un nombre de usuario de base de datos para cada entidad principal de Kerberos (nombre de usuario de Active Directory) al que desee otorgar acceso a la base de datos. Utilice el nombre de usuario canónico (identidad) tal como se define en la instancia de Active Directory, es decir, un `alias` en minúsculas (nombre de usuario en Active Directory) y el nombre en mayúsculas del dominio de Active Directory para ese nombre de usuario. El nombre de usuario de Active Directory es un usuario autenticado externamente, así que utilice comillas alrededor del nombre tal como se muestra a continuación.

```
postgres=> CREATE USER "username@CORP.EXAMPLE.COM" WITH LOGIN;
CREATE ROLE
```

3. Otorgue el rol `rds_ad` al usuario de la base de datos.

```
postgres=> GRANT rds_ad TO "username@CORP.EXAMPLE.COM";
GRANT ROLE
```

Cuando termine de crear todos los usuarios de PostgreSQL para sus identidades de usuario de Active Directory, los usuarios podrán acceder a la instancia de base de datos de RDS para PostgreSQL con sus credenciales de Kerberos.

Es necesario que los usuarios de bases de datos que se autentican mediante Kerberos lo hagan desde máquinas de cliente que sean miembros del dominio de Active Directory.

Los usuarios de bases de datos a los que se les ha otorgado el rol `rds_ad` tampoco pueden tener el rol `rds_iam`. Esto se aplica también a las membresías anidadas. Para obtener más información, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

Paso 8: configurar un cliente de PostgreSQL

Para configurar un cliente de PostgreSQL, siga los pasos siguientes:

- Cree un archivo krb5.conf (o equivalente) para apuntar al dominio.
- Verifique que el tráfico puede fluir entre el host cliente y AWS Directory Service. Use una utilidad de red como, por ejemplo, Netcat para lo siguiente:
  - Verificar el tráfico sobre DNS para el puerto 53.

  - Verificar el tráfico sobre TCP/UDP para el puerto 52 y para Kerberos, lo que incluye los puertos 88 y 464 para AWS Directory Service.
- Verifique que el tráfico puede fluir entre el host cliente y la instancia de base de datos sobre el puerto de base de datos. Por ejemplo, utilice psql para conectarse y acceder a la base de datos.

A continuación, se muestra el contenido krb5.conf para AWS Managed Microsoft AD.

```
[libdefaults]
 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
```

A continuación, se muestra el contenido krb5.conf de ejemplo para un Microsoft Active Directory local.

```
[libdefaults]
 default_realm = EXAMPLE.COM
[realms]
 EXAMPLE.COM = {
  kdc = example.com
  admin_server = example.com
 }
 ONPREM.COM = {
  kdc = onprem.com
  admin_server = onprem.com
 }
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
 .onprem.com = ONPREM.COM
 onprem.com = ONPREM.COM
 .rds.amazonaws.com = EXAMPLE.COM
 .amazonaws.com.cn = EXAMPLE.COM
 .amazon.com = EXAMPLE.COM
```

Administración de una instancia de base de datos de RDS para PostgreSQL en un dominio de Active Directory

Puede usar la consola, la CLI o la API de RDS para administrar la instancia de base de datos y su relación con Microsoft Active Directory. Puede, por ejemplo, asociar un Active Directory para habilitar la autenticación Kerberos. También puede eliminar la asociación para un Active Directory para deshabilitar la autenticación Kerberos. También puede mover una instancia de base de datos que va a ser autenticada externamente por un Microsoft Active Directory a otro.

Por ejemplo, con la CLI, puede hacer lo siguiente:

- Para volver a intentar habilitar la autenticación Kerberos para una suscripción con error, use el comando modify-db-instance de la CLI. Especifique el ID de directorio de pertenencia actual para la opción `--domain`.
- Para deshabilitar la autenticación Kerberos en una instancia de base de datos, utilice el comando modify-db-instance de la CLI. Especifique `none` para la opción `--domain`.
- Para mover una instancia de base de datos desde un dominio a otro, utilice el comando modify-db-instance de la CLI. Especifique el identificador de dominio del nuevo dominio para la opción `--domain`.

Descripción de la pertenencia a los dominios

Después de crear o modificar la instancia de base de datos, se convierte en miembro de un dominio. Puede ver el estado de la suscripción al dominio en la consola o ejecutando el comando describe-db-instances de la CLI. El estado de la instancia de base de datos puede ser uno de los siguientes:

- `kerberos-enabled`: la instancia de base de datos tiene habilitada la autenticación Kerberos.
- `enabling-kerberos` - AWS está en proceso de habilitar la autenticación Kerberos en esta instancia de base de datos.
- `pending-enable-kerberos`: la habilitación de la autenticación Kerberos está pendiente en esta instancia de base de datos.
- `pending-maintenance-enable-kerberos` - AWS intentará habilitar la autenticación Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `pending-disable-kerberos`: la deshabilitación de la autenticación Kerberos está pendiente en esta instancia de base de datos.

- `pending-maintenance-disable-kerberos` - AWS intentará desactivar la autenticación Kerberos en la instancia de base de datos durante el próximo periodo de mantenimiento programado.
- `enable-kerberos-failed` - Un problema de configuración ha impedido que AWS habilite la autenticación Kerberos en la instancia de base de datos. Corrija el problema de configuración antes de volver a ejecutar el comando para modificar la instancia de base de datos.
- `disabling-kerberos` - AWS está en proceso de desactivar la autenticación Kerberos en esta instancia de base de datos.

Una solicitud para habilitar la autenticación Kerberos puede generar un error a causa de un problema de conectividad de la red o de un rol de IAM incorrecto. En algunos casos, el intento de habilitar la autenticación Kerberos podría producir un error al crear o modificar una instancia de base de datos. En tal caso, asegúrese de que está utilizando el rol de IAM correcto, a continuación modifique la instancia de base de datos para unirse al dominio.

> **Note**
>
> Solo la autenticación Kerberos con RDS para PostgreSQL envía tráfico a los servidores DNS del dominio. Las otras solicitudes de DNS se tratan como acceso de red saliente en las instancias de bases de datos que ejecutan PostgreSQL. Para obtener más información acerca del acceso de red saliente con RDS para PostgreSQL, consulte Uso de un servidor de DNS personalizado para el acceso a la red de salida..

Conexión a PostgreSQL con autenticación Kerberos

Puede conectarse a PostgreSQL con autenticación Kerberos con la interfaz pgAdmin o con una interfaz de línea de comandos como, por ejemplo, psql. Para obtener más información acerca de las conexiones, consulte Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL . Para obtener información sobre cómo obtener el punto de conexión, el número de puerto y otros detalles necesarios para la conexión, consulte Conexión a la instancia de base de datos PostgreSQL.

> **Note**
>
> La autenticación y el cifrado GSSAPI en PostgreSQL están implementados por la biblioteca Kerberos `libkrb5.so`. Características como `postgres_fdw` y `dblink` también se basan en esta misma biblioteca para las conexiones salientes con autenticación o cifrado Kerberos.

pgAdmin

Para utilizar pgAdmin para conectarse a PostgreSQL con la autenticación Kerberos, siga estos pasos:

1. Lance la aplicación pgAdmin en su equipo cliente.
2. En la pestaña Dashboard (Panel), elija Add New Server (Añadir nuevo servidor).
3. En el cuadro de diálogo Crear - Servidor, escriba un nombre en la pestaña General para identificar el servidor en pgAdmin.
4. En la pestaña Connection (Conexión), introduzca la siguiente información de su base de datos RDS for PostgreSQL de :
   - En Host, introduzca el punto de conexión de la Instancia de base de datos RDS para PostgreSQL. Un punto de conexión tiene un aspecto similar al siguiente:

     ```
     RDS-DB-instance.111122223333.aws-region.rds.amazonaws.com
     ```

     Para conectarse a un Microsoft Active Directory en las instalaciones desde un cliente de Windows, utilice el nombre de dominio del Active Directory administrado por AWS en lugar de `rds.amazonaws.com` en el punto de conexión del host. Por ejemplo, suponga que el nombre de dominio de AWS Managed Active Directory es `corp.example.com`. Luego, para Host, el punto de conexión se especificaría de la siguiente manera:

     ```
     RDS-DB-instance.111122223333.aws-region.corp.example.com
     ```
   - En Puerto, escriba el puerto asignado.
   - En Base de datos de mantenimiento, escriba el nombre de la base de datos inicial a la que se conectará el cliente.
   - En Nombre de usuario, escriba el nombre de usuario que especificó para la autenticación Kerberos en Paso 7: crear usuarios de PostgreSQL para las entidades principales de Kerberos .

5. Seleccione Save.

Psql

Para utilizar psql para conectar a PostgreSQL con autenticación Kerberos, siga los pasos siguientes:

1. En el símbolo del sistema, ejecute el siguiente comando.

   ```
   kinit username
   ```

   Sustituya *username* por el nombre de usuario. En el símbolo del sistema, introduzca la contraseña almacenada en Microsoft Active Directory para el usuario.
2. Si la instancia de base de datos de PostgreSQL utiliza una VPC accesible públicamente, coloque una dirección IP para su punto de conexión de instancia de base de datos en su archivo `/etc/hosts` en el cliente EC2. Por ejemplo, los comandos siguientes obtienen la dirección IP y, a continuación, la ponen en el archivo `/etc/hosts`.

   ```
   % dig +short PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com
   ;; Truncated, retrying in TCP mode.
   ec2-34-210-197-118.AWS-Region.compute.amazonaws.com.
   34.210.197.118

   % echo " 34.210.197.118  PostgreSQL-endpoint.AWS-Region.rds.amazonaws.com" >> /etc/
   hosts
   ```

   Si utiliza un Microsoft Active Directory en las instalaciones desde un cliente de Windows, tiene que conectarse mediante un punto de enlace especializado. En lugar de utilizar el dominio de Amazon `rds.amazonaws.com` en el punto de conexión del host, utilice el nombre de dominio de AWS Managed Active Directory.

   Por ejemplo, suponga que el nombre de dominio de su AWS Managed Active Directory es `corp.example.com`. A continuación, use el formato *PostgreSQL-endpoint.AWS-Region.corp.example.com* para el punto de enlace y colóquelo en el archivo `/etc/hosts`.

   ```
   % echo " 34.210.197.118  PostgreSQL-endpoint.AWS-Region.corp.example.com" >> /etc/
   hosts
   ```
3. Utilice el comando psql siguiente para iniciar sesión en una instancia de de base de datos de PostgreSQL que está integrada con Active Directory.

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-
Region.rds.amazonaws.com postgres
```

Para iniciar sesión en el clúster de base de datos de PostgreSQL desde un cliente de Windows utilizando un Active Directory en las instalaciones, utilice el siguiente comando psql con el nombre de dominio del paso anterior (`corp.example.com`):

```
psql -U username@CORP.EXAMPLE.COM -p 5432 -h PostgreSQL-endpoint.AWS-
Region.corp.example.com postgres
```

Uso de un servidor de DNS personalizado para el acceso a la red de salida.

RDS for PostgreSQL admite ahora el acceso de red de salida en las instancias de base de datos y permite resoluciones del servicio de nombres de dominio (DNS) desde un servidor de DNS personalizado propiedad del cliente. Solo es posible resolver nombres de dominio completos desde una instancia de base de datos de RDS for PostgreSQL a través de un servidor DNS personalizado.

Temas

- Activación de la resolución de DNS personalizada
- Desactivación de la resolución de DNS personalizada
- Configuración de un servidor DNS personalizado

Activación de la resolución de DNS personalizada

Para activar la resolución de DNS en la VPC de su cliente, debe asociar primero un grupo de parámetros de base de datos personalizado a su instancia de RDS for PostgreSQL. A continuación, active el parámetro `rds.custom_dns_resolution` configurándolo en 1 y luego reinicie la instancia de base de datos para que los cambios surtan efecto.

Desactivación de la resolución de DNS personalizada

Para desactivar la resolución de DNS en la VPC del cliente, primero desactive el parámetro `rds.custom_dns_resolution` de su grupo de parámetros de base de datos personalizado estableciéndolo en 0. Luego reinicie la instancia de base de datos para que los cambios surtan efecto.

Configuración de un servidor DNS personalizado

Después de configurar un servidor de nombres DNS personalizado, se tardan hasta 30 minutos en propagar los cambios a la instancia de base de datos. Una vez que se propaguen los cambios a la instancia de base de datos, todo el tráfico de red saliente que requiera una búsqueda de DNS consultará el servidor DNS personalizado a través del puerto 53.

> **Note**
>
> Si no configura un servidor DNS personalizado y configura `rds.custom_dns_resolution` en 1, los hosts se resuelven mediante una zona privada de Amazon Route 53. Para obtener más información, consulte Uso de zonas alojadas privadas.

Para configurar un servidor DNS personalizado para una instancia de base de datos de RDS for PostgreSQL

1. Desde el conjunto de opciones del protocolo de configuración dinámica de host (DHCP) asociado a la VPC, configure la opción `domain-name-servers` en la dirección IP del servidor de nombres DNS. Para obtener más información, consulte Conjuntos de opciones de DHCP.

   > **Note**
   >
   > La opción `domain-name-servers` acepta hasta cuatro valores, pero la instancia de base de datos de Amazon RDS solo utiliza el primer valor.

2. Asegúrese de que el servidor DNS puede resolver todas las consultas de búsqueda, incluidos los nombres de DNS públicos, los nombres de DNS privados de Amazon EC2 y los nombres de DNS específicos del cliente. Si el tráfico de red saliente contiene búsquedas de DNS que el servidor DNS no puede resolver, este debe tener configurados los proveedores de DNS correspondientes.
3. Configure el servidor DNS para que genere respuestas de protocolo de datagramas de usuario (UDP) de 512 bytes como máximo.
4. Configure el servidor DNS para que genere respuestas de protocolo de control de transmisión (TCP) de 1024 bytes o menos.
5. Configure el servidor DNS para que permita el tráfico entrante desde las instancias de bases de datos de Amazon RDS a través del puerto 53. Si el servidor DNS está en una Amazon VPC, la VPC debe tener un grupo de seguridad que contenga reglas entrantes que permitan el tráfico UDP y TCP en el puerto 53. Si el servidor DNS no está en una Amazon VPC, debe tener la configuración de firewall apropiada para permitir el tráfico de entrada UDP y TCP en el puerto 53.

   Para obtener más información, consulte Grupos de seguridad de su VPC y Adición, eliminación y actualización de reglas.

6. Configure la VPC de la instancia de base de datos de Amazon RDS para que permita el tráfico saliente a través del puerto 53. La VPC debe tener un grupo de seguridad que contenga reglas salientes que permitan el tráfico UDP y TCP en el puerto 53.

   Para obtener más información, consulte Grupos de seguridad de su VPC y Adición y eliminación de reglas en la Guía del usuario de Amazon VPC.

7. Asegúrese de que el trayecto de enrutamiento entre la instancia de base de datos de Amazon RDS y el servidor DNS esté configurado correctamente para permitir el tráfico de DNS.

   Además, si la instancia de base de datos de Amazon RDS y el servidor DNS no están en la misma VPC, debe establecerse un emparejamiento entre ellos. Para obtener más información, consulte ¿Qué es un emparejamiento de VPC? en la Guía de emparejamiento de VPC de Amazon.

Actualizaciones del motor de base de datos de RDS para PostgreSQL

Hay dos tipos de actualizaciones que se pueden administrar para su base de datos de PostgreSQL:

- Actualizaciones del sistema operativo: a veces, Amazon RDS puede necesitar actualizar el sistema operativo subyacente de su base de datos para aplicar correcciones de seguridad o cambios del sistema operativo. Puede indicar cuándo Amazon RDS debe aplicar las actualizaciones del SO mediante la consola de RDS, la AWS Command Line Interface (AWS CLI) o la API de RDS. Para obtener más información acerca de las actualizaciones del sistema operativo, consulte Aplicación de actualizaciones a una instancia de base de datos.
- Actualizaciones del motor de la base de datos: cuando Amazon RDS admita una nueva versión de un motor de base de datos, puede actualizar sus bases de datos a la nueva versión.

En este contexto, una base de datos es una instancia de base de datos de RDS para PostgreSQL o un clúster de base de datos Multi-AZ.

Hay dos tipos de actualizaciones de motores de bases de datos de PostgreSQL: actualizaciones de versiones principales y actualizaciones de versiones secundarias.

Actualizaciones de la versión principal

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de las aplicaciones. Por lo tanto, debe realizar manualmente las actualizaciones de versiones principales de sus bases de datos. Puede iniciar una actualización de versión principal modificando su instancia de base de datos o clúster de base de datos Multi-AZ. Antes de realizar la actualización de una versión principal, recomendamos que siga los pasos descritos en Elección de una versión principal para una actualización de RDS para PostgreSQL.

Amazon RDS gestiona las actualizaciones de las versiones principales de multi-AZ de las siguientes maneras:

- Implementación de instancia de base de datos multi-AZ: Amazon RDS actualiza simultáneamente la instancia principal y cualquier instancia en espera. Es posible que la base de datos no esté disponible durante varios minutos mientras se completa la actualización.

- Implementación de clúster de base de datos multi-AZ: Amazon RDS actualiza de forma simultánea las instancias del lector y del escritor. Es posible que la base de datos no esté disponible durante varios minutos mientras se completa la actualización.

Si actualiza una instancia de base de datos que tiene réplicas de lectura en la región, Amazon RDS actualiza las réplicas junto con la instancia de base de datos principal.

Amazon RDS no actualiza réplicas de lectura de clústeres de base de datos Multi-AZ. Si actualiza la versión principal de un clúster de base de datos multi-AZ, el estado de replicación de las réplicas de lectura cambia a terminado. Debe eliminar las réplicas de lectura y volver a crearlas de forma manual una vez finalizada la actualización.

> **Tip**
>
> Puede minimizar el tiempo de inactividad necesario para la actualización de una versión principal mediante una implementación azul/verde. Para obtener más información, consulte Uso de las implementaciones azul/verde para actualizar las bases de datos.

Actualizaciones de la versión secundaria

Por su parte, las actualizaciones de versiones secundarias solo incluyen cambios compatibles con las versiones anteriores de las aplicaciones. Puede iniciar manualmente una actualización de versiones secundarias modificando su base de datos. O puede habilitar la opción Actualización automática de versiones secundarias al crear o modificar una base de datos. Si lo hace, Amazon RDS actualizará automáticamente su base de datos tras probar y aprobar la nueva versión.

Amazon RDS gestiona las actualizaciones de las versiones secundarias de multi-AZ de las siguientes maneras:

- Implementación de instancia de base de datos multi-AZ: Amazon RDS actualiza simultáneamente la instancia principal y cualquier instancia en espera. Es posible que la base de datos no esté disponible durante varios minutos mientras se completa la actualización.
- Implementación de clúster de base de datos multi-AZ: Amazon RDS actualiza las instancias de base de datos del lector de una en una. A continuación, una de las instancias de base de datos de lector pasa a ser la nueva instancia de base de datos de escritor. Amazon RDS actualiza luego la antigua instancia de escritor (que ahora es una instancia de lector). Los clústeres de bases de datos multi-AZ suelen reducir el tiempo de inactividad de las actualizaciones de versiones secundarias a aproximadamente 35 segundos. Cuando se utilizan con RDS Proxy,

se puede reducir aún más el tiempo de inactividad a un segundo o menos. Para obtener más información, consulte Amazon RDS Proxy. Otra opción, puede utilizar un proxy de base de datos de código abierto como ProxySQL, PgBouncer o el controlador de contenedor JDBC avanzado de AWS.

Si la base de datos tiene réplicas de lectura, debe actualizar primero todas las réplicas de lectura antes de actualizar la instancia o el clúster de origen.

Para obtener más información, consulte Actualizaciones de versiones secundarias automáticas de RDS para PostgreSQL. Para obtener más información acerca de cómo realizar manualmente una actualización de versiones secundarias, consulte Actualización manual de la versión del motor.

Para obtener más información acerca de las versiones del motor de base de datos y la política para dar de baja versiones del motor de base de datos, consulte Versiones del motor de base de datos en las Preguntas frecuentes de Amazon RDS.

Temas

- Aspectos a tener en cuenta sobre las actualizaciones de PostgreSQL
- Búsqueda de objetivos de actualización válidos
- Números de versión de PostgreSQL
- Números de versión de RDS en RDS para PostgreSQL
- Elección de una versión principal para una actualización de RDS para PostgreSQL
- Realización de una actualización de la versión principal de RDS para PostgreSQL
- Actualizaciones de versiones secundarias automáticas de RDS para PostgreSQL
- Actualización de las extensiones de PostgreSQL en bases de datos de RDS para PostgreSQL

Aspectos a tener en cuenta sobre las actualizaciones de PostgreSQL

Para actualizar de forma segura las bases de datos, Amazon RDS usa la utilidad `pg_upgrade` descrita en la documentación de PostgreSQL.

Si el periodo de retención de copia de seguridad es mayor que 0, Amazon RDS toma dos instantáneas de base de datos durante el proceso de actualización. La primera instantánea de base de datos es la de la base de datos antes de que se haya llevado a cabo ningún cambio. Si la

actualización de sus bases de datos da por resultado un error, puede restaurar esta instantánea para crear una base de datos en la que se ejecuta la versión antigua. La segunda instantánea de base de datos se crea cuando se completa la actualización. Estas instantáneas de bases de datos se eliminan automáticamente una vez que expira el periodo de retención de la copia de seguridad.

> **Note**
>
> Amazon RDS toma instantáneas de base de datos durante el proceso de actualización solo si ha definido el período de retención de copia de seguridad de su base de datos en un número mayor que 0. Para modificar el período de retención de copia de seguridad de una instancia de base de datos, consulte the section called “Modificación de una instancia de base de datos”. No puede configurar un período de retención de copia de seguridad personalizado para un clúster de base de datos Multi-AZ.

Al actualizar la versión principal de una instancia de base de datos, todas las réplicas de lectura dentro de la región también se actualizan automáticamente. Una vez que se inicia el flujo de trabajo de actualización, las réplicas de lectura esperan a que `pg_upgrade` se complete correctamente en la instancia de base de datos principal. A continuación, la actualización de la instancia de base de datos principal espera a que se complete la actualización de la réplica de lectura. Habrá una interrupción hasta que se complete la actualización. Cuando actualiza la versión principal de un clúster de base de datos Multi-AZ, el estado de replicación de las réplicas de lectura cambia a terminado.

Una vez completada una actualización, no puede volver a la versión anterior del motor de base de datos. Si desea volver a la versión anterior, restaure la instantánea de base de datos que se realizó antes de la actualización para crear una nueva base de datos.

Búsqueda de objetivos de actualización válidos

Cuando se utiliza la AWS Management Console para actualizar una base de datos, muestra los destinos de actualización válidos para la base de datos. También puede utilizar el siguiente comando de la AWS CLI para identificar los destinos de actualización válidos de una base de datos:

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
  --engine postgres \
```

```
  --engine-version version-number \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
  --engine postgres ^
  --engine-version version-number ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Por ejemplo, para identificar los destinos de actualización válidos para una base de datos de la versión 16.1 de PostgreSQL, ejecute el siguiente comando de la AWS CLI:

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
  --engine postgres \
  --engine-version 16.1 \
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
  --engine postgres ^
  --engine-version 16.1 ^
  --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

Números de versión de PostgreSQL

La secuencia de numeración de versiones para el motor de base de datos PostgreSQL es la siguiente:

- Para las versiones 10 y posteriores de PostgreSQL, el número de versión del motor tiene el formato principal.secundaria. El número de versión principal es la parte entera del número de versión. El número de versión secundaria es la parte fraccional del número de versión.

Una actualización de versión principal aumenta la parte entera del número de versión, como la actualización de 10.secundaria a 11.secundaria.

- Para las versiones de PostgreSQL anteriores a 10, el número de versión del motor tiene el formato principal.principal.secundaria. El número de versión principal del motor es tanto el entero como la primera parte fraccional del número de versión. Por ejemplo, 9.6 es una versión principal. El número de versión secundaria es la tercera parte del número de versión. Por ejemplo, para la versión 9.6.12, el 12 es el número de versión secundaria.

  Una actualización de versión principal aumenta la parte principal del número de versión. Por ejemplo, una actualización de 9.6.12 a 11.14 es una actualización de versión principal, donde 9.6 y 11 son los números de la versión principal.

Para obtener información sobre la numeración de versiones del Soporte extendido de RDS, consulte Nombre de versiones con el Soporte extendido de Amazon RDS.

Números de versión de RDS en RDS para PostgreSQL

Los números de versión de RDS utilizan el esquema de nomenclatura *major*.*minor*.*patch*. Una versión de parche de RDS incluye correcciones de errores importantes que se agregan a una versión secundaria después de su lanzamiento. Para obtener información sobre la numeración de versiones del Soporte extendido de RDS, consulte Nombre de versiones con el Soporte extendido de Amazon RDS.

Para identificar el número de versión de Amazon RDS de la base de datos, primero debe crear la extensión `rds_tools` mediante el siguiente comando:

```
CREATE EXTENSION rds_tools;
```

A partir del lanzamiento de la versión 15.2-R2 de PostgreSQL, puede averiguar el número de la versión de RDS de la base de datos de RDS para PostgreSQL con la siguiente consulta SQL:

```
postgres=> SELECT rds_tools.rds_version();
```

Por ejemplo, la consulta de una bases de datos de RDS para PostgreSQL 15.2 muestra lo siguiente:

```
rds_version
----------------
 15.2.R2
```

```
(1 row)
```

Elección de una versión principal para una actualización de RDS para PostgreSQL

Las actualizaciones de la versión principal pueden contener cambios realizados en la base de datos que no son compatibles con las versiones anteriores de la base de datos. La nueva funcionalidad puede hacer que sus aplicaciones existentes dejen de funcionar correctamente. Por este motivo, Amazon RDS no aplica automáticamente actualizaciones de la versión principal. Para realizar una actualización de versión principal, modifique la base de datos manualmente. Pruebe exhaustivamente cualquier actualización para comprobar que las aplicaciones funcionen correctamente antes de aplicar la actualización a sus bases de datos de producción. Cuando realice una actualización de versión principal de PostgreSQL, recomendamos que siga los pasos descritos en Realización de una actualización de la versión principal de RDS para PostgreSQL.

Cuando actualiza una implementación de instancia de base de datos Multi-AZ o instancia de base de datos Single-AZ de PostgreSQL o a su siguiente versión principal, todas las réplicas de lectura asociadas a la base de datos también se actualizan a la siguiente versión principal. En algunos casos, cuando hace una actualización puede saltar hasta una versión principal superior. Si la actualización omite una versión principal, las réplicas de lectura también se actualizan a esa versión principal de destino. Las actualizaciones a la versión 11 que omiten otras versiones principales tienen ciertas limitaciones. Puede encontrar los detalles en los pasos descritos en Realización de una actualización de la versión principal de RDS para PostgreSQL.

La mayoría de las extensiones de PostgreSQL no se actualizan durante la actualización del motor PostgreSQL. Estas deben actualizarse por separado. Para obtener más información, consulte Actualización de las extensiones de PostgreSQL en bases de datos de RDS para PostgreSQL.

Puede averiguar qué versiones principales están disponibles para su base de datos de RDS para PostgreSQL mediante la ejecución de las siguientes consultas de la:AWS CLI

```
aws rds describe-db-engine-versions --engine postgres  --engine-version your-version
 --query "DBEngineVersions[*].ValidUpgradeTarget[*].{EngineVersion:EngineVersion}" --
output text
```

En la tabla siguiente se resumen los resultados de esta consulta para todas las versiones disponibles. Un asterisco (*) en el número de versión significa que la versión ya no es compatible. Si la versión actual ya nos es compatible, le recomendamos que actualice al destino de actualización de

versión secundaria más reciente o a uno de los otros destinos de actualización disponibles para esa versión.

Versión de origen actual	Destinos de actualización
17.5	Ninguno
17.4	17.5
17.3	17.5, 17.4
17.2	17.5, 17.4, 17.3
17.1	17.5, 17.4, 17.3 , 17.2
16.9	17.5
16.8	17.5, 17.4
16.7	17.5, 17.4, 17.3 16.8
16.6	17.5, 17.4, 17.3 , 17.2 16.8, 16.7
16.5	17.5, 17.4, 17.3, 17.2, 17.1 16.8, 16.7, 16.6
16.4	17.5, 17.4, 17.3, 17.2, 17.1 16.8, 16.7, 16.6, 16.5
16.3	17.5, 17.4, 17.3, 17.2, 17.1 16.8, 16.7, 16.6, 16.5, 16.4
16.2	17.5, 17.4, 17.3, 17.2, 17.1 16.8, 16.7, 16.6, 16.5, 16.4, 16.3

Versión de origen actual	Destinos de actualización
16.1	17.5, 17.4, 17.3, 17.2, 17.1 16.8, 16.7, 16.6, 16.5, 16.4, 16.3, 16.2
15.13	17.5 16.9
15.12	17.4 16.9, 16.8 15.13
15.11	17.3 16.9, 16.8, 16.7 15.13, 15.12
15.10	17.2 16.9, 16.8, 16.7, 16.6 15.13, 15.12, 15.11
15.9	17.1 16.9, 16.8, 16.7, 16.6, 16.5 15.13, 15.12, 15.11, 15.10
15.8	16.9, 16.8, 16.7, 16.6, 16.5, 16.4 15.13, 15.12, 15.11, 15.10, 15.9
15.7	16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.3 15.13, 15.12, 15.11, 15.10, 15.9, 15.8

Versión de origen actual	Destinos de actualización
15.6	16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.3, 16.2 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7
15.5	16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.3, 16.2, 16.1 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6
15.4	16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.3, 16.2, 16.1 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5
15.3	16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.3, 16.2, 16.1 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4
15.2*	16.9, 16.8, 16.7, 16.6, 16.5, 16.4, 16.3, 16.2, 16.1 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4
14.18	17.5 16.9 15.13

Versión de origen actual	Destinos de actualización
14.17	17.4 16.8 15.13, 15.12 14.18
14.16	17.3 16.7 15.13, 15.12, 15.11 14.18, 14.17
14.15	17.2 16.6 15.13, 15.12, 15.11, 15.10 14.18, 14.17, 14.16
14.14	17.1 16.5 15.13, 15.12, 15.11, 15.10, 15.9 14.18, 14.17, 14.16, 14.15
14.13	16.4 15.13, 15.12, 15.11, 15.10, 15.9, 15.8 14.18, 14.17, 14.16, 14.15, 14.14

Versión de origen actual	Destinos de actualización
14.12	16.3 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7 14.18, 14.17, 14.16, 14.15, 14.14, 14.13
14.11	16.2 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12
14.10	16.1 15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11
14.9	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10
14.8	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9
14.7*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9

Versión de origen actual	Destinos de actualización
14.6*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9
14.5*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9
14.4*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9
14.3*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9
14.2*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9
14.1*	15.13, 15.12, 15.11, 15.10, 15.9, 15.8, 15.7, 15.6, 15.5, 15.4 14.18, 14.17, 14.16, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9

Versión de origen actual	Destinos de actualización
13.21	17.5 16.9 15.13 14.17
13.20	17.4 16.8 15.12 14.18, 14.17 13.21
13.19	17.3 16.7 15.11 14.18, 14.17, 14.16 13.21, 13.20
13.18	16.6 15.10 14.18, 14.17, 14.15 13.21, 13.20, 13.19

Versión de origen actual	Destinos de actualización
13.17	16.5 15.9 14.18, 14.17, 14.15, 14.14 13.21, 13.20, 13.19, 13.18
13.16	16.4 15.8 14.18, 14.17, 14.15, 14.14, 14.13 13.21, 13.20, 13.19, 13.18, 13.17
13.15	16.3 15.8, 15.7 14.18, 14.17, 14.15, 14.14, 14.13, 14.12 13.21, 13.20, 13.19, 13.18, 13.17, 13.16
13.14	16.2 15.6 14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.15

Versión de origen actual	Destinos de actualización
13.13	16.1 15.5 14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.15, 13.14
13.12	15.4 14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.15, 13.14, 13.13
13.11	15.3 14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12
13.10*	15.2 14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.12, 13.11
13.9*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.12, 13.11

Versión de origen actual	Destinos de actualización
13.8*	14.18, 14.17, 14.1514.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.12, 13.11
13.7*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.11
13.6*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.11
13.5*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.11
13.4*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.11
13.3*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.11

Versión de origen actual	Destinos de actualización
13.2*, 13.1*	14.18, 14.17, 14.15, 14.14, 14.13, 14.12, 14.11, 14.10, 14.9 13.21, 13.20, 13.19, 13.18, 13.17, 13.16, 13.14, 13.13, 13.11
12.22	17.2 16.6 15.10 14.15 13.18
12.21	17.1 16.5 15.9 14.14 13.18, 13.17 12.22
12.20	16.4 15.8 14.13 13.18, 13.17, 13.16 12.22, 12.21

Versión de origen actual	Destinos de actualización
12.19	16.3 15.7 14.12 13.18, 13.17, 13.16, 13.15 12.22, 12.21, 12.20
12.18	16.2 15.6 14.11 13.18, 13.17, 13.16, 13.15, 13.14 12.22, 12.21, 12.20, 12.19
12.17	16.1 15.5 14.10 13.18, 13.17, 13.16, 13.15, 13.14, 13.13 12.22, 12.21, 12.20, 12.19, 12.18
12.16	15.4 14.9 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12 12.22, 12.21, 12.20, 12.19, 12.18, 12.17

Versión de origen actual	Destinos de actualización
12.15	15.3 14.8 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20**12.19**, 12.18, 12.17, 12.16
12.14*	15.2 14.7 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
12.13*	14.6 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
12.12*	14.5 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15

Versión de origen actual	Destinos de actualización
12.11*	14.4 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
12.10*	14.2 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
12.9*	14.1 13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
12.8*	13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
12.7*	13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15

Versión de origen actual	Destinos de actualización
12.6*, 12.5*, 12.4*, 12.3*, 12.2*	13.18, 13.17, 13.16, 13.15, 13.14, 13.13, 13.12, 13.11 12.22, 12.21, 12.20, 12.19, 12.18, 12.17, 12.16, 12.15
11.22	16.1 15.5 14.10 13.13 12.17 11.22-RDS.20240418

* Esta versión ya no es compatible.

Realización de una actualización de la versión principal de RDS para PostgreSQL

Se recomienda seguir el siguiente proceso al realizar una actualización de versión principal en una base de datos de Amazon RDS para PostgreSQL:

1. Tenga preparado un grupo de parámetros compatibles con la versión: si utiliza un grupo de parámetros personalizado, tiene dos opciones. Puede especificar un grupo de parámetros predeterminado para la nueva versión del motor de base de datos. O bien puede crear su propio grupo de parámetros personalizado para la nueva versión del motor de base de datos. Para obtener más información, consulte the section called “Grupos de parámetros” y the section called “Grupos de parámetros de clúster de bases de datos”.
2. Compruebe si hay clases de base de datos no admitidas: compruebe que la clase de instancia de la base de datos sea compatible con la versión de PostgreSQL a la que está actualizando. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.

3. Compruebe si hay algún uso no admitido:

   - Transacciones preparadas: confirme o revierta todas las transacciones preparadas abiertas antes de intentar una actualización.

     Puede usar la siguiente consulta para comprobar que no haya transacciones preparadas abiertas en la base de datos.

     ```
     SELECT count(*) FROM pg_catalog.pg_prepared_xacts;
     ```

   - Tipos de datos reg*: elimine todos los tipos de datos reg* utilizados antes de intentar realizar una actualización. Salvo en el caso de `regtype` y `regclass`, no se puede actualizar los tipos de datos reg*. La utilidad `pg_upgrade` no puede hacer persistir este tipo de datos, que Amazon RDS utiliza para realizar la actualización.

     Para comprobar que no se usan tipos de datos reg* incompatibles, utilice la consulta siguiente en cada base de datos.

     ```
     SELECT count(*) FROM pg_catalog.pg_class c, pg_catalog.pg_namespace n,
      pg_catalog.pg_attribute a
       WHERE c.oid = a.attrelid
           AND NOT a.attisdropped
           AND a.atttypid IN ('pg_catalog.regproc'::pg_catalog.regtype,
                              'pg_catalog.regprocedure'::pg_catalog.regtype,
                              'pg_catalog.regoper'::pg_catalog.regtype,
                              'pg_catalog.regoperator'::pg_catalog.regtype,
                              'pg_catalog.regconfig'::pg_catalog.regtype,
                              'pg_catalog.regdictionary'::pg_catalog.regtype)
           AND c.relnamespace = n.oid
           AND n.nspname NOT IN ('pg_catalog', 'information_schema');
     ```

4. Compruebe si hay bases de datos no válidas:

   - Asegúrese de que no haya bases de datos no válidas. La columna `datconnlimit` del catálogo de `pg_database` incluye un valor de `-2` para marcar como no válidas las bases de datos que se interrumpieron durante una operación `DROP DATABASE`.

     Utilice la siguiente consulta para comprobar si hay bases de datos no válidas:

     ```
     SELECT datname FROM pg_database WHERE datconnlimit = - 2;
     ```

- La consulta anterior devuelve nombres de bases de datos no válidos. Puede utilizar `DROP DATABASE` *`invalid_db_name`*`;` para eliminar las bases de datos no válidas. También puede utilizar el siguiente comando para eliminar bases de datos no válidas:

```
SELECT 'DROP DATABASE ' || quote_ident(datname) || ';' FROM pg_database WHERE
 datconnlimit = -2 \gexec
```

Para obtener más información sobre las bases de datos no válidas, consulte Comportamiento de autovacuum con bases de datos no válidas.

5. Gestione los espacios de replicación lógicos: no se puede llevar a cabo una actualización si la base de datos tiene espacios de replicación lógicos. Los espacios de replicación lógicos se utilizan habitualmente para la migración de AWS DMS y la replicación de tablas de la base de datos a lagos de datos, herramientas de inteligencia empresarial (BI) y otros destinos. Antes de actualizar, asegúrese de conocer el propósito de los espacios de replicación lógicos que se están utilizando y confirme que es correcto eliminarlos. Si los espacios de replicación lógicos se siguen utilizando, no debe eliminarlos y no puede continuar con la actualización.

   Si no se necesitan los espacios de replicación lógicos, puede eliminarlos con el siguiente SQL:

```
SELECT * FROM pg_replication_slots WHERE slot_type NOT LIKE 'physical';
SELECT pg_drop_replication_slot(slot_name);
```

   Las configuraciones de replicación lógica que utilizan la extensión `pglogical` también deben tener espacios eliminados para que la actualización de la versión principal se realice correctamente. Para obtener información sobre cómo identificar y eliminar los espacios creados con la extensión `pglogical`, consulte Administración de ranuras de replicación lógica para RDS para PostgreSQL.

6. Gestione las réplicas de lectura: una actualización de una implementación de una instancia de base de datos Single-AZ o una instancia de base de datos Multi-AZ también actualiza las réplicas de lectura dentro de la región junto con la instancia de base de datos principal. Amazon RDS no actualiza réplicas de lectura de clústeres de base de datos Multi-AZ.

   No puede actualizar las réplicas de lectura por separado. Si pudiera, podría dar lugar a situaciones en las que las bases de datos principal y de réplica tienen distintas versiones principales de PostgreSQL. Sin embargo, las actualizaciones de réplica de lectura pueden aumentar el tiempo de inactividad en la instancia de base de datos principal. Para evitar una actualización de réplica de

lectura, promueva la réplica a una instancia independiente o elimínela antes de iniciar el proceso de actualización.

El proceso de actualización vuelve a crear el grupo de parámetros de la réplica de lectura basado en el grupo de parámetros actual de la réplica de lectura. Puede aplicar un grupo de parámetros personalizado a una réplica de lectura solo una vez finalizada la actualización con la modificación de la réplica de lectura. Para obtener más información acerca de las réplicas de lectura, consulte Uso de réplicas de lectura para Amazon RDS para PostgreSQL.

7. Haga una copia de seguridad: es recomendable que realice una copia de seguridad antes de ejecutar la actualización de versión principal a fin de tener un punto de restauración conocido para la base de datos. Si el período de retención de copia de seguridad es mayor que 0, el proceso de actualización crea instantáneas de base de datos de su base de datos antes y después de la actualización. Para cambiar el periodo de retención de copia de seguridad, consulte Modificación de una instancia de base de datos de Amazon RDS y the section called “Modificación de un clúster de base de datos Multi-AZ”.

   Para realizar manualmente una copia de seguridad, consulte the section called “Creación de una instantánea de base de datos para una instancia de base de datos single-AZ” y the section called “Creación de una instantánea de un clúster de base de datos Multi-AZ”.

8. Actualice determinadas extensiones antes de la actualización de versión principal: si prevé omitir una versión principal con la actualización, tiene que actualizar determinadas extensiones antes de llevar a cabo la actualización de versión principal. Por ejemplo, la actualización de las versiones 9.5.x o 9.6.x a las versiones 11.x omite una versión principal. Las extensiones que se van a actualizar incluyen PostGIS y las extensiones relacionadas para procesar datos espaciales.

   - `address_standardizer`
   - `address_standardizer_data_us`
   - `postgis_raster`
   - `postgis_tiger_geocoder`
   - `postgis_topology`

   No puede actualizar directamente a la versión 17 de PostgreSQL si utiliza `rdkit` versión 4.6.0 o anterior y PostgreSQL versión 16 o anterior, debido a una incompatibilidad `rdkit`. A continuación se muestran las opciones de actualización:

   - Si utiliza la versión 13 o anterior de PostgreSQL, primero debe realizar una actualización de la versión principal a la versión 14.14 y a las versiones 14 posteriores, 15.9 y versiones 15

posteriores o 16.5 y versiones 16 posteriores primero y, a continuación, realizar la actualización a PostgreSQL 17.

- Si utiliza las versiones 14, 15 o 16 de PostgreSQL, primero debe realizar una actualización de la versión secundaria a la versión 14.14 y a las versiones 14 posteriores, 15.9 y versiones 15 posteriores o 16.5 y versiones 16 posteriores y, a continuación, realizar la actualización a PostgreSQL versión 17.

Ejecute el comando siguiente para cada extensión que utilice:

```
ALTER EXTENSION PostgreSQL-extension UPDATE TO 'new-version';
```

Para obtener más información, consulte Actualización de las extensiones de PostgreSQL en bases de datos de RDS para PostgreSQL. Para obtener más información acerca de la actualización de PostGIS, consulte Paso 6: Actualice la extensión de PostGIS.

9. Eliminar determinadas extensiones antes de la actualización de versión principal: una actualización que omite una versión principal a la versión 11.x no es compatible con la actualización de la extensión `pgRouting`. La actualización de las versiones 9.4.x, 9.5.x o 9.6.x a las versiones 11.x omite una versión principal. Es seguro eliminar la extensión `pgRouting` y, a continuación, volver a instalarla en una versión compatible después de la actualización. Para conocer las versiones de extensión que puede actualizar, consulte Versiones de extensiones de PostgreSQL compatibles.

   Las extensiones `tsearch2` y `chkpass` ya no se admiten para PostgreSQL versiones 11 o posteriores. Si está actualizando a la versión 11.x, elimine las extensiones `tsearch2` y `chkpass` antes de la actualización.

10. Elimine los tipos de datos desconocidos: elimine los tipos de datos `unknown` según la versión de destino.

    En la versión 10 de PostgreSQL se dejo de admitir el tipo de datos `unknown`. Si una base de datos de versión 9.6 utiliza el tipo de datos `unknown`, una actualización a una versión 10 muestra un mensaje de error como el siguiente:

```
Database instance is in a state that cannot be upgraded: PreUpgrade checks failed:
The instance could not be upgraded because the 'unknown' data type is used in user
 tables.
Please remove all usages of the 'unknown' data type and try again."
```

Para buscar el tipo de datos unknown en la base de datos de modo que pueda eliminar la columna problemática o cambiarla a un tipo de datos compatible, utilice el siguiente SQL:

```
SELECT DISTINCT data_type FROM information_schema.columns WHERE data_type ILIKE
 'unknown';
```

11. Ejecute un simulacro de actualización: es muy recomendable probar la actualización de versión principal en un duplicado de la base de datos de producción antes de intentar llevarla a cabo en la base de datos de producción. Puede monitorizar los planes de ejecución de la base de datos de prueba duplicada para detectar posibles regresiones del plan de ejecución y evaluar su rendimiento. Para crear una instancia de prueba duplicada, puede restaurar su base de datos a partir de una instantánea reciente o realizar una restauración de un momento dado de su base de datos en el último momento que se pueda restaurar.

    Para obtener más información, consulte the section called “Restauración a partir de una instantánea” o the section called “Recuperación a un momento dado”. Para los clústeres de base de datos Multi-AZ, consulte the section called “Restauración de una instantánea de clúster de base de datos Multi-AZ” o the section called “Restauración de un clúster de base de datos Multi-AZ a un momento indicado”.

    Para obtener información detallada sobre la realización de la actualización, consulte the section called “Actualización manual de la versión del motor”.

    Al actualizar una base de datos de la versión 9.6 a la versión 10, tenga en cuenta que PostgreSQL 10 habilita consultas paralelas de forma predeterminada. Para probar el impacto del paralelismo antes de la actualización, cambie el parámetro `max_parallel_workers_per_gather` de la base de datos de prueba a 2.

    > **Note**
    >
    > El valor predeterminado del parámetro `max_parallel_workers_per_gather` del grupo de parámetros de base de datos `default.postgresql10` es 2.

    Para más información, consulte Parallel Query (Consulta paralela) en la documentación de PostgreSQL. Para desactivar el paralelismo en la versión 10, establezca el parámetro `max_parallel_workers_per_gather` a 0.

Durante la actualización de la versión principal, se cambia temporalmente el nombre de las bases de datos `public` y `template1`, y del esquema `public` en todas las bases de datos. Estos objetos aparecen en los registros con su nombre original y una cadena aleatoria añadida. La cadena se añade de manera que ajustes personalizados, como `locale` y `owner`, se conserven durante la actualización de la versión principal. Cuando se complete la actualización, el nombre de los objetos se vuelve a cambiar al original.

> **Note**
>
> Durante el proceso de actualización a la versión principal, no puede realizar una restauración a un momento dado de la instancia de base datos o el clúster de base de datos Multi-AZ. Cuando Amazon RDS finaliza la actualización, realiza una copia de seguridad automática de la base de datos. Puede realizar una restauración a momentos anteriores al inicio de la actualización y posteriores a la finalización que la copia de seguridad automática de la base de datos.

12. Si una actualización devuelve un error de procedimiento de comprobación previa: durante el proceso de actualización de versión principal, Amazon RDS for PostgreSQL primero ejecuta un procedimiento de comprobación previa para identificar algún problema que pueda provocar un error de actualización. El procedimiento de comprobación previa comprueba todas las posibles condiciones incompatibles en todas las bases de datos en la instancia.

    Si la comprobación previa encuentra un error, crea un evento de registro que indica que se ha producido un error en la comprobación previa de actualización. Los detalles del proceso de comprobación previa están en un registro de actualización denominado `pg_upgrade_precheck.log` para todas las bases de datos de una base de datos. Amazon RDS agrega una marca temporal al nombre de archivo. Para obtener más información acerca de cómo visualizar los archivos de registro, consulte Supervisión de archivos de registro de Amazon RDS.

    Si una actualización de réplica de lectura falla en la comprobación previa, la replicación en la réplica de lectura fallida se rompe y la réplica de lectura se pone en estado terminado. Elimine la réplica de lectura y vuelva a crear una nueva réplica de lectura basada en la instancia de base de datos principal actualizada.

Resuelva todos los problemas identificados en el registro de comprobación previa y, a continuación, vuelva a intentar la actualización de versión principal. A continuación se muestra un ejemplo de un registro de comprobación previa.

```
-------------------------------------------------------------------------
Upgrade could not be run on Wed Apr 4 18:30:52 2018
-------------------------------------------------------------------------
The instance could not be upgraded from 9.6.11 to 10.6 for the following reasons.
Please take appropriate action on databases that have usage incompatible with the
 requested major engine version upgrade and try the upgrade again.

* There are uncommitted prepared transactions. Please commit or rollback all prepared
 transactions.* One or more role names start with 'pg_'. Rename all role names that
 start with 'pg_'.

* The following issues in the database 'my"million$"db' need to be corrected before
 upgrading:** The ["line","reg*"] data types are used in user tables. Remove all
 usage of these data types.
** The database name contains characters that are not supported by RDS for
 PostgreSQL. Rename the database.
** The database has extensions installed that are not supported on the target
 database version. Drop the following extensions from your database: ["tsearch2"].

* The following issues in the database 'mydb' need to be corrected before
 upgrading:** The database has views or materialized views that depend on
 'pg_stat_activity'. Drop the views.
```

13. Si se produce un error en una actualización de réplica de lectura al actualizar la base de datos, resuelva el problema: una réplica de lectura con error se coloca en el estado `incompatible-restore` y la replicación termina en la base de datos. Elimine la réplica de lectura y vuelva a crear una nueva réplica de lectura basada en la instancia de base de datos principal actualizada.

> **Note**
>
> Amazon RDS no actualiza réplicas de lectura de clústeres de base de datos Multi-AZ. Si actualiza la versión principal de un clúster de base de datos multi-AZ, el estado de replicación de las réplicas de lectura cambia a terminado.

Una actualización de réplica de lectura puede devolver un error por los siguientes motivos:

- No se ha podido poner al día con la instancia de base de datos principal incluso después de un tiempo de espera.
- Se encontraba en un estado de ciclo de vida de terminal o incompatible, como almacenamiento completo, restauración incompatible, etc.
- Cuando se inició la actualización de la instancia de base de datos principal, había una actualización de versión secundaria independiente ejecutándose en la réplica de lectura.
- La instancia de réplica de lectura utilizó parámetros incompatibles.
- La réplica de lectura no ha podido comunicarse con la instancia de base de datos principal para sincronizar la carpeta de datos.

14 Actualice su base de datos de producción: si el simulacro de actualización de la versión principal se ha completado correctamente, debe poder actualizar su base de datos de producción con confianza. Para obtener más información, consulte Actualización manual de la versión del motor.

15 Ejecute la operación `ANALYZE` para actualizar la tabla `pg_statistic`. Debe hacerlo para cada base de datos en todas las bases de datos de PostgreSQL. Las estadísticas del optimizador no se transfieren durante una actualización de la versión principal, por lo que debe regenerar todas las estadísticas para evitar problemas de rendimiento. Ejecute el comando sin parámetros para generar estadísticas para todas las tablas normales de la base de datos actual, de la siguiente manera:

```
ANALYZE VERBOSE;
```

La marca `VERBOSE` es opcional, pero su uso muestra el progreso. Para obtener más información, consulte ANALYZE en la documentación de PostgreSQL.

> **Note**
>
> Ejecute ANALYZE en el sistema después de la actualización para evitar problemas de rendimiento.

Una vez completada una actualización de versión principal, le recomendamos lo siguiente:

- Una actualización de PostgreSQL no actualiza ninguna extensión de PostgreSQL. Para actualizar extensiones, consulte Actualización de las extensiones de PostgreSQL en bases de datos de RDS para PostgreSQL.

- Como opción, utilice Amazon RDS para ver dos registros que produce la utilidad `pg_upgrade`. Estos son `pg_upgrade_internal.log` y `pg_upgrade_server.log`. Amazon RDS agrega una marca temporal al nombre de archivo de estos registros. Puede ver estos registros como cualquier otro registro. Para obtener más información, consulte Supervisión de archivos de registro de Amazon RDS.

  También puede cargar los registros de actualización en registros de Amazon Cloudwatch. Para obtener más información, consulte Publicación de registros de PostgreSQL en Amazon CloudWatch Logs.
- Para comprobar que todo funciona del modo previsto, pruebe su aplicación en la base de datos actualizada con una carga de trabajo similar. Cuando haya comprobado la actualización, podrá eliminar esta instancia de prueba.

Actualizaciones de versiones secundarias automáticas de RDS para PostgreSQL

Si habilita la opción Actualización automática de versiones secundarias al crear o modificar una instancia de base de datos o un clúster de base de datos Multi-AZ, puede hacer que la base de datos se actualice automáticamente.

RDS asigna una versión secundaria como la versión de actualización automática para cada versión principal de RDS for PostgreSQL. Después de que Amazon RDS pruebe y apruebe una versión secundaria, la actualización de versión secundaria se produce automáticamente durante el periodo de mantenimiento. RDS no configura automáticamente versiones secundarias publicadas recientemente como la versión de actualización automática. Antes de que RDS asigne una versión de actualización automática más reciente, deben considerarse algunos criterios, como, por ejemplo, los que se indican a continuación:

- Problemas de seguridad conocidos
- Errores en la versión de la comunidad de PostgreSQL
- Estabilidad general de la flota desde que se publicó la versión secundaria

Puede utilizar el siguiente comando de la AWS CLI para determinar la versión actual de destino de actualización secundaria automática para una versión secundaria de PostgreSQL especificada en una Región de AWS específica.

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine postgres \
--engine-version minor-version \
--region region \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output text
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine postgres ^
--engine-version minor-version ^
--region region ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output text
```

Por ejemplo, el siguiente comando de la AWS CLI determina el destino de actualización secundaria automática para la versión secundaria 16.1 de PostgreSQL en la Región de AWS de Este de EE. UU. (Ohio) (us-east-2).

Para Linux, macOS o Unix:

```
aws rds describe-db-engine-versions \
--engine postgres \
--engine-version 16.1 \
--region us-east-2 \
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" \
--output table
```

Para Windows:

```
aws rds describe-db-engine-versions ^
--engine postgres ^
--engine-version 16.1 ^
--region us-east-2 ^
--query "DBEngineVersions[*].ValidUpgradeTarget[*].
{AutoUpgrade:AutoUpgrade,EngineVersion:EngineVersion}" ^
--output table
```

Su resultado es similar al siguiente.

```
---------------------------------
|    DescribeDBEngineVersions    |
+--------------+-----------------+
|  AutoUpgrade |  EngineVersion  |
+--------------+-----------------+
|  False       |  16.2           |
|  True        |  16.3           |
|  False       |  16.4           |
|  False       |  16.5           |
|  False       |  16.6           |
|  False       |  17.1           |
|  False       |  17.2           |
+--------------+-----------------+
```

En este ejemplo, el valor `AutoUpgrade` es `True` para la versión 16.3 de PostgreSQL. Por lo tanto, el destino de actualización secundaria automática es la versión 16.3 de PostgreSQL, que está resaltado en el resultado.

Una base de datos de PostgreSQL se actualiza automáticamente durante el periodo de mantenimiento si se cumplen los siguientes criterios:

- La base de datos tiene habilitada la Actualización automática de versiones secundarias.
- La base de datos se ejecuta en una versión secundaria del motor de base de datos que es anterior a la versión secundaria de actualización automática actual.

Para obtener más información, consulte Actualización automática de la versión secundaria del motor.

> **Note**
>
> Una actualización de PostgreSQL no actualiza extensiones de PostgreSQL. Para actualizar extensiones, consulte Actualización de las extensiones de PostgreSQL en bases de datos de RDS para PostgreSQL.

Actualización de las extensiones de PostgreSQL en bases de datos de RDS para PostgreSQL

Una actualización del motor de PostgreSQL no actualiza la mayoría de las extensiones de PostgreSQL. Para actualizar una extensión después de una actualización de versiones, utilice el comando `ALTER EXTENSION UPDATE`.

> **Note**
>
> Para obtener información sobre la actualización de la extensión de PostGIS, consulte Administración de datos espaciales con la extensión PostGIS(Paso 6: Actualice la extensión de PostGIS).
> Para actualizar la extensión `pg_repack`, elimínela y, a continuación, cree la nueva versión en la base de datos actualizada. Para obtener más información, consulte pg_repack installation (Instalación de pg_repack) en la documentación de `pg_repack`.

Para actualizar una extensión, utilice el siguiente comando.

```
ALTER EXTENSION extension_name UPDATE TO 'new_version';
```

Para consultar la lista de versiones compatibles de extensiones de PostgreSQL, vea Versiones de extensiones de PostgreSQL compatibles.

Para enumerar las extensiones instaladas actualmente, utilice el catálogo pg_extension de PostgreSQL en el siguiente comando.

```
SELECT * FROM pg_extension;
```

Para ver una lista de las versiones específicas de la extensión que están disponibles para su instalación, utilice la visualización pg_available_extension_versions de PostgreSQL en el siguiente comando.

```
SELECT * FROM pg_available_extension_versions;
```

Actualización de una versión del motor de instantáneas de base de datos de PostgreSQL

Con Amazon RDS, puede crear una instantánea de base de datos de volumen de almacenamiento de su instancia de base de datos de PostgreSQL. Cuando se crea una instantánea de base de datos, se basa en la versión del motor empleada por la instancia de Amazon RDS. Puede actualizar la versión del motor para las instantáneas de base de datos.

Después de restaurar una instantánea de base de datos actualizada a una nueva versión del motor, asegúrese que la actualización se ha realizado correctamente. Para obtener más información acerca de una actualización de versión principal, consulte Actualizaciones del motor de base de datos de RDS para PostgreSQL. Para aprender a restaurar una instantánea de base de datos, consulte Restauración a una instancia de base de datos.

Puede actualizar las instantáneas de base de datos manuales que están cifradas o no.

Para ver las versiones de motor disponibles para la instantánea de base de datos de RDS para PostgreSQL, utilice el siguiente ejemplo de AWS CLI.

```
aws rds describe-db-engine-versions --engine postgres  --engine-version example-
engine-version --query "DBEngineVersions[*].ValidUpgradeTarget[*].
{EngineVersion:EngineVersion}" --output text --include-all
```

Para obtener más información sobre las versiones de motor disponibles para las instantáneas de base de datos de RDS para PostgreSQL, consulte Elección de una versión principal para una actualización de RDS para PostgreSQL.

> **Note**
>
> No puede actualizar las instantáneas de base de datos automatizadas que se creen durante el proceso de backup automatizado.

Consola

Para actualizar una instantánea de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija la instantánea que desea actualizar.
4. En Actions (Acciones), seleccione Upgrade Snapshot (Actualizar instantánea). Aparece la página Upgrade snapshot.
5. Elija la New engine version (Nueva versión del motor) a la que actualizarse.
6. Elija Save changes (Guardar cambios) para actualizar la instantánea.

   Durante el proceso de actualización, todas las acciones están deshabilitadas para esta instantánea de base de datos. Además, el estado de la instantánea de base de datos cambia de available a upgrading y después cambia a active al completarse. Si la instantánea de base de datos no se puede actualizar porque se ha dañado, el estado cambia a unavailable. No puede recuperar el snapshot desde este estado.

   > **Note**
   >
   > Si la actualización de la base de datos falla, la instantánea se revierte al estado original con la versión original.

AWS CLI

Para actualizar una instantánea de base de datos a una nueva versión del motor de base de datos, use el comando modify-db-snapshot de la AWS CLI.

Parámetros

- `--db-snapshot-identifier`: identificador de la instantánea de base de datos que se va a actualizar. El identificador debe ser un Nombre de recurso de Amazon (ARN). Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.
- `--engine-version`: versión del motor a la que se va a actualizar la instantánea de base de datos.

Example

Para Linux, macOS o:Unix

```
aws rds modify-db-snapshot \
    --db-snapshot-identifier my_db_snapshot \
```

```
    --engine-version new_version
```

En:Windows

```
aws rds modify-db-snapshot ^
    --db-snapshot-identifier my_db_snapshot ^
    --engine-version new_version
```

API de RDS

Para actualizar una instantánea de base de datos a una nueva versión del motor de base de datos, llame a la operación ModifyDBSnapshot de la API de Amazon RDS.

- `DBSnapshotIdentifier`: identificador de la instantánea de base de datos que se va a actualizar. El identificador debe ser un Nombre de recurso de Amazon (ARN). Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.
- `EngineVersion`: versión del motor a la que se va a actualizar la instantánea de base de datos.

Uso de réplicas de lectura para Amazon RDS para PostgreSQL

Puede escalar las lecturas de sus instancias de base de datos de Amazon RDS para PostgreSQL añadiendo réplicas de lectura a las instancias. Al igual que con otros motores de bases de datos de Amazon RDS, RDS para PostgreSQL utiliza los mecanismos de replicación nativos de PostgreSQL para mantener las réplicas de lectura actualizadas con los cambios en la base de datos de origen. Para obtener información general acerca de las réplicas y Amazon RDS, consulte Trabajo con réplicas de lectura de instancias de base de datos.

A continuación, encontrará información específica sobre cómo utilizar réplicas de lectura con RDS para PostgreSQL.

Decodificación lógica en una réplica de lectura

RDS para PostgreSQL admite la replicación lógica desde instancias en espera con PostgreSQL 16.1. Esto le permite crear una decodificación lógica desde una instancia en espera de solo lectura, lo que reduce la carga de la instancia de base de datos principal. Puede lograr una mayor disponibilidad para las aplicaciones que necesitan sincronizar datos en varios sistemas. Esta característica aumenta el rendimiento del almacenamiento de datos y del análisis de datos.

Además, las ranuras de replicación de una instancia en espera determinada mantienen la promoción de esa instancia en espera a una principal. Esto significa que, en caso de que se produzca una conmutación por error de una instancia de base de datos principal o de que se promueva una instancia en espera para ser la nueva instancia principal, las ranuras de replicación se mantendrán y los suscriptores en espera anteriores no se verán afectados.

Creación de una decodificación lógica en una réplica de lectura

1. Active la replicación lógica: para crear una decodificación lógica en una instancia en espera, debe activar la replicación lógica en la instancia de base de datos de origen y en su réplica física. Para obtener más información, consulte Configuración de réplicas de lectura con PostgreSQL.

    - Para activar la replicación lógica de una instancia de base de datos de RDS para PostgreSQL recién creada: cree un nuevo grupo de parámetros personalizados de base de datos y establezca el parámetro estático `rds.logical_replication` en 1. A continuación, asocie este grupo de parámetros de base de datos a la instancia de base de datos de origen y a su

réplica de lectura física. Para obtener más información, consulte Asociación de un grupo de parámetros de base de datos con una instancia de base de datos en Amazon RDS.

- Para activar la replicación lógica de una instancia de base de datos de RDS para PostgreSQL existente: modifique el grupo de parámetros personalizados de base de datos de la instancia de base de datos de origen y su réplica de lectura física para establecer el parámetro estático `rds.logical_replication` en 1. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

> **Note**
>
> Debe reiniciar las instancias de base de datos para aplicar estos cambios en los parámetros.

Puede utilizar la siguiente consulta para comprobar los valores de `wal_level` y `rds.logical_replication` en la instancia de base de datos de origen y su réplica de lectura física.

```
Postgres=>SELECT name,setting FROM pg_settings WHERE name IN
 ('wal_level','rds.logical_replication');

 name                    | setting
-------------------------+---------
 rds.logical_replication | on
 wal_level               | logical
(2 rows)
```

2. Cree una tabla en la base de datos de origen: conéctese a la base de datos de su instancia de base de datos de origen. Para obtener más información, consulte Conexión a una instancia de base de datos que ejecuta el motor de base de datos de PostgreSQL.

   Utilice las siguientes consultas para crear una tabla en la base de datos de origen e insertar valores:

```
Postgres=>CREATE TABLE LR_test (a int PRIMARY KEY);
CREATE TABLE
```

```
Postgres=>INSERT INTO LR_test VALUES (generate_series(1,10000));
INSERT 0 10000
```

3. Cree una publicación para la tabla de origen: utilice la siguiente consulta para crear una publicación para la tabla en la instancia de base de datos de origen.

```
Postgres=>CREATE PUBLICATION testpub FOR TABLE LR_test;
CREATE PUBLICATION
```

Utilice una consulta SELECT para comprobar los detalles de la publicación que se creó tanto en la instancia de base de datos de origen como en la instancia de réplica de lectura física.

```
Postgres=>SELECT * from pg_publication;

oid    | pubname | pubowner | puballtables | pubinsert | pubupdate | pubdelete |
 pubtruncate | pubviaroot
-------+---------+----------+--------------+-----------+-----------+-----------
+-------------+------------
 16429 | testpub |    16413 | f            | t         | t         | t         | t
          | f
(1 row)
```

4. Cree una suscripción a partir de una instancia de réplica lógica: cree otra instancia de base de datos de RDS para PostgreSQL como instancia de réplica lógica. Asegúrese de que la VPC esté configurada correctamente para garantizar que esta instancia de réplica lógica pueda acceder a la instancia de réplica de lectura física. Para obtener más información, consulte VPC de Amazon y Amazon RDS. Si la instancia de base de datos de origen está inactiva, es posible que se produzcan problemas de conectividad y que la instancia principal no envíe los datos a la instancia en espera.

```
Postgres=>CREATE SUBSCRIPTION testsub CONNECTION 'host=Physical replica host name
 port=port
                dbname=source_db_name user=user password=password'
 PUBLICATION testpub;
NOTICE:  created replication slot "testsub" on publisher
CREATE SUBSCRIPTION
```

```
Postgres=>CREATE TABLE LR_test (a int PRIMARY KEY);
CREATE TABLE
```

Utilice una consulta SELECT para comprobar los detalles de la suscripción en la instancia de la réplica lógica.

```
Postgres=>SELECT oid,subname,subenabled,subslotname,subpublications FROM
 pg_subscription;

oid    | subname | subenabled | subslotname | subpublications
-------+---------+------------+-------------+-----------------
 16429 | testsub | t          | testsub     | {testpub}
(1 row)
postgres=> select count(*) from LR_test;
 count
-------
 10000
(1 row)
```

5. Inspeccione el estado de la ranura de replicación lógica: solo puede ver la ranura de replicación física en la instancia de base de datos de origen.

```
Postgres=>select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;

slot_name                                  | slot_type | confirmed_flush_lsn
-------------------------------------------+-----------+---------------------
 rds_us_west_2_db_dhqfsmo5wbbjqrn3m6b6ivdhu4 | physical  |
(1 row)
```

Sin embargo, en la instancia de la réplica de lectura, puede ver la ranura de replicación lógica y el valor de `confirmed_flush_lsn` cambia a medida que la aplicación consume activamente los cambios lógicos.

```
Postgres=>select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;

slot_name | slot_type | confirmed_flush_lsn
----------+-----------+---------------------
 testsub   | logical   | 0/500002F0
(1 row)
```

```
Postgres=>select slot_name, slot_type, confirmed_flush_lsn from
 pg_replication_slots;

slot_name | slot_type | confirmed_flush_lsn
-----------+-----------+---------------------
 testsub   | logical   | 0/5413F5C0
(1 row)
```

Limitaciones de las réplicas de lectura con PostgreSQL

A continuación se indican las limitaciones de las réplicas de lectura de PostgreSQL:

- Las réplicas de lectura de PostgreSQL son de solo lectura. Aunque una réplica de lectura no es una instancia de base de datos grabable, puede promocionarla para que se convierta en un RDS independiente para una instancia de base de datos de PostgreSQL. Sin embargo, el proceso no es reversible.
- No puede crear una réplica de lectura a partir de otra réplica de lectura si su instancia de base de datos de RDS para PostgreSQL ejecuta una versión de PostgreSQL anterior a la 14.1. RDS para PostgreSQL solo admite réplicas de lectura en cascada en RDS para PostgreSQL versión 14.1 y versiones superiores. Para obtener más información, consulte Uso de réplicas de lectura en cascada con RDS para PostgreSQL.
- Si promociona una réplica de lectura de PostgreSQL, se convierte en una instancia de base de datos grabable. Deja de recibir archivos de write-ahead log (WAL, registro de escritura anticipada) de una instancia de base de datos de origen y ya no es una instancia de solo lectura. Puede crear nuevas réplicas de lectura a partir de la instancia de base de datos promocionada como lo hace para cualquier instancia de base de datos de RDS para PostgreSQL. Para obtener más información, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.
- Si promociona una réplica de lectura de PostgreSQL desde una cadena de replicación (una serie de réplicas de lectura en cascada), cualquier réplica de lectura descendente existente continúa recibiendo archivos WAL de la instancia promocionada, automáticamente. Para obtener más información, consulte Uso de réplicas de lectura en cascada con RDS para PostgreSQL.
- Si no se están ejecutando transacciones de usuario en la instancia de base de datos de origen, la réplica de lectura de PostgreSQL asociada registra un retardo de replicación de hasta cinco minutos. El retraso de la réplica se calcula como `currentTime -`

`lastCommitedTransactionTimestamp`, lo que significa que cuando no se procesan transacciones, el valor del retraso de la réplica aumenta durante un período de tiempo hasta que cambia el segmento del registro de escritura anticipada (WAL). De forma predeterminada, RDS para PostgreSQL cambia el segmento WAL cada 5 minutos, lo que da como resultado un registro de transacciones y una disminución del retardo comunicado.

- No puede activar las copias de seguridad automatizadas para las réplicas de lectura de RDS para PostgreSQL de versiones anteriores a 14.1. Las copias de seguridad automatizadas para réplicas de lectura se admiten únicamente para RDS para PostgreSQL 14.1 y versiones posteriores. Para RDS para PostgreSQL 13 y versiones anteriores, cree una instantánea a partir de una réplica de lectura si desea realizar una copia de seguridad de ella.
- La Point-in-time recovery (PITR, recuperación en un momento dado) no se admite para las réplicas de lectura. Puede utilizar PITR solo con una instancia principal (escritor), no con una réplica de lectura. Para obtener más información, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.
- Las réplicas de lectura para las versiones 12 y menores de PostgreSQL se reinician automáticamente durante el periodo de mantenimiento de 60 a 90 días para aplicar la rotación de contraseñas. Si la réplica pierde conexión al origen antes del reinicio programado, seguirá reiniciándose para que se reanude la replicación. Para las versiones 13 y superiores de PostgreSQL, las réplicas de lectura pueden sufrir breves desconexiones y reconexiones de replicación durante el proceso de rotación de contraseñas.

Configuración de réplicas de lectura con PostgreSQL

RDS para PostgreSQL utiliza la replicación de streaming nativa de PostgreSQL para crear una copia de solo lectura de una instancia de base de datos de origen. La instancia de base de datos de réplica de lectura es una réplica física de la instancia de la base de datos de origen creada de forma asíncrona. Se crea mediante una conexión especial que transmite los datos de los registros de escritura previa (WAL) entre la instancia de base de datos de origen y la réplica de lectura. Para obtener más información, consulte Replicación de streaming en la documentación de PostgreSQL.

PostgreSQL transmite de forma asíncrona los cambios de la base de datos a esta conexión segura a medida que se realizan en la instancia de base de datos de origen. Puede cifrar las comunicaciones de las aplicaciones cliente a la instancia de base de datos de origen o cualquier réplica de lectura configurando el parámetro `ssl` en 1. Para obtener más información, consulte Uso de SSL con una instancia de base de datos PostgreSQL.

PostgreSQL usa un rol de replicación para realizar la replicación en streaming. El rol tiene privilegios, pero no se puede usar para modificar ningún dato. PostgreSQL usa un único proceso para gestionar la replicación.

Puede crear una réplica de lectura de PostgreSQL sin que afecte a las operaciones o usuarios de la instancia de base de datos de origen. Amazon RDS establece los parámetros y los permisos necesarios en la instancia de base de datos de origen y la réplica de lectura sin que afecte al servicio. Se toma una instantánea de la instancia de base de datos de origen, y esta instantánea se utiliza para crear la réplica de lectura. Si elimina la réplica de lectura en algún momento futuro, no se produce ninguna interrupción.

Puede crear hasta 15 réplicas de lectura a partir de una instancia de base de datos de origen dentro de la misma región. A partir de RDS para PostgreSQL 14.1, también puede crear hasta tres niveles de réplica de lectura en una cadena (cascada) a partir de una instancia de base de datos de origen. Para obtener más información, consulte Uso de réplicas de lectura en cascada con RDS para PostgreSQL. En todos los casos, la instancia de base de datos de origen debe tener configuradas copias de seguridad automatizadas. Para ello, debe establecer el periodo de retención de copia de seguridad en su instancia de base de datos en cualquier valor distinto de 0. Para obtener más información, consulte Creación de una réplica de lectura.

Puede crear réplicas de lectura para su instancia de base de datos de RDS para PostgreSQL en la misma Región de AWS que la instancia de base de datos de origen. Esto se denomina replicación dentro de la región. También puede crear réplicas de lectura en una Regiones de AWS diferente de la instancia de base de datos de origen. Esto se denomina replicación entre regiones. Para obtener información sobre la configuración de réplicas de lectura entre regiones, consulte Creación de una réplica de lectura en una Región de AWS distinta. Los diversos mecanismos que admiten el proceso de replicación para dentro de la región y entre regiones difieren ligeramente en función de la versión de RDS para PostgreSQL, como se explica en Cómo funciona la replicación de streaming en diferentes versiones de RDS para PostgreSQL.

Para que la replicación sea eficaz, cada réplica de lectura debe tener la misma cantidad de recursos de computación y de almacenamiento que la instancia de base de datos de origen. Si modifica la escala de la instancia de base de datos de origen, asegúrese de ajustar también la escala de las réplicas de lectura.

Amazon RDS anula los parámetros incompatibles de una réplica de lectura si impiden que la réplica de lectura se inicie. Por ejemplo, supongamos que el valor del parámetro `max_connections` es mayor en la instancia de base de datos de origen que en la réplica de lectura. En ese caso, Amazon

RDS actualiza el parámetro en la réplica de lectura para que tenga el mismo valor que el de la instancia de base de datos de origen.

Las réplicas de lectura de RDS para PostgreSQL tienen acceso a bases de datos externas que están disponibles a través de foreign data wrappers (FDW, envoltorios de datos externos) en la instancia de base de datos de origen. Por ejemplo, suponga que su instancia de base de datos de RDS para PostgreSQL utiliza el envoltorio `mysql_fdw` para acceder a los datos de RDS para MySQL. Si es así, las réplicas de lectura también pueden acceder a esos datos. Otros FDW admitidos incluyen `oracle_fdw`, `postgres_fdw` y `tds_fdw`. Para obtener más información, consulte Uso de los contenedores de datos externos compatibles para Amazon RDS for PostgreSQL.

Uso de RDS para réplicas de lectura de PostgreSQL con configuraciones Multi-AZ

Puede crear una réplica de lectura a partir de una instancia de base de datos Single-AZ o Multi-AZ. Puede utilizar implementaciones Multi-AZ para mejorar la durabilidad y la disponibilidad de los datos críticos, con una réplica en espera. Una réplica en espera es una réplica de lectura dedicada que puede asumir la carga de trabajo si la base de datos de origen falla. No puede usar su réplica en espera para servir tráfico de lectura. Sin embargo, puede crear réplicas de lectura a partir de una instancia de base de datos Multi-AZ con un tráfico elevado para descargar las consultas de solo lectura. Para obtener más información sobre las implementaciones Multi-AZ, consulte Habilitación de implementaciones de instancias de bases de datos multi-AZ para Amazon RDS.

Si la instancia de base de datos de origen de una implementación Multi-AZ conmuta por error, las réplicas de lectura asociadas cambian para utilizar la instancia en espera (ahora principal) como origen de replicación. Es posible que las réplicas de lectura deban reiniciarse, según la versión de RDS para PostgreSQL, de la siguiente manera:

- PostgreSQL 13 y versiones superiores: no es obligatorio reiniciar. Las réplicas de lectura se sincronizan automáticamente con el nuevo elemento principal. Sin embargo, en algunos casos, la aplicación cliente podría almacenar en caché los detalles del Domain Name Service (DNS, servicio de nombres de dominio) de las réplicas de lectura. Si es así, configure el valor de time-to-live (TTL, tiempo de vida) en menos de 30 segundos. Esto impide que la réplica de lectura se mantenga en una dirección IP obsoleta (y, por lo tanto, impide que se sincronice con el nuevo elemento principal). Para obtener más información sobre esta y otras prácticas recomendadas, consulte Directrices operativas básicas de Amazon RDS.
- PostgreSQL 12 y todas las versiones anteriores: las réplicas de lectura se reinician automáticamente después de una conmutación por error en la réplica en espera porque la espera

(ahora principal) tiene una dirección IP y un nombre de instancia diferente. El reinicio sincroniza la réplica de lectura con el nuevo elemento principal.

Para obtener más información sobre la conmutación por error, consulte Conmutación por error de una instancia de base de datos multi-AZ para Amazon RDS. Para obtener más información sobre cómo funcionan las réplicas de lectura en una implementación Multi-AZ, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Para proporcionar soporte de conmutación por error para una réplica de lectura, puede crear la réplica de lectura como una instancia de base de datos Multi-AZ para que Amazon RDS cree una espera de su réplica en otra zona de disponibilidad (AZ). La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ.

Uso de réplicas de lectura en cascada con RDS para PostgreSQL

A partir de la versión 14.1, RDS para PostgreSQL admite réplicas de lectura en cascada. Con réplicas de lectura en cascada, puede escalar las lecturas sin agregar sobrecarga a su instancia de base de datos de RDS para PostgreSQL de origen. La instancia de base de datos de origen no envía las actualizaciones del registro WAL a cada réplica de lectura. En cambio, cada réplica de lectura de una serie en cascada envía actualizaciones de registro WAL a la siguiente réplica de lectura de la serie. Esto reduce la carga de la instancia de base de datos de origen.

Con réplicas de lectura en cascada, la instancia de base de datos de RDS para PostgreSQL envía datos WAL a la primera réplica de lectura de la cadena. Esa réplica de lectura envía datos WAL a la segunda réplica de la cadena, etc. El resultado final es que todas las réplicas de lectura de la cadena tienen los cambios de la instancia de base de datos de RDS para PostgreSQL, pero sin la sobrecarga únicamente en la instancia de base de datos de origen.

Puede crear una serie de hasta tres réplicas de lectura en cadena a partir de una instancia de base de datos RDS para PostgreSQL de origen. Por ejemplo, suponga que tiene una instancia de base de datos de RDS para PostgreSQL 14.1, `rpg-db-main`. Puede hacer lo siguiente:

- A partir de `rpg-db-main`, cree la primera réplica de lectura de la cadena, `read-replica-1`.
- A continuación, a partir de `read-replica-1`, cree la siguiente réplica de lectura de la cadena, `read-replica-2`.
- Por último, a partir de `read-replica-2`, cree la tercera réplica de lectura de la cadena, `read-replica-3`.

No se puede crear otra réplica de lectura más allá de esta tercera réplica de lectura en cascada de la serie para `rpg-db-main`. Una serie completa de instancias desde una instancia de base de datos de origen de RDS para PostgreSQL hasta el final de una serie de réplicas de lectura en cascada puede constar de cuatro instancias de base de datos como máximo.

Para que las réplicas de lectura en cascada funcionen, active las copias de seguridad automáticas en su RDS para PostgreSQL. Cree primero la réplica de lectura y, a continuación, active las copias de seguridad automáticas en la instancia de base de datos de RDS para PostgreSQL. El proceso es el mismo que para otros motores de base de datos de Amazon RDS. Para obtener más información, consulte Creación de una réplica de lectura.

Al igual que con cualquier réplica de lectura, puede promocionar una réplica de lectura que forma parte de una cascada. La promoción de una réplica de lectura desde dentro de una cadena de réplicas de lectura elimina esa réplica de la cadena. Por ejemplo, suponga que desea quitar parte de la carga de trabajo de su Instancia de base de datos de `rpg-db-main` a una nueva instancia para que la utilice únicamente el departamento de contabilidad. Tomando la cadena de tres réplicas de lectura del ejemplo, decide promocionar `read-replica-2`. La cadena se ve afectada de la siguiente manera:

- Promover `read-replica-2` la elimina de la cadena de replicación.
  - Ahora es una instancia de base de datos de lectura o escritura completa.
  - Continúa replicando en `read-replica-3`, tal como hacía antes de la promoción.
- Su `rpg-db-main` sigue replicándose en `read-replica-1`.

Para obtener más información acerca de la promoción de réplicas de lectura, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

> **Note**
>
> - RDS para PostgreSQL no admite actualizaciones de versiones principales para réplicas en cascada. Antes de realizar una actualización de versión principal, debe eliminar las réplicas en cascada. Puede volver a crearlas después de completar la actualización en la instancia de base de datos de origen y en las réplicas de primer nivel.
> - Para las réplicas de lectura en cascada, RDS para PostgreSQL admite 15 réplicas de lectura para cada instancia de base de datos de origen en el primer nivel de replicación y 5

réplicas de lectura para cada instancia de base de datos de origen en el segundo y tercer nivel de replicación.

Creación de réplicas de lectura en cascada entre regiones con RDS para PostgreSQL

RDS para PostgreSQL admite las réplicas de lectura en cascada entre regiones. Puede crear una réplica entre regiones a partir de la instancia de base de datos de origen y, a continuación, crear réplicas de la misma región a partir de ella. Puede crear una réplica de la misma región a partir de la instancia de base de datos de origen y, a continuación, crear réplicas entre regiones a partir de ella.

Creación de una réplica entre regiones y, a continuación, de réplicas de la misma región

Puede usar una instancia de base de datos de RDS para PostgreSQL con la versión 14.1 o superior, `rpg-db-main`, para hacer lo siguiente:

1. Comience con `rpg-db-main` (US-EAST-1) y cree la primera réplica de lectura entre regiones de la cadena, `read-replica-1` (US-WEST-2).
2. Con la primera `read-replica-1` (US-WEST-2) entre regiones, cree la segunda réplica de lectura en la cadena, `read-replica-2` (US-WEST-2).
3. Con `read-replica-2`, cree la tercera réplica de lectura de la cadena, `read-replica-3` (US-WEST-2).

Creación de una réplica de la misma región y, a continuación, de réplicas entre regiones

Puede usar una instancia de base de datos de RDS para PostgreSQL con la versión 14.1 o superior, `rpg-db-main`, para hacer lo siguiente:

1. Comience con `rpg-db-main` (US-EAST-1) y cree la primera réplica de lectura en la cadena, `read-replica-1` (US-EAST-1).
2. Con `read-replica-1` (US-EAST-1), cree la primera réplica de lectura entre regiones de la cadena, `read-replica-2` (US-WEST-2).
3. Con `read-replica-2` (US-WEST-2), cree la tercera réplica en la cadena, `read-replica-3` (US-WEST-2).

Limitaciones en la creación de réplicas de lectura entre regiones

- Una cadena en cascada de réplicas de bases de datos entre regiones puede abarcar un máximo de dos regiones, con un máximo de cuatro niveles. Los cuatro niveles incluyen el origen de la base de datos y tres réplicas de lectura.

Ventajas de usar réplicas de lectura en cascada

- Escalabilidad de lectura mejorada: al distribuir las consultas de lectura entre varias réplicas, la replicación en cascada contribuye a equilibrar la carga. Esto mejora el rendimiento, sobre todo en aplicaciones de lectura intensiva, al reducir la tensión en la base de datos del escritor.
- Distribución geográfica: las réplicas en cascada se pueden colocar en diferentes ubicaciones geográficas. Esto reduce la latencia de los usuarios que se encuentran lejos de la base de datos principal y proporciona una réplica de lectura local, lo que mejora el rendimiento y la experiencia del usuario.
- Alta disponibilidad y recuperación de desastres: en caso de que se produzca un fallo en el servidor principal, las réplicas se pueden convertir en principales, lo que garantiza la continuidad. La replicación en cascada mejora aún más esta situación, ya que proporciona varios niveles de opciones de conmutación por error, lo que mejora la resiliencia general del sistema.
- Flexibilidad y crecimiento modular: a medida que el sistema crece, se pueden agregar nuevas réplicas en diferentes niveles sin necesidad de una reconfiguración importante de la base de datos principal. Este enfoque modular permite un crecimiento escalable y administrable de la configuración de replicación.

Práctica recomendada para usar réplicas de lectura entre regiones

- Antes de promocionar una réplica, cree réplicas adicionales. Esto ahorrará tiempo y proporcionará un manejo eficiente de la carga de trabajo.

Cómo funciona la replicación de streaming en diferentes versiones de RDS para PostgreSQL

Como se discute en Configuración de réplicas de lectura con PostgreSQL, RDS para PostgreSQL utiliza el protocolo de replicación de streaming nativo de PostgreSQL para enviar datos WAL desde la instancia de base de datos de origen. Envía datos WAL de origen a réplicas de lectura tanto para

réplicas de lectura dentro de la región como entre regiones. Con la versión 9.4, PostgreSQL introdujo slots de replicación física como mecanismo de soporte para el proceso de replicación.

Una slot de replicación física impide que una instancia de base de datos de origen elimine los datos WAL antes de que todas las réplicas de lectura los consuman. Cada réplica de lectura tiene su propia slot física en la instancia de base de datos de origen. La slot realiza un seguimiento del WAL más antiguo (por número de secuencia lógica, LSN) que podría necesitar la réplica. Después de que todas las slots y conexiones de base de datos hayan progresado más allá de un WAL (LSN) determinado, ese LSN se convierte en candidato para su eliminación en el siguiente punto de control.

Amazon RDS utiliza Amazon S3 para archivar datos WAL. En las réplicas de lectura dentro de la región, puede utilizar estos datos archivados para recuperar la réplica de lectura cuando sea necesario. Un ejemplo de cuándo podría hacerse es si la conexión entre la base de datos de origen y la réplica de lectura se interrumpe por cualquier motivo.

En la tabla siguiente, encontrará un resumen de las diferencias entre las versiones de PostgreSQL y los mecanismos de soporte para dentro de la región y entre regiones que utiliza RDS para PostgreSQL.

Versión	En región	Entre regiones
PostgreSQL 14.1 y versiones posteriores	• Slots de replicación • Archivo de Amazon S3	• Slots de replicación
PostgreSQL 13 y versiones anteriores	• Archivo de Amazon S3	• Slots de replicación

Para obtener más información, consulte Supervisión y ajuste del proceso de replicación.

Descripción de los parámetros que controlan la replicación de PostgreSQL

Los siguientes parámetros afectan al proceso de replicación y determinan qué tal se actualizan las réplicas de lectura con la instancia de base de datos de origen:

max_wal_senders

El parámetro `max_wal_senders` especifica el número máximo de conexiones que la instancia de base de datos de origen puede admitir al mismo tiempo a través del protocolo de replicación de streaming.

El valor predeterminado varía para las versiones de RDS para PostgreSQL:

- Para las versiones 13, 14 y 15, el valor predeterminado es 20.
- Para las versiones 16 y posteriores, el valor predeterminado es 35.

Este parámetro debe establecerse en ligeramente superior al número real de réplicas de lectura. Si este parámetro se establece demasiado bajo para el número de réplicas de lectura, la replicación se detiene.

Para obtener más información, consulte see max_wal_senders enla documentación de PostgreSQL.

> **Note**
>
> `max_wal_senders` es un parámetro estático que requiere un reinicio de la instancia de base de datos para que los cambios surtan efecto.

wal_keep_segments

El parámetro `wal_keep_segments` especifica el número de archivos de registro de escritura anticipada (WAL) que mantiene la instancia de base de datos de origen en el directorio `pg_wal`. La configuración predeterminada es 32.

Si `wal_keep_segments` no tiene un valor lo suficientemente grande para su implementación, una réplica de lectura puede quedarse tan rezagada que se detenga la replicación en streaming. Si es así, Amazon RDS genera un error de replicación e inicia la recuperación en la réplica de lectura. Para ello, reproduce los datos WAL archivados de la instancia de base de datos de origen desde Amazon S3. Este proceso de recuperación continúa hasta que la réplica de lectura reduce el retraso lo suficiente para seguir con la replicación en streaming. Puede ver este proceso en acción tal como lo captó el registro de PostgreSQL en Ejemplo: Cómo se recupera una réplica de lectura de las interrupciones de la replicación.

> **Note**
>
> En la versión 13 de PostgreSQL, el parámetro `wal_keep_segments` se denomina `wal_keep_size`. Tiene el mismo propósito que `wal_keep_segments`, pero su valor predeterminado está en megabytes (MB) (2048 MB) en lugar del número de archivos.

Para obtener más información, consulte wal_keep_segments y wal_keep_size en la documentación de PostgreSQL.

max_slot_wal_keep_size

El parámetro `max_slot_wal_keep_size` controla la cantidad de datos WAL que conserva la instancia de base de datos de RDS para PostgreSQL en el directorio `pg_wal` para servir slots. Este parámetro se utiliza para configuraciones que utilizan slots de replicación. El valor predeterminado para este parámetro es `-1`, lo que significa que no hay límite en cuanto a la cantidad de datos WAL que se conservan en la instancia de base de datos de origen. Para obtener información sobre cómo supervisar las slots de replicación, consulte Supervisión de las slots de replicación de su instancia de base de datos de RDS para PostgreSQL.

Para obtener más información sobre este parámetro, consulte max_slot_wal_keep_size en la documentación de PostgreSQL.

Siempre que se interrumpe el flujo que proporciona los datos de WAL a una réplica de lectura, PostgreSQL cambia al modo de recuperación. Restaura la réplica de lectura mediante datos de WAL archivados de Amazon S3 o mediante el uso de datos de WAL asociados a la ranura de replicación. Cuando finaliza este proceso, PostgreSQL restablece la replicación en streaming.

Ejemplo: Cómo se recupera una réplica de lectura de las interrupciones de la replicación

En el siguiente ejemplo, encontrará los detalles del registro que muestran el proceso de recuperación de una réplica de lectura. El ejemplo procede de una instancia de base de datos de RDS para PostgreSQL que ejecuta la versión 12.9 de PostgreSQL en la misma Región de AWS que la base de datos de origen, por lo que no se utilizan slots de replicación. El proceso de recuperación es el mismo para otras instancias de base de datos de PostgreSQL que ejecutan PostgreSQL anterior a la versión 14.1 con réplicas de lectura dentro de la región.

Cuando la réplica de lectura perdió el contacto con la instancia de base de datos de origen, Amazon RDS registra el problema en el registro como el mensaje `FATAL: could not receive data from WAL stream`, junto con `ERROR: requested WAL segment ... has already been removed`. Como se muestra en la línea en negrita, Amazon RDS recupera la réplica reproduciendo un archivo WAL archivado.

```
2014-11-07 19:01:10 UTC::@:[23180]:DEBUG:  switched WAL source from archive to stream
 after failure
```

```
2014-11-07 19:01:10 UTC::@:[11575]:LOG: started streaming WAL from primary at 1A/
D3000000 on timeline 1
2014-11-07 19:01:10 UTC::@:[11575]:FATAL: could not receive data from WAL stream:
ERROR:  requested WAL segment 000000010000001A000000D3 has already been removed
2014-11-07 19:01:10 UTC::@:[23180]:DEBUG: could not restore file "00000002.history"
 from archive: return code 0
2014-11-07 19:01:15 UTC::@:[23180]:DEBUG: switched WAL source from stream to archive
 after failure recovering 000000010000001A000000D3
2014-11-07 19:01:16 UTC::@:[23180]:LOG:  restored log file "000000010000001A000000D3"
 from archive
```

Cuando Amazon RDS reproduce suficientes datos de WAL archivados en la réplica para ponerse al corriente, el streaming a la réplica de lectura comienza de nuevo. Cuando se reanuda el streaming, Amazon RDS escribe una entrada en el archivo de registro, similar a la siguiente.

```
2014-11-07 19:41:36 UTC::@:[24714]:LOG:started streaming WAL from primary at 1B/
B6000000 on timeline 1
```

Configuración de los parámetros que controlan la memoria compartida

Los parámetros que establezca determinan el tamaño de la memoria compartida para rastrear los identificadores de las transacciones, los bloqueos y las transacciones preparadas. La estructura de la memoria compartida de una instancia en espera debe ser igual o mayor que la de una instancia principal. Esto garantiza que la primera no se quede sin memoria compartida durante la recuperación. Si los valores de los parámetros de la réplica son inferiores a los valores de los parámetros de la principal, Amazon RDS ajustará automáticamente los parámetros de la réplica y reiniciará el motor.

Los parámetros afectados son:

- max_connections
- max_worker_processes
- max_wal_senders
- max_prepared_transactions
- max_locks_per_transaction

Para evitar que RDS reinicie las réplicas por falta de memoria, se recomienda aplicar los cambios de los parámetros como un reinicio progresivo en cada réplica. Al configurar los parámetros, debe aplicar las siguientes reglas:

- Aumentar los valores de los parámetros:
  - En primer lugar, siempre debe aumentar los valores de los parámetros de todas las réplicas de lectura y realizar un reinicio progresivo de todas las réplicas. A continuación, aplique los cambios de los parámetros a la instancia principal y reinicie.
- Disminuir los valores de los parámetros:
  - En primer lugar, debe reducir los valores de los parámetros de la instancia principal y llevar a cabo un reinicio. A continuación, aplique los cambios de los parámetros a todas las réplicas de lectura asociadas y lleve a cabo un reinicio progresivo.

Supervisión y ajuste del proceso de replicación

Le recomendamos encarecidamente que supervise de forma rutinaria su instancia de base de datos de RDS para PostgreSQL y réplicas de lectura. Debe asegurarse de que las réplicas de lectura se mantengan al día con los cambios en la instancia de base de datos de origen. Amazon RDS recupera de forma transparente sus réplicas de lectura cuando se producen interrupciones en el proceso de replicación. Sin embargo, es mejor evitar la necesidad de recuperarse en absoluto. La recuperación mediante slots de replicación es más rápida que utilizar el archivo de Amazon S3, pero cualquier proceso de recuperación puede afectar al rendimiento de lectura.

Para determinar qué tal se mantienen las réplicas de lectura con la instancia de base de datos de origen, puede hacer lo siguiente:

- Compruebe la cantidad de **`ReplicaLag`** entre la instancia de base de datos de origen y las réplicas. El retardo de réplica es la cantidad de retardo, en segundos, que una réplica de lectura acumula con respecto a la instancia de base de datos de origen. Esta métrica informa del resultado de la siguiente consulta.

  ```
  SELECT extract(epoch from now() - pg_last_xact_replay_timestamp()) AS "ReplicaLag";
  ```

  El retraso de réplica indica qué tal se mantiene una réplica de lectura con la instancia de base de datos de origen. Es la cantidad de latencia entre la instancia de base de datos de origen y una instancia de lectura específica. Un valor elevado para el retraso de réplica puede indicar una discrepancia entre las clases de instancia de base de datos o los tipos de almacenamiento (o ambos) utilizados por la instancia de base de datos de origen y sus réplicas de lectura. La clase de instancia de base de datos y los tipos de almacenamiento de la instancia de origen de base de datos y todas las réplicas de lectura deben ser iguales.

El retraso de la réplica también puede ser el resultado de problemas de conexión intermitentes. Puede monitorizar el retardo de replicación en Amazon CloudWatch mediante la visualización de la métrica `ReplicaLag` de Amazon RDS. Para obtener más información sobre `ReplicaLag` y otras métricas de Amazon RDS, consulte Métricas de Amazon CloudWatch para Amazon RDS.

- Consulte el registro de PostgreSQL para obtener información que puede utilizar para ajustar la configuración. En cada punto de control, el registro de PostgreSQL captura el número de archivos de registro de transacciones reciclados, como se muestra en el siguiente ejemplo.

```
2014-11-07 19:59:35 UTC::@:[26820]:LOG:  checkpoint complete: wrote 376 buffers
 (0.2%);
0 transaction log file(s) added, 0 removed, 1 recycled; write=35.681 s, sync=0.013 s,
 total=35.703 s;
sync files=10, longest=0.013 s, average=0.001 s
```

  Puede utilizar esta información para averiguar cuántos archivos de transacciones se reciclarán en un periodo de tiempo determinado. Puede cambiar la configuración de `wal_keep_segments` si es necesario. Suponga, por ejemplo, que el registro de PostgreSQL `checkpoint complete` muestra `35 recycled` durante un intervalo de 5 minutos. En este caso, el valor predeterminado de `wal_keep_segments` de 32 no es suficiente para seguir el ritmo de la actividad de streaming, con lo que debe aumentar el valor de este parámetro.

- Utilice Amazon CloudWatch para supervisar las métricas que pueden predecir problemas de replicación. En lugar de analizar el registro de PostgreSQL directamente, puede utilizar Amazon CloudWatch para comprobar las métricas recopiladas. Por ejemplo, puede comprobar el valor de la métrica `TransactionLogsGeneration` para ver cuántos datos WAL está generando la instancia de base de datos de origen. En algunos casos, la carga de trabajo de la instancia de base de datos podría generar una gran cantidad de datos WAL. De ser así, puede que tenga que cambiar la clase de la instancia de base de datos de origen y de las réplicas de lectura. El uso de una clase de instancia con un rendimiento de red alto (10 Gbps) puede reducir el retraso de las réplicas.

Supervisión de las slots de replicación de su instancia de base de datos de RDS para PostgreSQL

Todas las versiones de RDS para PostgreSQL utilizan slots de replicación para réplicas de lectura entre regiones. RDS para PostgreSQL 14.1 y versiones posteriores utilizan slots de replicación para réplicas de lectura en región. Las réplicas de lectura dentro de la región también utilizan Amazon S3 para archivar datos WAL. En otras palabras, si la instancia de base de datos y las réplicas de lectura

ejecutan PostgreSQL 14.1 o superior, las slots de replicación y los archivos de Amazon S3 están disponibles para recuperar la réplica de lectura. La recuperación de una réplica de lectura mediante su slot de replicación es más rápida que la recuperación del archivo Amazon S3. Por lo tanto, le recomendamos que supervise las slots de replicación y las métricas relacionadas.

Puede ver las slots de replicación en sus instancias de base de datos de RDS para PostgreSQL consultando la vista de `pg_replication_slots`, de la siguiente manera.

```
postgres=> SELECT * FROM pg_replication_slots;
slot_name                  | plugin | slot_type | datoid | database | temporary |
 active | active_pid | xmin | catalog_xmin | restart_lsn | confirmed_flush_lsn |
 wal_status | safe_wal_size | two_phase
---------------------------+--------+-----------+--------+----------+-----------
+--------+------------+------+--------------+-------------+---------------------
+------------+---------------+-----------
rds_us_west_1_db_555555555 |        | physical  |        |          | f         | t
  |      13194 |      |              | 23/D8000060 |                     | reserved   |
               | f
(1 row)
```

El `wal_status` del valor `reserved` significa que la cantidad de datos WAL que mantiene la slot se encuentra dentro de los límites del parámetro `max_wal_size`. En otras palabras, la slot de replicación tiene el tamaño adecuado. Otros posibles valores de los estados son los siguientes:

- `extended`: la slot supera el ajuste `max_wal_size`, pero los datos de WAL se conservan.
- `unreserved`: la slot ya no tiene todos los datos WAL necesarios. Parte se eliminará en el siguiente punto de control.
- `lost`: se han eliminado algunos datos de WAL obligatorios. La slot ya no se puede utilizar.

Los estados `unreserved` y `lost` de `wal_status` solo se ven cuando `max_slot_wal_keep_size` no es negativo.

La vista de `pg_replication_slots` muestra el estado actual de las slots de replicación. Para evaluar el rendimiento de sus slots de replicación, puede utilizar Amazon CloudWatch y supervisar las siguientes métricas:

- **`OldestReplicationSlotLag`**: muestra la cantidad de datos del registro de escritura anticipada (WAL) en el origen que no ha consumido la réplica más retrasada.

- **`TransactionLogsDiskUsage`**: muestra cuánto almacenamiento se usa para los datos de WAL. Cuando una réplica de lectura se retrasa significativamente, el valor de esta métrica puede aumentar sustancialmente.

Para obtener más información acerca del uso de Amazon CloudWatch y las métricas de RDS para PostgreSQL, consulte Supervisión de métricas de Amazon RDS con Amazon CloudWatch. Para obtener más información sobre cómo supervisar la replicación de streaming en sus instancias de base de datos de RDS para PostgreSQL, consulte Best practices for Amazon RDS PostgreSQL replication en AWSDatabase Blog.

Solución de problemas de réplicas de lectura de RDS para PostgreSQL

A continuación, encontrará ideas para solucionar algunos problemas comunes de las réplicas de lectura de RDS para PostgreSQL.

Finalice la consulta que provoca el retardo de la réplica de lectura

Las transacciones activas o inactivas en un estado de transacción que se estén ejecutando durante mucho tiempo en la base de datos pueden interferir con el proceso de replicación de WAL y, por lo tanto, aumentar el retardo de la replicación. Por lo tanto, asegúrese de supervisar el tiempo de ejecución de estas transacciones con la vista `pg_stat_activity` de PostgreSQL.

Ejecute una consulta en la instancia principal similar a la siguiente para encontrar el ID de proceso (PID) de la consulta que lleva mucho tiempo ejecutándose:

```
SELECT datname, pid,usename, client_addr, backend_start,
xact_start, current_timestamp - xact_start AS xact_runtime, state,
backend_xmin FROM pg_stat_activity WHERE state='active';
```

```
SELECT now() - state_change as idle_in_transaction_duration, now() - xact_start as
 xact_duration,*
FROM  pg_stat_activity
WHERE state  = 'idle in transaction'
AND   xact_start is not null
ORDER BY 1 DESC;
```

Tras identificar el PID de la consulta, puede optar por finalizarla.

Ejecute una consulta en la instancia principal similar a la siguiente para finalizar la consulta que lleva mucho tiempo ejecutándose:

```
SELECT pg_terminate_backend(PID);
```

Mejora del rendimiento de las consultas de RDS para PostgreSQL con lecturas optimizadas para Amazon RDS

Puede lograr un procesamiento de consultas más rápido en RDS para PostgreSQL con las lecturas optimizadas para Amazon RDS. Una instancia de base de datos de RDS para PostgreSQL o un clúster de base de datos Multi-AZ que utilice lecturas optimizadas para RDS puede procesar las consultas hasta un 50 % más rápido en comparación con una instancia que no las use.

Temas

- Información general de las lecturas optimizadas para RDS en PostgreSQL
- Casos de uso de lecturas optimizadas para RDS
- Prácticas recomendadas para lecturas optimizadas de RDS
- Uso de lecturas optimizadas de RDS
- Supervisión de instancias de base de datos que utilizan lecturas optimizadas de RDS
- Limitaciones de las lecturas optimizadas para RDS en PostgreSQL

Información general de las lecturas optimizadas para RDS en PostgreSQL

Las lecturas optimizadas están disponibles de forma predeterminada en RDS para PostgreSQL versiones 15.2 y posteriores, 14.7 y posteriores y 13.10 y posteriores al usar clases de instancias de base de datos basadas en NVMe. Para ver las especificaciones de hardware que indican qué instancias utilizan NVMe, consulte Especificaciones de hardware para clases de instancia de base de datos .

Cuando utiliza una instancia de base de datos de RDS para PostgreSQL o un clúster de base de datos Multi-AZ que tiene activadas las lecturas optimizadas para RDS, consigue un rendimiento de consulta hasta un 50 % más rápido utilizando el almacenamiento local a nivel de bloque basado en unidades de estado sólido (SSD) de memoria rápida no volátil (NVMe). Puede procesar las consultas más rápido si coloca las tablas temporales generadas por PostgreSQL en el almacenamiento local, lo que reduce el tráfico a Elastic Block Storage (EBS) a través de la red.

En PostgreSQL, los objetos temporales se asignan a un espacio de nombres temporal que se elimina automáticamente al final de la sesión. Al borrar el espacio de nombres temporal, se eliminan todos los objetos que dependen de la sesión, incluidos los objetos que cumplen los requisitos del esquema, como tablas, funciones, operadores o incluso extensiones.

En RDS para PostgreSQL, el parámetro `temp_tablespaces` se configura para esta área de trabajo temporal donde se almacenan los objetos temporales.

Las siguientes consultas devuelven el nombre del espacio de tablas y su ubicación.

```
postgres=> show temp_tablespaces;
temp_tablespaces
--------------------
rds_temp_tablespace
(1 row)
```

`rds_temp_tablespace` es un espacio de tabla configurado por RDS que apunta hacia el almacenamiento local de NVMe. Siempre puede volver al almacenamiento de Amazon EBS modificando este parámetro en el `Parameter group` con la AWS Management Console para apuntar a cualquier espacio de tablas que no sea `rds_temp_tablespace`. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS. También puede utilizar el comando SET para modificar el valor del parámetro `temp_tablespaces` a `pg_default` a nivel de sesión. La modificación del parámetro redirige el área de trabajo temporal a Amazon EBS. Resulta útil volver a Amazon EBS cuando el almacenamiento local de la instancia o el clúster de RDS no es suficiente para realizar una operación SQL específica.

```
postgres=> SET temp_tablespaces TO 'pg_default';
SET
```

```
postgres=> show temp_tablespaces;

 temp_tablespaces
------------------
 pg_default
```

Casos de uso de lecturas optimizadas para RDS

Estos son algunos casos de uso que pueden beneficiarse de las lecturas optimizadas:

- Consultas analíticas que incluyen expresiones comunes de tabla (CTE), tablas derivadas y operaciones de agrupación.
- Réplicas de lectura que gestionan consultas no optimizadas de una aplicación.

- Consultas de informes dinámicas o bajo demanda con operaciones complejas, como GROUP BY y ORDER BY, que no siempre pueden utilizar los índices adecuados.
- Otras cargas de trabajo que utilizan tablas temporales internas.
- Operaciones `CREATE INDEX` o `REINDEX` de ordenación.

Prácticas recomendadas para lecturas optimizadas de RDS

Utilice estas prácticas recomendadas para utilizar lecturas optimizadas de RDS:

- Añada una lógica de reintento para las consultas de solo lectura en caso de que fallen debido a que el almacén de instancias está lleno durante la ejecución.
- Supervise el espacio de almacenamiento disponible en el almacén de instancias con la métrica de CloudWatch `FreeLocalStorage`. Si el almacén de instancias está alcanzando su límite debido a la carga de trabajo de la instancia de base de datos o del clúster de base de datos Multi-AZ, modifíquelo para usar una clase de instancia de base de datos más grande.

Uso de lecturas optimizadas de RDS

Al aprovisionar una instancia de base de datos RDS para PostgreSQL con una de las clases de instancia de base de datos basadas en NVMe en una implementación de instancia de base de datos Single-AZ, en una implementación de instancia de base de datos Multi-AZ o en una implementación de clúster de base de datos Multi-AZ, la instancia de base de datos utiliza automáticamente lecturas optimizadas de RDS.

Para obtener más información sobre la implementación multi-AZ, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Para activar las lecturas optimizadas de RDS, realice una de las siguientes acciones:

- Para crear una instancia de base de datos de RDS para PostgreSQL o un clúster de base de datos Multi-AZ, utilice una de las clases de instancia de base de datos basadas en NVMe. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.
- Modifique una instancia de base de datos de RDS para PostgreSQL o un clúster de base de datos Multi-AZ para utilizar una de las clases de instancia de base de datos basadas en NVMe. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Las lecturas optimizadas de RDS están disponibles en todas las Regiones de AWS donde se admite una o más de las clases de instancia de base de datos con almacenamiento SSD NVMe local. Para obtener más información, consulte Clases de instancia de base de datos de .

Para volver a una instancia de RDS con lecturas no optimizadas, modifique la clase de instancia de base de datos de su instancia de RDS o del clúster por una clase de instancia similar que solo admita el almacenamiento de EBS para las cargas de trabajo de la base de datos. Por ejemplo, si la clase de instancia de base de datos actual es db.r6gd.4xlarge, elija db.r6g.4xlarge para volver atrás. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.

Supervisión de instancias de base de datos que utilizan lecturas optimizadas de RDS

Puede supervisar las instancias de base de datos que utilizan lecturas optimizadas para RDS con las siguientes métricas de CloudWatch:

- `FreeLocalStorage`
- `ReadIOPSLocalStorage`
- `ReadLatencyLocalStorage`
- `ReadThroughputLocalStorage`
- `WriteIOPSLocalStorage`
- `WriteLatencyLocalStorage`
- `WriteThroughputLocalStorage`

Estas métricas proporcionan datos sobre el almacén de instancias disponible, las IOPS y el rendimiento. Para obtener más información sobre estas métricas, consulte Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS.

Para supervisar el uso actual del almacenamiento local, inicie sesión en la base de datos y ejecute la siguiente consulta:

```
SELECT
    spcname AS "Name",
    pg_catalog.pg_size_pretty(pg_catalog.pg_tablespace_size(oid)) AS "size"
FROM
    pg_catalog.pg_tablespace
```

```
WHERE
    spcname IN ('rds_temp_tablespace');
```

Para obtener más información sobre los archivos temporales y su uso, consulte Administración de archivos temporales con PostgreSQL.

Limitaciones de las lecturas optimizadas para RDS en PostgreSQL

Las limitaciones siguientes se aplican a las lecturas optimizadas para RDS en PostgreSQL:

- Las transacciones pueden fallar cuando el almacén de instancias está lleno.

Importación de datos en PostgreSQL en Amazon RDS

Supongamos que tiene una implementación de PostgreSQL existente que quiere pasar a Amazon RDS. La complejidad de la tarea dependerá del tamaño de la base de datos y de los tipos de objetos de base de datos que se van a transferir. Por ejemplo, considere una base de datos que contenga conjuntos de datos de tamaños del orden de gigabytes, junto con disparadores y procedimientos almacenados. Esta base de datos será más complicada que una base de datos sencilla con tan solo unos cuantos megabytes de datos de prueba sin disparadores ni procedimientos almacenados.

Es recomendable usar las herramientas de migración de bases de datos de PostgreSQL nativas si se dan las condiciones siguientes:

- Se trata de una migración homogénea, en la que se migra desde una base de datos con el mismo motor de base de datos que la base de datos de destino.
- Se va a migrar una base de datos completa.
- Las herramientas nativas permiten migrar el sistema con un tiempo de inactividad mínimo.

En la mayoría de los demás casos, realizar una migración de base de datos mediante Database Migration Service (AWS DMS) de AWS es el mejor enfoque. AWS DMS puede migrar bases de datos sin tiempo de inactividad y, para numerosos motores de base de datos, continuar la reproducción en curso hasta que todo esté preparado para cambiar a la base de datos de destino. Puede migrar al mismo motor de base de datos o a un motor de base de datos diferente con DMS de AWS. Si va a migrar a un motor de base de datos distinto del de la base de datos origen, puede usar la AWS Schema Conversion Tool (AWS SCT). Se utiliza AWS SCT para migrar objetos de esquema que AWS DMS no ha migrado. Para obtener más información acerca del uso de DMS de AWS, consulte ¿Qué es AWS Database Migration Service?

Modifique el grupo de parámetros de base de datos para incluir la siguiente configuración solo para su importación. Debe probar la configuración de los parámetros para encontrar los ajustes más eficientes para el tamaño de su instancia de base de datos. También tiene que volver a los valores de producción para esos parámetros cuando se complete la importación.

Modifique la configuración de su instancia de base de datos como se indica a continuación:

- Deshabilite los backups de la instancia de base de datos (defina backup_retention como 0).
- Deshabilite el uso de Multi-AZ.

Modifique el grupo de parámetros de base de datos para incluir la siguiente configuración. Solo debe usar estos ajustes al importar los datos. Debe probar la configuración de los parámetros para encontrar los ajustes más eficientes para el tamaño de su instancia de base de datos. También tiene que volver a los valores de producción para esos parámetros cuando se complete la importación.

Parámetro	Valor recomendado al importar	Descripción
`maintenance_work_mem`	524288, 1048576, 2097152, o 4194304 (in KB). Estos valores son comparables a 512 MB, 1 GB, 2 GB y 4 GB.	El valor de este ajuste depende del tamaño de su host. Este parámetro se usa en las declaraciones CREATE INDEX y cada comando paralelo puede usar esa cantidad de memoria. Calcule el mejor valor para no elegir uno demasiado alto y quedarse sin memoria.
`max_wal_size`	256 (para la versión 9.6), 4096 (para las versiones 10 y posteriores)	Tamaño máximo para permitir que el WAL crezca durante los puntos de control automáticos. Aumentar este parámetro puede aumentar la cantidad de tiempo necesario para la recuperación de fallos. Este parámetro reemplaza `checkpoint_segments` a la versión 9.6 y versiones posteriores de PostgreSQL. Para la versión 9.6 de PostgreSQL, este valor está en unidades de 16 MB. Para versiones posteriores, el valor está en unidades de 1 MB. Por ejemplo, en la versión 9.6, 128 significa 128 fragmentos que tienen un tamaño de 16 MB cada uno. En la versión 12.4, 2048 significa 2048 fragmentos que tienen un tamaño de 1 MB cada uno.
`checkpoint_timeout`	1800	El valor de este ajuste reduce la frecuencia de la rotación de WAL.
`synchronous_commit`	Desact.	Deshabilite este ajuste para acelerar las operaciones de escritura. La desactivación de

Parámetro	Valor recomendado al importar	Descripción
		este parámetro puede aumentar el riesgo de pérdida de datos si se bloquea el servidor (no desactive FSYNC).
`wal_buffers`	8192	Este valor está en unidades de 8 KB. Esto mejora la velocidad de generación de WAL.
`autovacuum`	0	Deshabilite el parámetro autovacuum de PostgreSQL mientras carga los datos para que no consuma recursos.

Use los comandos `pg_dump -Fc` (comprimido) o `pg_restore -j` (paralelo) con estos ajustes.

> **Note**
>
> El comando PostgreSQL `pg_dumpall` requiere permisos de super_user que no se conceden al crear una instancia de base de datos, por lo que no se puede usar para importar los datos.

Temas

- Importación de una base de datos de PostgreSQL desde una instancia Amazon EC2
- Uso del comando \copy para importar datos en una tabla en una instancia de base de datos PostgreSQL
- Importación de datos de Amazon S3 en una instancia de base de datos de RDS para PostgreSQL
- Transporte de bases de datos de PostgreSQL entre instancias de base de datos

Importación de una base de datos de PostgreSQL desde una instancia Amazon EC2

Si tiene datos en un servidor de PostgreSQL en una instancia de Amazon EC2 y desea moverlos a una instancia de base de datos de PostgreSQL, puede seguir este proceso para migrar los datos.

1. Use pg_dump para crear un archivo que contenga los datos que se van a cargar

2. Cree la instancia de base de datos de destino
3. Use psql para crear la base de datos en la instancia de base de datos y cargar los datos
4. Cree una instantánea de base de datos de la instancia de la base de datos

En las siguientes secciones. se proporciona más información sobre cada uno de los pasos mencionados anteriormente.

Paso 1: cree un archivo utilizando pg_dump que contiene los datos que se van a cargar

La utilidad `pg_dump` usa el comando COPY para crear un esquema y un volcado de datos de una base de datos de PostgreSQL. El script de volcado generado por `pg_dump` carga los datos en una base de datos con el mismo nombre y vuelve a crear las tablas, los índices y las claves externas. Puede usar el comando `pg_restore` y el parámetro `-d` para restaurar los datos en una base de datos con un nombre diferente.

Antes de crear el volcado de datos, debe consultar las tablas que se van a volcar para obtener un recuento de filas que le permita confirmar el recuento en la instancia de base de datos de destino.

El siguiente comando crea un archivo de volcado llamado mydb2dump.sql para una base de datos llamada mydb2.

```
prompt>pg_dump dbname=mydb2 -f mydb2dump.sql
```

Paso 2: cree la instancia de base de datos de destino

Cree la instancia de base de datos PostgreSQL de destino con la consola de Amazon RDS, la AWS CLI o la API. Cree la instancia con el ajuste de retención de backup definido en 0 y deshabilite el uso de Multi-AZ. Esto le permitirá acelerar la importación de los datos. Debe crear una instancia de base de datos en la instancia para poder volcar los datos. La base de datos puede tener el mismo nombre que la base de datos que contiene los datos volcados. Si lo prefiere, puede crear una base de datos con un nombre diferente. En este caso, puede usar el comando `pg_restore` y el parámetro `-d` para restaurar los datos en la base de datos que acaba de nombrar.

Por ejemplo, los siguientes comandos se pueden usar para volcar, restaurar y cambiar de nombre una base de datos.

```
pg_dump -Fc -v -h [endpoint of instance] -U [master username] [database]
 > [database].dump
```

```
createdb [new database name]
pg_restore -v -h [endpoint of instance] -U [master username] -d [new database
 name] [database].dump
```

Paso 3: use psql para crear la base de datos en la instancia de base de datos y cargar los datos

Puede usar la misma conexión que utilizó para ejecutar el comando pg_dump para conectar con la instancia de base de datos de destino y volver a crear la base de datos. Con psql, puede usar el nombre del usuario maestro y la contraseña maestra para crear la base de datos en la instancia de base de datos.

El ejemplo siguiente usa psql y un archivo de volcado llamado mydb2dump.sql para crear una base de datos llamada mydb2 en una instancia de base de datos PostgreSQL llamada mypginstance:

Para Linux, macOS o:Unix

```
psql \
   -f mydb2dump.sql \
   --host mypginstance.555555555555.aws-region.rds.amazonaws.com \
   --port 8199 \
   --username myawsuser \
   --password password \
   --dbname mydb2
```

En:Windows

```
psql ^
   -f mydb2dump.sql ^
   --host mypginstance.555555555555.aws-region.rds.amazonaws.com ^
   --port 8199 ^
   --username myawsuser ^
   --password password ^
   --dbname mydb2
```

> **Note**
>
> Especifique una contraseña distinta de la que se muestra aquí como práctica recomendada de seguridad.

Paso 4: cree una instantánea de base de datos de la instancia de base de datos

Una vez que haya comprobado que los datos se han cargado en su instancia de base de datos, es recomendable que cree una instantánea de base de datos de la instancia de base de datos PostgreSQL de destino. Las instantáneas de base de datos son copias de seguridad completos de una instancia de base de datos que se pueden usar para restaurarla a un estado conocido. Una instantánea de base de datos tomada inmediatamente después de la carga le evita tener que volver a cargar los datos en caso de error. También puede usar dicha instantánea para inicializar nuevas instancias de bases de datos. Para obtener más información acerca de la creación de una instantánea de base de datos, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

Uso del comando \copy para importar datos en una tabla en una instancia de base de datos PostgreSQL

El comando `\copy` PostgreSQL es un metacomando disponible desde la herramienta de cliente interactiva de `psql`. Puede usar `\copy` para importar datos a una tabla de su instancia de base de datos de RDS for PostgreSQL. Para usar el comando `\copy`, primero debe crear la estructura de la tabla en la instancia de base de datos de destino para que `\copy` tenga un destino para los datos que se copian.

Puede usar `\copy` para cargar los datos de un archivo de valores separados por comas (CSV), como uno que se haya exportado y guardado en su estación de trabajo de cliente.

Para importar los datos CSV a la instancia de base de datos de RDS for PostgreSQL de destino, primero conéctese a la instancia de base de datos de destino con `psql`.

```
psql --host=db-instance.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=target-db
```

A continuación, se ejecuta el comando `\copy` con los siguientes parámetros para identificar el destino de los datos y su formato.

- `target_table`: el nombre de la tabla que debe recibir los datos que se copian del archivo CSV.
- `column_list`: las especificaciones de las columnas de la tabla.
- `'filename'`: la ruta completa del archivo CSV en la estación de trabajo local.

```
 \copy target_table from '/path/to/local/filename.csv' WITH DELIMITER ',' CSV;
```

Si el archivo CSV tiene información sobre el encabezamiento de las columnas, puede utilizar esta versión del comando y los parámetros.

```
\copy target_table (column-1, column-2, column-3, ...)
    from '/path/to/local/filename.csv' WITH DELIMITER ',' CSV HEADER;
```

Si el comando `\copy` falla, PostgreSQL genera mensajes de error.

Creación de una nueva instancia de base de datos en el entorno de vista previa de bases de datos utilizando el comando `psql` con el metacomando `\copy`, tal y como se muestra en los siguientes ejemplos. Este ejemplo usa source-table como nombre de la tabla de origen, source-table.csv como archivo .csv y target-db como base de datos de destino:

Para Linux, macOS o:Unix

```
$psql target-db \
    -U <admin user> \
    -p <port> \
    -h <DB instance name> \
    -c "\copy source-table from 'source-table.csv' with DELIMITER ','"
```

En:Windows

```
$psql target-db ^
    -U <admin user> ^
    -p <port> ^
    -h <DB instance name> ^
    -c "\copy source-table from 'source-table.csv' with DELIMITER ','"
```

Para obtener más información sobre el comando `\copy`, consulte la página de psql en la documentación de PostgreSQL, en la sección Meta-Commands (Metacomandos).

Importación de datos de Amazon S3 en una instancia de base de datos de RDS para PostgreSQL

Puede importar los datos que se hayan almacenado mediante Amazon Simple Storage Service a una tabla en una instancia de base de datos de RDS para PostgreSQL. Para ello, primero debe instalar

la extensión de RDS para PostgreSQL `aws_s3`. Esta extensión proporciona las funciones que se utilizan para importar datos de un bucket de Amazon S3. Un bucket es un contenedor de objetos o archivos de Amazon S3. Los datos pueden estar en un archivo de valores separados por comas (CSV), un archivo de texto o un archivo comprimido (gzip). A continuación, aprenderá a instalar la extensión y a importar datos de Amazon S3 en una tabla.

Para hacer la importación de Simple Storage Service (Amazon S3) hacia RDS for PostgreSQL, la base de datos debe ejecutar la versión de PostgreSQL 10.7 o superior.

Si no tiene datos almacenados en Amazon S3, primero debe crear un bucket y almacenar los datos. Para obtener más información, consulte los siguientes temas en la guía del usuario de Amazon Simple Storage Service.

- Crear un bucket
- Añadir un objeto a un bucket.

Se admite la importación entre cuentas desde Amazon S3. Para obtener más información, consulte Concesión de permisos entre cuentas en la Guía del usuario de Amazon Simple Storage Service.

Puede utilizar la clave administrada por el cliente para el cifrado al importar datos desde S3. Para obtener más información, consulte Claves de KMS almacenadas en AWS KMS en la Guía del usuario de Amazon Simple Storage Service.

Temas

- Instalación de la extensión aws_s3
- Información general sobre la importación de datos desde los datos de Amazon S3
- Configuración del acceso a un bucket de Amazon S3
- Importación de datos de Amazon S3 a una instancia de base de datos de RDS para PostgreSQL
- Referencia de funciones

Instalación de la extensión aws_s3

Antes de poder usar Amazon S3 con su instancia de base de datos de RDS para PostgreSQL, debe instalar la extensión `aws_s3`. Esta extensión proporciona funciones para importar datos desde Amazon S3. También proporciona funciones para exportar datos desde una instancia de base de datos de RDS para PostgreSQL a un bucket de Amazon S3. Para obtener más información, consulte

Exportación de datos de una de Amazon S3. La extensión `aws_s3` depende de algunas de las funciones de ayuda en la extensión de `aws_commons`, que se instala automáticamente cuando es necesario.

Para instalar la extensión de **`aws_s3`**

1. Utilice psql (o pgAdmin) para conectarse a la instancia de base de datos de RDS para PostgreSQL como usuario que tiene privilegios de `rds_superuser`. Si mantuvo el nombre predeterminado durante el proceso de configuración, conéctese como `postgres`.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password
```

2. Para instalar la extensión, ejecute el siguiente comando:

```
postgres=> CREATE EXTENSION aws_s3 CASCADE;
NOTICE: installing required extension "aws_commons"
CREATE EXTENSION
```

3. Para comprobar que la extensión está instalada, puede usar el metacomando psql `\dx`.

```
postgres=> \dx
       List of installed extensions
    Name     | Version |   Schema   |                 Description
-------------+---------+------------+---------------------------------------------
 aws_commons | 1.2     | public     | Common data types across AWS services
 aws_s3      | 1.1     | public     | AWS S3 extension for importing data from S3
 plpgsql     | 1.0     | pg_catalog | PL/pgSQL procedural language
(3 rows)
```

Ya están disponibles las funciones para importar datos de Amazon S3 y para exportar datos a Amazon S3.

Información general sobre la importación de datos desde los datos de Amazon S3

Para importar datos de S3 a Amazon RDS, lleve a cabo el siguiente procedimiento:

Primero, reúna los detalles que necesita proporcionar a la función. Entre ellos se incluye el nombre de la tabla en la instancia de base de datos RDS para PostgreSQL, y el nombre del bucket, la ruta del archivo, el tipo de archivo y la Región de AWS donde se almacenan los datos de Amazon S3.

Para obtener más información, consulte el tema para ver un objeto en la guía del usuario de Amazon Simple Storage Service.

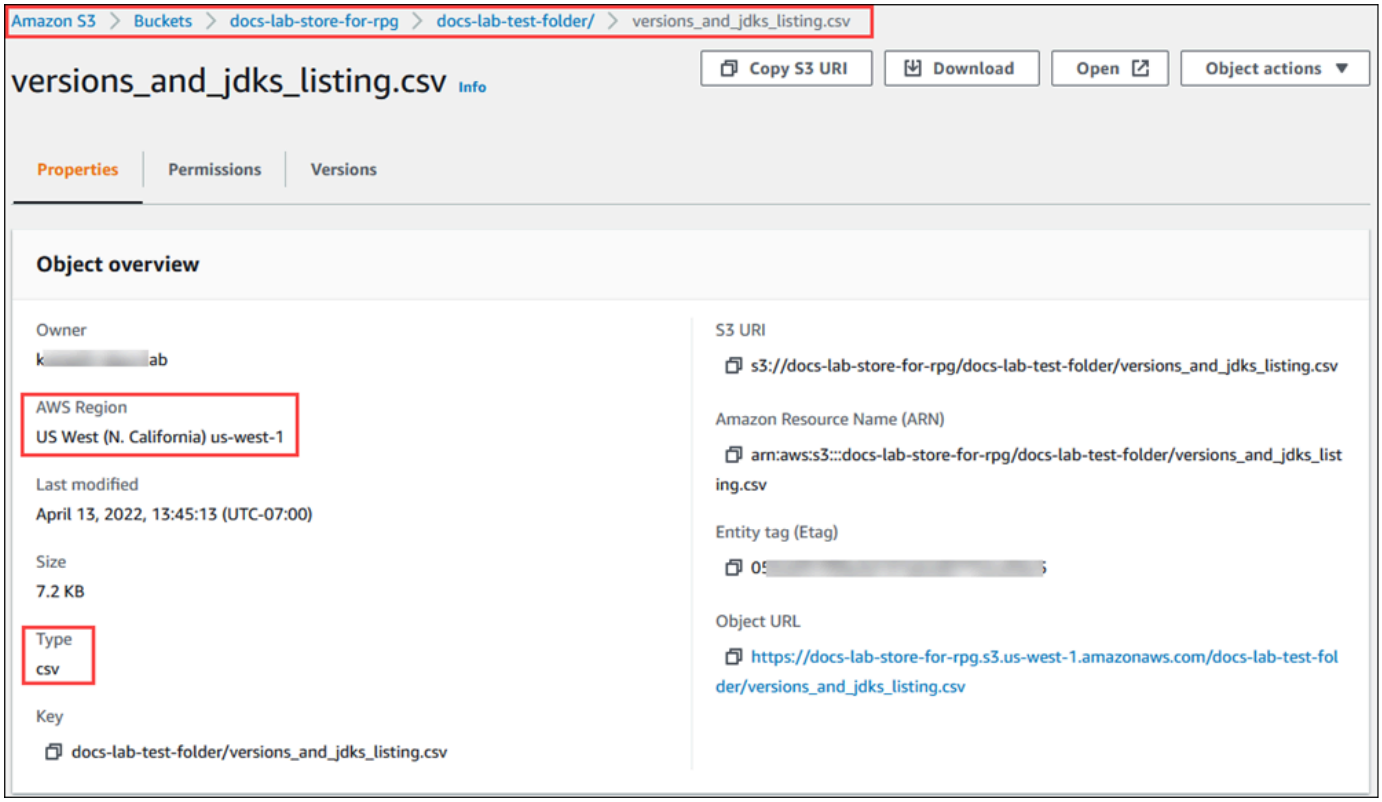
> **Note**
>
> Actualmente no se admite la importación de datos multiparte desde Amazon S3.

1. Obtenga el nombre de la tabla en la que la función `aws_s3.table_import_from_s3` va a importar los datos. A modo de ejemplo, el siguiente comando crea una tabla `t1` que se puede utilizar en pasos posteriores.

   ```
   postgres=> CREATE TABLE t1
       (col1 varchar(80),
       col2 varchar(80),
       col3 varchar(80));
   ```

2. Obtenga información sobre el bucket de Amazon S3 y los datos que se van a importar. Para ello, abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/ y elija Buckets. Busque el bucket que contiene sus datos en la lista. Elija el bucket, abra la página de información general de objetos y, a continuación, Properties (Propiedades).

   Anote el nombre del bucket, la ruta, la Región de AWS y el tipo de archivo. Necesitará el nombre de recurso de Amazon (ARN) más adelante para configurar el acceso a Amazon S3 a través de un rol de IAM. Para obtener más información, consulte Configuración del acceso a un bucket de Amazon S3. En la siguiente imagen se muestra un ejemplo.



3. Para verificar la ruta a los datos en el bucket de Amazon S3, utilice el comando de AWS CLI `aws s3 cp`. Si la información es correcta, este comando descarga una copia del archivo de Amazon S3.

```
aws s3 cp s3://amzn-s3-demo-bucket/sample_file_path ./
```

4. Configure los permisos de instancia de base de datos de RDS para PostgreSQL para permitir el acceso al archivo en el bucket de Amazon S3. Para ello, utilice un rol de AWS Identity and Access Management (IAM) o las credenciales de seguridad. Para obtener más información, consulte Configuración del acceso a un bucket de Amazon S3.

5. Proporcione la ruta y otros detalles del objeto de Amazon S3 recopilados (consulte el paso 2) para la función `create_s3_uri` para construir un objeto URI de Amazon S3. Para obtener más información sobre esta función, consulte aws_commons.create_s3_uri. A continuación se muestra un ejemplo de cómo construir este objeto durante una sesión de psql.

```
postgres=> SELECT aws_commons.create_s3_uri(
   'docs-lab-store-for-rpg',
   'versions_and_jdks_listing.csv',
   'us-west-1'
) AS s3_uri \gset
```

En el paso siguiente, pase este objeto (`aws_commons._s3_uri_1`) a la función `aws_s3.table_import_from_s3` para importar los datos a la tabla.

6. Invoque la función `aws_s3.table_import_from_s3` para importar los datos de Amazon S3 a la tabla. Para obtener información de referencia, consulte aws_s3.table_import_from_s3. Para ver ejemplos, consulta Importación de datos de Amazon S3 a una instancia de base de datos de RDS para PostgreSQL.

Configuración del acceso a un bucket de Amazon S3

Para importar datos de un archivo de Amazon S3, conceda permiso a la instancia de base de datos de RDS for PostgreSQL del para obtener acceso al bucket de Amazon S3 en el que se encuentra el archivo. Puede proporcionar acceso a un bucket de Amazon S3 de una de las dos formas siguientes, tal y como se describe en los siguientes temas.

Temas

- Uso de un rol de IAM para obtener acceso a un bucket de Amazon S3
- Uso de credenciales de seguridad para obtener acceso a un bucket de Amazon S3
- Solución de errores de acceso a Amazon S3

Uso de un rol de IAM para obtener acceso a un bucket de Amazon S3

Antes de cargar los datos de un archivo de Amazon S3, conceda permiso a la instancia de RDS para la base de datos de PostgreSQL para obtener acceso al bucket de Amazon S3 en el que se encuentra el archivo. De esta forma, no tiene que facilitar ni administrar información adicional de credenciales en la llamada a la función aws_s3.table_import_from_s3.

Para ello, cree una política de IAM que proporcione acceso al bucket de Amazon S3. Cree un rol de IAM y conecte la política a dicho rol. A continuación, asigne el rol de IAM a la instancia de base de datos.

Para dar a una instancia de base de datos de RDS for PostgreSQL acceso a Simple Storage Service (Amazon S3) a través de un rol de IAM, lleve a cabo el siguiente procedimiento:

1. Cree una política de IAM.

   Esta política concede los permisos de bucket y objeto que permiten que la instancia de RDS para base de datos de PostgreSQL tenga acceso a Amazon S3.

Incluya las siguientes acciones requeridas en la política para permitir la transferencia de archivos de un bucket de Amazon S3 a Amazon RDS:

- `s3:GetObject`
- `s3:ListBucket`

Incluya los siguientes recursos en la política para identificar el bucket de Amazon S3 y los objetos incluidos en este. A continuación se muestra el formato de nombre de recurso de Amazon (ARN) para obtener acceso a Amazon S3.

- arn:aws:s3:::*amzn-s3-demo-bucket*
- arn:aws:s3:::*amzn-s3-demo-bucket*/*

Para obtener información adicional sobre cómo crear una política de IAM para RDS para PostgreSQL, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM. Consulte también el Tutorial: Crear y asociar su primera política administrada por el cliente en la Guía del usuario de IAM.

El siguiente comando de la AWS CLI crea una política de IAM denominada `rds-s3-import-policy` con estas opciones. Otorga acceso a un bucket denominado *amzn-s3-demo-bucket*.

> **Note**
>
> Anote el Nombre de recurso de Amazon (ARN) de la política que devolvió este comando. Al asociar la política a un rol de IAM, se necesita el ARN para realizar un paso posterior.

Example

Para Linux, macOS o Unix:

```
aws iam create-policy \
   --policy-name rds-s3-import-policy \
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3import",
```

```
        "Action": [
          "s3:GetObject",
          "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket",
          "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
      }
    ]
  }'
```

Para Windows:

```
aws iam create-policy ^
   --policy-name rds-s3-import-policy ^
   --policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "s3import",
         "Action": [
           "s3:GetObject",
           "s3:ListBucket"
         ],
         "Effect": "Allow",
         "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket",
           "arn:aws:s3:::amzn-s3-demo-bucket/*"
         ]
       }
     ]
   }'
```

2. Crear un rol de IAM.

   Haga esto para que Amazon RDS pueda asumir este rol de IAM para obtener acceso a los buckets de Amazon S3. Para obtener más información, vea Crear un rol para delegar permisos a un usuario de IAM en Guía del usuario de IAM.

Le recomendamos que utilice las claves de contexto de condición globales de `aws:SourceArn` y `aws:SourceAccount` en las políticas basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

Si utiliza claves de contexto de condición globales y el valor `aws:SourceArn` contiene el ID de cuenta, el valor `aws:SourceAccount` y la cuenta en el valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utiliza en la misma instrucción de política.

- Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
- Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

En la política, asegúrese de utilizar la clave de contexto de condición global `aws:SourceArn` con el ARN completo del recurso. En el siguiente ejemplo se muestra cómo se usa el comando de la AWS CLI para crear un rol denominado `rds-s3-import-role`.

Example

Para Linux, macOS o Unix:

```
aws iam create-role \
   --role-name rds-s3-import-role \
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
             }
       }
     ]
```

```
   }'
```

Para Windows:

```
aws iam create-role ^
   --role-name rds-s3-import-role ^
   --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
             }
       }
     ]
   }'
```

3. Asocie la política de IAM que creó al rol de IAM creado.

   El siguiente comando AWS CLI adjunta la política creada en el paso anterior al rol denominado `rds-s3-import-role`. Sustituya *`your-policy-arn`* por el ARN de la política que ha anotado en un paso anterior.

   Example

   Para Linux, macOS o Unix:

```
aws iam attach-role-policy \
   --policy-arn your-policy-arn \
   --role-name rds-s3-import-role
```

   Para Windows:

```
aws iam attach-role-policy ^
```

```
    --policy-arn your-policy-arn ^
    --role-name rds-s3-import-role
```

4. Añada el rol de IAM a la instancia de base de datos.

   Para ello, utilice la AWS Management Console o la AWS CLI, tal y como se describe a continuación.

Consola

Para añadir un rol de IAM para una instancia de base de datos de PostgreSQL utilizando la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione el nombre de instancia de base de datos de PostgreSQL para mostrar sus detalles.
3. En la pestaña Connectivity & security (Conectividad y seguridad), en la sección Manage IAM roles (Administrar roles de IAM), elija el rol que desee agregar en la instancia Add IAM roles to this (Agregar roles de IAM a este clúster) .
4. En Feature Feature (Característica), elija s3Import.
5. Seleccione Add role (Añadir rol).

AWS CLI

Para añadir un rol de IAM para una instancia de base de datos de PostgreSQL utilizando la CLI

- Utilice el siguiente comando para añadir el rol a la instancia de base de datos de PostgreSQL denominada `my-db-instance`. Sustituya *`your-role-arn`* por el ARN del rol que ha anotado en el paso anterior. Utilice `s3Import` para el valor de la opción `--feature-name`.

  Example

  Para Linux, macOS o Unix:

```
aws rds add-role-to-db-instance \
    --db-instance-identifier my-db-instance \
    --feature-name s3Import \
    --role-arn your-role-arn   \
    --region your-region
```

Para Windows:

```
aws rds add-role-to-db-instance ^
   --db-instance-identifier my-db-instance ^
   --feature-name s3Import ^
   --role-arn your-role-arn ^
   --region your-region
```

API de RDS

Para agregar un rol de IAM para una instancia de base de datos de PostgreSQL mediante la API de Amazon RDS, llame a la operación AddRoleToDBInstance.

Uso de credenciales de seguridad para obtener acceso a un bucket de Amazon S3

Si lo prefiere, puede utilizar credenciales de seguridad para proporcionar acceso a un bucket de Amazon S3, en lugar de proporcionar acceso con un rol de IAM. Para ello, especifique el parámetro `credentials` en la llamada a la función aws_s3.table_import_from_s3.

El parámetro `credentials` es una estructura de tipo `aws_commons._aws_credentials_1`, que contiene credenciales de AWS. Utilice la función aws_commons.create_aws_credentials para establecer la clave de acceso y la clave secreta en una estructura `aws_commons._aws_credentials_1`, como se muestra a continuación.

```
postgres=> SELECT aws_commons.create_aws_credentials(
   'sample_access_key', 'sample_secret_key', '')
AS creds \gset
```

Tras crear la estructura `aws_commons._aws_credentials_1` , utilice la función aws_s3.table_import_from_s3 con el parámetro `credentials` para importar los datos, tal y como se muestra a continuación.

```
postgres=> SELECT aws_s3.table_import_from_s3(
   't', '', '(format csv)',
   :'s3_uri',
   :'creds'
);
```

O bien puede incluir la llamada a la función aws_commons.create_aws_credentials insertada dentro de la llamada a la función `aws_s3.table_import_from_s3`.

```
postgres=> SELECT aws_s3.table_import_from_s3(
   't', '', '(format csv)',
   :'s3_uri',
   aws_commons.create_aws_credentials('sample_access_key', 'sample_secret_key', '')
);
```

Solución de errores de acceso a Amazon S3

Si tiene problemas de conexión al intentar importar los datos de Amazon S3, consulte las recomendaciones que se indican a continuación:

- Solución de problemas de identidades y accesos en Amazon RDS
- Solución de problemas de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service
- Solución de problemas de Amazon S3 e IAM en la Guía del usuario de IAM

Importación de datos de Amazon S3 a una instancia de base de datos de RDS para PostgreSQL

Para importar datos desde su bucket de Amazon S3, utilice la función `table_import_from_s3` de la extensión aws_s3. Para obtener información de referencia, consulte aws_s3.table_import_from_s3.

> **Note**
>
> En los siguientes ejemplos se utiliza el método de rol de IAM para permitir el acceso al bucket de Amazon S3. Por tanto, no hay parámetros de credenciales en las llamadas a la función `aws_s3.table_import_from_s3`.

A continuación se muestra un ejemplo típico.

```
postgres=> SELECT aws_s3.table_import_from_s3(
   't1',
   '',
   '(format csv)',
   :'s3_uri'
```

```
);
```

Los parámetros son los siguientes:

- `t1`: nombre de la tabla en la instancia de base de datos de PostgreSQL en la que desea copiar los datos.
- `''`: lista opcional de columnas en la tabla de la base de datos. Puede utilizar este parámetro para indicar qué columnas de los datos de S3 van en las columnas de la tabla. Si no se especifica ninguna columna, se copian en la tabla todas las columnas. Para obtener un ejemplo de uso de una lista de columnas, consulte Importación de un archivo de Amazon S3 que utiliza un delimitador personalizado.
- `(format csv)`: argumentos de COPY de PostgreSQL. El proceso de copia utiliza los argumentos y el formato del comando COPY de PostgreSQL para importar los datos. Las opciones de formato incluyen un valor separado por comas (CSV), como se muestra en este ejemplo, texto y binario. El valor predeterminado es texto.
- `s3_uri`: una estructura que contiene la información que identifica el archivo de Amazon S3. Para ver un ejemplo de cómo utilizar la función aws_commons.create_s3_uri para crear una estructura `s3_uri`, consulte Información general sobre la importación de datos desde los datos de Amazon S3.

Para obtener más información acerca de esta función, consulte aws_s3.table_import_from_s3.

La función `aws_s3.table_import_from_s3` devuelve texto. Para especificar otros tipos de archivos que se van a importar desde un bucket de Amazon S3, consulte uno de los siguientes ejemplos.

> **Note**
>
> Si importa 0 bytes, se producirá un error.

Temas

- Importación de un archivo de Amazon S3 que utiliza un delimitador personalizado
- Importación de un archivo comprimido (gzip) de Amazon S3
- Importación de un archivo de Amazon S3 codificado

Importación de un archivo de Amazon S3 que utiliza un delimitador personalizado

En el siguiente ejemplo se muestra cómo importar un archivo que utiliza un delimitador personalizado. También se muestra cómo controlar dónde colocar los datos en la tabla de la base de datos usando el parámetro `column_list` de la función aws_s3.table_import_from_s3.

En este ejemplo, supongamos que la siguiente información está organizada en columnas delimitadas por barras verticales en el archivo de Amazon S3.

```
1|foo1|bar1|elephant1
2|foo2|bar2|elephant2
3|foo3|bar3|elephant3
4|foo4|bar4|elephant4
...
```

Para importar un archivo que utiliza un delimitador personalizado

1. Cree una tabla en la base de datos para los datos importados.

   ```
   postgres=> CREATE TABLE test (a text, b text, c text, d text, e text);
   ```

2. Utilice el siguiente formulario de la función aws_s3.table_import_from_s3 para importar datos desde el archivo de Amazon S3.

   Puede incluir la llamada a la función aws_commons.create_s3_uri insertada dentro de la llamada a la función `aws_s3.table_import_from_s3` para especificar el archivo.

   ```
   postgres=> SELECT aws_s3.table_import_from_s3(
      'test',
      'a,b,d,e',
      'DELIMITER ''|''',
      aws_commons.create_s3_uri('amzn-s3-demo-bucket', 'pipeDelimitedSampleFile', 'us-
   east-2')
   );
   ```

Los datos se encuentran ahora en la tabla en las siguientes columnas.

```
postgres=> SELECT * FROM test;
a | b | c | d | e
---+------+---+---+------+-----------
```

```
1 | foo1 | | bar1 | elephant1
2 | foo2 | | bar2 | elephant2
3 | foo3 | | bar3 | elephant3
4 | foo4 | | bar4 | elephant4
```

Importación de un archivo comprimido (gzip) de Amazon S3

El siguiente ejemplo muestra cómo importar un archivo comprimido con gzip desde Amazon S3. El archivo que se importa debe tener los siguientes metadatos de Simple Storage Service (Amazon S3):

- Clave: `Content-Encoding`
- Valor: `gzip`

Si carga el archivo con la AWS Management Console, el sistema suele aplicar los metadatos. Para obtener información sobre cómo cargar archivos en Simple Storage Service (Amazon S3) con la AWS Management Console, la AWS CLI o la API, consulte Carga de objetos en la Guía del usuario de Amazon Simple Storage Service.

Para obtener más información acerca de los metadatos de Simple Storage Service (Amazon S3) y detalles acerca de los metadatos proporcionados por el sistema, consulte Edición de metadatos de objeto en la consola de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Importe el archivo gzip en su instancia de RDS para la base de datos PostgreSQL como se muestra a continuación.

```
postgres=> CREATE TABLE test_gzip(id int, a text, b text, c text, d text);
postgres=> SELECT aws_s3.table_import_from_s3(
 'test_gzip', '', '(format csv)',
 'amzn-s3-demo-bucket', 'test-data.gz', 'us-east-2'
);
```

Importación de un archivo de Amazon S3 codificado

El siguiente ejemplo muestra cómo importar un archivo desde Amazon S3 que tenga codificación Windows-1252.

```
postgres=> SELECT aws_s3.table_import_from_s3(
 'test_table', '', 'encoding ''WIN1252''',
 aws_commons.create_s3_uri('amzn-s3-demo-bucket', 'SampleFile', 'us-east-2')
);
```

Referencia de funciones

Funciones

- aws_s3.table_import_from_s3
- aws_commons.create_s3_uri
- aws_commons.create_aws_credentials

aws_s3.table_import_from_s3

Importa datos de Amazon S3 en una tabla Amazon RDS. La extensión `aws_s3` proporciona la función `aws_s3.table_import_from_s3`. El valor de devolución es texto.

Sintaxis

Los parámetros obligatorios son `table_name`, `column_list` y `options`. Estos identifican la tabla de la base de datos y especifican cómo se copian los datos en la tabla.

Asimismo, puede utilizar los siguientes parámetros:

- El parámetro `s3_info` especifica el archivo Amazon S3 que se va a importar. Cuando utilice este parámetro, se proporciona acceso a Amazon S3 mediante un rol de IAM para la instancia de base de datos de PostgreSQL.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   s3_info aws_commons._s3_uri_1
)
```

- El parámetro `credentials` especifica las credenciales para acceder a Amazon S3. Cuando utilice este parámetro, no utilice un rol de IAM.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   s3_info aws_commons._s3_uri_1,
   credentials aws_commons._aws_credentials_1
)
```

Parámetros

table_name

Cadena de texto obligatoria que contiene el nombre de la tabla de la base de datos de PostgreSQL a la que importar los datos.

column_list

Cadena de texto obligatoria que contiene una lista opcional de las columnas de la tabla de la base de datos de PostgreSQL en la que se copiarán los datos. Si la cadena está vacía, se utilizan todas las columnas de la tabla. Para ver un ejemplo, consulte Importación de un archivo de Amazon S3 que utiliza un delimitador personalizado.

options

Cadena de texto obligatoria que contiene argumentos para el comando `COPY` de PostgreSQL. Estos argumentos especifican cómo se copian los datos en la tabla PostgreSQL. Para obtener más detalles, consulte la documentación de COPY de PostgreSQL.

s3_info

Tipo compuesto `aws_commons._s3_uri_1` que contiene la siguiente información sobre el objeto de S3:

- `bucket`: el nombre del bucket de Amazon S3 que contiene el archivo.
- `file_path` –: la ruta de Amazon S3 del archivo.
- `region`: la región de AWS en la que se encuentra el archivo. Para ver una lista de los nombres de regiones de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

credenciales

Tipo compuesto `aws_commons._aws_credentials_1` que contiene las siguientes credenciales para usar en la operación de importación:

- Clave de acceso
- Clave secreta
- Token de sesión

Para obtener información sobre la creación de una estructura compuesta `aws_commons._aws_credentials_1`, consulte aws_commons.create_aws_credentials.

Sintaxis alternativa

Como ayuda en las pruebas, puede utilizar un conjunto de parámetros expandido en lugar de los parámetros `s3_info` y `credentials`. A continuación, se incluyen variaciones de sintaxis adicionales para la función:`aws_s3.table_import_from_s3`

- En lugar de utilizar el parámetro `s3_info` para identificar un archivo de Amazon S3, utilice la combinación de los parámetros `bucket`, `file_path` y `region`. Con esta forma de la función, se facilita acceso a Amazon S3 mediante un rol de IAM en la instancia de base de datos de PostgreSQL.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   bucket text,
   file_path text,
   region text
)
```

- En lugar de utilizar el parámetro `credentials` para especificar el acceso a Amazon S3, utilice la combinación de parámetros `access_key`, `session_key` y `session_token`.

```
aws_s3.table_import_from_s3 (
   table_name text,
   column_list text,
   options text,
   bucket text,
   file_path text,
   region text,
   access_key text,
   secret_key text,
   session_token text
)
```

Parámetros alternativos

bucket

Cadena de texto que incluye el nombre del bucket de Amazon S3 que contiene el archivo.

file_path

Cadena de texto que contiene la ruta de Amazon S3 del archivo.

region

Una cadena de texto que identifique la ubicación de Región de AWS del archivo. Para ver una lista de los nombres de Región de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

access_key

Cadena de texto que contiene la clave de acceso que se va a utilizar para la operación de importación. El valor predeterminado es NULL.

secret_key

Cadena de texto que contiene la clave secreta que se va a usar para la operación de importación. El valor predeterminado es NULL.

session_token

(Opcional) Cadena de texto que contiene la clave de la sesión que se va a utilizar para la operación de importación. El valor predeterminado es NULL.

aws_commons.create_s3_uri

Crea una estructura `aws_commons._s3_uri_1` para contener la información de archivos de Amazon S3. Utilice los resultados de la función `aws_commons.create_s3_uri` en el parámetro `s3_info` de la función aws_s3.table_import_from_s3.

Sintaxis

```
aws_commons.create_s3_uri(
   bucket text,
   file_path text,
   region text
)
```

Parámetros

bucket

Cadena de texto obligatoria que contiene el nombre del bucket de Amazon S3 del archivo.

file_path

Cadena de texto requerida que contiene la ruta de Amazon S3 del archivo.

region

Cadena de texto obligatoria que contiene la Región de AWS en la que se encuentra el archivo. Para ver una lista de los nombres de Región de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

aws_commons.create_aws_credentials

Establece una clave de acceso y una clave secreta en una estructura `aws_commons._aws_credentials_1`. Utilice los resultados de la función `aws_commons.create_aws_credentials` en el parámetro `credentials` de la función aws_s3.table_import_from_s3.

Sintaxis

```
aws_commons.create_aws_credentials(
   access_key text,
   secret_key text,
   session_token text
)
```

Parámetros

access_key

Cadena de texto obligatoria que contiene la clave de acceso que se va a utilizar para importar un archivo de Amazon S3. El valor predeterminado es NULL.

secret_key

Cadena de texto obligatoria que contiene la clave secreta que se va a utilizar para importar un archivo de Amazon S3. El valor predeterminado es NULL.

session_token

Cadena de texto opcional que contiene el token de la sesión que se va a utilizar para importar un archivo de Amazon S3. El valor predeterminado es NULL. Si facilita un `session_token` opcional, puede usar credenciales temporales.

Transporte de bases de datos de PostgreSQL entre instancias de base de datos

Cuando utilice bases de datos transportables de PostgreSQL para Amazon RDS, puede trasladar una base de datos de PostgreSQL entre dos instancias de base de datos. Es una forma muy rápida de migrar bases de datos grandes entre distintas instancias de base de datos. Para utilizar este enfoque, ambas instancias de base de datos deben ejecutar la misma versión principal de PostgreSQL.

Esta capacidad requiere que instale la extensión `pg_transport` tanto en la instancia de base de datos de origen como en la de destino. La extensión `pg_transport` proporciona un mecanismo físico de transporte que traslada los archivos de base de datos con un procesamiento mínimo. Este mecanismo traslada los datos mucho más rápido que los procesos tradicionales de volcado y carga, con menos tiempo de inactividad.

> **Note**
>
> Las bases de datos transportables de PostgreSQL están disponibles para la versión 11.5 y las versiones posteriores de RDS for PostgreSQL, al igual que para la versión 10.10 y las versiones posteriores.

Para transportar una instancia de base de datos de PostgreSQL de una instancia de base de datos de RDS for PostgreSQL a otra, primero configure las instancias de origen y destino según se detalla en Configuración de una instancia de base de datos para transporte. A continuación, puede transportar la base de datos mediante la función descrita en Transporte de una base de datos de PostgreSQL.

Temas

- Lo que ocurre durante el transporte de base de datos
- Limitaciones del uso de bases de datos transportables de PostgreSQL
- Configuración de transporte de una base de datos de PostgreSQL
- Transporte de una base de datos PostgreSQL al destino desde el origen
- Referencia de función de bases de datos transportables
- Referencia de parámetros de bases de datos transportables

Lo que ocurre durante el transporte de base de datos

La característica de bases de datos transportables de PostgreSQL utiliza un modelo de extracción para importar la base de datos de la instancia de base de datos de origen a la de destino. La función `transport.import_from_server` crea la base de datos en tránsito en la instancia de base de datos de destino. No se puede acceder a la base de datos en tránsito en la instancia de base de datos de destino mientras dura el transporte.

Cuando el transporte comienza, finalizan todas las sesiones actuales en la base de datos de origen. Cualquier base de datos distinta a la base de datos de origen en la instancia de base de datos de origen no se ve afectada por el transporte.

La base de datos de origen se pone en un modo de solo lectura especial. Mientras está en este modo, puede conectar a la base de datos de origen y ejecutar consultas de solo lectura. Sin embargo, las consultas habilitadas para escritura y algunos otros tipos de comandos están bloqueados. Solo la base de datos de origen específica que se transporta se ve afectada por estas restricciones.

Durante el transporte, no puede restaurar la instancia de base de datos de destino a un momento en el tiempo. Esto se debe a que el transporte no es transaccional y no utiliza el registro antes de la escritura de PostgreSQL para registrar cambios. Si la instancia de base de datos de destino tiene habilitadas las copias de seguridad automáticas, se realiza automáticamente una copia de seguridad una vez que se completa el transporte. Las restauraciones a un momento dado están disponibles para momentos después de que finalice la copia de seguridad.

Si el transporte devuelve un error, la extensión `pg_transport` intenta deshacer todos los cambios en las instancias de base de datos de origen y de destino. Esto incluye eliminar la base de datos transportada parcialmente del destino. En función del tipo de error, la base de datos de origen podría seguir rechazando consultas habilitadas para escritura. Si esto ocurre, utilice el comando siguiente para permitir consultas habilitadas para escritura.

```
ALTER DATABASE db-name SET default_transaction_read_only = false;
```

Limitaciones del uso de bases de datos transportables de PostgreSQL

Las bases de datos transportables tienen las limitaciones siguientes:

- Réplicas de lectura: no puede utilizar bases de datos transportables en réplicas de lectura o instancias principales de réplicas de lectura.

- Tipos de columna no admitidos: no puede usar los tipos de datos `reg` en las tablas de base de datos que tenga previsto transportar con este método. Estos tipos depende de los ID de objeto (OID) de catálogo del sistema, que suelen cambiar durante el transporte.
- Espacios de tablas: todos los objetos de base de datos de origen deben estar en el espacio de tablas `pg_default` predeterminado.
- Compatibilidad: tanto las instancias de base de datos de origen como destino deben ejecutar la misma versión principal de PostgreSQL.
- Extensiones: la instancia de base de datos de origen solo puede tener la extensión `pg_transport` instalada.
- Roles y ACL: los privilegios de acceso y base de datos de origen y la información de propiedad no se traslada a la base de datos de destino. Todos los objetos de base de datos los crea y son propiedad del usuario de destino local del transporte.
- Transportes simultáneos: una única instancia de base de datos puede admitir hasta 32 transportes simultáneos, incluidas tanto las importaciones como las exportaciones, si los procesos de trabajo se han configurado correctamente.
- Únicamente para instancias de bases de datos de RDS for PostgreSQL: las bases de datos transportables de PostgreSQL solo son compatibles en instancias de bases de datos de RDS for PostgreSQL. No puede usarlo con bases de datos locales o bases de datos que se ejecutan en Amazon EC2.

Configuración de transporte de una base de datos de PostgreSQL

Antes de comenzar, asegúrese de que las instancias de base de datos de RDS for PostgreSQL cumplan los siguientes requisitos:

- Las instancias de base de datos de RDS for PostgreSQL de origen y destino deben ejecutar la misma versión de PostgreSQL.
- La base de datos de destino no puede tener una base de datos del mismo nombre que la base de datos de origen que desea transportar.
- La cuenta que utiliza para gestionar el transporte necesita privilegios `rds_superuser` tanto en la base de datos de origen como en la base de datos de destino.
- El grupo de seguridad de la instancia de base de datos de origen debe permitir el acceso entrante desde la instancia de base de datos de destino. Es posible que esto ya ocurra si las instancias de base de datos de origen y destino se encuentran en la VPC. Para obtener más información acerca de los grupos de seguridad, consulte Control de acceso con grupos de seguridad.

El transporte de bases de datos desde una instancia de base de datos de origen a una instancia de base de datos de destino requiere varios cambios en el grupo de parámetros de base de datos asociado a cada instancia. Esto significa que debe crear un grupo de parámetros de base de datos personalizado para la instancia de base de datos de origen y otro para la instancia de base de datos de destino.

> **Note**
>
> Si las instancias de base de datos ya están configuradas mediante grupos de parámetros de base de datos personalizados, puede comenzar con el paso 2 del siguiente procedimiento.

Para configurar los parámetros de grupo de bases de datos personalizados para transportar bases de datos

Para los siguientes pasos, utilice una cuenta que tenga privilegios `rds_superuser`.

1. Si las instancias de base de datos de origen y destino utilizan un grupo de parámetros de base de datos predeterminado, debe crear un grupo de parámetros de base de datos personalizado con la versión adecuada para sus instancias. Haga esto para poder cambiar los valores de varios parámetros. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
2. En el grupo de parámetros de base de datos personalizado, cambie los valores de los siguientes parámetros:

   - `shared_preload_libraries` – Agregue `pg_transport` a la lista de bibliotecas.
   - `pg_transport.num_workers` – El valor predeterminado es 3. Aumente o reduzca este valor según sea necesario para su base de datos. Para una base de datos de 200 GB, recomendamos que no sea superior a 8. Tenga en cuenta que si aumenta el valor predeterminado de este parámetro, también debe aumentar el valor de `max_worker_processes`.
   - `pg_transport.work_mem` – El valor predeterminado es 128 MB o 256 MB, según la versión de PostgreSQL. Por lo general, la configuración predeterminada se puede dejar sin cambios.
   - `max_worker_processes`: el valor de este parámetro debe establecerse utilizando el siguiente cálculo:

     ```
     (3 * pg_transport.num_workers) + 9
     ```

Este valor es necesario en el destino para gestionar varios procesos de trabajo en segundo plano involucrados en el transporte. Para obtener más información sobre `max_worker_processes`, y otros parámetros, consulte Consumo de recursos en la documentación de PostgreSQL.

Para obtener más información acerca de los parámetros `pg_transport`, consulte Referencia de parámetros de bases de datos transportables .

3. Reinicie la instancia de base de datos de origen de RSD for PostgreSQL y la instancia de destino para que la configuración de los parámetros surta efecto.
4. Conéctese a una instancia de base de datos de origen de RDS for PostgreSQL.

```
psql --host=source-instance.111122223333.aws-region.rds.amazonaws.com --port=5432
 --username=postgres --password
```

5. Elimine extensiones extrañas del esquema público de la instancia de base de datos. Solo se permite la extensión `pg_transport` durante la operación de transporte real.
6. Instale la extensión `pg_transport` de la siguiente manera:

```
postgres=> CREATE EXTENSION pg_transport;
CREATE EXTENSION
```

7. Conéctese a una instancia de base de datos de destino de RDS for PostgreSQL. Elimine las extensiones extrañas y, a continuación, instale la extensión `pg_transport`.

```
postgres=> CREATE EXTENSION pg_transport;
CREATE EXTENSION
```

Transporte de una base de datos PostgreSQL al destino desde el origen

Después de completar el proceso descrito en Configuración de transporte de una base de datos de PostgreSQL, puede comenzar el transporte. Para ello, ejecute la función `transport.import_from_server` en la instancia de base de datos de destino. En la siguiente sintaxis, puede encontrar los parámetros de la función.

```
SELECT transport.import_from_server(
   'source-db-instance-endpoint',
```

```
    source-db-instance-port,
   'source-db-instance-user',
   'source-user-password',
   'source-database-name',
   'destination-user-password',
   false);
```

El valor `false` que se muestra en el ejemplo indica a la función que no se trata de una prueba. Para probar la configuración de transporte, puede especificar `true` para la opción `dry_run` cuando ejecute la función, como se muestra a continuación:

```
postgres=> SELECT transport.import_from_server(
    'docs-lab-source-db.666666666666aws-region.rds.amazonaws.com', 5432,
    'postgres', '********', 'labdb', '******', true);
INFO:  Starting dry-run of import of database "labdb".
INFO:  Created connections to remote database        (took 0.03 seconds).
INFO:  Checked remote cluster compatibility          (took 0.05 seconds).
INFO:  Dry-run complete                          (took 0.08 seconds total).
 import_from_server
--------------------

(1 row)
```

Las líneas de INFO se generan porque el parámetro `pg_transport.timing` se establece en su valor predeterminado `true`. Configure `dry_run` en `false` cuando ejecute el comando y la base de datos de origen se importe al destino, como se muestra a continuación:

```
INFO:  Starting import of database "labdb".
INFO:  Created connections to remote database        (took 0.02 seconds).
INFO:  Marked remote database as read only           (took 0.13 seconds).
INFO:  Checked remote cluster compatibility          (took 0.03 seconds).
INFO:  Signaled creation of PITR blackout window     (took 2.01 seconds).
INFO:  Applied remote database schema pre-data       (took 0.50 seconds).
INFO:  Created connections to local cluster          (took 0.01 seconds).
INFO:  Locked down destination database              (took 0.00 seconds).
INFO:  Completed transfer of database files          (took 0.24 seconds).
INFO:  Completed clean up                            (took 1.02 seconds).
INFO:  Physical transport complete               (took 3.97 seconds total).
import_from_server
--------------------
(1 row)
```

Esta función requiere que proporcione contraseñas de usuario de base de datos. De esta manera, le recomendamos que cambie las contraseñas de los roles de usuario que ha utilizado después de completar el transporte. O, puede utilizar variables de enlace SQL para crear roles de usuario temporales. Utilice estos roles temporales para el transporte y, a continuación, descarte los roles con posterioridad.

Si el transporte no se realiza correctamente, es posible que vea un mensaje de error similar al siguiente:

```
pg_transport.num_workers=8 25% of files transported failed to download file data
```

El mensaje de error “Failed to download file data” (No se pudo descargar los datos de archivo) indica que el número de procesos de trabajo no está configurado correctamente para el tamaño de la base de datos. Es posible que tenga que aumentar o disminuir el valor establecido para `pg_transport.num_workers`. Cada error informa el porcentaje de finalización, de modo que pueda ver el impacto de los cambios. Por ejemplo, cambiar la configuración de 8 a 4 en un caso dio lugar a lo siguiente:

```
pg_transport.num_workers=4 75% of files transported failed to download file data
```

Tenga en cuenta que el parámetro `max_worker_processes` también se tiene en cuenta durante el proceso de transporte. En otras palabras, es posible que tenga que modificar tanto `pg_transport.num_workers` como `max_worker_processes` para transportar correctamente la base de datos. El ejemplo que se muestra finalmente funcionó cuando `pg_transport.num_workers` se estableció en 2:

```
pg_transport.num_workers=2 100% of files transported
```

Para obtener más información sobre la funcionalidad `transport.import_from_server` y sus parámetros, consulte Referencia de función de bases de datos transportables.

Referencia de función de bases de datos transportables

La función `transport.import_from_server` transporta una base de datos de PostgreSQL importándola desde una instancia de base de datos de origen en una instancia de base de datos de destino. Lo hace utilizando un mecanismo de transporte de conexión de base de datos física.

Antes de iniciar el transporte, esta función verifica que las instancias de base de datos de origen y de destino sean la misma versión y sean compatibles para la migración. También confirma que la instancia de base de datos de destino tenga suficiente espacio para la de origen.

Sintaxis

```
transport.import_from_server(
   host text,
   port int,
   username text,
   password text,
   database text,
   local_password text,
   dry_run bool
)
```

Valor de retorno

Ninguno.

Parámetros

Puede buscar las descripciones de los parámetros de función `transport.import_from_server` en la tabla siguiente.

Parámetro	Descripción
`host`	El punto de enlace de una instancia de base de datos de origen.
`port`	Un entero que representa el puerto de la instancia de base de datos de origen. Las instancias de base de datos de PostgreSQL suelen utilizar el puerto 5432.
`username`	El usuario de la instancia de base de datos de origen. Este usuario debe ser un miembro del rol `rds_superuser` .
`password`	La contraseña de usuario de la instancia de base de datos de origen.
`database`	El nombre de la base de datos en la instancia de base de datos de origen que transportar.

Parámetro	Descripción
`local_password`	La contraseña local del usuario actual para la instancia de base de datos de destino. Este usuario debe ser un miembro del rol `rds_superuser` .
`dry_run`	Un valor booleano opcional que especifique si realizar un simulacro. El valor predeterminado es `false`, lo que significa que el transporte continúa. Para confirmar la compatibilidad entre las instancias de base de datos de origen y destino sin llevar a cabo el transporte real, defina `dry_run` en `true`.

Ejemplo

Para ver un ejemplo, consulte Transporte de una base de datos PostgreSQL al destino desde el origen.

Referencia de parámetros de bases de datos transportables

Varios parámetros controlan el comportamiento de la extensión `pg_transport`. A continuación, puede encontrar las descripciones de estos parámetros.

`pg_transport.num_workers`

El número de empleados que se necesitarán para el proceso de transporte. El valor predeterminado es 3. Los valores válidos están comprendidos entre 1 y 32. Incluso los transportes de base de datos más grandes normalmente requieren menos de 8 empleados. El valor de esta configuración en la instancia de base de datos de destino se utiliza tanto en las instancias de base de datos de destino y de origen durante el transporte.

`pg_transport.timing`

Especifica si se debe notificar la información de tiempo durante el transporte. El valor predeterminado es `true`, lo que significa que se informa la información de los plazos. Le recomendamos que deje este parámetro configurado en `true` para que pueda supervisar el progreso. Para ejemplo de salida, consulte Transporte de una base de datos PostgreSQL al destino desde el origen.

`pg_transport.work_mem`

La cantidad de memoria máxima que asignar para cada proceso de trabajo. El valor predeterminado es 131 072 kilobytes (KB) o 262 144 KB (256 MB), según la versión de

PostgreSQL. El valor mínimo es 64 megabytes (65 536 KB). Los valores válidos están en kilobytes (KB) como unidades binarias de base 2, donde 1 KB = 1024 bytes.

El transporte podría utilizar menos memoria que la que se especifica en este parámetro. Incluso los transportes de base de datos grandes normalmente requieren menos de 256 MB (262 144 KB) de memoria por proceso de trabajo.

Exportación de datos de una de Amazon S3

Puede consultar datos de una RDS for PostgreSQL y exportarlos directamente a archivos almacenados en un bucket de Amazon S3. Para ello, primero debe instalar la extensión de RDS para PostgreSQL `aws_s3`. Esta extensión le proporciona las funciones que utiliza para exportar los resultados de las consultas a Amazon S3. A continuación, puede averiguar cómo instalar la extensión y cómo exportar datos de Amazon S3.

> **Note**
>
> No se ha agregado compatibilidad con la exportación entre cuentas a Amazon S3.

Todas las versiones disponibles actualmente de RDS para PostgreSQL admiten la exportación de datos a Amazon Simple Storage Service. Para obtener información detallada sobre la versión, consulte las actualizaciones de Amazon RDS para PostgreSQL en las notas de la versión de Amazon RDS para PostgreSQL.

Si no tienes un bucket configurado para la exportación, consulta los siguientes temas: Guía del usuario de Amazon Simple Storage Service.

- Configuración de Amazon S3
- Crear un bucket

De forma predeterminada, los datos exportados desde RDS para PostgreSQL a Amazon S3 utilizan cifrado del servidor con una Clave administrada de AWS. Si utiliza cifrado de buckets, el bucket de Amazon S3 debe cifrarse con una clave AWS Key Management Service (AWS KMS) (SSE-KMS). En la actualidad, no se admiten buckets cifrados con claves administradas de Amazon S3 (SSE-S3).

> **Note**
>
> Puede guardar datos de instantáneas de base de datos en Amazon S3 mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3 para Amazon RDS.

Temas

- Instalación de la extensión aws_s3
- Información general de la exportación de datos a Amazon S3
- Especificación de la ruta del archivo de Amazon S3 a exportar
- Configuración del acceso a un bucket de Amazon S3
- Exportación de datos de consulta mediante la función aws_s3.query_export_to_s3
- Referencia de funciones
- Solución de errores de acceso a Amazon S3

Instalación de la extensión aws_s3

Antes de poder usar Amazon Simple Storage Service con su Instancia de base de datos de RDS para PostgreSQL, debe instalar la extensión `aws_s3`. Esta extensión proporciona funciones para exportar datos desde una instancia de base de datos de RDS para PostgreSQL a un bucket de Amazon S3. También proporciona funciones para importar datos desde Amazon S3. Para obtener más información, consulte Importación de datos de Amazon S3 en una instancia de base de datos de RDS para PostgreSQL. La extensión `aws_s3` depende de algunas de las funciones de ayuda en la extensión de `aws_commons`, que se instala automáticamente cuando es necesario.

Para instalar la extensión de **`aws_s3`**

1. Utilice psql (o pgAdmin) para conectarse a la instancia de base de datos de RDS para PostgreSQL como usuario que tiene privilegios de `rds_superuser`. Si mantuvo el nombre predeterminado durante el proceso de configuración, conéctese como `postgres`.

   ```
   psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password
   ```

2. Para instalar la extensión, ejecute el siguiente comando:

   ```
   postgres=> CREATE EXTENSION aws_s3 CASCADE;
   NOTICE: installing required extension "aws_commons"
   CREATE EXTENSION
   ```

3. Para comprobar que la extensión está instalada, puede usar el metacomando psql `\dx`.

   ```
   postgres=> \dx
          List of installed extensions
       Name     | Version |   Schema   |                Description
   ```

```
-------------+---------+------------+--------------------------------------------
 aws_commons | 1.2     | public     | Common data types across AWS services
 aws_s3      | 1.1     | public     | AWS S3 extension for importing data from S3
 plpgsql     | 1.0     | pg_catalog | PL/pgSQL procedural language
(3 rows)
```

Ya están disponibles las funciones para importar datos de Amazon S3 y para exportar datos a Amazon S3.

Confirme que su versión de RDS for PostgreSQL admite exportaciones a Amazon S3.

Puede comprobar que su versión de RDS para PostgreSQL admite la exportación a Amazon S3 mediante el comando `describe-db-engine-versions`. En el siguiente ejemplo se verifica la compatibilidad con la versión 10.14.

```
aws rds describe-db-engine-versions --region us-east-1
--engine postgres --engine-version 10.14 | grep s3Export
```

Si en la salida se recoge la cadena de texto `"s3Export"`, el motor admite las exportaciones de Amazon S3 . Si no es así, el motor no las admite.

Información general de la exportación de datos a Amazon S3

Para exportar datos almacenados en una RDS for PostgreSQL a un bucket de Amazon S3, utilice el siguiente procedimiento.

Para exportar RDS for PostgreSQL datos a S3

1. Identifique la ruta de archivo de Amazon S3 que se va a utilizar para exportar datos. Para obtener más información sobre este proceso, consulte Especificación de la ruta del archivo de Amazon S3 a exportar.
2. Conceda permiso para acceder al bucket de Amazon S3.

   Para exportar datos a un archivo de Amazon S3, conceda permiso a la instancia de base de datos de RDS para PostgreSQL para obtener acceso al bucket de Amazon S3 que la exportación usará para el almacenamiento. Esto incluye los siguientes pasos:

   1. Cree una política de IAM que proporcione acceso al bucket de Amazon S3 al que se desea exportar.

2. Cree un rol de IAM.
3. Asocie la política que ha creado al rol que ha creado.
4. Agregue este rol de IAM a la instancia de base de datos.

   Para obtener más información sobre este proceso, consulte Configuración del acceso a un bucket de Amazon S3.

3. Identifique una consulta de base de datos para obtener los datos. Exporte los datos de consulta llamando a la función `aws_s3.query_export_to_s3`.

   Después de completar las tareas de preparación anteriores, utilice la función aws_s3.query_export_to_s3 para exportar los resultados de la consulta a Amazon S3. Para obtener más información sobre este proceso, consulte Exportación de datos de consulta mediante la función aws_s3.query_export_to_s3.

Especificación de la ruta del archivo de Amazon S3 a exportar

Especifique la siguiente información para identificar la ubicación de Amazon S3 a la que desea exportar los datos:

- Nombre de bucket: un bucket es un contenedor para objetos o archivos de Amazon S3.

  Para obtener más información sobre cómo almacenar datos con Amazon S3, consulte Crear un bucket y Trabajar con objetos en la Guía del usuario de Amazon Simple Storage Service.
- Ruta del archivo: la ruta del archivo identifica dónde se almacena la exportación en el bucket de Amazon S3. La ruta del archivo consta de lo siguiente:
  - Un prefijo de ruta opcional que identifica una ruta de carpeta virtual.
  - Un prefijo de archivo que identifica uno o varios archivos que se van a almacenar. Las exportaciones más grandes se almacenan en varios archivos, cada uno con un tamaño máximo de aproximadamente 6 GB. Los nombres de archivo adicionales tienen el mismo prefijo de archivo, pero con `_part`*XX* anexado. *XX* representa 2, luego 3, y así sucesivamente.

  Por ejemplo, una ruta de archivo con una carpeta `exports` y un prefijo de archivo `query-1-export` es `/exports/query-1-export`.
- Región de AWS (opcional): la región de AWS donde se encuentra el bucket de Amazon S3. Si no especifica un valor de región de AWS, Amazon RDS guarda sus archivos en Amazon S3, en la misma región de AWS que la instancia de base de datos de exportación.

> **Note**
>
> Actualmente, la región de AWS debe ser la misma región que la del e instancia de base de datos de exportación.

Para ver una lista de los nombres de regiones de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

Para mantener la información del archivo de Amazon S3 acerca de dónde se va a almacenar la exportación, puede utilizar la función aws_commons.create_s3_uri para crear una estructura compuesta `aws_commons._s3_uri_1` de la siguiente manera.

```
psql=> SELECT aws_commons.create_s3_uri(
   'amzn-s3-demo-bucket',
   'sample-filepath',
   'us-west-2'
) AS s3_uri_1 \gset
```

Más adelante, proporcione este valor `s3_uri_1` como un parámetro en la llamada a la función aws_s3.query_export_to_s3. Para ver ejemplos, consulte Exportación de datos de consulta mediante la función aws_s3.query_export_to_s3.

Configuración del acceso a un bucket de Amazon S3

Para exportar datos a Amazon S3, conceda permiso a la instancia de base de datos de PostgreSQL para acceder al bucket de Amazon S3 al que irán los archivos.

Para ello, siga el procedimiento que se indica a continuación.

Para proporcionar a la instancia de base de datos de PostgreSQL acceso a Amazon S3 a través de un rol de IAM

1. Cree una política de IAM.

   Esta política concede los permisos de bucket y objeto que permiten a la instancia de base de datos de PostgreSQL acceder a Amazon S3.

   Como parte de la creación de esta política, realice los siguientes pasos:

a. Incluya las siguientes acciones necesarias en la política para permitir la transferencia de archivos de la instancia de base de datos de PostgreSQL a un bucket de Amazon S3:

   - `s3:PutObject`
   - `s3:AbortMultipartUpload`

b. Incluye el nombre de recurso de Amazon (ARN) que identifica el bucket de Amazon S3 y los objetos del bucket. El formato del ARN para acceder a Amazon S3 es: `arn:aws:s3:::`*`amzn-s3-demo-bucket`*`/*`

Para obtener información adicional sobre cómo crear una política de IAM para Amazon RDS for PostgreSQL, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM. Consulte también el Tutorial: Crear y asociar su primera política administrada por el cliente en la Guía del usuario de IAM.

El siguiente comando de la AWS CLI crea una política de IAM denominada `rds-s3-export-policy` con estas opciones. Otorga acceso a un bucket denominado *`amzn-s3-demo-bucket`*.

> **Warning**
>
> Le recomendamos que configure la base de datos en una VPC privada que tenga políticas de punto de enlace configuradas para acceder a buckets específicos. Para obtener más información, consulte Uso de políticas de punto de enlace para Amazon S3 en la Guía del usuario de Amazon VPC.
> Recomendamos encarecidamente que no cree una política con acceso a todos los recursos. Este acceso puede representar una amenaza para la seguridad de los datos. Si crea una política que da acceso `S3:PutObject` a todos los recursos mediante `"Resource":"*"`, un usuario con privilegios de exportación puede exportar datos a todos los buckets de su cuenta. Además, el usuario puede exportar datos a cualquier bucket en el que se pueda escribir públicamente dentro de su región de AWS.

Después de crear la política, anote el nombre de recurso de Amazon (ARN) de la política. Cuando asocia la política a un rol de IAM, necesita el ARN para realizar un paso posterior.

```
aws iam create-policy  --policy-name rds-s3-export-policy  --policy-document '{
     "Version": "2012-10-17",
```

```
    "Statement": [
      {
        "Sid": "s3export",
        "Action": [
          "s3:PutObject*",
          "s3:ListBucket",
          "s3:GetObject*",
          "s3:DeleteObject*",
          "s3:GetBucketLocation",
          "s3:AbortMultipartUpload"
        ],
        "Effect": "Allow",
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
      }
    ]
  }'
```

2. Cree un rol de IAM.

   Realiza este paso para que Amazon RDS pueda asumir este rol de IAM en su nombre para obtener acceso a los buckets de Amazon S3. Para obtener más información, consulte Creación de un rol para delegar permisos a un usuario de IAM en la Guía del usuario de IAM.

   Le recomendamos que utilice las claves de contexto de condición globales de `aws:SourceArn` y `aws:SourceAccount` en las políticas basadas en recursos para limitar los permisos del servicio a un recurso específico. Esta es la forma más eficaz de protegerse contra el problema del suplente confuso.

   Si utiliza claves de contexto de condición globales y el valor `aws:SourceArn` contiene el ID de cuenta, el valor `aws:SourceAccount` y la cuenta en el valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utiliza en la misma instrucción de política.

   - Use `aws:SourceArn` si quiere acceso entre servicios para un único recurso.
   - Use `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

   En la política, asegúrese de utilizar la clave de contexto de condición global `aws:SourceArn` con el ARN completo del recurso. En el siguiente ejemplo se muestra cómo se usa el comando de la AWS CLI para crear un rol denominado `rds-s3-export-role`.

Example

Para Linux, macOS o Unix:

```
aws iam create-role  \
    --role-name rds-s3-export-role  \
    --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
                }
             }
       }
     ]
   }'
```

Para Windows:

```
aws iam create-role  ^
    --role-name rds-s3-export-role  ^
    --assume-role-policy-document '{
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
            "Service": "rds.amazonaws.com"
          },
         "Action": "sts:AssumeRole",
         "Condition": {
             "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "arn:aws:rds:us-east-1:111122223333:db:dbname"
```

```
                }
            }
        }
    ]
}'
```

3. Asocie la política de IAM que creó al rol de IAM creado.

   El siguiente comando de la AWS CLI asocia la política creada anteriormente al rol denominado `rds-s3-export-role.`. Sustituya *`your-policy-arn`* por el ARN de la política que ha anotado en un paso anterior.

```
aws iam attach-role-policy  --policy-arn your-policy-arn  --role-name rds-s3-export-role
```

4. Añada el rol de IAM a la instancia de base de datos. Para ello, utilice la AWS Management Console o la AWS CLI, tal y como se describe a continuación.

Consola

Para añadir un rol de IAM para una instancia de base de datos de PostgreSQL utilizando la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccione el nombre de instancia de base de datos de PostgreSQL para mostrar sus detalles.
3. En la pestaña Connectivity & security (Conectividad y seguridad), en la sección Manage IAM roles (Administrar roles de IAM), elija el rol que desee añadir en Add IAM roles to this instance (Añadir roles de IAM a esta instancia).
4. En Feature (Característica), elija s3Export.
5. Seleccione Add role (Añadir rol).

AWS CLI

Para añadir un rol de IAM para una instancia de base de datos de PostgreSQL utilizando la CLI

- Utilice el siguiente comando para añadir el rol a la instancia de base de datos de PostgreSQL denominada `my-db-instance`. Sustituya *`your-role-arn`* por el ARN del rol que ha anotado en el paso anterior. Utilice `s3Export` para el valor de la opción `--feature-name`.

Example

Para Linux, macOS o Unix:

```
aws rds add-role-to-db-instance \
   --db-instance-identifier my-db-instance \
   --feature-name s3Export \
   --role-arn your-role-arn   \
   --region your-region
```

Para Windows:

```
aws rds add-role-to-db-instance ^
   --db-instance-identifier my-db-instance ^
   --feature-name s3Export ^
   --role-arn your-role-arn ^
   --region your-region
```

Exportación de datos de consulta mediante la función aws_s3.query_export_to_s3

Exporte sus datos de PostgreSQL a Amazon S3 llamando a la función aws_s3.query_export_to_s3.

Temas

- Requisitos previos
- Llamar a aws_s3.query_export_to_s3
- Exportación a un archivo CSV que utiliza un delimitador personalizado
- Exportación a un archivo binario con codificación

Requisitos previos

Antes de utilizar la función `aws_s3.query_export_to_s3`, asegúrese de completar los siguientes requisitos previos:

- Instale las extensiones de PostgreSQL necesarias como se describe en Información general de la exportación de datos a Amazon S3.

- Determine a dónde exportar los datos en Amazon S3 como se describe en Especificación de la ruta del archivo de Amazon S3 a exportar.
- Tenga cuidado de que la del clúster de base de datos tenga acceso de exportación a Amazon S3 según se describe en Configuración del acceso a un bucket de Amazon S3.

Los ejemplos siguientes utilizan una tabla de base de datos llamada `sample_table`. Estos ejemplos exportan los datos a un bucket llamado *`amzn-s3-demo-bucket`*. La tabla y los datos de ejemplo se crean con las siguientes instrucciones SQL en psql.

```
psql=> CREATE TABLE sample_table (bid bigint PRIMARY KEY, name varchar(80));
psql=> INSERT INTO sample_table (bid,name) VALUES (1, 'Monday'), (2,'Tuesday'), (3,
 'Wednesday');
```

Llamar a aws_s3.query_export_to_s3

A continuación, se muestran las formas básicas de llamar a la función aws_s3.query_export_to_s3.

En estos ejemplos se utiliza la variable `s3_uri_1` para identificar una estructura que contiene la información que identifica el archivo de Amazon S3. Utilice la función aws_commons.create_s3_uri para crear la estructura.

```
psql=> SELECT aws_commons.create_s3_uri(
   'amzn-s3-demo-bucket',
   'sample-filepath',
   'us-west-2'
) AS s3_uri_1 \gset
```

Aunque los parámetros varían para las dos llamadas a funciones siguientes `aws_s3.query_export_to_s3`, los resultados son los mismos para estos ejemplos. Todas las filas de la tabla `sample_table` se exportan a un bucket llamado *`amzn-s3-demo-bucket`*.

```
psql=> SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM
 sample_table', :'s3_uri_1');

psql=> SELECT * FROM aws_s3.query_export_to_s3('SELECT * FROM
 sample_table', :'s3_uri_1', options :='format text');
```

Los parámetros se describen de la siguiente manera:

- `'SELECT * FROM sample_table'`: el primer parámetro es una cadena de texto requerida que contiene una consulta SQL. El motor de PostgreSQL ejecuta esta consulta. Los resultados de la consulta se copian en el bucket de S3 identificado en otros parámetros.
- `:'s3_uri_1'`: este parámetro es una estructura que identifica el archivo de Amazon S3. En este ejemplo se utiliza una variable para identificar la estructura creada anteriormente. En su lugar, puede crear la estructura incluyendo la llamada a la función `aws_commons.create_s3_uri` insertada dentro de la llamada a la función `aws_s3.query_export_to_s3` de la siguiente manera.

```
SELECT * from aws_s3.query_export_to_s3('select * from sample_table',
   aws_commons.create_s3_uri('amzn-s3-demo-bucket', 'sample-filepath', 'us-west-2')
);
```

- `options :='format text'`: el parámetro `options` es una cadena de texto opcional que contiene argumentos `COPY` de PostgreSQL. El proceso de copia utiliza los argumentos y el formato del comando COPY de PostgreSQL.

Si el archivo especificado no existe en el bucket de Amazon S3, se crea. Si el archivo ya existe, se sobrescribe. La sintaxis para acceder a los datos exportados en Amazon S3 es la siguiente.

```
s3-region://bucket-name[/path-prefix]/file-prefix
```

Las exportaciones más grandes se almacenan en varios archivos, cada uno con un tamaño máximo de aproximadamente 6 GB. Los nombres de archivo adicionales tienen el mismo prefijo de archivo, pero con `_part`*XX* anexado. *XX* representa 2, luego 3, y así sucesivamente. Por ejemplo, supongamos que especifica la ruta donde almacena los archivos de datos como sigue.

```
s3-us-west-2://amzn-s3-demo-bucket/my-prefix
```

Si la exportación tiene que crear tres archivos de datos, el bucket de Amazon S3 contiene los siguientes archivos de datos.

```
s3-us-west-2://amzn-s3-demo-bucket/my-prefix
s3-us-west-2://amzn-s3-demo-bucket/my-prefix_part2
s3-us-west-2://amzn-s3-demo-bucket/my-prefix_part3
```

Para obtener la referencia completa de esta función y formas adicionales de llamarla, consulte aws_s3.query_export_to_s3. Para obtener más información sobre el acceso a archivos en Amazon S3, consulte Ver un objeto en la Guía del usuario de Amazon Simple Storage Service.

Exportación a un archivo CSV que utiliza un delimitador personalizado

En el ejemplo siguiente se muestra cómo llamar a la función aws_s3.query_export_to_s3 para exportar datos a un archivo que utiliza un delimitador personalizado. En el ejemplo se utilizan argumentos del comando COPY de PostgreSQL para especificar el formato de valor separado por comas (CSV) y un delimitador de dos puntos (:).

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
 options :='format csv, delimiter $$:$$');
```

Exportación a un archivo binario con codificación

En el ejemplo siguiente se muestra cómo llamar a la función aws_s3.query_export_to_s3 para exportar datos a un archivo binario que tiene codificación Windows-1253.

```
SELECT * from aws_s3.query_export_to_s3('select * from basic_test', :'s3_uri_1',
 options :='format binary, encoding WIN1253');
```

Referencia de funciones

Funciones

- aws_s3.query_export_to_s3
- aws_commons.create_s3_uri

aws_s3.query_export_to_s3

Exporta un resultado de consulta PostgreSQL a un bucket de Amazon S3. La extensión `aws_s3` proporciona la función `aws_s3.query_export_to_s3`.

Los parámetros obligatorios son `query` y `s3_info`. Definen la consulta que se va a exportar e identifican el bucket de Amazon S3 al que se va a exportar. Un parámetro opcional llamado `options` proporciona la definición de varios parámetros de exportación. Para obtener ejemplos sobre el uso de la función `aws_s3.query_export_to_s3`, consulte Exportación de datos de consulta mediante la función aws_s3.query_export_to_s3.

Sintaxis

```
aws_s3.query_export_to_s3(
    query text,
    s3_info aws_commons._s3_uri_1,
    options text,
    kms_key text
)
```

Parámetros de entrada

consulta

Cadena de texto necesaria que contiene una consulta SQL que ejecuta el motor de PostgreSQL. Los resultados de esta consulta se copian en un bucket de S3 identificado en el parámetro `s3_info`.

s3_info

Tipo compuesto `aws_commons._s3_uri_1` que contiene la siguiente información sobre el objeto de S3:

- `bucket`: el nombre del bucket de Amazon S3 que contiene el archivo.
- `file_path` –: la ruta de Amazon S3 del archivo.
- `region`: la región de AWS en la que se encuentra el bucket. Para ver una lista de los nombres de regiones de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

  Actualmente, este valor debe ser la misma región de AWS que la del e instancia de base de datos de exportación. El valor predeterminado es la región de AWS del e instancia de base de datos de exportación.

Para crear una estructura compuesta `aws_commons._s3_uri_1`, consulte la función aws_commons.create_s3_uri.

options

Cadena de texto opcional que contiene argumentos para el comando `COPY` de PostgreSQL. Estos argumentos especifican cómo se copian los datos cuando se exportan. Para obtener más detalles, consulte la documentación de COPY de PostgreSQL.

kms_key text

Una cadena de texto opcional que contiene la clave KMS administrada por el cliente del bucket de S3 al que se exportan los datos.

Parámetros de entrada alternativos

Como ayuda en las pruebas, puede utilizar un conjunto de parámetros expandido en lugar del parámetro `s3_info`. A continuación, se incluyen otras variaciones de la sintaxis de la función `aws_s3.query_export_to_s3`.

En lugar de utilizar el parámetro `s3_info` para identificar un archivo de Amazon S3, utilice la combinación de los parámetros `bucket`, `file_path` y `region`.

```
aws_s3.query_export_to_s3(
    query text,
    bucket text,
    file_path text,
    region text,
    options text,
    kms_key text
)
```

consulta

Cadena de texto necesaria que contiene una consulta SQL que ejecuta el motor de PostgreSQL. Los resultados de esta consulta se copian en un bucket de S3 identificado en el parámetro `s3_info`.

bucket

Cadena de texto obligatoria que incluye el nombre del bucket de Amazon S3 que contiene el archivo.

file_path

Cadena de texto requerida que contiene la ruta de Amazon S3 del archivo.

region

Cadena de texto opcional que contiene la región de AWS en la que se encuentra el bucket. Para ver una lista de los nombres de regiones de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

Actualmente, este valor debe ser la misma región de AWS que la del e instancia de base de datos de exportación. El valor predeterminado es la región de AWS del e instancia de base de datos de exportación.

options

Cadena de texto opcional que contiene argumentos para el comando `COPY` de PostgreSQL. Estos argumentos especifican cómo se copian los datos cuando se exportan. Para obtener más detalles, consulte la documentación de COPY de PostgreSQL.

kms_key text

Una cadena de texto opcional que contiene la clave KMS administrada por el cliente del bucket de S3 al que se exportan los datos.

Parámetros de salida

```
aws_s3.query_export_to_s3(
    OUT rows_uploaded bigint,
    OUT files_uploaded bigint,
    OUT bytes_uploaded bigint
)
```

rows_uploaded

Número de filas de tabla que se cargaron correctamente a Amazon S3 para la consulta dada.

files_uploaded

El número de archivos cargados en Amazon S3. Los archivos se crean en tamaños de aproximadamente 6 GB. Cada archivo adicional creado tiene `_part`*XX* anexado al nombre. *XX* representa 2, luego 3, y así sucesivamente según sea necesario.

bytes_uploaded

El número total de bytes cargados a Amazon S3.

Ejemplos

```
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'amzn-s3-demo-bucket', 'sample-filepath');
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'amzn-s3-demo-bucket', 'sample-filepath','us-west-2');
```

```
psql=> SELECT * from aws_s3.query_export_to_s3('select * from sample_table', 'amzn-s3-demo-bucket', 'sample-filepath','us-west-2','format text');
```

aws_commons.create_s3_uri

Crea una estructura `aws_commons._s3_uri_1` para contener la información de archivos de Amazon S3. Debe utilizar los resultados de la función `aws_commons.create_s3_uri` en el parámetro `s3_info` de la función aws_s3.query_export_to_s3. Para ver un ejemplo de uso de la función `aws_commons.create_s3_uri`, consulte Especificación de la ruta del archivo de Amazon S3 a exportar.

Sintaxis

```
aws_commons.create_s3_uri(
   bucket text,
   file_path text,
   region text
)
```

Parámetros de entrada

bucket

Cadena de texto obligatoria que contiene el nombre del bucket de Amazon S3 del archivo.

file_path

Cadena de texto requerida que contiene la ruta de Amazon S3 del archivo.

region

Cadena de texto obligatoria que contiene la región de AWS en la que se encuentra el archivo. Para ver una lista de los nombres de regiones de AWS y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

Solución de errores de acceso a Amazon S3

Si se producen problemas de conexión al intentar exportar los datos a Amazon S3, confirme primero que las reglas de acceso saliente del grupo de seguridad de la VPC asociado a la instancia de base de datos permitan la conectividad de red. En concreto, el grupo de seguridad debe tener una regla que permita que la instancia de base de datos envíe tráfico TCP al puerto 443 y a cualquier dirección

IPv4 (0.0.0.0/0). Para obtener más información, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

También consulte las recomendaciones siguientes:

- Solución de problemas de identidades y accesos en Amazon RDS
- Solución de problemas de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service
- Solución de problemas de Amazon S3 e IAM en la Guía del usuario de IAM

Invocación de una función de AWS Lambda desde una instancia de base de datos de RDS for PostgreSQL

AWS Lambda es un servicio de computación controlado por eventos que permite ejecutar código sin aprovisionar ni administrar servidores. Está disponible para su uso con muchos servicios de AWS, incluidos RDS for PostgreSQL. Por ejemplo, puede utilizar funciones de Lambda para procesar notificaciones de eventos desde una base de datos o para cargar datos desde archivos cada vez que se carga un nuevo archivo en Simple Storage Service (Amazon S3). Para obtener más información sobre Lambda, consulte ¿Qué es AWS Lambda? en la Guía para desarrolladores de AWS Lambda.

> **Note**
>
> La invocación de una función de AWS Lambda se admite en estas versiones de RDS for PostgreSQL:
>
> - Todas las versiones 17 de PostgreSQL
> - Todas las versiones 16 de PostgreSQL
> - Todas las versiones 15 de PostgreSQL
> - PostgreSQL 14.1 y versiones secundarias posteriores
> - PostgreSQL 13.2 y versiones secundarias posteriores
> - PostgreSQL 12.6 y versiones secundarias posteriores

La configuración de RDS for PostgreSQL para trabajar con las funciones de Lambda es un proceso de varios pasos que incluye AWS Lambda, IAM, su VPC y su instancia de base de datos de RDS for PostgreSQL. A continuación, se muestran resúmenes de los pasos necesarios.

Para obtener más información acerca de las funciones de Lambda, consulte Introducción a Lambda y Conceptos básicos de AWS Lambda en la Guía para desarrolladores de AWS Lambda.

Temas

- Paso 1: configure la instancia de base de datos de RDS for PostgreSQL para conexiones salientes a AWS Lambda.
- Paso 2: configure IAM para su instancia de base de datos de RDS for PostgreSQL y AWS Lambda.

- Paso 3: instale la extensión de aws_lambda para una instancia de base de datos de RDS for PostgreSQL
- Paso 4: utilice las funciones auxiliares de Lambda con su instancia de base de datos de RDS for PostgreSQL (Opcional)
- Paso 5: invoque una función de Lambda desde su instancia de base de datos de RDS for PostgreSQL
- Paso 6: Conceder permiso a otros usuarios para invocar las funciones de Lambda
- Ejemplos: invoque las funciones de Lambda desde su instancia de base de datos de RDS for PostgreSQL
- Mensajes de error de la función de Lambda
- Referencia de parámetros y funciones de AWS Lambda

Paso 1: configure la instancia de base de datos de RDS for PostgreSQL para conexiones salientes a AWS Lambda.

Las funciones de Lambda siempre se ejecutan dentro de una Amazon VPC propiedad del servicio de AWS Lambda. Lambda aplica acceso a la red y reglas de seguridad a esta VPC y mantiene y supervisa la VPC automáticamente. Su instancia de base de datos de RDS for PostgreSQL envía tráfico de red a la VPC del servicio de Lambda. La manera en que se configura esto depende de si la instancia de base de datos es pública o privada.

- Instancia de base de datos de RDS for PostgreSQL pública: una instancia de base de datos es pública si se encuentra en una subred pública de la VPC y si la propiedad “PubliclyAccessible” de la instancia es `true`. Para encontrar el valor de esta propiedad, puede utilizar el comando describe-db-instances de AWS CLI. O, si lo desea, puede utilizar AWS Management Console para abrir la pestaña Connectivity & security (Conectividad y seguridad) y verificar que Publicly accessible (Acceso público) sea Yes (Sí). Para comprobar que la instancia está en la subred pública de la VPC, puede utilizar la AWS Management Console o la AWS CLI.

  Para configurar el acceso a Lambda, utilice la AWS Management Console o la AWS CLI para crear una regla de salida en el grupo de seguridad de la VPC. La regla de salida especifica que TCP puede utilizar el puerto 443 para enviar paquetes a cualquier dirección IPv4 (0.0.0.0/0).
- Clúster Instancia de base de datos de RDS PostgreSQL: en este caso, la propiedad “PubliclyAccessible” de la instancia es `false` o está en una subred privada. Para permitir el funcionamiento de la instancia con Lambda, puede utilizar una puerta de enlace de traducción

de direcciones de red (NAT). Para obtener más información, consulte Puerta de enlace NAT. O bien, puede configurar su VPC con un punto de conexión de VPC para Lambda. Para obtener más información, consulte Puntos de enlace de la VPC en la Guía del usuario de Amazon VPC. El punto de conexión responde a las llamadas hechas por su instancia de base de datos de RDS para PostgreSQL a las funciones de Lambda. El punto de conexión de VPC utiliza su propia resolución DNS privada. RDS for PostgreSQL no puede utilizar el punto de conexión de VPC de Lambda hasta que cambie el valor de `rds.custom_dns_resolution` de su valor predeterminado 0 (no habilitado) a 1. Para ello:

- Cree un grupo de parámetros de base de datos personalizado.
- Cambie el valor del parámetro `rds.custom_dns_resolution` del valor predeterminado de `0` a `1`.
- Modifique la instancia de base de datos para usar el grupo de parámetros de base de datos personalizado.
- Reinicie la instancia para que el parámetro modificado tenga efecto.

La VPC ahora puede interactuar con la VPC de AWS Lambda en el ámbito de red. A continuación, debe configurar los permisos mediante IAM.

Paso 2: configure IAM para su instancia de base de datos de RDS for PostgreSQL y AWS Lambda.

La invocación de funciones de Lambda desde su instancia de base de datos de RDS for PostgreSQL requiere ciertos privilegios. Para configurar los privilegios necesarios, recomendamos crear una política de IAM que permita invocar funciones de Lambda, asignarla a un rol y, a continuación, aplicar el rol a su instancia de base de datos. Este enfoque da a la instancia de base de datos privilegios para invocar la función de Lambda especificada en su nombre. En los pasos siguientes se muestra cómo hacer esto con AWS CLI.

Para configurar los permisos de IAM para utilizar su instancia de Amazon RDS con Lambda, lleve a cabo el siguiente procedimiento.

1. Utilice el comando create-policy de AWS CLI para crear una política de IAM que permita a su instancia de base de datos de RDS for PostgreSQL invocar la función de Lambda especificada. (El ID de instrucción [Sid] es una descripción opcional de la instrucción de política y no afecta al uso). Esta política proporciona a su instancia de base de datos los permisos mínimos necesarios para invocar la función de Lambda especificada.

```
aws iam create-policy  --policy-name rds-lambda-policy --policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "AllowAccessToExampleFunction",
        "Effect": "Allow",
        "Action": "lambda:InvokeFunction",
        "Resource": "arn:aws:lambda:aws-region:444455556666:function:my-function"
        }
    ]
}'
```

También puede utilizar la política predefinida de `AWSLambdaRole` que le permite invocar cualquiera de las funciones de Lambda. Para obtener más información, consulte Políticas de IAM basadas en identidades para Lambda.

2. Utilice el comando de la AWS CLI create-role para crear un rol de IAM que la política pueda asumir en tiempo de ejecución.

```
aws iam create-role  --role-name rds-lambda-role --assume-role-policy-document '{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
            "Service": "rds.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
        }
    ]
}'
```

3. Aplique la política al rol mediante el comando attach-role-policy de AWS CLI.

```
aws iam attach-role-policy \
    --policy-arn arn:aws:iam::444455556666:policy/rds-lambda-policy \
    --role-name rds-lambda-role --region aws-region
```

4. Aplique el rol a su instancia de base de datos de RDS for PostgreSQL mediante el comando add-role-to-db-instance de la AWS CLI. En este último paso se permite a los usuarios de bases de datos de su instancia de base de datos invocar funciones de Lambda.

```
aws rds add-role-to-db-instance \
       --db-instance-identifier my-instance-name \
       --feature-name Lambda \
       --role-arn  arn:aws:iam::444455556666:role/rds-lambda-role   \
       --region aws-region
```

Con la VPC y las configuraciones de IAM completadas, ahora puede instalar la extensión de `aws_lambda`. (Tenga en cuenta que puede instalar la extensión en cualquier momento, pero hasta que no configure la compatibilidad con VPC y los privilegios de IAM correctos, la extensión de `aws_lambda` no agrega nada a las capacidades de su instancia de base de datos de RDS for PostgreSQL.

Paso 3: instale la extensión de **`aws_lambda`** para una instancia de base de datos de RDS for PostgreSQL

Para utilizar AWS Lambda con su instancia de base de datos de RDS para PostgreSQL, agregue la extensión de PostgreSQL de `aws_lambda` a su instancia de base de datos de RDS para PostgreSQL. Esta extensión proporciona a su instancia de base de datos de RDS for PostgreSQL la capacidad de llamar a funciones de Lambda desde PostgreSQL.

Para instalar la extensión de **`aws_lambda`** en su instancia de base de datos de RDS for PostgreSQL

Utilice la línea de comandos `psql` de PostgreSQL o la herramienta pgAdmin para conectarse a su instancia de base de datos de RDS for PostgreSQL.

1. Conéctese a su instancia de base de datos de RDS for PostgreSQL como usuario con privilegios de `rds_superuser`. El valor predeterminado de usuario de `postgres` se muestra en el ejemplo.

   ```
   psql -h instance.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
   ```

2. Instale la extensión de `aws_lambda`. La extensión de `aws_commons` también es necesaria. Proporciona funciones auxiliares para `aws_lambda` y muchas otras extensiones de Aurora para PostgreSQL. Si aún no está en su instancia de base de datos de RDS for PostgreSQL, se instala con `aws_lambda` como se muestra a continuación.

   ```
   CREATE EXTENSION IF NOT EXISTS aws_lambda CASCADE;
   NOTICE:  installing required extension "aws_commons"
   ```

```
CREATE EXTENSION
```

La extensión de `aws_lambda` se instala en su instancia de base de datos Ahora puede crear estructuras de conveniencia para invocar las funciones de Lambda.

Paso 4: utilice las funciones auxiliares de Lambda con su instancia de base de datos de RDS for PostgreSQL (Opcional)

Puede utilizar las funciones auxiliares en la extensión de `aws_commons` para preparar entidades que puede invocar con más facilidad desde PostgreSQL. Para ello, debe tener la siguiente información sobre las funciones de Lambda:

- Nombre de la función: el nombre, el nombre de recurso de Amazon (ARN), la versión o el alias de la función de Lambda. La política de IAM creada en Paso 2: configure IAM para su instancia y Lambda requiere el ARN, por lo que recomendamos utilizar el ARN de su función.
- Región de AWS: (Opcional) la región de AWS en la que se encuentra la función de Lambda si no se encuentra en la misma región que su instancia de base de datos de RDS for PostgreSQL.

Para mantener la información del nombre de la función Lambda, utilice la función aws_commons.create_lambda_function_arn. Esta función auxiliar crea una estructura compuesta de `aws_commons._lambda_function_arn_1` con los detalles necesarios para la función de invocación. A continuación, encontrará tres enfoques alternativos para configurar esta estructura compuesta.

```
SELECT aws_commons.create_lambda_function_arn(
   'my-function',
   'aws-region'
) AS aws_lambda_arn_1 \gset
```

```
SELECT aws_commons.create_lambda_function_arn(
   '111122223333:function:my-function',
   'aws-region'
) AS lambda_partial_arn_1 \gset
```

```
SELECT aws_commons.create_lambda_function_arn(
   'arn:aws:lambda:aws-region:111122223333:function:my-function'
) AS lambda_arn_1 \gset
```

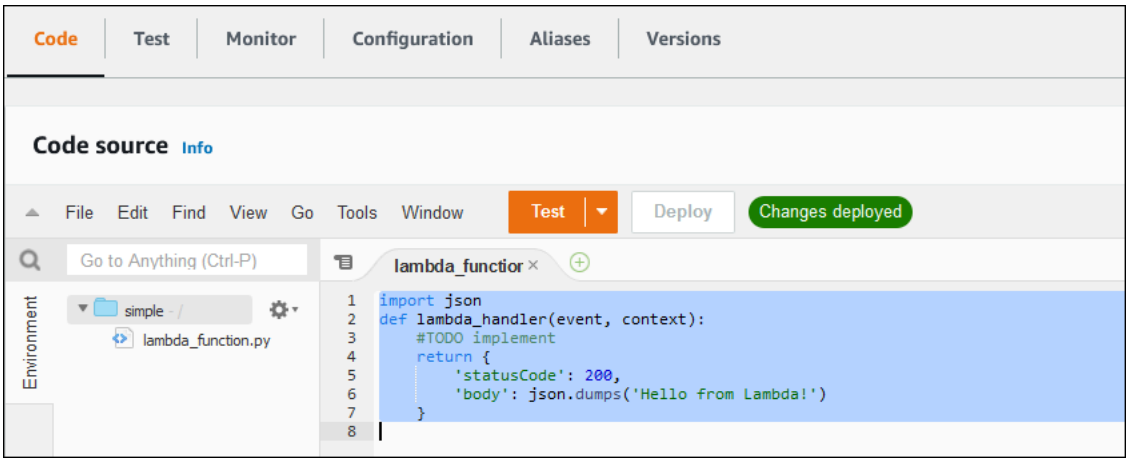
Cualquiera de estos valores se puede utilizar en las llamadas a la función aws_lambda.invoke. Para ver ejemplos, consulta Paso 5: invoque una función de Lambda desde su instancia de base de datos de RDS for PostgreSQL.

Paso 5: invoque una función de Lambda desde su instancia de base de datos de RDS for PostgreSQL

La función `aws_lambda.invoke` se comporta de forma sincrónica o asíncrona, según `invocation_type`. Las dos alternativas para este parámetro son `RequestResponse` (el valor predeterminado) y `Event`, como se muestra a continuación.

- **`RequestResponse`**: este tipo de invocación es sincrónico. Es el comportamiento predeterminado cuando la llamada se hace sin especificar un tipo de invocación. La carga de respuesta incluye los resultados de la función `aws_lambda.invoke`. Utilice este tipo de invocación cuando el flujo de trabajo requiera recibir los resultados de la función de Lambda antes de continuar.
- **`Event`**: este tipo de invocación es asíncrono. La respuesta no incluye una carga que contenga resultados. Utilice este tipo de invocación cuando el flujo de trabajo no necesite un resultado de la función de Lambda para continuar con el procesamiento.

Como simple prueba de la configuración, puede conectarse a la instancia de base de datos mediante `psql` e invocar una función de ejemplo desde la línea de comandos. Supongamos que tiene una de las funciones básicas configuradas en su servicio Lambda, como la sencilla función de Python que se muestra en la siguiente captura de pantalla.



Para invocar una función de ejemplo

1. Conéctese a la instancia de base de datos con `psql` o pgAdmin.

```
psql -h instance.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
```

2. Invoque la función mediante su ARN.

```
SELECT * from
 aws_lambda.invoke(aws_commons.create_lambda_function_arn('arn:aws:lambda:aws-
region:444455556666:function:simple', 'us-west-1'), '{"body": "Hello from
 Postgres!"}'::json );
```

La respuesta tiene el siguiente aspecto.

```
status_code |                        payload                         |
 executed_version | log_result
-------------+--------------------------------------------------------
+------------------+------------
         200 | {"statusCode": 200, "body": "\"Hello from Lambda!\""} | $LATEST
     |
(1 row)
```

Si el intento de invocación no se lleva a cabo correctamente, consulte Mensajes de error de la función de Lambda .

Paso 6: Conceder permiso a otros usuarios para invocar las funciones de Lambda

En este punto de los procedimientos, solo usted como `rds_superuser` puede invocar las funciones de Lambda. Para permitir que otros usuarios puedan invocar cualquier función que haya creado usted, deberá otorgarles permiso.

Para otorgar permiso para invocar una función de Lambda

1. Conéctese a la instancia de base de datos con `psql` o pgAdmin.

```
psql -h instance.444455556666.aws-region.rds.amazonaws.com -U postgres -p 5432
```

2. Ejecute los siguientes comandos SQL:

```
postgres=>  GRANT USAGE ON SCHEMA aws_lambda TO db_username;
```

```
GRANT EXECUTE ON ALL FUNCTIONS IN SCHEMA aws_lambda TO db_username;
```

Ejemplos: invoque las funciones de Lambda desde su instancia de base de datos de RDS for PostgreSQL

A continuación, puede encontrar varios ejemplos de llamada a la función de aws_lambda.invoke. La mayoría de ejemplos utilizan la estructura compuesta `aws_lambda_arn_1` que se crea en Paso 4: utilice las funciones auxiliares de Lambda con su instancia de base de datos de RDS for PostgreSQL (Opcional) para simplificar la transferencia de los detalles de la función. Para obtener un ejemplo de invocación asincrónica, consulte Ejemplo: invocación asincrónica (Event) de funciones de Lambda. El resto de ejemplos enumerados utilizan la invocación sincrónica.

Para obtener más información acerca de los tipos de invocación de Lambda, consulte Invocación de funciones de Lambda en la Guía para desarrolladores de AWS Lambda. Para obtener más información acerca de `aws_lambda_arn_1`, consulte aws_commons.create_lambda_function_arn.

Lista de ejemplos

- Ejemplo: invocación sincrónica (RequestResponse) de funciones de Lambda
- Ejemplo: invocación asincrónica (Event) de funciones de Lambda
- Ejemplo: captura del registro de ejecución de Lambda en una respuesta de función
- Ejemplo: inclusión del contexto del cliente en una función Lambda
- Ejemplo: invocación de una versión específica de una función de Lambda

Ejemplo: invocación sincrónica (RequestResponse) de funciones de Lambda

Lo que sigue son dos ejemplos de una invocación de función de Lambda sincrónica. Los resultados de estas llamadas de funciones de `aws_lambda.invoke` son iguales.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json);
```

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json, 'RequestResponse');
```

Los parámetros se describen de la siguiente manera:

- `:'aws_lambda_arn_1'`: este parámetro identifica la estructura compuesta creada en Paso 4: utilice las funciones auxiliares de Lambda con su instancia de base de datos de RDS for PostgreSQL (Opcional), con la función auxiliar de `aws_commons.create_lambda_function_arn`. También puede crear esta estructura en línea dentro de su llamada de `aws_lambda.invoke` de la siguiente manera.

```
SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-function',
 'aws-region'),
'{"body": "Hello from Postgres!"}'::json
);
```

- `'{"body": "Hello from PostgreSQL!"}'::json` – La carga útil JSON que se va a pasar a la función Lambda.
- `'RequestResponse'` – El tipo de invocación Lambda.

Ejemplo: invocación asincrónica (Event) de funciones de Lambda

Lo que sigue es un ejemplo de una invocación de función asincrónica Lambda. El tipo de invocación `Event` programa la invocación de la función Lambda con la carga útil de entrada especificada y regresa inmediatamente. Utilice el tipo de invocación `Event` en ciertos flujos de trabajo que no dependen de los resultados de la función Lambda.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json, 'Event');
```

Ejemplo: captura del registro de ejecución de Lambda en una respuesta de función

Puede incluir los últimos 4 KB del registro de ejecución en la respuesta de función mediante el parámetro `log_type` en su llamada a funciones de `aws_lambda.invoke`. De forma predeterminada, este parámetro se establece en `None`, pero puede especificar `Tail` para capturar los resultados del registro de ejecución de Lambda en la respuesta, como se muestra a continuación.

```
SELECT *, select convert_from(decode(log_result, 'base64'), 'utf-8') as log FROM
 aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}'::json,
 'RequestResponse', 'Tail');
```

Establezca el parámetro aws_lambda.invoke de la función `log_type` en `Tail` para incluir el registro de ejecución en la respuesta. El valor predeterminado para el parámetro `log_type` es `None`.

El `log_result` que se devuelve es una cadena codificada `base64`. Puede decodificar el contenido utilizando una combinación de las funciones `decode` y `convert_from` PostgreSQL.

Para obtener más información acerca de `log_type`, consulte aws_lambda.invoke.

Ejemplo: inclusión del contexto del cliente en una función Lambda

La función `aws_lambda.invoke` tiene un parámetro `context` que puede utilizar para pasar la información por separado de la carga, como se muestra a continuación.

```
SELECT *, convert_from(decode(log_result, 'base64'), 'utf-8') as log FROM
 aws_lambda.invoke(:'aws_lambda_arn_1', '{"body": "Hello from Postgres!"}'::json,
 'RequestResponse', 'Tail');
```

Para incluir el contexto del cliente, utilice un objeto JSON para el parámetro aws_lambda.invoke de la función `context`.

Para obtener más información sobre los parámetros de `context`, consulte la referencia de aws_lambda.invoke.

Ejemplo: invocación de una versión específica de una función de Lambda

Se puede especificar una versión concreta de una función de Lambda mediante el parámetro `qualifier` con la llamada de `aws_lambda.invoke`. A continuación, encontrará información sobre el ejemplo que hace esto mediante '*`custom_version`*' como alias de la versión.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json, 'RequestResponse', 'None', NULL, 'custom_version');
```

Además, puede proporcionar un calificador de función de Lambda con los detalles del nombre de función en su lugar de la siguiente manera.

```
SELECT * FROM aws_lambda.invoke(aws_commons.create_lambda_function_arn('my-
function:custom_version', 'us-west-2'),
'{"body": "Hello from Postgres!"}'::json);
```

Para obtener más información acerca de `qualifier` y otros parámetros, consulte la referencia de aws_lambda.invoke.

Mensajes de error de la función de Lambda

En la siguiente lista encontrará información sobre los mensajes de error, con posibles causas y soluciones.

- Problemas de configuración de la VPC

  Los problemas de configuración de la VPC pueden generar los siguientes mensajes de error al intentar conectarse:

  ```
  ERROR:  invoke API failed
  DETAIL: AWS Lambda client returned 'Unable to connect to endpoint'.
  CONTEXT:  SQL function "invoke" statement 1
  ```

  Una causa común de este error es configurar erróneamente el grupo de seguridad de la VPC. Asegúrese de tener abierta una regla de salida para TCP en el puerto 443 de su grupo de seguridad de la VPC para que la VPC pueda conectarse a la VPC de Lambda.

  Si la instancia de base de datos es privada, verifique la configuración de DNS privada de la VPC. Asegúrese de establecer el parámetro de `rds.custom_dns_resolution` en 1 y configure AWS PrivateLink tal como se describe en Paso 1: configure la instancia de base de datos de RDS for PostgreSQL para conexiones salientes a AWS Lambda.. Para obtener más información, consulte Puntos de conexión de VPC de la interfaz (AWS PrivateLink).
- Falta de permisos necesarios para invocar funciones de Lambda

  Si ve alguno de los siguientes mensajes de error, significa que el usuario (rol) que invoca la función no tiene los permisos adecuados.

  ```
  ERROR:  permission denied for schema aws_lambda
  ```

  ```
  ERROR:  permission denied for function invoke
  ```

  Se deben otorgar permisos específicos a un usuario (rol) para que pueda invocar funciones de Lambda. Para obtener más información, consulte Paso 6: Conceder permiso a otros usuarios para invocar las funciones de Lambda.
- Gestión incorrecta de errores en las funciones de Lambda

Si una función Lambda lanza una excepción durante el procesamiento de la solicitud, `aws_lambda.invoke` se produce un error de PostgreSQL como el siguiente.

```
SELECT * FROM aws_lambda.invoke('aws_lambda_arn_1', '{"body": "Hello from
 Postgres!"}'::json);
ERROR:  lambda invocation failed
DETAIL:  "arn:aws:lambda:us-west-2:555555555555:function:my-function" returned error
 "Unhandled", details: "<Error details string>".
```

Asegúrese de controlar los errores en las funciones de Lambda o en la aplicación de PostgreSQL.

Referencia de parámetros y funciones de AWS Lambda

A continuación, se presenta la referencia de las funciones y parámetros que se pueden utilizar para invocar Lambda con RDS para PostgreSQL.

Funciones y parámetros

- aws_lambda.invoke
- aws_commons.create_lambda_function_arn
- Parámetros de aws_lambda

aws_lambda.invoke

Ejecuta una Lambda función destinada a un de datos RDS para la instancia de base de datos PostgreSQL.

Para obtener más detalles acerca de la invocación de funciones de Lambda, consulte también Invoke en la guía para desarrolladores de AWS Lambda.

Sintaxis

JSON

```
aws_lambda.invoke(
IN function_name TEXT,
IN payload JSON,
IN region TEXT DEFAULT NULL,
IN invocation_type TEXT DEFAULT 'RequestResponse',
```

```
IN log_type TEXT DEFAULT 'None',
IN context JSON DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSON,
OUT executed_version TEXT,
OUT log_result TEXT)
```

```
aws_lambda.invoke(
IN function_name aws_commons._lambda_function_arn_1,
IN payload JSON,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSON DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSON,
OUT executed_version TEXT,
OUT log_result TEXT)
```

JSONB

```
aws_lambda.invoke(
IN function_name TEXT,
IN payload JSONB,
IN region TEXT DEFAULT NULL,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSONB DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
OUT status_code INT,
OUT payload JSONB,
OUT executed_version TEXT,
OUT log_result TEXT)
```

```
aws_lambda.invoke(
IN function_name aws_commons._lambda_function_arn_1,
IN payload JSONB,
IN invocation_type TEXT DEFAULT 'RequestResponse',
IN log_type TEXT DEFAULT 'None',
IN context JSONB DEFAULT NULL,
IN qualifier VARCHAR(128) DEFAULT NULL,
```

```
OUT status_code INT,
OUT payload JSONB,
OUT executed_version TEXT,
OUT log_result TEXT
)
```

Parámetros de entrada

function_name

El nombre de identificación de la función Lambda. El valor puede ser el nombre de la función, un ARN o un ARN parcial. Para obtener una lista de los formatos posibles, consulte los formatos de nombres de función de Lambda en la guía para desarrolladores de AWS Lambda.

payload

La entrada de la función Lambda. El formato puede ser JSON o JSONB. Para obtener más información, consulte la documentación de PostgreSQL sobre Tipos de JSON.

region

(Opcional) La región Lambda de la función. De forma predeterminada, RDS resuelve la región de AWS desde el ARN completo en `function_name` o utiliza la región de instancia de base de datos de RDS for PostgreSQL. Si este valor de región entra en conflicto con el proporcionado en el ARN `function_name`, se genera un error.

invocation_type

Tipo de invocación de la función Lambda. El valor distingue entre mayúsculas y minúsculas. Entre los valores posibles se incluyen:

- `RequestResponse` – El valor de tiempo de espera predeterminado. Este tipo de invocación para una función Lambda es sincrónica y devuelve una carga útil de respuesta en el resultado. Utilice el tipo de invocación de `RequestResponse` cuando el flujo de trabajo dependa de recibir el resultado de la función Lambda inmediatamente.
- `Event` – Este tipo de invocación para una función Lambda es asincrónica y regresa inmediatamente sin una carga útil devuelta. Utilice el tipo de invocación `Event` cuando no necesite resultados de la función Lambda antes de que el flujo de trabajo avance.
- `DryRun` – Este tipo de invocación prueba el acceso sin ejecutar la función Lambda.

log_type

El tipo de registro Lambda que se va a devolver en el parámetro `log_result` de salida. El valor distingue entre mayúsculas y minúsculas. Entre los valores posibles se incluyen:

- Final – El parámetro de salida `log_result` devuelto incluirá los últimos 4 KB del registro de ejecución.
- Ninguno – No se devuelve ninguna información de registro Lambda.

context

Contexto del cliente en formato JSON o JSONB. Los campos que se van a utilizar incluyen `custom` y `env`.

Calificador

Un calificador que identifica la versión de una función Lambda que se va a invocar. Si este valor entra en conflicto con uno proporcionado en el ARN `function_name`, se genera un error.

Parámetros de salida

status_code

Un código de respuesta de estado HTTP. Para obtener más información, consulte los elementos de respuesta de invocación de Lambda en la guía para desarrolladores de AWS Lambda.

payload

La información devuelta de la función Lambda que se ejecutó. El formato está en JSON o JSONB.

executed_version

La versión de la función Lambda que se ejecutó.

log_result

La información del registro de ejecución devuelta si el valor `log_type` es `Tail` cuando se invocó la función Lambda. El resultado contiene los últimos 4 KB del registro de ejecución codificado en Base64.

aws_commons.create_lambda_function_arn

Crea una estructura `aws_commons._lambda_function_arn_1` para contener la información del nombre de función Lambda. Puede utilizar los resultados de la función `aws_commons.create_lambda_function_arn` en el parámetro `function_name` de la función aws_lambda.invoke aws_lambda.invoke.

Sintaxis

```
aws_commons.create_lambda_function_arn(
    function_name TEXT,
    region TEXT DEFAULT NULL
    )
    RETURNS aws_commons._lambda_function_arn_1
```

Parámetros de entrada

function_name

Una cadena de texto obligatoria que contiene el nombre de la función Lambda. El valor puede ser un nombre de función, un ARN parcial o un ARN completo.

region

Una cadena de texto opcional que contiene la región de AWS en la que se encuentra la función de Lambda. Para ver una lista de los nombres de regiones de y los valores asociados, consulte Regiones, zonas de disponibilidad y Local Zones.

Parámetros de aws_lambda

En esta tabla verá los parámetros asociados a la función `aws_lambda`.

Parámetro	Descripción
`aws_lambda.connect_timeout_ms`	Se trata de un parámetro dinámico y establece el tiempo máximo de espera durante la conexión a AWS Lambda. El valor predeterminado es `1000`. Los valores permitidos para este parámetro son de 1 a 900 000.
`aws_lambda.request_timeout_ms`	Se trata de un parámetro dinámico y establece el tiempo máximo de espera a la respuesta de AWS Lambda. El valor

Parámetro	Descripción
	predeterminado es `3000`. Los valores permitidos para este parámetro son de 1 a 900 000.
`aws_lambda.endpoint_override`	Especifica el punto de conexión que se puede utilizar para conectarse a AWS Lambda. Una cadena vacía selecciona el punto de conexión de AWS Lambda predeterminado para la región. Debe reiniciar la base de datos para que se aplique el cambio en este parámetro estático.

Tareas comunes de los administradores de base de datos (DBA) para Amazon RDS para PostgreSQL

Los administradores de bases de datos (DBA) realizan una variedad de tareas cuando administran una instancia de base de datos de Amazon RDS para PostgreSQL. Si ya está familiarizado con PostgreSQL, debe conocer algunas de las diferencias importantes entre ejecutar PostgreSQL en su hardware y RDS para PostgreSQL. Por ejemplo, debido a que es un servicio administrado, Amazon RDS no permite el acceso mediante shell a las instancias de base de datos. Eso significa que no tiene acceso directo a `pg_hba.conf` y a otros archivos de configuración. En el caso de RDS para PostgreSQL, los cambios que normalmente se realizan en el archivo de configuración de PostgreSQL de una instancia local se realizan en un grupo de parámetros de base de datos personalizado asociado a la instancia de base de datos de RDS para PostgreSQL. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

Tampoco puede acceder a los archivos de registro de la misma manera que lo hace con una instancia de PostgreSQL en las instalaciones. Para obtener más información acerca de los registros, consulte Archivos de registro de bases de datos de RDS para PostgreSQL.

Otro ejemplo, no tiene acceso a la cuenta de `superuser` de PostgreSQL. En RDS para PostgreSQL, el rol `rds_superuser` es el más privilegiado, y se concede a `postgres` en el momento de la configuración. Ya sea que esté familiarizado con el uso de PostgreSQL en las instalaciones o completamente nuevo en RDS para PostgreSQL, le recomendamos que aprenda el rol `rds_superuser` y cómo trabajar con roles, usuarios, grupos y permisos. Para obtener más información, consulte Descripción de los roles y permisos de PostgreSQL.

Las siguientes son algunas tareas comunes de DBA para RDS for PostgreSQL.

Temas

- Intercalaciones admitidas en RDS para PostgreSQL
- Descripción de los roles y permisos de PostgreSQL
- Gestión de conexiones inactivas en PostgreSQL
- Uso de autovacuum de PostgreSQL en Amazon RDS para PostgreSQL
- Uso de mecanismos de registro admitidos por RDS for PostgreSQL
- Administración de archivos temporales con PostgreSQL
- Uso de pgBadger para el análisis de registros con PostgreSQL

- Uso de PGSnapper para supervisar PostgreSQL
- Uso de parámetros en su instancia de base de datos de RDS for PostgreSQL

Intercalaciones admitidas en RDS para PostgreSQL

Las intercalaciones son un conjunto de reglas que determinan cómo se ordenan y comparan las cadenas de caracteres almacenadas en la base de datos. Las intercalaciones desempeñan un papel fundamental en el sistema de computación y se incluyen como parte del sistema operativo. Las intercalaciones cambian con el tiempo cuando se añaden nuevos caracteres a los lenguajes o cuando cambian las reglas de ordenación.

Las bibliotecas de intercalaciones definen reglas y algoritmos específicos para una intercalación. Las bibliotecas de intercalaciones más populares utilizadas en PostgreSQL son GNU C (glibc) y los componentes de internacionalización de Unicode (ICU). De forma predeterminada, RDS para PostgreSQL utiliza la intercalación glibc, que incluye ordenaciones de caracteres Unicode para secuencias de caracteres de varios bytes.

Al crear una nueva instancia de base de datos en RDS para PostgreSQL, se comprueba en el sistema operativo la intercalación disponible. Los parámetros de PostgreSQL del comando `CREATE DATABASE` `LC_COLLATE` y `LC_CTYPE` se utilizan para especificar una intercalación, que es la intercalación predeterminada en esa base de datos. Como alternativa, también puede utilizar el parámetro `LOCALE` en `CREATE DATABASE` para establecer estos parámetros. Esto determina la intercalación predeterminada de las cadenas de caracteres de la base de datos y las reglas para clasificar los caracteres como letras, números o símbolos. También puede elegir una intercalación para utilizarla en una columna, un índice o una consulta.

RDS para PostgreSQL depende de la biblioteca glibc del sistema operativo para admitir las intercalaciones. La instancia de RDS para PostgreSQL se actualiza periódicamente con las versiones más recientes del sistema operativo. Estas actualizaciones a veces incluyen una versión más reciente de la biblioteca glibc. En raras ocasiones, las versiones más recientes de glibc cambian la ordenación o la intercalación de algunos caracteres, lo que puede provocar que los datos se ordenen de forma diferente o generar entradas de índice no válidas. Si durante una actualización detecta problemas de ordenación para la intercalación, es posible que tenga que volver a generar los índices.

Para reducir el posible impacto de las actualizaciones de glibc, RDS para PostgreSQL incluye ahora una biblioteca de intercalaciones predeterminada independiente. Esta biblioteca de intercalaciones está disponible en RDS para PostgreSQL 14.6, 13.9, 12.13, 11.18, 10.23 y versiones secundarias

posteriores. Es compatible con glibc 2.26-59.amzn2 y proporciona estabilidad en la ordenación para evitar resultados de consultas incorrectos.

Descripción de los roles y permisos de PostgreSQL

Al crear una instancia de base de datos de RDS for PostgreSQL utilizando la AWS Management Console, se crea una cuenta de administrador al mismo tiempo. De forma predeterminada su nombre es `postgres`, tal y como se muestra en la siguiente captura de pantalla:



Puede elegir otro nombre en lugar de aceptar el valor predeterminado (`postgres`). Si lo hace, el nombre que elija debe empezar por una letra y tener entre 1 y 16 caracteres alfanuméricos. Por simplicidad, nos referimos a esta cuenta de usuario principal por su valor predeterminado (`postgres`) en toda esta guía.

Si utiliza `create-db-instance` de la AWS CLI en lugar de la AWS Management Console, crea el nombre pasándolo con el parámetro `master-username` en el comando. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS.

Ya sea que utilice la AWS Management Console, la AWS CLI o la API de Amazon RDS y si usa el nombre predeterminado `postgres` o elige otro nombre, esta primera cuenta de usuario de la base de datos es miembro del grupo `rds_superuser` y tiene `rds_superuser` privilegios.

Temas

- Descripción del rol rds_superuser
- Control del acceso de los usuarios a la base de datos de PostgreSQL
- Delegación y control de la administración de contraseñas de usuario
- Uso de SCRAM para el cifrado de contraseñas de PostgreSQL

Descripción del rol rds_superuser

En PostgreSQL, un rol puede definir un usuario, un grupo o un conjunto de permisos específicos concedidos a un grupo o usuario para varios objetos de la base de datos. Comandos de PostgreSQL para `CREATE USER` y `CREATE GROUP` se han sustituido por los más generales, `CREATE ROLE` con propiedades específicas para distinguir a los usuarios de bases de datos. Un usuario de base de datos se puede concebir como un rol con el privilegio LOGIN.

> **Note**
>
> Los comandos `CREATE USER` y `CREATE GROUP` se pueden seguir utilizando. Para obtener más información, consulte Roles de base de datos en la documentación de PostgreSQL.

El usuario `postgres` es el usuario de base de datos más privilegiado de la instancia de base de datos de RDS for PostgreSQL. Tiene las características definidas mediante la siguiente instrucción `CREATE ROLE`.

```
CREATE ROLE postgres WITH LOGIN NOSUPERUSER INHERIT CREATEDB CREATEROLE NOREPLICATION
 VALID UNTIL 'infinity'
```

Las propiedades `NOSUPERUSER`, `NOREPLICATION`, `INHERIT` y `VALID UNTIL 'infinity'` son las opciones predeterminadas de CREATE ROLE, a menos que se especifique lo contrario.

De forma predeterminada, `postgres` tiene privilegios otorgados al rol `rds_superuser` y permisos para crear roles y bases de datos. El rol `rds_superuser` permite al usuario `postgres` hacer lo siguiente:

- Añadir extensiones que estén disponibles para el uso con Amazon RDS. Para obtener más información, consulte Uso de las características de PostgreSQL admitidas por Amazon RDS para PostgreSQL
- Cree roles para los usuarios y conceder privilegios a los usuarios. Para obtener más información, consulte CREATE ROLE y GRANT en la documentación de PostgreSQL.
- Creación de bases de datos Para obtener más información, consulte CREATE DATABASE en la documentación de PostgreSQL.
- Conceder privilegios de `rds_superuser` a los roles de usuario que no tengan estos privilegios y revocarlos según sea necesario. Le recomendamos que conceda este rol solo a los usuarios que

realizan tareas de superusuario. En otras palabras, puede conceder este rol a los administradores de bases de datos (DBA) o a los administradores del sistema.

- Conceda (y revoque) el rol `rds_replication` a usuarios de bases de datos que no tengan el rol `rds_superuser`.
- Conceder (y revocar) el rol `rds_password` a usuarios de bases de datos que no tengan el rol `rds_superuser`.
- Obtener información de estado sobre todas las conexiones de base de datos mediante la vista `pg_stat_activity`. Cuando sea necesario, `rds_superuser` puede detener cualquier conexión mediante `pg_terminate_backend` o `pg_cancel_backend`.

En la instrucción `CREATE ROLE postgres...`, se puede ver que el rol de usuario `postgres` no permite específicamente permisos `superuser` de PostgreSQL. RDS for PostgreSQL es un servicio administrado, por lo que no puede acceder al sistema operativo host y no puede conectarse con la cuenta `superuser` de PostgreSQL. Muchas de las tareas que requieren acceso `superuser` en un PostgreSQL independiente se administra automáticamente mediante Amazon RDS.

Para obtener más información sobre la concesión de privilegios, consulte GRANT en la documentación de PostgreSQL.

El rol `rds_superuser` es uno de varios roles predefinidos en un Instancia de base de datos RDS for PostgreSQL.

> **Note**
>
> En PostgreSQL 13 y versiones anteriores, los roles predefinidos se denominan roles predeterminados.

En la siguiente lista encontrará algunos de los otros roles predefinidos que se crean automáticamente para un nuevo Instancia de base de datos RDS para PostgreSQL Los roles predefinidos y sus privilegios no se pueden cambiar. No se pueden eliminar, cambiar de nombre ni modificar los privilegios de estos roles predefinidos. Intentar realizar una de estas operaciones producirá un error.

- rds_password: rol que puede cambiar las contraseñas y configurar restricciones de contraseña para los usuarios de bases de datos. Al rol `rds_superuser` se le otorga este rol de forma

predeterminada y puede otorgarlo a los usuarios de la base de datos. Para obtener más información, consulte Control del acceso de los usuarios a la base de datos de PostgreSQL.

  - En las versiones de RDS para PostgreSQL anteriores a la 14, el rol `rds_password` puede cambiar las contraseñas y establecer restricciones de contraseña para los usuarios de la base de datos y los usuarios con el rol `rds_superuser`. A partir de la versión 14 de RDS para PostgreSQL, el rol `rds_password` puede cambiar las contraseñas y establecer restricciones de contraseña solo para los usuarios de la base de datos. Solo los usuarios con el rol `rds_superuser` pueden realizar estas acciones en otros usuarios con el rol `rds_superuser`.
- rdsadmin: rol creado para administrar muchas de las tareas de administración que el administrador con privilegios de `superuser` realizaría en una base de datos PostgreSQL independiente. Este rol lo utiliza internamente RDS for PostgreSQLpara muchas tareas de administración.
- rdstopmgr: rol que Amazon RDS utiliza internamente para admitir implementaciones multi-AZ.
- rds_reserved: función que Amazon RDS utiliza internamente para reservar conexiones a bases de datos.

Visualización los de roles y sus privilegios

Puede ver los roles predefinidos y sus privilegios en la instancia de base de datos de RDS para PostgreSQL mediante distintos comandos en función de la versión de PostgreSQL.

Para PostgreSQL 15 y versiones anteriores

Conéctese a la instancia de base de datos de RDS para PostgreSQL y use el comando \du en psql:

```
postgres=> \du
                                                   List of roles
    Role name    |                         Attributes                         |
                 Member of
-----------------+------------------------------------------------------------
+-------------------------------------------------
 postgres        | Create role, Create DB                                    +|
 {rds_superuser}
                 | Password valid until infinity                              |
 rds_ad          | Cannot login                                               | {}
 rds_iam         | Cannot login                                               | {}
 rds_password    | Cannot login                                               | {}
 rds_replication | Cannot login                                               | {}
 rds_superuser   | Cannot login                                               |
 {pg_monitor,pg_signal_backend,rds_password,rds_replication}
```

```
 rdsadmin        | Superuser, Create role, Create DB, Replication, Bypass RLS+| {}
                 | Password valid until infinity                              |
```

Para PostgreSQL 16 y versiones posteriores

A partir de PostgreSQL 16, utilice el comando `\drg+` para ver información detallada sobre la pertenencia a roles:

```
postgres=> \drg+
                              List of role grants
   Role name   |          Member of          |       Options       | Grantor
---------------+-----------------------------+---------------------+----------
 postgres      | rds_superuser               | INHERIT, SET        | rdsadmin
 rds_superuser | pg_checkpoint               | ADMIN, INHERIT, SET | rdsadmin
 rds_superuser | pg_monitor                  | ADMIN, INHERIT, SET | rdsadmin
 rds_superuser | pg_signal_backend           | ADMIN, INHERIT, SET | rdsadmin
 rds_superuser | pg_use_reserved_connections | ADMIN, INHERIT, SET | rdsadmin
 rds_superuser | rds_password                | ADMIN, INHERIT, SET | rdsadmin
 rds_superuser | rds_replication             | ADMIN, INHERIT, SET | rdsadmin
```

Para comprobar la pertenencia a roles independientemente de la versión de PostgreSQL, puede utilizar la siguiente consulta SQL:

```
SELECT m.rolname AS "Role name", r.rolname AS "Member of"
FROM pg_catalog.pg_roles m
JOIN pg_catalog.pg_auth_members pam ON (pam.member = m.oid)
LEFT JOIN pg_catalog.pg_roles r ON (pam.roleid = r.oid)
LEFT JOIN pg_catalog.pg_roles g ON (pam.grantor = g.oid)
WHERE m.rolname !~ '^pg_'
ORDER BY 1, 2;
```

En la salida, puede ver que `rds_superuser` no es un rol de usuario de base de datos (no puede iniciar sesión), pero tiene los privilegios de muchos otros roles. También puede ver que el usuario de la base de datos `postgres` es miembro del rol `rds_superuser`. Como se ha mencionado anteriormente, `postgres` es el valor predeterminado de Create database (Crear base de datos) de la consola de Amazon RDS. Si ha elegido otro nombre, ese nombre se muestra en la lista de roles.

Control del acceso de los usuarios a la base de datos de PostgreSQL

Las nuevas bases de datos de PostgreSQL siempre se crean con un conjunto predeterminado de privilegios en el esquema `public` de la base de datos que permite a todos los usuarios y roles de la

base de datos crear objetos. Estos privilegios permiten a los usuarios de la base de datos conectarse a la base de datos, or ejemplo, y crear tablas temporales mientras están conectados.

Para controlar mejor el acceso de los usuarios a las instancias de bases de datos que cree en su instancia de base de datos de RDS for PostgreSQL, le recomendamos que revoque estos privilegios de `public` predeterminados. Después de ello, conceda a continuación los privilegios específicos a los usuarios de base de datos de forma más detallada, como se muestra en el siguiente procedimiento.

Para configurar roles y privilegios para una nueva instancia de base de datos

Supongamos que está configurando una base de datos en Instancia de base de datos de RDS for PostgreSQL de reciente creación para que lo utilicen varios investigadores, todos los cuales necesitan acceso de lectura y escritura a la base de datos.

1. Use `psql` (o pgAdmin) para conectarse a su instancia de base de datos de RDS for PostgreSQL:

   ```
   psql --host=your-db-instance.666666666666.aws-region.rds.amazonaws.com --port=5432
    --username=postgres --password
   ```

   Escriba la contraseña cuando se le solicite. El cliente `psql` se conecta y muestra la base de datos de conexión administrativa predeterminada, `postgres=>`, como el símbolo del sistema.
2. Para evitar que los usuarios de la base de datos creen objetos en el esquema `public`, realice una de las siguientes opciones:

   ```
   postgres=> REVOKE CREATE ON SCHEMA public FROM PUBLIC;
   REVOKE
   ```
3. A continuación, cree una nueva instancia de base de datos:

   ```
   postgres=> CREATE DATABASE lab_db;
   CREATE DATABASE
   ```
4. Revoque todos los privilegios del esquema `PUBLIC` de esta nueva base de datos.

   ```
   postgres=> REVOKE ALL ON DATABASE lab_db FROM public;
   REVOKE
   ```
5. Cree un rol para los usuarios de bases de datos.

```
postgres=> CREATE ROLE lab_tech;
CREATE ROLE
```

6. Otorgue a los usuarios de bases de datos que tengan este rol la posibilidad de conectarse a la base de datos.

```
postgres=> GRANT CONNECT ON DATABASE lab_db TO lab_tech;
GRANT
```

7. Conceda a todos los usuarios que tengan el rol `lab_tech` todos los privilegios de esta base de datos.

```
postgres=> GRANT ALL PRIVILEGES ON DATABASE lab_db TO lab_tech;
GRANT
```

8. Cree usuarios de bases de datos de la siguiente manera:

```
postgres=> CREATE ROLE lab_user1 LOGIN PASSWORD 'change_me';
CREATE ROLE
postgres=> CREATE ROLE lab_user2 LOGIN PASSWORD 'change_me';
CREATE ROLE
```

9. Conceda a estos dos usuarios los privilegios asociados al rol lab_tech:

```
postgres=> GRANT lab_tech TO lab_user1;
GRANT ROLE
postgres=> GRANT lab_tech TO lab_user2;
GRANT ROLE
```

En este punto,`lab_user1` y `lab_user2` se pueden conectar a la base de datos de `lab_db`. En este ejemplo no se siguen las prácticas recomendadas para el uso empresarial, que pueden incluir la creación de varias instancias de base de datos, distintos esquemas y la concesión de permisos limitados. Para obtener más información y escenarios adicionales, consulte Administración de usuarios y roles de PostgreSQL.

Para obtener más información sobre los privilegios en las bases de datos de PostgreSQL, consulte el comando GRANT en la documentación de PostgreSQL.

Delegación y control de la administración de contraseñas de usuario

Como DBA, es posible que desee delegar la administración de contraseñas de usuario. O bien, puede que desee evitar que los usuarios de la base de datos cambien sus contraseñas o reconfiguren las restricciones de contraseña, como la duración de la contraseña. Para asegurarse de que solo los usuarios de la base de datos que elija puedan cambiar la configuración de contraseñas, puede activar la función de administración de contraseñas restringidas. Cuando activa esta función, solo pueden administrar contraseñas aquellos usuarios de base de datos a los que se les haya concedido el rol `rds_password`.

> **Note**
>
> Para utilizar la administración de contraseñas restringida, su instancia de base de datos RDS for PostgreSQL debe estar ejecutando para 10.6 o una versión posterior.

De forma predeterminada, esta función es `off`, tal y como se muestra en el ejemplo siguiente:

```
postgres=> SHOW rds.restrict_password_commands;
  rds.restrict_password_commands
--------------------------------
 off
(1 row)
```

Para activar esta función, utilice un grupo de parámetros personalizado y cambie la configuración de `rds.restrict_password_commands` a 1. Asegúrese de reiniciar su Instancia de base de datos de RDS for PostgreSQL para que la configuración surta efecto.

Con esta función activa, se necesitan privilegios de `rds_password` para los siguientes comandos SQL:

```
CREATE ROLE myrole WITH PASSWORD 'mypassword';
CREATE ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2023-01-01';
ALTER ROLE myrole WITH PASSWORD 'mypassword' VALID UNTIL '2023-01-01';
ALTER ROLE myrole WITH PASSWORD 'mypassword';
ALTER ROLE myrole VALID UNTIL '2023-01-01';
ALTER ROLE myrole RENAME TO myrole2;
```

Cambiar el nombre de un rol (`ALTER ROLE myrole RENAME TO newname`) también está restringido si la contraseña utiliza el algoritmo hash MD5.

Con esta función activa, intentar cualquiera de estos comandos SQL sin los permisos de rol `rds_password`, genera el siguiente error:

```
ERROR: must be a member of rds_password to alter passwords
```

Recomendamos que otorgar el `rds_password` solamente a unos cuantos roles que utilice únicamente para la administración de contraseñas. Si concede privilegios de `rds_password` a usuarios de bases de datos que no tengan privilegios de `rds_superuser`, también debe otorgarles el atributo `CREATEROLE`.

Asegúrese de que comprueba los requisitos de las contraseñas del lado del cliente, como el vencimiento y la complejidad necesaria. Si utiliza su propia utilidad del lado del cliente para cambios relacionados con la contraseña, la utilidad debe ser miembro de `rds_password` tener privilegios de `CREATE ROLE`.

Uso de SCRAM para el cifrado de contraseñas de PostgreSQL

El mecanismo de autenticación mediante desafío-respuesta discontinuo (SCRAM) es una alternativa al algoritmo de resumen de mensajes (MD5) predeterminado de PostgreSQL para cifrar contraseñas. El mecanismo de autenticación SCRAM se considera más seguro que MD5. Para obtener más información sobre estos dos enfoques diferentes para proteger las contraseñas, consulte Password Authentication (Autenticación de contraseñas) en la documentación de PostgreSQL.

Le recomendamos que utilice SCRAM en lugar de MD5 como esquema de cifrado de contraseñas para su . Instancia de base de datos RDS para PostgreSQL. Es un mecanismo criptográfico de desafío-respuesta que utiliza el algoritmo scram-sha-256 algorithm para la autenticación y el cifrado de contraseñas.

Es posible que deba actualizar las bibliotecas de las aplicaciones cliente para que sean compatibles con SCRAM. Por ejemplo, las versiones de JDBC anteriores a la 42.2.0 no admiten SCRAM. Para obtener más información, consulte PostgreSQL JDBC Driver (Controlador JDBC de PostgreSQL) en la documentación del controlador JDBC de PostgreSQL. Para ver una lista de otros controladores de PostgreSQL y la compatibilidad con SCRAM, consulte List of drivers (Lista de controladores) en la documentación de PostgreSQL.

RDS para PostgreSQL versión 13.1 y posteriores admite scram-sha-256. Estas versiones también le permiten configurar la instancia de la base de datos para que requiera SCRAM, como se explica en los siguientes procedimientos.

Configuración de la instancia de base de datos de Aurora para que requiera SCRAM

puede requerir que la instancia de RDS para PostgreSQL DB acepte únicamente contraseñas que utilicen el algoritmo scram-sha-256.

> **Important**
>
> En el caso de los proxies RDS existentes con bases de datos de PostgreSQL, si modifica la autenticación de la base de datos para utilizar únicamente `SCRAM`, el proxy dejará de estar disponible durante un máximo de 60 segundos. Para evitar este problema, lleve a cabo alguna de las siguientes operaciones:
>
> - Asegúrese de que la base de datos permita la autenticación `SCRAM` y `MD5`.
> - Para utilizar únicamente la autenticación `SCRAM`, cree un nuevo proxy, migre el tráfico de la aplicación al nuevo proxy y, a continuación, elimine el proxy previamente asociado a la base de datos.

Antes de realizar cambios en el sistema, asegúrese de entender el proceso completo, como se indica a continuación:

- Obtenga información sobre todos los roles y el cifrado de las contraseñas de todos los usuarios de la base de datos.
- Compruebe de nuevo la configuración de los parámetros de la instancia de base de datos de Aurora correspondiente a los parámetros que controlan el cifrado de las contraseñas.
- Si la instancia de base de datos de RDS para PostgreSQL utiliza un grupo de parámetros predeterminado, deberá crear un grupo de parámetros de base de datos personalizado y aplicarlo a la instancia de base de datos de RDS para PostgreSQL para poder modificar los parámetros cuando sea necesario. Si la instancia de base de datos de RDS para PostgreSQL utiliza un grupo de parámetros personalizado, puede modificar los parámetros necesarios más adelante en el proceso, según sea necesario.
- Cambie el parámetro `password_encryption` por `scram-sha-256`.
- Notifique a todos los usuarios de la base de datos que deben actualizar las contraseñas. Haga lo mismo con su cuenta de `postgres`. Las nuevas contraseñas se cifran y almacenan mediante el algoritmo scram-sha-256.
- Verifique que todas las contraseñas están cifradas con el tipo de cifrado.

- Si todas las contraseñas utilizan scram-sha-256, puede cambiar el parámetro `rds.accepted_password_auth_method` de `md5+scram` a `scram-sha-256`.

> **Warning**
>
> Después de cambiar `rds.accepted_password_auth_method` a scram-sha-256 únicamente, no podrá conectarse ningún usuario (rol) con una contraseña cifrada con `md5`.

Preparativos para requerir SCRAM en la instancia de base de datos de RDS para PostgreSQL

Antes de realizar cambios en la instancia de RDS para PostgreSQL, compruebe todas las cuentas de usuario de base de datos existentes. Compruebe también el tipo de cifrado utilizado para las contraseñas. Puede hacer estas tareas con la extensión `rds_tools`. Para ver qué versiones de PostgreSQL son compatibles con `rds_tools`, consulte Versiones de extensión para Amazon RDS para PostgreSQL.

Para obtener una lista de usuarios de base de datos (roles) y métodos de cifrado de contraseñas

1. Use `psql` para conectarse a la instancia de base de datos de RDS para PostgreSQL, tal como se muestra a continuación.

```
psql --host=db-name.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password
```

2. Instale la extensión de `rds_tools`.

```
postgres=> CREATE EXTENSION rds_tools;
CREATE EXTENSION
```

3. Obtenga una lista de los roles y el cifrado.

```
postgres=> SELECT * FROM
      rds_tools.role_password_encryption_type();
```

Se muestra una salida similar a la siguiente.

```
       rolname        | encryption_type
----------------------+-----------------
```

```
 pg_monitor           |
 pg_read_all_settings |
 pg_read_all_stats    |
 pg_stat_scan_tables  |
 pg_signal_backend    |
 lab_tester           | md5
 user_465             | md5
 postgres             | md5
(8 rows)
```

Creación de un grupo de parámetros de base de datos personalizado

> **Note**
>
> Si la instancia de base de datos de RDS para PostgreSQL ya utiliza un grupo de parámetros personalizado, no necesita crear uno nuevo.

Para obtener información general sobre los grupos de parámetros para Amazon RDS, consulte Uso de parámetros en su instancia de base de datos de RDS for PostgreSQL.

El tipo de cifrado de contraseñas que se usa para las contraseñas se establece a un parámetro, `password_encryption`. El cifrado que permite la instancia de base de datos de RDS para PostgreSQL se establece a otro parámetro, `rds.accepted_password_auth_method`. Para cambiar cualquiera de los valores predeterminados, es necesario crear un grupo de parámetros de base de datos personalizado y aplicarlo a la instancia.

También puede utilizar la AWS Management Console o la API de RDS para crear un grupo de parámetros de base de datos personalizado. Para obtener más información, consulte

Ahora puede asociar el grupo de parámetros personalizado con su instancia de base de datos.

Para crear un grupo de parámetros de base de datos personalizado

1. Utilice el comando `create-db-parameter-group` de la CLI para crear el grupo de parámetros de base de datos personalizado. En este ejemplo se utiliza `postgres13` como origen de este grupo de parámetros personalizado.

   Para Linux, macOS o Unix:

```
aws rds create-db-parameter-group --db-parameter-group-name 'docs-lab-scram-passwords' \
  --db-parameter-group-family postgres13  --description 'Custom parameter group for SCRAM'
```

Para Windows:

```
aws rds create-db-parameter-group --db-parameter-group-name "docs-lab-scram-passwords" ^
  --db-parameter-group-family postgres13  --description "Custom DB parameter group for SCRAM"
```

2. Utilice el comando modify-db-instance de la CLI para aplicar este grupo de parámetros personalizado al clúster de base de datos de RDS para PostgreSQL.

   Para Linux, macOS o Unix:

   ```
   aws rds modify-db-instance --db-instance-identifier 'your-instance-name' \
           --db-parameter-group-name "docs-lab-scram-passwords
   ```

   Para Windows:

   ```
   aws rds modify-db-instance --db-instance-identifier "your-instance-name" ^
           --db-parameter-group-name "docs-lab-scram-passwords
   ```

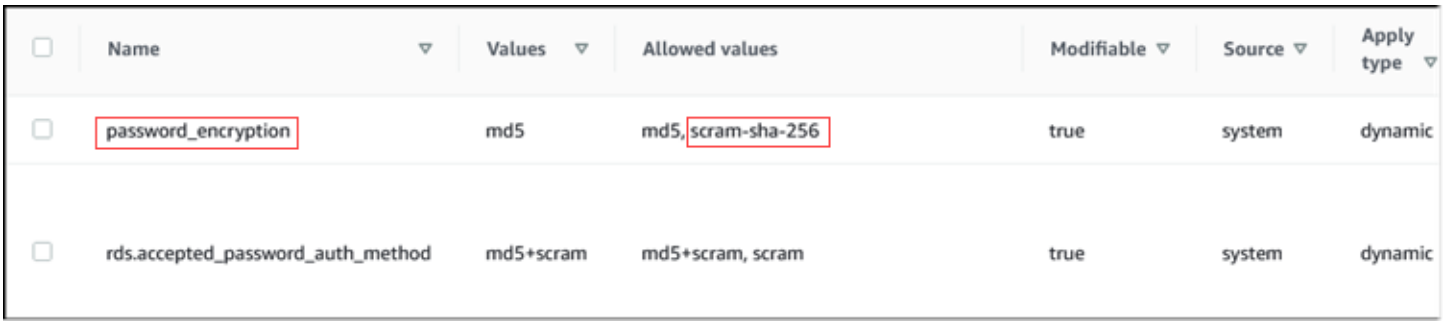
   Para volver a sincronizar la instancia de base de datos de RDS para PostgreSQL con el grupo de parámetros de base de datos personalizado, debe reiniciar la instancia principal y todas las demás instancias del clúster. Para minimizar el impacto en sus usuarios, programe esto para que se produzca durante su periodo de mantenimiento regular.

Configuración del cifrado de contraseñas para utilizar SCRAM

El mecanismo de cifrado de contraseñas que utiliza una instancia de base de datos de RDS para PostgreSQL se establece al grupo de parámetros de base de datos en el parámetro `password_encryption`. Los valores permitidos son: no establecido, `md5` o `scram-sha-256`. El valor predeterminado depende de la versión de RDS para PostgreSQL del modo que se indica a continuación:

- RDS para PostgreSQL 14 y versiones posteriores: el valor predeterminado es `scram-sha-256`
- RDS para PostgreSQL 13: el valor predeterminado es `md5`

Con un grupo de parámetros de base de datos personalizado adjuntado a la instancia de base de datos de RDS para PostgreSQL, puede modificar los valores del parámetro de cifrado de contraseñas.



Name	Values	Allowed values	Modifiable	Source	Apply type
password_encryption	md5	md5, scram-sha-256	true	system	dynamic
rds.accepted_password_auth_method	md5+scram	md5+scram, scram	true	system	dynamic

Para cambiar la configuración de cifrado de contraseñas a scram-sha-256

- Cambie el valor del cifrado de contraseñas a scram-sha-256, como se muestra a continuación. El cambio se puede aplicar inmediatamente porque el parámetro es dinámico, por lo que no se requiere un reinicio para que el cambio surta efecto.

  Para Linux, macOS o Unix:

  ```
  aws rds modify-db-parameter-group --db-parameter-group-name \
    'docs-lab-scram-passwords' --parameters
   'ParameterName=password_encryption,ParameterValue=scram-
  sha-256,ApplyMethod=immediate'
  ```

  Para Windows:

  ```
  aws rds modify-db-parameter-group --db-parameter-group-name ^
    "docs-lab-scram-passwords" --parameters
   "ParameterName=password_encryption,ParameterValue=scram-
  sha-256,ApplyMethod=immediate"
  ```

Migración de las contraseñas de los roles de usuario a SCRAM

Puede migrar las contraseñas de los roles de usuario a SCRAM, tal y como se describe a continuación.

Para migrar las contraseñas de usuario (rol) de base de datos de MD5 a SCRAM

1. Inicie sesión como usuario administrador (nombre de usuario predeterminado, `postgres`) como se muestra a continuación.

```
psql --host=db-name.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password
```

2. Compruebe la configuración del parámetro `password_encryption` en la instancia de base de datos de RDS para PostgreSQL con el siguiente comando.

```
postgres=> SHOW password_encryption;
 password_encryption
---------------------
 md5
 (1 row)
```

3. Cambie el valor de este parámetro a scram-sha-256. Se trata de un parámetro dinámico, por lo que no es necesario reiniciar la instancia después de realizar este cambio. Compruebe de nuevo el valor para asegurarse de que ahora está establecido en `scram-sha-256`, como se indica a continuación.

```
postgres=> SHOW password_encryption;
 password_encryption
---------------------
 scram-sha-256
 (1 row)
```

4. Notifique a todos los usuarios de base de datos que deben cambiar la contraseña. Asegúrese de cambiar también su propia contraseña para la cuenta `postgres` (el usuario de base de datos con privilegios `rds_superuser`).

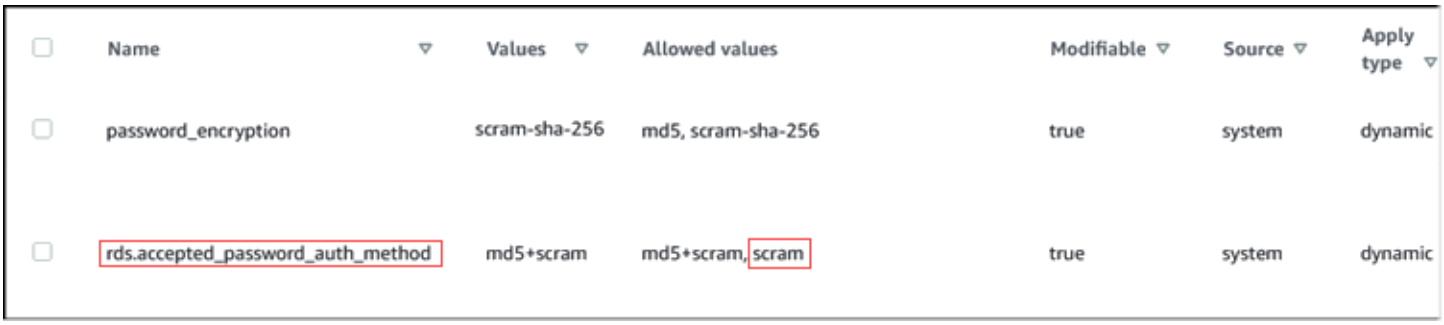
```
labdb=> ALTER ROLE postgres WITH LOGIN PASSWORD 'change_me';
ALTER ROLE
```

5. Repita el proceso para todas las bases de datos del Instancia de base de datos RDS para PostgreSQL.

Cambio del parámetro para requerir SCRAM

Este es el último paso del proceso. Después de realizar el cambio en el siguiente procedimiento, ninguna cuenta de usuario (rol) que aún utilice el cifrado `md5` para las contraseñas podrá iniciar sesión en el . Instancia de base de datos RDS para PostgreSQL.

Con `rds.accepted_password_auth_method` se especifica el método de cifrado que la instancia de base de datos de RDS para PostgreSQL acepta una contraseña de usuario durante el proceso de inicio de sesión. El valor predeterminado es `md5+scram`, lo que significa que se acepta cualquiera de los dos métodos. En la siguiente imagen, puede encontrar la configuración predeterminada de este parámetro.



Name	Values	Allowed values	Modifiable	Source	Apply type
password_encryption	scram-sha-256	md5, scram-sha-256	true	system	dynamic
rds.accepted_password_auth_method	md5+scram	md5+scram, scram	true	system	dynamic

Los valores permitidos para este parámetro son:`md5+scram` o `scram` solo. El cambio de este valor de parámetro a `scram` lo convierte en un requisito.

Para cambiar el valor de parámetro para requerir la autenticación SCRAM para las contraseñas

1. Verifique que todas las contraseñas de los usuarios de base de datos de la instancia de base de datos de RDS para PostgreSQL utilizan `scram-sha-256` para el cifrado de contraseña. Para ello, consulte `rds_tools` para el rol (usuario) y el tipo de cifrado, de la siguiente manera.

```
postgres=> SELECT * FROM rds_tools.role_password_encryption_type();
  rolname        | encryption_type
  ---------------------+----------------
  pg_monitor           |
  pg_read_all_settings |
  pg_read_all_stats    |
  pg_stat_scan_tables  |
  pg_signal_backend    |
  lab_tester           | scram-sha-256
  user_465             | scram-sha-256
  postgres             | scram-sha-256
  ( rows)
```

2. Repita la consulta en todas las instancias de base de datos del Instancia de base de datos RDS para PostgreSQL.

   Si todas las contraseñas usan scram-sha-256, puede continuar.

3. Cambie el valor de la autenticación de contraseña aceptada a scram-sha-256, como se indica a continuación.

   Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group --db-parameter-group-name 'docs-lab-scram-
passwords' \
  --parameters
 'ParameterName=rds.accepted_password_auth_method,ParameterValue=scram,ApplyMethod=immediat
```

   Para Windows:

```
aws rds modify-db-parameter-group --db-parameter-group-name "docs-lab-scram-
passwords" ^
  --parameters
 "ParameterName=rds.accepted_password_auth_method,ParameterValue=scram,ApplyMethod=immediat
```

Gestión de conexiones inactivas en PostgreSQL

Las conexiones inactivas se producen cuando una sesión de base de datos permanece activa en el servidor a pesar de que la aplicación cliente se haya abandonado o terminado de forma anormal. Esta situación suele producirse cuando los procesos del cliente se bloquean o terminan de forma inesperada sin cerrar correctamente las conexiones de la base de datos ni cancelar las solicitudes en curso.

PostgreSQL identifica y limpia de manera eficiente las conexiones inactivas cuando los procesos del servidor están inactivos o intentan enviar datos a los clientes. Sin embargo, la detección es difícil en el caso de las sesiones que están inactivas, esperan la intervención del cliente o en las que se están ejecutando consultas de forma activa. Para gestionar estos escenarios, PostgreSQL proporciona los parámetros `tcp_keepalives_*`, `tcp_user_timeout`, y `client_connection_check_interval`.

Temas

- Descripción de keepalive de TCP

- Parámetros clave keepalive de TCP en RDS para PostgreSQL
- Casos de uso de la configuración de keepalive de TCP
- Prácticas recomendadas

Descripción de keepalive de TCP

Keepalive de TCP es un mecanismo en el nivel de protocolo que ayuda a mantener y verificar la integridad de la conexión. Cada conexión TCP mantiene configuraciones en el nivel del kernel que rigen el comportamiento de keepalive. Cuando el temporizador de keepalive expira, el sistema realiza lo siguiente:

- Envía un paquete de sondeo sin datos y con el indicador ACK activado.
- Espera una respuesta del punto de conexión remoto de acuerdo con las especificaciones de TCP/IP.
- Administra el estado de la conexión en función de la respuesta o la falta de respuesta.

Parámetros clave keepalive de TCP en RDS para PostgreSQL

Parámetro	Descripción	Valores predeterminados
`tcp_keepalives_idle`	Specifies number of seconds of inactivity before sending keepalive message.	300
`tcp_keepalives_interval`	Specifies number of seconds between retransmissions of unacknowledged keepalive messages.	30
`tcp_keepalives_count`	Maximum lost keepalive messages before declaring connection dead	2
`tcp_user_timeout`	Specifies how long (in Milliseconds) unacknowledged	0

Parámetro	Descripción	Valores predeterminados
	data can remain before forcibly closing the connection.	
`client_connection_check_interval`	Sets the interval (in Milliseconds) for checking client connection status during long-running queries. This ensures quicker detection of closed connections.	0

Casos de uso de la configuración de keepalive de TCP

Mantenimiento de las sesiones inactivas como activas

Para evitar que los firewalls o enrutadores terminen las conexiones inactivas debido a la inactividad:

- Configure `tcp_keepalives_idle` para enviar paquetes de keepalive a intervalos regulares.

Detección de conexiones inactivas

Para detectar rápidamente las conexiones inactivas:

- Ajuste `tcp_keepalives_idle`, `tcp_keepalives_interval` y `tcp_keepalives_count`. Por ejemplo, con los valores predeterminados de Aurora PostgreSQL, se tarda aproximadamente un minuto (2 sondas × 30 segundos) en detectar una conexión inactiva. Reducir estos valores puede acelerar la detección.
- Utilice `tcp_user_timeout` para especificar el tiempo máximo de espera para una confirmación.

La configuración de keepalive de TCP ayuda al kernel a detectar conexiones inactivas, pero PostgreSQL puede no actuar hasta que se utilice el socket. Si una sesión está ejecutando una consulta larga, es posible que las conexiones inactivas solo se detecten una vez completada la consulta. En PostgreSQL 14 y versiones posteriores, `client_connection_check_interval` puede acelerar la detección de conexiones inactivas consultando periódicamente el socket durante la ejecución de la consulta.

Prácticas recomendadas

- Establezca intervalos de keepalive razonables: ajuste `tcp_user_timeout`, `tcp_keepalives_idle`, `tcp_keepalives_count` y `tcp_keepalives_interval` para equilibrar la velocidad de detección y el uso de recursos.
- Optimice para su entorno: alinee la configuración con el comportamiento de la red, las políticas de firewall y las necesidades de la sesión.
- Aproveche las características de PostgreSQL: utilice `client_connection_check_interval` en PostgreSQL 14 y versiones posteriores para comprobar la conexión de forma eficaz.

Uso de autovacuum de PostgreSQL en Amazon RDS para PostgreSQL

Le recomendamos que use la característica autovacuum para mantener en buen estado su instancia de base de datos de PostgreSQL. Autovacuum automatiza el comienzo de los comandos VACUUM y ANALYZE. Comprueba las tablas con una gran cantidad de tuplas insertadas, actualizadas o eliminadas. Después de esta verificación, recupera el almacenamiento mediante la eliminación de datos obsoletos o tuplas de la base de datos de PostgreSQL.

De forma predeterminada, autovacuum está activado para las instancias de base de datos de RDS para PostgreSQL que crea por medio de cualquiera de los grupos de parámetros de base de datos de PostgreSQL predeterminados. Otros parámetros de configuración asociados con la característica autovacuum también se establecen de forma predeterminada. Debido a que estos valores predeterminados son algo genéricos, puede beneficiarse de ajustar algunos de los parámetros asociados con la característica autovacuum para su carga de trabajo específica.

A continuación, puede encontrar más información sobre autovacuum y cómo ajustar algunos de sus parámetros en la instancia de base de datos de RDS para PostgreSQL. Para obtener información más específica, consulte Prácticas recomendadas para trabajar con PostgreSQL.

Temas

- Asignación de memoria para autovacuum
- Reducción de la probabilidad de reinicio del identificador de transacción
- Determinar si las tablas de una base de datos necesitan vacío
- Determinar qué tablas cumplen actualmente los requisitos de autovacuum
- Determinar si autovacuum se está ejecutando actualmente y durante cuánto tiempo
- Realización de una inmovilización de vacío manual

- Reindexar una tabla cuando autovacuum se está ejecutando
- Administración de autovacuum con índices de gran tamaño
- Otros parámetros que afectan a autovacuum
- Establecimiento de parámetros autovacuum de nivel de tabla
- Registro de actividades de autovacuum y vacuum
- Comportamiento de autovacuum con bases de datos no válidas
- Identificación y resolución de los bloqueadores de vaciado intensivo en RDS para PostgreSQL

Asignación de memoria para autovacuum

Uno de los parámetros más importantes que afectan al desempeño de autovacuum es el parámetro `autovacuum_work_mem`. En las versiones 14 y anteriores de RDS para PostgreSQL, el parámetro `autovacuum_work_mem` se establece en -1, lo que indica que en su lugar se utiliza la configuración de `maintenance_work_mem`. En todas las demás versiones, `autovacuum_work_mem` se determina mediante GREATEST({DBInstanceClassMemory/32768}, 65536).

Las operaciones de limpieza manual siempre utilizan la configuración de `maintenance_work_mem`, con la configuración predeterminada de GREATEST ({DBInstanceClassMemory/63963136*1024}, 65536), y también se puede ajustar en la sesión mediante el comando `SET` para operaciones manuales de `VACUUM` más específicas.

`autovacuum_work_mem` determina que la memoria de autovacuum conserve los identificadores de tuplas inactivas (`pg_stat_all_tables.n_dead_tup`) para los índices de limpieza.

Cuando realice los cálculos para determinar el valor del parámetro `autovacuum_work_mem`, tenga en cuenta lo siguiente:

- Si define el parámetro en un valor demasiado bajo, el proceso de limpieza puede tener que examinar la tabla varias veces para completar su trabajo. Esta variedad de análisis puede tener un impacto negativo en el rendimiento. Para instancias mayores, configurar `maintenance_work_mem` o `autovacuum_work_mem` a 1 GB como mínimo puede mejorar el rendimiento de las tablas de limpieza con un número elevado de tuplas inactivas. Sin embargo, en las versiones 16 y anteriores de PostgreSQL, el uso de memoria de la operación de limpieza está limitado a 1 GB, que es suficiente para procesar aproximadamente 179 millones de tuplas inactivas de una sola pasada. Si una tabla tiene más tuplas inactivas que las indicadas, la operación de limpieza tendrá que realizar varias pasadas por los índices de la tabla, lo que aumentará

considerablemente el tiempo necesario. A partir de la versión 17 de PostgreSQL, no hay un límite de 1 GB y autovacuum puede procesar más de 179 millones de tuplas mediante árboles radix.

Un identificador de tupla tiene un tamaño de 6 bytes. Con el fin de calcular la memoria necesaria para limpiar un índice de una tabla, realice una consulta a `pg_stat_all_tables.n_dead_tup` para buscar el número de tuplas inactivas y, a continuación, multiplique este número por 6 para determinar la memoria necesaria para limpiar el índice de una sola pasada. Puede utilizar la siguiente consulta:

```
SELECT
    relname AS table_name,
    n_dead_tup,
    pg_size_pretty(n_dead_tup * 6) AS estimated_memory
FROM
    pg_stat_all_tables
WHERE
    relname = 'name_of_the_table';
```

- El parámetro `autovacuum_work_mem` funciona en combinación con el parámetro `autovacuum_max_workers`. Cada empleado de `autovacuum_max_workers` puede utilizar la memoria que asigne. Si tiene demasiadas tablas pequeñas, asigne más `autovacuum_max_workers` y menos `autovacuum_work_mem`. Si tiene tablas grandes (de 100 GB o más), asigne más memoria y menos procesos de trabajo. Debe tener suficiente memoria asignada para que funcione en la tabla más grande. Por lo tanto, asegúrese de que la combinación de procesos de trabajo y memoria sea igual a la memoria total que desea asignar.

Reducción de la probabilidad de reinicio del identificador de transacción

En algunos casos, la configuración de grupos de parámetros relacionada con autovacuum puede no ser lo suficientemente agresiva como para evitar el reinicio del identificador de transacción. Para solucionar esto, RDS para PostgreSQL proporciona un mecanismo que adapta los valores de los parámetros de autovacuum automáticamente. Autovacuum adaptativo es una característica para RDS para PostgreSQL. Puede encontrar una explicación detallada sobre el reinicio del identificador de transacción en la documentación de PostgreSQL.

Autovacuum adaptativo está activado de forma predeterminada para las instancias de RDS para PostgreSQL con el parámetro dinámico `rds.adaptive_autovacuum` establecido en Activado. Le recomendamos encarecidamente que mantenga esta opción activada. Sin

embargo, para apagar el ajuste de parámetros autovacuum adaptativo, establezca el parámetro `rds.adaptive_autovacuum` en 0 u OFF.

El reinicio de ID de transacción sigue siendo posible incluso cuando Amazon RDS Amazon RDS ajusta los parámetros de autovacuum. Le animamos a implementar una alarma Amazon CloudWatch para el reinicio de identificador de transacción. Para obtener más información, consulte la publicación Implement an early warning system for transaction ID wraparound in RDS for PostgreSQL (Implementar un sistema de alerta temprana para el ajuste de ID de transacción en RDS for PostgreSQL) en el Blog de Base de datos de AWS.

Con el ajuste de parámetros de autovacuum adaptable activado, Amazon RDS comienza a ajustar los parámetros de autovacuum cuando la métrica de CloudWatch `MaximumUsedTransactionIDs` alcanza el valor del parámetro `autovacuum_freeze_max_age` o 500 000 000, el que sea mayor.

Amazon RDS continúa ajustando los parámetros para el autovacuum si una tabla continúa tendiendo hacia el ajuste de ID de transacción. Cada uno de estos ajustes dedica más recursos a autovacuum para evitar el reinicio. Amazon RDS actualiza los siguientes parámetros relacionados con autovacuum:

- autovacuum_vacuum_cost_delay
- autovacuum_vacuum_cost_limit
- `autovacuum_work_mem`
- autovacuum_naptime

RDS modifica estos parámetros solo si el nuevo valor hace que autovacuum sea más agresivo. Estos parámetros se modifican en la memoria en la instancia de base de datos. Los valores en el grupo de parámetros no han cambiado. Para ver la configuración en memoria actual, utilice el comando de SQL PostgreSQL SHOW de PostgreSQL.

Cuando Amazon RDS modifica alguno de estos parámetros de autovacuum, genera un evento para la instancia de base de datos afectada. Este evento se puede ver en la AWS Management Console y a través de la API de Amazon RDS. Una vez que la métrica CloudWatch `MaximumUsedTransactionIDs` vuelve por debajo del límite, Amazon RDS restablece los parámetros relacionados con el autovacuum en la memoria a los valores especificados en el grupo de parámetros. Luego, genera otro evento correspondiente a este cambio.

Determinar si las tablas de una base de datos necesitan vacío

Puede utilizar la siguiente consulta para mostrar el número de transacciones descongeladas en una base de datos. La columna `datfrozenxid` de una fila `pg_database` de una base de datos es un límite inferior en los identificadores de transacción normales que aparecen en esa base de datos. Esta columna es el mínimo de los valores `relfrozenxid` por tabla dentro de la base de datos.

```
SELECT datname, age(datfrozenxid) FROM pg_database ORDER BY age(datfrozenxid) desc
 limit 20;
```

Por ejemplo, los resultados de ejecutar la consulta anterior podrían ser los siguientes.

```
datname    | age
mydb       | 1771757888
template0  | 1721757888
template1  | 1721757888
rdsadmin   | 1694008527
postgres   | 1693881061
(5 rows)
```

Cuando la antigüedad de una base de datos llega a los dos mil millones de identificadores de transacción, se produce el reinicio de los TransactionID (XID) y la base de datos cambia al modo de solo lectura. Puede usar esta consulta para generar una métrica y ejecutarla varias veces al día. De manera predeterminada, autovacuum está configurado para mantener la antigüedad de las transacciones en un máximo de 200,000,000 (`autovacuum_freeze_max_age`).

Una estrategia de monitorización de muestra podría ser la siguiente:

- Establezca el valor `autovacuum_freeze_max_age` en 200 millones de transacciones.
- Si una tabla llega a 500 millones de transacciones descongeladas, se dispara una alarma de gravedad baja. No es un valor disparatado, pero podría indicar que autovacuum no puede mantener el ritmo.
- Si una tabla llega a mil millones, se debe interpretar como una alarma para adoptar medidas. En general, conviene mantener las antigüedades más cerca de `autovacuum_freeze_max_age` por motivos de rendimiento. Le recomendamos que investigue utilizando las recomendaciones que siguen.
- Si una tabla llega a 1500 millones de transacciones sin vaciar, se dispara una alarma de gravedad alta. En función de la velocidad con la que la base de datos use los identificadores de transacción,

esta alarma puede indicar que el sistema está agotando el tiempo para ejecutar autovacuum. En ese caso, le recomendamos una solución inmediata.

Si una tabla supera constantemente estos límites, modifique aún más sus parámetros de autovacuum. De manera predeterminada, usar VACUUM manualmente (que tiene deshabilitados los retardos basados en el costo) es un procedimiento más agresivo que usar el autovacuum predeterminado, pero es también más intrusivo para el sistema en su conjunto.

Le recomendamos lo siguiente:

- Esté atento y active un mecanismo de supervisión para que esté al tanto de la antigüedad de sus transacciones.

  A fin de obtener información acerca de la creación de un proceso que advierta sobre el reinicio del ID de transacción, consulte la publicación de blog de la base de datos de AWS sobre la implementación de un sistema de advertencia temprana para el reinicio de un ID de transacción en Amazon RDS for PostgreSQL.
- Para las tablas con más actividad, lleve a cabo una inmovilización manual de vacío con regularidad durante una ventana de mantenimiento además de confiar en autovacuum. Para obtener información acerca de la ejecución de una inmovilización de vacío manual, consulte Realización de una inmovilización de vacío manual.

Determinar qué tablas cumplen actualmente los requisitos de autovacuum

A menudo, hay una o dos tablas que necesitan vacío. Autovacuum se dirige siempre a las tablas cuyo valor `relfrozenxid` sea superior al número de transacciones en `autovacuum_freeze_max_age`. De lo contrario, si el número de tuplas obsoletas desde el último VACUUM supera el límite de vacío, la tabla se vacía.

El umbral de autovacuum se define como:

```
Vacuum-threshold = vacuum-base-threshold + vacuum-scale-factor * number-of-tuples
```

donde el `vacuum base threshold` es `autovacuum_vacuum_threshold`, el `vacuum scale factor` es `autovacuum_vacuum_scale_factor` y el `number of tuples` es `pg_class.reltuples`.

Mientras está conectado a la base de datos, ejecute la siguiente consulta para ver una lista de tablas que autovacuum considera aptas para el vacío.

```
WITH vbt AS (SELECT setting AS autovacuum_vacuum_threshold FROM
pg_settings WHERE name = 'autovacuum_vacuum_threshold'),
vsf AS (SELECT setting AS autovacuum_vacuum_scale_factor FROM
pg_settings WHERE name = 'autovacuum_vacuum_scale_factor'),
fma AS (SELECT setting AS autovacuum_freeze_max_age FROM pg_settings WHERE name =
 'autovacuum_freeze_max_age'),
sto AS (select opt_oid, split_part(setting, '=', 1) as param,
split_part(setting, '=', 2) as value from (select oid opt_oid, unnest(reloptions)
 setting from pg_class) opt)
SELECT '"'||ns.nspname||'"."'||c.relname||'"' as relation,
pg_size_pretty(pg_table_size(c.oid)) as table_size,
age(relfrozenxid) as xid_age,
coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
 autovacuum_freeze_max_age,
(coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
coalesce(cvsf.value::float,autovacuum_vacuum_scale_factor::float) * c.reltuples)
AS autovacuum_vacuum_tuples, n_dead_tup as dead_tuples FROM
pg_class c join pg_namespace ns on ns.oid = c.relnamespace
join pg_stat_all_tables stat on stat.relid = c.oid join vbt on (1=1) join vsf on (1=1)
 join fma on (1=1)
left join sto cvbt on cvbt.param = 'autovacuum_vacuum_threshold' and c.oid =
 cvbt.opt_oid
left join sto cvsf on cvsf.param = 'autovacuum_vacuum_scale_factor' and c.oid =
 cvsf.opt_oid
left join sto cfma on cfma.param = 'autovacuum_freeze_max_age' and c.oid = cfma.opt_oid
WHERE c.relkind = 'r' and nspname <> 'pg_catalog'
AND (age(relfrozenxid) >= coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
OR coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
coalesce(cvsf.value::float,autovacuum_vacuum_scale_factor::float) *
c.reltuples <= n_dead_tup)
ORDER BY age(relfrozenxid) DESC LIMIT 50;
```

Determinar si autovacuum se está ejecutando actualmente y durante cuánto tiempo

Si necesita aspirar manualmente una tabla, asegúrese de determinar si el autovacuum se está ejecutando actualmente. Si es así, es posible que deba ajustar los parámetros para que funcione de manera más eficiente o desactivar el autovacuum temporalmente para que pueda ejecutar manualmente VACUUM.

Use la siguiente consulta para determinar si se está ejecutando autovacuum, cuánto tiempo lleva en ejecución y si se encuentra en espera en otra sesión.

```
SELECT datname, usename, pid, state, wait_event, current_timestamp - xact_start AS
 xact_runtime, query
FROM pg_stat_activity
WHERE upper(query) LIKE '%VACUUM%'
ORDER BY xact_start;
```

Después de ejecutar la consulta, debería ver un resultado similar al siguiente.

```
 datname | usename  |  pid  | state  | wait_event |      xact_runtime       | query
 --------+----------+-------+--------+------------+-------------------------
+-------------------------------------------------------------------------------------------------
 mydb    | rdsadmin | 16473 | active |            | 33 days 16:32:11.600656 |
 autovacuum: VACUUM ANALYZE public.mytable1 (to prevent wraparound)
 mydb    | rdsadmin | 22553 | active |            | 14 days 09:15:34.073141 |
 autovacuum: VACUUM ANALYZE public.mytable2 (to prevent wraparound)
 mydb    | rdsadmin | 41909 | active |            | 3 days 02:43:54.203349  |
 autovacuum: VACUUM ANALYZE public.mytable3
 mydb    | rdsadmin |   618 | active |            | 00:00:00                |
 SELECT datname, usename, pid, state, wait_event, current_timestamp - xact_start AS
 xact_runtime, query+
         |          |       |        |            |                         | FROM
 pg_stat_activity
           +
         |          |       |        |            |                         | WHERE
 query like '%VACUUM%'
          +
         |          |       |        |            |                         | ORDER BY
 xact_start;
       +
```

Existen varios problemas que pueden provocar una sesión de autovaccum de larga duración (es decir, que tarde varios días). El problema más común es que el valor del parámetro `maintenance_work_mem` sea demasiado bajo para el tamaño de la tabla o la velocidad de las actualizaciones.

Le recomendamos que utilice la siguiente fórmula para establecer el valor del parámetro `maintenance_work_mem`.

```
GREATEST({DBInstanceClassMemory/63963136*1024},65536)
```

Las sesiones de autovacuum con una duración corta también pueden indicar problemas:

- Pueden indicar que no hay un número de `autovacuum_max_workers` suficientemente alto para la carga de trabajo. En ese caso, tendrá que especificar el número de procesos de trabajo.
- Puede indicar que hay una corrupción de índice (autovacuum falla y se reinicia en la misma relación pero no avanza). En este caso, ejecute un manual `vacuum freeze verbose table` para ver la causa exacta.

Realización de una inmovilización de vacío manual

Puede ocurrir que desee realizar una operación de vacío manual en una tabla que ya tenga un proceso de vacío en ejecución. Esto resulta útil si se ha identificado una tabla con una antigüedad cercana a dos mil millones de transacciones (o por encima del umbral que esté monitorizando).

Los siguientes pasos son pautas, con varias variaciones en el proceso. Por ejemplo, durante las pruebas, suponga que descubre que el parámetro `maintenance_work_mem` se definió en un valor demasiado bajo y que tiene que adoptar medidas de forma inmediata en una tabla. Sin embargo, quizás no desea rebotar la instancia en ese momento. Con las consultas de las secciones anteriores, puede determinar qué tabla está causando el problema y comprobar que hay una sesión de autovacuum que lleva mucho tiempo en ejecución. Sabe que tiene que cambiar el ajuste del parámetro `maintenance_work_mem`, pero también tiene que adoptar medidas de inmediato y aplicar el vacío en la tabla afectada. El siguiente procedimiento muestra qué hacer en esa situación.

Para realizar manualmente una inmovilización de vacío

1. Abra dos sesiones en la base de datos que contiene la tabla en la que desea ejecutar el vacío. Para la segunda sesión, use "screen" u otra utilidad que mantenga la sesión activa si se interrumpe la conexión.
2. En la sesión uno, obtenga el ID de proceso (PID) de la sesión de autovacuum que se ejecuta en la tabla.

   Ejecute la siguiente consulta para obtener el PID de la sesión de autovacuum.

   ```
   SELECT datname, usename, pid, current_timestamp - xact_start
   AS xact_runtime, query
   FROM pg_stat_activity WHERE upper(query) LIKE '%VACUUM%' ORDER BY
   ```

```
xact_start;
```

3. En la sesión dos, calcule la cantidad de memoria que necesitará para esta operación. En este ejemplo, determinamos que podemos permitirnos usar un máximo de 2 GB de memoria para esta operación y, por tanto, definimos `maintenance_work_mem` en 2 GB para la sesión actual.

```
SET maintenance_work_mem='2 GB';
SET
```

4. En la sesión dos, ejecute el comando `vacuum freeze verbose` para la tabla. El ajuste de informe detallado resulta útil porque, aunque PostgreSQL no ofrece actualmente un informe de progreso para esto, se puede ver la actividad.

```
\timing on
Timing is on.
vacuum freeze verbose pgbench_branches;
```

```
INFO:  vacuuming "public.pgbench_branches"
INFO:  index "pgbench_branches_pkey" now contains 50 row versions in 2 pages
DETAIL:  0 index row versions were removed.
0 index pages have been deleted, 0 are currently reusable.
CPU 0.00s/0.00u sec elapsed 0.00 sec.
INFO:  index "pgbench_branches_test_index" now contains 50 row versions in 2 pages
DETAIL:  0 index row versions were removed.
0 index pages have been deleted, 0 are currently reusable.
CPU 0.00s/0.00u sec elapsed 0.00 sec.
INFO:  "pgbench_branches": found 0 removable, 50 nonremovable row versions
     in 43 out of 43 pages
DETAIL:  0 dead row versions cannot be removed yet.
There were 9347 unused item pointers.
0 pages are entirely empty.
CPU 0.00s/0.00u sec elapsed 0.00 sec.
VACUUM
Time: 2.765 ms
```

5. En la sesión uno, si la limpieza automática bloqueaba la sesión de vacío, `pg_stat_activity` muestra que la espera es T para la sesión de vacío. En este caso, finalice el proceso de limpieza automática de la siguiente manera.

```
SELECT pg_terminate_backend('the_pid');
```

> **Note**
>
> Algunas versiones anteriores de Amazon RDS no pueden finalizar un proceso de limpieza automática mediante el comando anterior y producen el siguiente error: `ERROR: 42501: must be a superuser to terminate superuser process LOCATION: pg_terminate_backend, signalfuncs.c:227`.

En este punto, comienza la sesión. La limpieza automática se reinicia inmediatamente, ya que esta tabla es probablemente la que ocupa una posición más alta en la lista de trabajo.

6. Inicie el comando `vacuum freeze verbose` en la sesión dos y luego finalice el proceso de autovacuum en la sesión uno.

Reindexar una tabla cuando autovacuum se está ejecutando

Si un índice se ha dañado, autovacuum seguirá procesando la tabla y generará errores. Si intenta realizar un vacío manual en esta situación, recibirá un mensaje de error como el siguiente.

```
postgres=>  vacuum freeze pgbench_branches;
ERROR: index "pgbench_branches_test_index" contains unexpected
   zero page at block 30521
HINT: Please REINDEX it.
```

Cuando el índice está dañado y autovacuum intenta ejecutarse en la tabla, se enfrenta a una sesión de autovacuum que ya se está ejecutando. Cuando ejecuta un comando REINDEX, elimina un bloqueo exclusivo en la tabla. Las operaciones de escritura están bloqueadas y también las operaciones de lectura que usan ese índice específico.

Para reindexar una tabla cuando autovacuum se está ejecutando en ella

1. Abra dos sesiones en la base de datos que contiene la tabla que desea vaciar. Para la segunda sesión, use "screen" u otra utilidad que mantenga la sesión activa si se interrumpe la conexión.
2. En la sesión uno, obtenga el PID de la sesión de autovacuum que se ejecuta en la tabla.

   Ejecute la siguiente consulta para obtener el PID de la sesión de autovacuum.

   ```
   SELECT datname, usename, pid, current_timestamp - xact_start
   ```

```
AS xact_runtime, query
FROM pg_stat_activity WHERE upper(query) like '%VACUUM%' ORDER BY
xact_start;
```

3. En la sesión dos, ejecute el comando reindex.

```
\timing on
Timing is on.
reindex index pgbench_branches_test_index;
REINDEX
  Time: 9.966 ms
```

4. En la sesión uno, si autovacuum estaba bloqueando, verá en `pg_stat_activity` que la espera es “T” para su sesión de vacío. En este caso, terminará el proceso de autovacuum.

```
SELECT pg_terminate_backend('the_pid');
```

   En este punto, comienza la sesión. Es importante tener en cuenta que autovacuum se reiniciará inmediatamente, ya que esta tabla es probablemente la que ocupa una posición más alta en su lista de trabajo.

5. Inicie el comando en la sesión dos y termine a continuación el proceso de autovacuum de la sesión 1.

Administración de autovacuum con índices de gran tamaño

Como parte de su funcionamiento, autovacuum realiza varias fases de vaciado mientras se ejecuta en una tabla. Antes de limpiar la tabla, primero se vacían todos sus índices. Al eliminar varios índices de gran tamaño, esta fase consume una cantidad importante de tiempo y recursos. Por lo tanto, como práctica recomendada, asegúrese de controlar el número de índices de una tabla y eliminar los no utilizados.

Para este proceso, compruebe primero el tamaño general del índice. A continuación, determine si hay índices que es posible que no se utilicen y que se puedan eliminar, tal y como se muestra en los siguientes ejemplos.

Para comprobar el tamaño de la tabla y sus índices

```
postgres=> select pg_size_pretty(pg_relation_size('pgbench_accounts'));
pg_size_pretty
```

```
6404 MB
(1 row)
```

```
postgres=> select pg_size_pretty(pg_indexes_size('pgbench_accounts'));
pg_size_pretty
11 GB
(1 row)
```

En este ejemplo, el tamaño de los índices es mayor que el de la tabla. Esta diferencia puede provocar problemas de rendimiento, ya que los índices están sobrecargados o no se utilizan, lo que afecta a las operaciones de autovacuum y de inserción.

Para comprobar si hay índices no utilizados

En la vista `pg_stat_user_indexes`, puede comprobar la frecuencia con la que se utiliza un índice con la columna `idx_scan`. En el siguiente ejemplo, los índices no utilizados tienen el valor `0` en `idx_scan`.

```
postgres=> select * from pg_stat_user_indexes where relname = 'pgbench_accounts' order
 by idx_scan desc;

relid  | indexrelid | schemaname | relname          | indexrelname          | idx_scan
 | idx_tup_read | idx_tup_fetch
-------+------------+------------+------------------+-----------------------+----------
+--------------+--------------
16433  | 16454      | public     | pgbench_accounts | index_f               | 6
 | 6            | 0
16433  | 16450      | public     | pgbench_accounts | index_b               | 3
 | 199999       | 0
16433  | 16447      | public     | pgbench_accounts | pgbench_accounts_pkey | 0
 | 0            | 0
16433  | 16452      | public     | pgbench_accounts | index_d               | 0
 | 0            | 0
16433  | 16453      | public     | pgbench_accounts | index_e               | 0
 | 0            | 0
16433  | 16451      | public     | pgbench_accounts | index_c               | 0
 | 0            | 0
16433  | 16449      | public     | pgbench_accounts | index_a               | 0
 | 0            | 0
(7 rows)
```

```
postgres=> select schemaname, relname, indexrelname, idx_scan from pg_stat_user_indexes
 where relname = 'pgbench_accounts' order by idx_scan desc;

schemaname  | relname          | indexrelname          | idx_scan
------------+------------------+-----------------------+----------
public      | pgbench_accounts | index_f               | 6
public      | pgbench_accounts | index_b               | 3
public      | pgbench_accounts | pgbench_accounts_pkey | 0
public      | pgbench_accounts | index_d               | 0
public      | pgbench_accounts | index_e               | 0
public      | pgbench_accounts | index_c               | 0
public      | pgbench_accounts | index_a               | 0
(7 rows)
```

> **Note**
>
> Estas estadísticas son incrementales desde el momento en que se restablecen las estadísticas. Supongamos que tiene un índice que solo se usa al final de un trimestre empresarial o solo para un informe específico. Es posible que este índice no se haya utilizado desde que se restablecieron las estadísticas. Para obtener más información, consulte Statistics Functions (Funciones de estadísticas). Los índices que se utilizan para garantizar la exclusividad no se analizan y no se deben identificar como índices no utilizados. Para identificar los índices no utilizados, debe tener un conocimiento profundo de la aplicación y sus consultas.

Para comprobar cuándo se restablecieron por última vez las estadísticas de una base de datos, utilice `pg_stat_database`.

```
postgres=> select datname, stats_reset from pg_stat_database where datname =
 'postgres';

datname   | stats_reset
----------+-------------------------------
postgres  | 2022-11-17 08:58:11.427224+00
(1 row)
```

Vaciado de una tabla lo más rápido posible

RDS para PostgreSQL 12 y versiones posteriores

Si tiene demasiados índices en una tabla grande, la instancia de base de datos podría estar a punto de reiniciar el identificador de transacción (XID), que es cuando el contador de XID vuelve a ponerse en cero. Si esta casilla no se marca, esta situación podría provocar la pérdida de datos. Sin embargo, puede vaciar rápidamente la tabla sin limpiar los índices. En RDS para PostgreSQL 12 y versiones posteriores, puede usar VACUUM con la cláusula `INDEX_CLEANUP`.

```
postgres=> VACUUM (INDEX_CLEANUP FALSE, VERBOSE TRUE) pgbench_accounts;

INFO: vacuuming "public.pgbench_accounts"
INFO: table "pgbench_accounts": found 0 removable, 8 nonremovable row versions in 1 out
 of 819673 pages
DETAIL: 0 dead row versions cannot be removed yet, oldest xmin: 7517
Skipped 0 pages due to buffer pins, 0 frozen pages.
CPU: user: 0.01 s, system: 0.00 s, elapsed: 0.01 s.
```

Si ya se está ejecutando una sesión de autovacuum, debe finalizarla para iniciar VACUUM manualmente. Para obtener información acerca de la ejecución de una inmovilización de vacío manual, consulte Realización de una inmovilización de vacío manual.

> **Note**
>
> Omitir la limpieza de índices con regularidad causa una sobrecarga de los índices, lo que degrada el rendimiento del análisis. El índice retiene las filas inactivas y la tabla retiene los punteros de línea inactivos. Como resultado, `pg_stat_all_tables.n_dead_tup` aumenta hasta que se ejecuta el vaciado automático o una operación VACUUM manual con limpieza de índices. Como práctica recomendada, use este procedimiento solo para impedir que el identificador se reinicie.

RDS para PostgreSQL 11 y versiones anteriores

Sin embargo, en RDS para PostgreSQL 11 y versiones anteriores, la única forma de hacer que el vacío se realice más rápidamente es reducir el número de índices de una tabla. La eliminación de un índice puede afectar a los planes de consulta. Le recomendamos que primero borre los índices no

utilizados y, a continuación, los índices cuando el reinicio de XID sea inminente. Una vez finalizado el proceso de vaciado, puede volver a crear estos índices.

Otros parámetros que afectan a autovacuum

La siguiente consulta mostrará los valores de algunos de los parámetros que afectan directamente a autovacuum y a su comportamiento. Los parámetros de autovacuum se describen en detalle en la documentación de PostgreSQL.

```
SELECT name, setting, unit, short_desc
FROM pg_settings
WHERE name IN (
'autovacuum_max_workers',
'autovacuum_analyze_scale_factor',
'autovacuum_naptime',
'autovacuum_analyze_threshold',
'autovacuum_analyze_scale_factor',
'autovacuum_vacuum_threshold',
'autovacuum_vacuum_scale_factor',
'autovacuum_vacuum_threshold',
'autovacuum_vacuum_cost_delay',
'autovacuum_vacuum_cost_limit',
'vacuum_cost_limit',
'autovacuum_freeze_max_age',
'maintenance_work_mem',
'vacuum_freeze_min_age');
```

Aunque todos estos parámetros afectan a autovacuum, estos son algunos de los más importantes:

- maintenance_work_mem
- autovacuum_freeze_max_age
- autovacuum_max_workers
- autovacuum_vacuum_cost_delay
- autovacuum_vacuum_cost_limit

Establecimiento de parámetros autovacuum de nivel de tabla

Los parámetros de almacenamiento relacionados con autovacuum se pueden definir en el nivel de tabla, algo que puede resultar mejor que alterar el comportamiento de toda la base de datos. Para

las tablas grandes, podría ser necesario definir unos ajustes agresivos, y es posible que no sea deseable que autovacuum se comporte de esa forma para todas las tablas.

La siguiente consulta mostrará qué tablas tienen habilitadas actualmente las opciones de nivel de tabla.

```
SELECT relname, reloptions
FROM pg_class
WHERE reloptions IS NOT null;
```

Un ejemplo en el que esto puede resultar útil es el de las tablas que son mucho más grandes que el resto de las tablas. Supongamos que dispone de una tabla de 300 GB y otras 30 tablas inferior a 1 GB. En ese caso, podría definir algunos parámetros concretos para la tabla grande con el fin de evitar alterar el comportamiento de todo el sistema.

```
ALTER TABLE mytable set (autovacuum_vacuum_cost_delay=0);
```

Al hacer esto, desactiva el retraso de autovacuum basado en costos para esta tabla a expensas de un mayor uso de recursos en su sistema. Normalmente, autovacuum hace una pausa por `autovacuum_vacuum_cost_delay` cada vez que se alcanza `autovacuum_cost_limit`. En la documentación de PostgreSQL, puede obtener información detallada relativa al vacío basado en el costo.

Registro de actividades de autovacuum y vacuum

La información sobre las actividades de autovacuum se envía a `postgresql.log` basado en el nivel especificado en el parámetro `rds.force_autovacuum_logging_level`. Los siguientes son los valores permitidos para este parámetro y las versiones de PostgreSQL para las que ese valor es la configuración predeterminada:

- `disabled` (PostgreSQL 10, PostgreSQL 9.6)
- `debug5`, `debug4`, `debug3`, `debug2`, `debug1`
- `info` (PostgreSQL 12, PostgreSQL 11)
- `notice`
- `warning` (PostgreSQL 13 y versiones posteriores)
- `error`, registro, `fatal`, `panic`

`rds.force_autovacuum_logging_level` funciona con el parámetro `log_autovacuum_min_duration`. El valor del parámetro `log_autovacuum_min_duration` es el límite (en milisegundos) por encima del cual se registran las acciones de autovacuum. Una configuración de `-1` no registra nada, mientras que una configuración de 0 registra todas las acciones. Al igual que con `rds.force_autovacuum_logging_level`, los valores predeterminados para `log_autovacuum_min_duration` dependen de la versión, como se indica a continuación:

- `10000 ms`: PostgreSQL 14, PostgreSQL 13, PostgreSQL 12 y PostgreSQL 11
- `(empty)`: no hay valor predeterminado para PostgreSQL 10 y PostgreSQL 9.6

Es recomendable que defina `rds.force_autovacuum_logging_level` como `WARNING`. También recomendamos configurar `log_autovacuum_min_duration` a un valor de 1000 a 5000. Una configuración de 5000 registra la actividad que tarda más de 5000 milisegundos. Cualquier configuración que no sea -1 también registra mensajes si la acción de autovaccum se omite debido a un bloqueo en conflicto o relaciones eliminadas al mismo tiempo. Para más información, visite Automatic Vacuuming (Vacío automático) en la documentación de PostgreSQL.

Para solucionar problemas, puede cambiar el parámetro `rds.force_autovacuum_logging_level` a uno de los niveles de depuración, desde `debug1` hasta `debug5` para obtener la información más detallada. Le recomendamos que utilice la configuración de depuración durante periodos cortos y solo con el objetivo de solucionar problemas. Para más información, visite When to log (Cuándo registrarse) en la documentación de PostgreSQL.

> **Note**
>
> PostgreSQL permite a la cuenta `rds_superuser` consultar sesiones de autovacuum en `pg_stat_activity`. Por ejemplo, podrá identificar y finalizar una sesión de autovacuum que bloquea la ejecución de un comando o que hace que se ejecute más despacio que un comando de vacío emitido manualmente.

Comportamiento de autovacuum con bases de datos no válidas

Se introduce un nuevo valor `-2` en la columna `datconnlimit` del catálogo `pg_database` para indicar que las bases de datos interrumpidas en mitad de la operación DROP DATABASE no son válidas.

Este nuevo valor está disponible en las siguientes versiones de RDS para PostgreSQL:

- Versión 15.4 y todas las versiones posteriores
- Versión 14.9 y posteriores
- Versión 13.12 y posteriores
- Versión 12.16 y posteriores
- Versión 11.21 y posteriores

Las bases de datos no válidas no afectan a la capacidad de autovacuum de bloquear la funcionalidad de las bases de datos válidas. Autovacuum ignora las bases de datos no válidas. Por lo tanto, las operaciones vacuum habituales seguirán funcionando de forma adecuada y eficiente en todas las bases de datos válidas de su entorno de PostgreSQL.

Temas

- Supervisión del ID de transacción
- Ajustes en la consulta de supervisión
- Resolución de problemas relacionados con bases de datos no válidas

Supervisión del ID de transacción

La función `age(datfrozenxid)` se suele utilizar para supervisar la antigüedad del ID de transacción (XID) de las bases de datos a fin de evitar que este se reinicie.

Como las bases de datos no válidas se excluyen del autovacuum, su contador de ID de transacción (XID) puede alcanzar el valor máximo de `2 billion`, reiniciarse en `- 2 billion` y continuar este ciclo indefinidamente. Una consulta típica para supervisar el reinicio del ID de transacción podría ser así:

```
SELECT max(age(datfrozenxid)) FROM pg_database;
```

Sin embargo, al introducir el valor -2 para `datconnlimit`, las bases de datos no válidas pueden sesgar los resultados de esta consulta. Como estas bases de datos no son válidas y no deberían formar parte de las comprobaciones de mantenimiento periódicas, pueden provocar falsos positivos y dar la impresión de que `age(datfrozenxid)` es mayor de lo que realmente es.

Ajustes en la consulta de supervisión

Para garantizar una supervisión precisa, debe ajustar la consulta de supervisión a fin de excluir las bases de datos no válidas. Siga esta consulta recomendada:

```
SELECT
    max(age(datfrozenxid))
FROM
    pg_database
WHERE
    datconnlimit <> -2;
```

Esta consulta garantiza que solo se tengan en cuenta las bases de datos válidas en el cálculo de `age(datfrozenxid)`, lo que aporta información fiable sobre la antigüedad del ID de transacción en todo el entorno de PostgreSQL.

Resolución de problemas relacionados con bases de datos no válidas

Al intentar conectarse a una base de datos no válida, es posible que vea un mensaje de error similar al siguiente:

```
postgres=> \c db1
connection to server at "mydb.xxxxxxxxxx.us-west-2.rds.amazonaws.com" (xx.xx.xx.xxx),
 port xxxx failed: FATAL:  cannot connect to invalid database "db1"
HINT:  Use DROP DATABASE to drop invalid databases.
Previous connection kept
```

Además, si el parámetro `log_min_messages` tiene un valor igual o superior a `DEBUG2`, es posible que vea que las siguientes entradas de registro muestran que el proceso de autovacuum omite la base de datos no válida:

```
2024-07-30 05:59:00 UTC::@:[32000]:DEBUG:  autovacuum: skipping invalid database "db6"
2024-07-30 05:59:00 UTC::@:[32000]:DEBUG:  autovacuum: skipping invalid database "db1"
```

Para resolver el problema, siga la `HINT` proporcionada durante el intento de conexión. Conéctese a cualquier base de datos válida mediante su cuenta maestra de RDS o una cuenta de base de datos con el rol `rds_superuser` y elimine las bases de datos no válidas.

```
SELECT
    'DROP DATABASE ' || quote_ident(datname) || ';'
FROM
    pg_database
WHERE
    datconnlimit = -2 \gexec
```

Identificación y resolución de los bloqueadores de vaciado intensivo en RDS para PostgreSQL

En PostgreSQL, la limpieza es fundamental para garantizar el buen estado de la base de datos, ya que recupera espacio de almacenamiento y evita problemas relacionados con los identificadores de transacciones. Sin embargo, hay situaciones que pueden impedir que el vaciado funcione como es debido, lo que puede mermar el rendimiento, provocar una sobrecarga de almacenamiento e incluso afectar a la disponibilidad de la instancia de base de datos debido a la superposición de ID de transacción. Por lo tanto, identificar y resolver estos problemas es esencial para lograr un rendimiento y una disponibilidad óptimos de la base de datos. Consulte Understanding autovacuum in Amazon RDS for PostgreSQL environments si desea conocer mejor la limpieza automática.

La función `postgres_get_av_diag()` ayuda a identificar los problemas que impiden o retrasan el avance de la limpieza agresiva. Se proporcionan sugerencias, entre otras, comandos para resolver el problema si es identificable o indicaciones para realizar diagnósticos adicionales cuando no se puede identificar el problema. Los bloqueadores de limpieza agresiva aparecen cuando su antigüedad supera el umbral de vacío automático adaptativo establecido por RDS, que es de 500 millones de identificadores de transacciones.

¿Qué antigüedad tiene el identificador de la transacción?

La función `age()` de identificadores de transacción calcula el número de transacciones que se han producido desde el identificador de transacción descongelado más antiguo de una base de datos (`pg_database.datfrozenxid`) o tabla (`pg_class.relfrozenxid`). Este valor indica la

actividad de la base de datos desde la última operación de limpieza agresiva y resalta la carga de trabajo probable para los próximos procesos de LIMPIEZA.

¿Qué es una limpieza agresiva?

Una operación de LIMPIEZA agresiva lleva a cabo un escaneo exhaustivo de todas las páginas de una tabla, incluidas las que normalmente se omiten durante las limpiezas normales. Este análisis exhaustivo tiene como objetivo congelar los ID de transacción que se acercan a su antigüedad máxima, evitando de forma eficaz una situación conocida como superposición de identificadores de transacción.

Para que `postgres_get_av_diag()` pueda detectar bloqueadores, el bloqueador debe haber realizado al menos 500 millones de transacciones.

Temas

- Instalación de herramientas de supervisión y diagnóstico de autovacuum en RDS para PostgreSQL
- Funciones de postgres_get_av_diag() en RDS para PostgreSQL
- Resolución de bloqueadores de vaciado identificables en RDS para PostgreSQL
- Resolución de bloqueadores de vaciado no identificables en RDS para PostgreSQL
- Resolución de problemas de rendimiento de vaciado en RDS para PostgreSQL
- Explicación de los mensajes de tipo NOTICE en RDS para PostgreSQL

Instalación de herramientas de supervisión y diagnóstico de autovacuum en RDS para PostgreSQL

La función `postgres_get_av_diag()` está disponible actualmente en las siguientes versiones de RDS para PostgreSQL:

- Versión 17.2 y otras versiones 17 superiores
- Versión 16.7 y otras versiones 16 superiores
- Versión 15.11 y otras versiones 15 superiores
- Versión 14.16 y otras versiones 14 superiores
- Versión 13.19 y otras versiones 13 superiores

Para utilizar `postgres_get_av_diag()`, cree la extensión `rds_tools`.

```
postgres=> CREATE EXTENSION rds_tools ;
```

```
CREATE EXTENSION
```

Compruebe que la extensión esté instalada.

```
postgres=> \dx rds_tools
             List of installed extensions
   Name    | Version |  Schema   |                    Description
 ----------+---------+-----------
+-------------------------------------------------------------
 rds_tools |   1.8   | rds_tools | miscellaneous administrative functions for RDS
 PostgreSQL
 1 row
```

Compruebe que la función se haya creado.

```
postgres=> SELECT
    proname function_name,
    pronamespace::regnamespace function_schema,
    proowner::regrole function_owner
FROM
    pg_proc
WHERE
    proname = 'postgres_get_av_diag';
    function_name     | function_schema | function_owner
----------------------+-----------------+----------------
 postgres_get_av_diag | rds_tools       | rds_superuser
(1 row)
```

Funciones de postgres_get_av_diag() en RDS para PostgreSQL

La función `postgres_get_av_diag()` recupera información de diagnóstico sobre los procesos de autovacuum que se bloquean o se retrasan en una base de datos de RDS para PostgreSQL. La consulta debe ejecutarse en la base de datos con el ID de transacción más antiguo para obtener resultados precisos. Para obtener más información sobre el uso de la base de datos con el ID de transacción más antiguo, consulte Not connected to the database with the age of oldest transaction ID

```
SELECT
    blocker,
    DATABASE,
    blocker_identifier,
```

```
    wait_event,
    TO_CHAR(autovacuum_lagging_by, 'FM9,999,999,999') AS autovacuum_lagging_by,
    suggestion,
    suggested_action
FROM (
    SELECT
        *
    FROM
        rds_tools.postgres_get_av_diag ()
    ORDER BY
        autovacuum_lagging_by DESC) q;
```

La función `postgres_get_av_diag()` devuelve una tabla con la siguiente información:

blocker

Especifica la categoría de actividad de la base de datos que bloquea el vaciado.

- Instrucción activa
- Inactividad en la transacción
- Transacción preparada
- Ranura de replicación lógica
- Réplica de lectura con ranura de replicación física
- Réplica de lectura con replicación de streaming
- Tablas temporales

database

Especifica el nombre de la base de datos, si está disponible y es compatible. Esta es la base de datos en la que la actividad está en curso y bloquea o bloqueará el autovacuum. Esta es la base de datos a la que debe conectarse y sobre la que debe actuar.

blocker_identifier

Especifica el identificador de la actividad que bloquea o bloqueará el autovacuum. El identificador puede ser un ID de proceso junto con una instrucción SQL, una transacción preparada, una dirección IP de una réplica de lectura y el nombre de la ranura de replicación, ya sea lógica o física.

wait_event

Especifica el evento de espera de la sesión de bloqueo y se aplica a los siguientes bloqueadores:

- Instrucción activa
- Inactividad en la transacción

autovacum_lagging_by

Especifica el número de transacciones que tiene pendiente el autovacuum según sus trabajos por realizar y por categoría.

suggestion

Especifica sugerencias para resolver el bloqueo. Estas instrucciones incluyen el nombre de la base de datos en la que existe la actividad, cuando proceda, el ID de proceso (PID) de la sesión, cuando proceda, y la acción que se debe realizar.

suggested_action

Sugiere la acción que se debe llevar a cabo para resolver el bloqueo.

Resolución de bloqueadores de vaciado identificables en RDS para PostgreSQL

Autovacuum lleva a cabo vaciados de forma intensiva y reduce la antigüedad de los ID de transacción hasta situarlos por debajo del umbral especificado por el parámetro `autovacuum_freeze_max_age` de la instancia de RDS. Esta antigüedad se puede consultar mediante la métrica `MaximumUsedTransactionIDs` de Amazon CloudWatch.

Para encontrar la configuración de `autovacuum_freeze_max_age` (que tiene un valor predeterminado de 200 millones de ID de transacción) para una instancia de Amazon RDS, puede utilizar la siguiente consulta:

```
SELECT
    TO_CHAR(setting::bigint, 'FM9,999,999,999') autovacuum_freeze_max_age
FROM
    pg_settings
WHERE
    name = 'autovacuum_freeze_max_age';
```

Tenga en cuenta que `postgres_get_av_diag()` solo comprueba si hay bloqueadores de vaciado intensivo cuando la antigüedad supera el umbral de autovacuum adaptativo de Amazon RDS de 500 millones de ID de transacción. Para que `postgres_get_av_diag()` detecte los bloqueadores, el bloqueador debe tener al menos 500 millones de transacciones de antigüedad.

La función `postgres_get_av_diag()` identifica los siguientes tipos de bloqueadores:

Temas

- Instrucción activa
- Inactividad en la transacción
- Transacción preparada
- Ranura de replicación lógica
- Réplicas de lectura
- Tablas temporales

Instrucción activa

En PostgreSQL, una instrucción activa es una instrucción SQL que la base de datos está ejecutando actualmente. Incluye consultas, transacciones o cualquier operación en curso. Al realizar la supervisión mediante `pg_stat_activity`, la columna de estado indica que el proceso con el PID correspondiente está activo.

La función `postgres_get_av_diag()` muestra un resultado similar al siguiente cuando identifica una instrucción que resulta ser una instrucción activa.

```
blocker               | Active statement
database              | my_database
blocker_identifier    | SELECT pg_sleep(20000);
wait_event            | Timeout:PgSleep
autovacuum_lagging_by | 568,600,871
suggestion            | Connect to database "my_database", review carefully and you
 may consider terminating the process using suggested_action. For more information, see
 Working with PostgreSQL autovacuum in the Amazon RDS User Guide.
suggested_action      | {"SELECT pg_terminate_backend (29621);"}
```

Acción sugerida

Siguiendo las instrucciones de la columna `suggestion`, el usuario puede conectarse a la base de datos en la que se encuentra la instrucción activa y, tal como se especifica en la columna `suggested_action`, se recomienda revisar detenidamente la opción de finalizar la sesión. Si la finalización es segura, se puede utilizar la función `pg_terminate_backend()` para finalizar la sesión. Esta acción la puede realizar un administrador (como la cuenta maestra de RDS) o un usuario con el privilegio `pg_terminate_backend()` necesario.

> **Warning**
>
> Al finalizar la sesión, se desharán (ROLLBACK) los cambios que haya realizado. En función de sus requisitos, es posible que quiera volver a ejecutar la instrucción. Sin embargo, se recomienda hacerlo únicamente después de que el proceso de autovacuum haya finalizado su operación de vaciado intensivo.

Inactividad en la transacción

El concepto de inactividad en una instrucción de transacción se refiere a cualquier sesión en la que se haya abierto una transacción explícita (por ejemplo, emitiendo una instrucción `BEGIN`), se haya realizado algún trabajo y se esté esperando a que el cliente pase más trabajo o dé la señal de finalización de la transacción emitiendo una instrucción `COMMIT`, `ROLLBACK` o `END` (lo que daría como resultado un `COMMIT` implícitamente).

La función `postgres_get_av_diag()` muestra un resultado similar al siguiente cuando identifica una instrucción `idle in transaction` como bloqueador.

```
blocker               | idle in transaction
database              | my_database
blocker_identifier    | INSERT INTO tt SELECT * FROM tt;
wait_event            | Client:ClientRead
autovacuum_lagging_by | 1,237,201,759
suggestion            | Connect to database "my_database", review carefully and you
 may consider terminating the process using suggested_action. For more information, see
 Working with PostgreSQL autovacuum in the Amazon RDS User Guide.
suggested_action      | {"SELECT pg_terminate_backend (28438);"}
```

Acción sugerida

Como se indica en la columna `suggestion`, puede conectarse a la base de datos en la que se encuentra la sesión de inactividad en la transacción y finalizar la sesión mediante la función `pg_terminate_backend()`. El usuario puede ser su usuario administrador (cuenta maestra de RDS) o un usuario con el privilegio `pg_terminate_backend()`.

> **Warning**
>
> Al finalizar la sesión, se desharán (ROLLBACK) los cambios que haya realizado. En función de sus requisitos, es posible que quiera volver a ejecutar la instrucción. Sin embargo, se

recomienda hacerlo únicamente después de que el proceso de autovacuum haya finalizado su operación de vaciado intensivo.

Transacción preparada

PostgreSQL permite realizar transacciones que forman parte de una estrategia de confirmación de dos fases denominada transacciones preparadas. Se habilitan al establecer el parámetro `max_prepared_transactions` en un valor distinto de cero. Las transacciones preparadas han sido diseñadas para garantizar que una transacción sea duradera y permanezca disponible incluso después de que la base de datos se bloquee, se reinicie o se desconecte del cliente. Al igual que las transacciones normales, se les asigna un identificador de transacción y pueden afectar al autovacuum. Si se deja en un estado preparado, el autovacuum no puede realizar la congelación y podría provocar un reinicio del ID de transacción.

Cuando las transacciones se dejan preparadas indefinidamente sin que las resuelva un administrador de transacciones, se convierten en transacciones preparadas huérfanas. La única forma de solucionar este problema es confirmar o revertir la transacción mediante los comandos `COMMIT PREPARED` o `ROLLBACK PREPARED` respectivamente.

> **Note**
>
> Tenga en cuenta que una copia de seguridad realizada durante una transacción preparada seguirá conteniendo esa transacción después de la restauración. Consulte la siguiente información sobre cómo localizar y cerrar dichas transacciones.

La función `postgres_get_av_diag()` muestra el siguiente resultado cuando identifica un bloqueador que es una transacción preparada.

```
blocker               | Prepared transaction
database              | my_database
blocker_identifier    | myptx
wait_event            | Not applicable
autovacuum_lagging_by | 1,805,802,632
suggestion            | Connect to database "my_database" and consider either COMMIT
 or ROLLBACK the prepared transaction using suggested_action. For more information, see
 Working with PostgreSQL autovacuum in the Amazon RDS User Guide.
suggested_action      | {"COMMIT PREPARED 'myptx';",[OR],"ROLLBACK PREPARED 'myptx';"}
```

Acción sugerida

Como se menciona en la columna de sugerencias, conéctese a la base de datos en la que se encuentre la transacción preparada. Sobre la base de la columna `suggested_action`, revise detenidamente si desea enviar una instrucción `COMMIT` o `ROLLBACK`, y realizar la acción correspondiente.

Para supervisar las transacciones preparadas en general, PostgreSQL ofrece una vista de catálogo llamada `pg_prepared_xacts`. Puede utilizar la siguiente consulta para buscar transacciones preparadas.

```
SELECT
    gid,
    prepared,
    owner,
    database,
    transaction AS oldest_xmin
FROM
    pg_prepared_xacts
ORDER BY
    age(transaction) DESC;
```

Ranura de replicación lógica

El propósito de una ranura de replicación es almacenar los cambios no consumidos hasta que se repliquen en un servidor de destino. Para obtener más información, consulte Logical replication de PostgreSQL.

Existen dos tipos de ranuras de replicación lógica.

Ranuras de replicación lógica inactivas

Cuando finaliza la replicación, los registros de transacciones no consumidas no se pueden eliminar y la ranura de replicación queda inactiva. Aunque un suscriptor no utilice actualmente una ranura de replicación lógica inactiva, esta permanece en el servidor, lo que provoca la retención de los archivos WAL y evita la eliminación de los registros de transacciones antiguos. Esto puede aumentar el uso del disco y, específicamente, impedir que autovacuum limpie las tablas del catálogo interno, ya que el sistema debe evitar que se sobrescriba la información de LSN. Si este problema no se soluciona, puede provocar una sobrecarga del catálogo, una degradación del rendimiento y un mayor riesgo de que se produzcan vaciados previos al reinicio, lo que podría causar tiempo de inactividad en las transacciones.

Ranuras de replicación lógica activas pero lentas

A veces, la eliminación de las tuplas inactivas del catálogo se retrasa debido a la degradación del rendimiento de la replicación lógica. Este retraso en la replicación ralentiza la actualización de `catalog_xmin` y puede provocar una sobrecarga del catálogo y un vaciado previo al reinicio.

La función `postgres_get_av_diag()` muestra un resultado similar al siguiente cuando encuentra una ranura de replicación lógica que funciona como bloqueador.

```
blocker               | Logical replication slot
database              | my_database
blocker_identifier    | slot1
wait_event            | Not applicable
autovacuum_lagging_by | 1,940,103,068
suggestion            | Ensure replication is active and resolve any lag for the slot
 if active. If inactive, consider dropping it using the command in suggested_action.
 For more information, see Working with PostgreSQL autovacuum in the Amazon RDS User
 Guide.
suggested_action      | {"SELECT pg_drop_replication_slot('slot1') FROM
 pg_replication_slots WHERE active = 'f';"}
```

Acción sugerida

Para resolver este problema, compruebe la configuración de la replicación para ver si hay problemas con el esquema o los datos de destino que puedan estar finalizando el proceso de aplicación. Los motivos más comunes son los siguientes:

- Columnas faltantes
- Tipos de datos incompatibles
- Discrepancia de datos
- Tabla faltante

Si el problema está relacionado con problemas de infraestructura:

- Problemas de red: ¿cómo resuelvo los problemas con una base de datos de Amazon RDS en un estado de red incompatible?
- La base de datos o la instancia de base de datos no están disponibles por una de las siguientes razones:

- La instancia de réplica se ha quedado sin espacio de almacenamiento: consulte qué hacer cuando las instancias de base de datos de Amazon RDS se quedan sin almacenamiento para obtener información sobre cómo añadir almacenamiento.
- Parámetros incompatibles: revise ¿Cómo puedo corregir una instancia de base de datos de Amazon RDS que está estancada en el estado parámetros incompatibles? para obtener más información acerca de cómo solucionar este problema.

Si la instancia está fuera de la red de AWS o en AWS EC2, consulte a su administrador sobre cómo resolver los problemas relacionados con la disponibilidad o la infraestructura.

Eliminación de la ranura inactiva

> **Warning**
>
> Precaución: Antes de eliminar una ranura de replicación, asegúrese exhaustivamente de que no tenga ninguna replicación en curso, de que esté inactiva y de que se encuentre en un estado irrecuperable. Si se elimina una ranura de forma prematura, se podría interrumpir la replicación o provocar la pérdida de datos.

Después de confirmar que la ranura de replicación ya no es necesaria, elimínela para permitir que el autovacuum continúe. La condición `active = 'f'` garantiza que solo se eliminará una ranura inactiva.

```
SELECT pg_drop_replication_slot('slot1') WHERE active ='f'
```

Réplicas de lectura

Cuando la configuración `hot_standby_feedback` está habilitada para las réplicas de lectura de Amazon RDS, evita que el autovacuum de la base de datos principal elimine determinadas filas inactivas que podrían seguir necesitando las consultas que se ejecuten en la réplica de lectura. Esto afecta a todos los tipos de réplicas de lectura físicas, incluidas las que se administran con o sin ranuras de replicación. Este comportamiento es necesario porque las consultas que se ejecutan en la réplica en espera requieren que esas filas permanezcan disponibles en el servidor principal, lo que evita cancelaciones y conflictos de consultas.

Réplica de lectura con ranura de replicación física

Las réplicas de lectura con ranuras de replicación físicas mejoran considerablemente la fiabilidad y la estabilidad de la replicación en RDS para PostgreSQL. Estas ranuras garantizan que la base de datos principal conserve los archivos de registro de escritura anticipada esenciales hasta que la réplica los procese, ya que esto mantiene la coherencia de datos incluso durante las interrupciones de la red.

A partir de la versión 14 de RDS para PostgreSQL, todas las réplicas utilizan ranuras de replicación. En las versiones anteriores, solo las réplicas entre regiones utilizaban ranuras de replicación.

La función `postgres_get_av_diag()` muestra un resultado similar al siguiente cuando encuentra una réplica de lectura con una ranura de replicación física como bloqueador.

```
blocker               | Read replica with physical replication slot
database              |
blocker_identifier    | rds_us_west_2_db_xxxxxxxxxxxxxxxxxxxx
wait_event            | Not applicable
autovacuum_lagging_by | 554,080,689
suggestion            | Run the following query on the replica
 "rds_us_west_2_db_xxxxxxxxxxxxxxxxxxx" to find the long running query:

                      | SELECT * FROM pg_catalog.pg_stat_activity WHERE
 backend_xmin::text::bigint = 757989377;

                      | Review carefully and you may consdier terminating the query on
 read replica using suggested_action. For more information, see Working with PostgreSQL
 autovacuum in the Amazon RDS User Guide.                                  +
          |
suggested_action      | {"SELECT pg_terminate_backend(pid) FROM
 pg_catalog.pg_stat_activity WHERE backend_xmin::text::bigint = 757989377;","
                                                                          +
                      | [OR]

                                                +
                      | ","Disable hot_standby_feedback","

                                                +
                      | [OR]

                                                +
                      | ","Delete the read replica if not needed"}
```

Réplica de lectura con replicación de streaming

Amazon RDS permite configurar réplicas de lectura sin una ranura de replicación física en versiones anteriores, hasta la versión 13. Este enfoque reduce la sobrecarga al permitir que el servidor principal recicle los archivos WAL de forma más intensiva, lo que resulta ventajoso en entornos con limitaciones del espacio en disco y en los que se pueda tolerar un ReplicaLag ocasional. Sin embargo, sin no dispone de una ranura, la réplica en espera debe permanecer sincronizada para evitar que se pierdan archivos WAL. Amazon RDS utiliza archivos WAL archivados para ayudar a la réplica a ponerse al día en caso de que se quede atrás, pero este proceso requiere una supervisión exhaustiva y puede resultar lento.

La función `postgres_get_av_diag()` muestra un resultado similar al siguiente cuando encuentra una réplica de lectura de streaming como bloqueador.

```
blocker               | Read replica with streaming replication slot
database              | Not applicable
blocker_identifier    | xx.x.x.xxx/xx
wait_event            | Not applicable
autovacuum_lagging_by | 610,146,760
suggestion            | Run the following query on the replica "xx.x.x.xxx" to find the
 long running query:
                                                                                +
                      | SELECT * FROM pg_catalog.pg_stat_activity WHERE
 backend_xmin::text::bigint = 348319343;

               +
                      | Review carefully and you may consdier terminating the query on
 read replica using suggested_action. For more information, see Working with PostgreSQL
 autovacuum in the Amazon RDS User Guide.                                        +
                      |
suggested_action      | {"SELECT pg_terminate_backend(pid) FROM
 pg_catalog.pg_stat_activity WHERE backend_xmin::text::bigint = 348319343;","

                       +
                      | [OR]

                                                                                +
                      | ","Disable hot_standby_feedback","

                                                                                +
                      | [OR]

                                                                                +
                      | ","Delete the read replica if not needed"}
```

Acción sugerida

Como se recomienda en la columna `suggested_action`, revise detenidamente estas opciones para desbloquear el autovacuum.

- Finalizar la consulta: de acuerdo con las instrucciones de la columna de sugerencias, puede conectarse a la réplica de lectura, tal y como se especifica en la columna suggested_action. Se recomienda revisar detenidamente la opción para finalizar la sesión. Si la finalización se considera segura, se puede utilizar la función `pg_terminate_backend()` para finalizar la sesión. Esta acción la puede realizar un administrador (como la cuenta maestra de RDS) o un usuario con el privilegio pg_terminate_backend() necesario.

  Puede ejecutar el siguiente comando SQL en la réplica de lectura para finalizar la consulta que impide que el proceso de vaciado en el principal pueda limpiar las filas antiguas. El valor de `backend_xmin` se indica en la salida de la función:

  ```
  SELECT
      pg_terminate_backend(pid)
  FROM
      pg_catalog.pg_stat_activity
  WHERE
      backend_xmin::text::bigint = backend_xmin;
  ```

- Desactivar la retroalimentación de espera activa: plantéese deshabilitar el parámetro `hot_standby_feedback` si provoca retrasos significativos en el vaciado.

  El parámetro `hot_standby_feedback` permite que una réplica de lectura informe al servidor principal sobre su actividad de consulta, lo que evita que el principal vacíe las tablas o filas que están en uso en la réplica en espera. Si bien esto garantiza la estabilidad de las consultas en la réplica en espera, puede retrasar considerablemente el vaciado en el principal. La desactivación de esta característica permite al servidor principal continuar con el vaciado sin tener que esperar a que la réplica en espera se ponga al día. Sin embargo, esto puede provocar cancelaciones o errores en las consultas en la réplica en espera si intenta acceder a las filas que ha vaciado el principal.

- Eliminar la réplica de lectura si no es necesaria: si la réplica de lectura ya no es necesaria, puede eliminarla. Esto eliminará la sobrecarga de replicación asociada y permitirá que el servidor principal recicle los registros de transacciones sin que la réplica se lo obstaculice.

Tablas temporales

Las tablas temporales, que se crean con la palabra clave `TEMPORARY`, residen en el esquema temporal (por ejemplo, pg_temp_xxx) y solo la sesión que las haya creado puede acceder a ellas. Las tablas temporales se eliminan al finalizar la sesión. Sin embargo, estas tablas son invisibles para el proceso de autovacuum de PostgreSQL y la sesión que las haya creado debe vaciarlas manualmente. Intentar vaciar la tabla temporal desde otra sesión no tiene ningún efecto.

En circunstancias poco habituales, puede existir una tabla temporal sin que sea propiedad de una sesión activa. Si la sesión propietaria finaliza inesperadamente debido a un bloqueo grave, un problema de red o un suceso similar, es posible que la tabla temporal no se limpie y quede como una tabla “huérfana”. Cuando el proceso de autovacuum de PostgreSQL detecta una tabla temporal huérfana, registra el siguiente mensaje:

```
LOG: autovacuum: found orphan temp table \"%s\".\"%s\" in database \"%s\"
```

La función `postgres_get_av_diag()` muestra un resultado similar al siguiente cuando identifica una tabla temporal como bloqueador. Para que la función muestre correctamente el resultado relacionado con las tablas temporales, debe ejecutarse en la misma base de datos en la que se encuentren esas tablas.

```
blocker               | Temporary table
database              | my_database
blocker_identifier    | pg_temp_14.ttemp
wait_event            | Not applicable
autovacuum_lagging_by | 1,805,802,632
suggestion            | Connect to database "my_database". Review carefully, you
 may consider dropping temporary table using command in suggested_action. For more
 information, see Working with PostgreSQL autovacuum in the Amazon RDS User Guide.
suggested_action      | {"DROP TABLE ttemp;"}
```

Acción sugerida

Siga las instrucciones que aparecen en la columna `suggestion` del resultado para identificar y eliminar la tabla temporal que impide la ejecución del autovacuum. Use el siguiente comando para eliminar la tabla temporal notificada por `postgres_get_av_diag()`. Reemplace el nombre de la tabla en función del resultado proporcionado por la función `postgres_get_av_diag()`.

```
DROP TABLE my_temp_schema.my_temp_table;
```

La siguiente consulta se puede utilizar para identificar tablas temporales:

```
SELECT
    oid,
    relname,
    relnamespace::regnamespace,
    age(relfrozenxid)
FROM
    pg_class
WHERE
relpersistence = 't'
ORDER BY
    age(relfrozenxid) DESC;
```

Resolución de bloqueadores de vaciado no identificables en RDS para PostgreSQL

En esta sección se analizan otros motivos que pueden impedir que el progreso del vaciado. Actualmente, la función `postgres_get_av_diag()` no puede identificar directamente estos problemas.

Temas

- Páginas no válidas
- Incoherencia en los índices
- Tasa de transacciones excepcionalmente alta

Páginas no válidas

Se produce un error de página no válida cuando PostgreSQL detecta una discrepancia en la suma de comprobación de una página al acceder a esa página. El contenido resulta ilegible, lo que impide que autovacuum congele las tuplas. Esto detiene de forma efectiva el proceso de limpieza. El siguiente error está escrito en el registro de PostgreSQL:

```
WARNING:  page verification failed, calculated checksum YYYYY but expected XXXX
ERROR:  invalid page in block ZZZZZ of relation base/XXXXX/XXXXX
CONTEXT:  automatic vacuum of table myschema.mytable
```

Determinar el tipo de objeto

```
ERROR: invalid page in block 4305910 of relation base/16403/186752608
```

```
WARNING: page verification failed, calculated checksum 50065 but expected 60033
```

A partir del mensaje de error, la ruta `base/16403/186752608` proporciona la siguiente información:

- “base” es el nombre del directorio de datos de PostgreSQL.
- “16403” es el OID de la base de datos, que puede buscar en el catálogo del sistema `pg_database`.
- “186752608” es el `relfilenode`, que puede utilizar para buscar el nombre del objeto y el esquema en el catálogo del sistema `pg_class`.

Al comprobar el resultado de la siguiente consulta en la base de datos afectada, puede determinar el tipo de objeto. La siguiente consulta recupera información de objeto para el oid: 186752608. Sustituya este OID por el correspondiente para el error que haya encontrado.

```
SELECT
    relname AS object_name,
    relkind AS object_type,
    nspname AS schema_name
FROM
    pg_class c
    JOIN pg_namespace n ON c.relnamespace = n.oid
WHERE
    c.oid = 186752608;
```

Para obtener más información, consulte la documentación de PostgreSQL sobre `pg_class` para ver todos los tipos de objetos compatibles, indicados en la columna `relkind` de `pg_class`.

Indicaciones

La solución más eficaz para este problema depende de la configuración de la instancia específica de Amazon RDS y del tipo de datos afectados por la página incoherente.

Si el tipo de objeto es un índice:

Se recomienda volver a crear el índice.

- Uso de la opción **`CONCURRENTLY`**: antes de la versión 12 de PostgreSQL, la reconstrucción de un índice requería un bloqueo de tabla exclusivo, lo que restringía el acceso a la misma. Con PostgreSQL versión 12 y versiones posteriores, la opción `CONCURRENTLY` permite el bloqueo por

filas, lo que mejora significativamente la disponibilidad de la tabla. A continuación, se muestra el comando:

```
REINDEX INDEX ix_name CONCURRENTLY;
```

Si bien CONCURRENTLY resulta menos disruptivo, puede ser más lento en tablas de uso intensivo. Si es posible, considere la posibilidad de crear el índice durante los períodos de poco tráfico.

Para obtener más información, consulte la documentación de PostgreSQL sobre REINDEX.

- Uso de la opción **INDEX_CLEANUP FALSE**: si los índices son grandes y se calcula que tardarán mucho en completarse, puede desbloquear el autovacuum ejecutando un VACUUM FREEZE manual y excluyendo los índices. Esta funcionalidad está disponible en la versión 12 y posteriores de PostgreSQL.

  Omitir los índices le permitirá saltarse el proceso de vaciado del índice incoherente y mitigar el problema del reinicio. Sin embargo, esto no resolverá el problema subyacente de la página no válida. Para solucionar por completo el problema de la página no válida y resolverlo, tendrá que volver a crear el índice.

Si el tipo de objeto es una vista materializada:

Si se produce un error de página no válida en una vista materializada, inicie sesión en la base de datos afectada y actualícela para resolver la página no válida:

Actualice la vista materializada:

```
REFRESH MATERIALIZED VIEW schema_name.materialized_view_name;
```

Si se produce un error al actualizar, intente volver a crearla:

```
DROP MATERIALIZED VIEW schema_name.materialized_view_name;
CREATE MATERIALIZED VIEW schema_name.materialized_view_name AS query;
```

Al actualizar o volver a crear la vista materializada, se restaura sin que esto afecte a los datos de la tabla subyacente.

Para todos los demás tipos de objetos:

Para todos los demás tipos de objetos, puede ponerse en contacto con el servicio de asistencia de AWS.

Incoherencia en los índices

Un índice que no sea coherente desde el punto de vista lógico puede impedir que avance el autovacuum. Los siguientes errores u otros similares se registran durante la fase de vaciado del índice o cuando se accede al índice mediante instrucciones SQL.

```
ERROR: right sibling's left-link doesn't match:block 5 links to 10 instead of expected
 2 in index ix_name
```

```
ERROR: failed to re-find parent key in index "XXXXXXXXXX" for deletion target page XXX
CONTEXT:  while vacuuming index index_name of relation schema.table
```

Indicaciones

Reconstruya el índice u omita los índices utilizando `INDEX_CLEANUP` con un `VACUUM FREEZE` manual. Para obtener información sobre cómo reconstruir el índice, consulte Si el tipo de objeto es un índice.

- Uso de la opción CONCURRENTLY: antes de la versión 12 de PostgreSQL, la reconstrucción de un índice requería un bloqueo de tabla exclusivo, lo que restringía el acceso a la misma. Con PostgreSQL versión 12 y versiones posteriores, la opción CONCURRENTLY permite el bloqueo por filas, lo que mejora significativamente la disponibilidad de la tabla. A continuación, se muestra el comando:

  ```
  REINDEX INDEX ix_name CONCURRENTLY;
  ```

  Si bien CONCURRENTLY resulta menos disruptivo, puede ser más lento en tablas de uso intensivo. Si es posible, considere la posibilidad de crear el índice durante los períodos de poco tráfico. Para obtener más información, consulte REINDEX en la documentación de PostgreSQL.
- Uso de la opción INDEX_CLEANUP FALSE: si los índices son grandes y se calcula que tardarán mucho en completarse, puede desbloquear el autovacuum ejecutando un VACUUM FREEZE manual y excluyendo los índices. Esta funcionalidad está disponible en la versión 12 y posteriores de PostgreSQL.

  Omitir los índices le permitirá saltarse el proceso de vaciado del índice incoherente y mitigar el problema del reinicio. Sin embargo, esto no resolverá el problema subyacente de la página no

válida. Para solucionar por completo el problema de la página no válida y resolverlo, tendrá que volver a crear el índice.

Tasa de transacciones excepcionalmente alta

En PostgreSQL, las tasas de transacción altas pueden afectar significativamente al rendimiento de autovacuum, lo que implica una limpieza más lenta de las tuplas inactivas y a un aumento del riesgo de reiniciar los ID de transacción. Puede supervisar la tasa de transacciones midiendo la diferencia en `max(age(datfrozenxid))` entre dos períodos de tiempo, normalmente por segundo. Además, puede utilizar las siguientes métricas de contador de Información de rendimiento de RDS para medir la tasa de transacciones (la suma de xact_commit y xact_rollback), que es el número total de transacciones.

Contador	Tipo	Unidad	Métrica
xact_commit	Transacciones	Confirmaciones por segundo	db.Transactions.xact_commit
xact_rollback	Transacciones	Restauraciones por segundo	db.Transactions.xact_rollback

Un aumento rápido indica una alta carga de transacciones, lo que puede ser excesivo para autovacuum y provocar sobrecargas, bloqueos y posibles problemas de rendimiento. Esto puede tener un impacto negativo en el proceso de autovacuum de dos maneras:

- Actividad de la tabla: la tabla específica que se está vaciando podría estar registrando un gran volumen de transacciones, lo que provocaría retrasos.
- Recursos del sistema: el sistema en general puede estar sobrecargado, lo que dificulta que autovacuum acceda a los recursos necesarios para funcionar de manera eficiente.

Plantéese las siguientes estrategias para permitir que autovacuum funcione de manera más eficaz y pueda seguir el ritmo de sus tareas:

1. Reduzca la tasa de transacciones si es posible. Plantéese la posibilidad de agrupar o agrupar transacciones similares cuando sea posible.

2. Utilice tablas que se actualicen con frecuencia mediante la operación `VACUUM FREEZE` manual cada noche, semana o quincena durante las horas de menor actividad.
3. Plantéese la posibilidad de escalar verticalmente su clase de instancia para asignar más recursos del sistema con el fin de administrar el volumen de transacciones elevado y el autovacuum.

Resolución de problemas de rendimiento de vaciado en RDS para PostgreSQL

En esta sección se analizan los factores que suelen contribuir a reducir el rendimiento del vaciado y cómo abordar estos problemas.

Temas

- Vaciado de índices grandes
- Demasiadas tablas o bases de datos que vaciar
- Se está ejecutando un vaciado intensivo (para evitar el reinicio)

Vaciado de índices grandes

VACUUM funciona a través de fases secuenciales: inicialización, escaneo del montón, vaciado de índices y montón, limpieza de índices, truncamiento del montón y limpieza final. Durante el escaneo del montón, el proceso elimina las páginas, las desfragmenta y las congela. Después de completar el escaneo del montón, VACUUM limpia los índices, se devuelven las páginas vacías al sistema operativo y se realizan tareas de limpieza final, como el vaciado del mapa del espacio libre y la actualización de las estadísticas.

Es posible que sea necesario realizar varias pasadas para el vaciado de índices cuando `maintenance_work_mem` (o `autovacuum_work_mem`) no es suficiente para procesar el índice. En la versión 16 y anteriores de PostgreSQL, un límite de memoria de 1 GB para almacenar los ID de tuplas inactivas a menudo forzaba varias pasadas en índices grandes. PostgreSQL 17 presenta `TidStore`, que asigna memoria de forma dinámica en lugar de utilizar una matriz de asignación única. Esto elimina la restricción de 1 GB, utiliza la memoria de manera más eficiente y reduce la necesidad de realizar varios análisis de índice por cada índice.

Es posible que los índices grandes aún requieran varias pasadas en PostgreSQL 17 si la memoria disponible no puede acomodar todo el procesamiento del índice de una vez. Por lo general, los índices mayores contienen más tuplas inactivas que requieren varias pasadas.

Detección de operaciones de limpieza lentas

La función `postgres_get_av_diag()` puede detectar cuando las operaciones de limpieza se ejecutan lentamente debido a memoria insuficiente. Para obtener más información sobre esta función, consulte Instalación de herramientas de supervisión y diagnóstico de autovacuum en RDS para PostgreSQL.

La función `postgres_get_av_diag()` emite los siguientes avisos cuando la memoria disponible no es suficiente para completar la limpieza del índice en una sola pasada.

`rds_tools` 1.8

```
NOTICE: Your database is currently running aggressive vacuum to prevent wraparound and
 it might be slow.
```

```
NOTICE: The current setting of autovacuum_work_mem is "XXX" and might not be
 sufficient. Consider increasing the setting, and if necessary, scaling up the Amazon
 RDS instance class for more memory.
       Additionally, review the possibility of manual vacuum with exclusion of indexes
 using (VACUUM (INDEX_CLEANUP FALSE, VERBOSE TRUE) table_name;).
```

`rds_tools` 1.9

```
NOTICE: Your database is currently running aggressive vacuum to prevent wraparound and
 it might be slow.
```

```
NOTICE: The current setting of autovacuum_work_mem is XX might not be sufficient.
 Consider increasing the setting to XXX, and if necessary, scaling up the RDS instance
 class for more
       memory. The suggested value is an estimate based on the current number of dead
 tuples for the table being vacuumed, which might not fully reflect the latest state.
 Additionally, review the possibility of manual
       vacuum with exclusion of indexes using (VACUUM (INDEX_CLEANUP FALSE, VERBOSE
 TRUE) table_name;). For more information, see
       Working with PostgreSQL autovacuum in the Amazon Amazon RDS User Guide
       .
```

> **Note**
>
> La función `postgres_get_av_diag()` se basa en `pg_stat_all_tables.n_dead_tup` para estimar la cantidad de memoria necesaria para el vaciado de índices.

Cuando la función `postgres_get_av_diag()` identifique una operación de limpieza lenta que requiera múltiples análisis de índice debido a que no hay suficiente `autovacuum_work_mem`, generará el siguiente mensaje:

```
NOTICE: Your vacuum is performing multiple index scans due to insufficient
 autovacuum_work_mem:XXX for index vacuuming.
       For more information, see Working with PostgreSQL autovacuum in the Amazon
 Amazon RDS User Guide.
```

Indicaciones

Puede aplicar las siguientes soluciones alternativas utilizando manualmente `VACUUM FREEZE` para acelerar la congelación de la tabla.

Aumentar la memoria de vaciado

Como sugiere la función `postgres_get_av_diag()`, se recomienda aumentar el parámetro `autovacuum_work_mem` para abordar las posibles restricciones de memoria en cada instancia. Aunque `autovacuum_work_mem` es un parámetro dinámico, es importante tener en cuenta que, para que la nueva configuración de memoria surta efecto, el daemon de autovacuum debe reiniciar sus procesos de trabajo. Para lograrlo:

1. Confirme que la nueva configuración esté establecida.
2. Finalice los procesos que actualmente estén ejecutando el autovacuum.

Este enfoque garantiza que la asignación de memoria ajustada se aplique a las nuevas operaciones de autovacuum.

Para obtener resultados más inmediatos, considere la posibilidad de realizar manualmente una operación `VACUUM FREEZE` con una configuración de `maintenance_work_mem` mayor durante la sesión:

```
SET maintenance_work_mem TO '1GB';
VACUUM FREEZE VERBOSE table_name;
```

Si utiliza Amazon RDS y descubre que necesita memoria adicional para poder utilizar valores más altos para `maintenance_work_mem` o `autovacuum_work_mem`, plantéese la posibilidad de actualizar a una clase de instancia con más memoria. Esto puede proporcionarle los recursos

necesarios para mejorar las operaciones de vaciado manuales y automáticas, lo que se traduce en una mejora del rendimiento general de vaciado y del de las bases de datos.

Desactivar INDEX_CLEANUP

El `VACUUM` manual de la versión 12 y posteriores de PostgreSQL permite omitir la fase de limpieza de índices, mientras que el autovacuum de emergencia en la versión 14 y posteriores de PostgreSQL lo hace automáticamente en función del parámetro `vacuum_failsafe_age`.

> **Warning**
>
> Omitir la limpieza de índices puede provocar una sobrecarga de índices y perjudicar el rendimiento de las consultas. Para mitigar esta situación, considere la posibilidad de volver a indexar o vaciar los índices afectados durante un período de mantenimiento.

Para obtener más información sobre cómo gestionar índices grandes, consulte la documentación en Administración de autovacuum con índices de gran tamaño .

Vaciado de índices en paralelo

A partir de PostgreSQL 13, los índices se pueden vaciar y limpiar en paralelo de forma predeterminada utilizando `VACUUM` de forma manual, con un proceso de trabajo de vaciado asignado a cada índice. Sin embargo, para que PostgreSQL determine si una operación de vaciado es apta para su ejecución en paralelo, se deben cumplir criterios específicos:

- Debe haber al menos dos índices.
- El parámetro `max_parallel_maintenance_workers` debe estar establecido al menos en 2.
- El tamaño del índice debe superar el límite `min_parallel_index_scan_size`, que de forma predeterminada es de 512 KB.

Puede ajustar la configuración `max_parallel_maintenance_workers` en función de la cantidad de vCPU disponibles en su instancia de Amazon RDS y la cantidad de índices de la tabla para optimizar el tiempo de respuesta del vaciado.

Para obtener más información, consulte Parallel vacuuming in Amazon RDS for PostgreSQL and Amazon Aurora PostgreSQL.

Demasiadas tablas o bases de datos que vaciar

Como se menciona en la documentación de PostgreSQL sobre el daemon autovacuum, este funciona mediante múltiples procesos. Esto incluye un lanzador de autovacuum persistente responsable de iniciar los procesos de trabajo de autovacuum para cada base de datos del sistema. El lanzador programa estos procesos de trabajo para que se inicien aproximadamente cada `autovacuum_naptime` segundos por cada base de datos.

Con “N” bases de datos, un nuevo proceso de trabajo comienza aproximadamente cada [`autovacuum_naptime`/N segundos]. Sin embargo, el número total de procesos de trabajo simultáneos está limitado por la configuración `autovacuum_max_workers`. Si el número de bases de datos o tablas que requieren vaciado supera este límite, la siguiente base de datos o tabla se procesará en cuanto haya un proceso de trabajo disponible.

Cuando muchas tablas o bases de datos grandes requieren un vaciado al mismo tiempo, todos los procesos de trabajo de autovacuum disponibles pueden permanecer ocupados durante un período prolongado, lo que retrasa el mantenimiento de otras tablas y bases de datos. En entornos con altas tasas de transacciones, este cuello de botella puede agravarse rápidamente y provocar posibles problemas de vaciado en su instancia de Amazon RDS.

Cuando `postgres_get_av_diag()` detecta un número elevado de tablas o bases de datos, proporciona la siguiente recomendación:

```
NOTICE: Your database is currently running aggressive vacuum to prevent wraparound and
 it might be slow.
```

```
NOTICE: The current setting of autovacuum_max_workers:3 might not be sufficient.
 Consider increasing the setting and, if necessary, consider scaling up the Amazon RDS
 instance class for more workers.
```

Indicaciones

Aumentar autovacuum_max_workers

Para agilizar el vaciado, recomendamos ajustar el parámetro `autovacuum_max_workers` para permitir que haya más procesos de trabajo de autovacuum simultáneos. Si persisten los cuellos de botella en el rendimiento, plantéese la posibilidad de escalar verticalmente su instancia de Amazon RDS a una clase con más vCPU, lo que puede mejorar aún más las capacidades de procesamiento en paralelo.

Se está ejecutando un vaciado intensivo (para evitar el reinicio)

La antigüedad de la base de datos (MaximumUsedTransactionIDs) en PostgreSQL solo disminuye cuando se completa correctamente un vaciado intensivo (para evitar el reinicio). Hasta que finalice este vaciado, la antigüedad seguirá aumentando en función de la velocidad de transacciones.

La función `postgres_get_av_diag()` genera el `NOTICE` siguiente cuando detecta un vaciado intensivo. Sin embargo, solo activa este resultado después de que el vaciado haya estado activo durante al menos dos minutos.

```
NOTICE: Your database is currently running aggressive vacuum to prevent wraparound,
 monitor autovacuum performance.
```

Para obtener más información sobre el vaciado intensivo, consulte When an aggressive vacuum is already running.

Puede comprobar si se está realizando un vaciado intensivo con la siguiente consulta:

```
SELECT
    a.xact_start AS start_time,
    v.datname "database",
    a.query,
    a.wait_event,
    v.pid,
    v.phase,
    v.relid::regclass,
    pg_size_pretty(pg_relation_size(v.relid)) AS heap_size,
    (
        SELECT
            string_agg(pg_size_pretty(pg_relation_size(i.indexrelid)) || ':' ||
 i.indexrelid::regclass || chr(10), ', ')
        FROM
            pg_index i
        WHERE
            i.indrelid = v.relid
    ) AS index_sizes,
    trunc(v.heap_blks_scanned * 100 / NULLIF(v.heap_blks_total, 0)) AS step1_scan_pct,
    v.index_vacuum_count || '/' || (
        SELECT
            count(*)
        FROM
            pg_index i
```

```
        WHERE
            i.indrelid = v.relid
    ) AS step2_vacuum_indexes,
    trunc(v.heap_blks_vacuumed * 100 / NULLIF(v.heap_blks_total, 0)) AS
 step3_vacuum_pct,
    age(CURRENT_TIMESTAMP, a.xact_start) AS total_time_spent_sofar
FROM
    pg_stat_activity a
    INNER JOIN pg_stat_progress_vacuum v ON v.pid = a.pid;
```

Para determinar si se trata de un vaciado intensivo (para evitar el reinicio), compruebe la columna de consulta del resultado. La expresión “para evitar el reinicio” indica que se trata de un vaciado intensivo.

```
query                 | autovacuum: VACUUM public.t3 (to prevent wraparound)
```

Por ejemplo, supongamos que hay un bloqueador en el valor de antigüedad de transacciones de 1000 millones y una tabla que requiere un vaciado intensivo para evitar el reinicio a esa misma antigüedad de transacciones. Además, hay otro bloqueador en el valor de antigüedad de transacciones de 750 millones. Tras superar el bloqueador en el valor de antigüedad de transacciones de 1000 millones, la antigüedad no se reducirá inmediatamente a 750 millones. Seguirá siendo alta hasta que se complete la tabla que necesita el vaciado intensivo o cualquier transacción con una antigüedad superior a los 750 millones. Durante este período, la antigüedad de las transacciones de su clúster de PostgreSQL seguirá aumentando. Una vez que se complete el proceso de vaciado, la antigüedad de las transacciones se reducirá a 750 millones, pero volverá a aumentar de nuevo hasta que se finalice todo el vaciado. Este ciclo continuará mientras se mantengan estas condiciones, hasta que la antigüedad de las transacciones finalmente se reduzca hasta el nivel configurado para su instancia de Amazon RDS, especificado por `autovacuum_freeze_max_age`.

Explicación de los mensajes de tipo NOTICE en RDS para PostgreSQL

La función `postgres_get_av_diag()` proporciona los siguientes mensajes de tipo NOTICE:

Cuando la antigüedad aún no ha alcanzado aún el umbral de supervisión

- El umbral de supervisión para que `postgres_get_av_diag()` identifique los bloqueadores es de 500 millones de transacciones por defecto. Si `postgres_get_av_diag()` genera el siguiente mensaje NOTICE, indica que la antigüedad de la transacción aún no ha alcanzado este umbral.

```
NOTICE: postgres_get_av_diag() checks for blockers that prevent aggressive vacuums
 only, it does so only after exceeding dvb_threshold which is 500,000,000 and age of
 this PostgreSQL cluster is currently at 2.
```

No está conectado a la base de datos que tenga la antigüedad del ID de transacción más antiguo

La función `postgres_get_av_diag()` proporciona el resultado más preciso cuando se conecta a la base de datos con el ID de transacción más antiguo. En su caso, la base de datos con el ID de transacción más antiguo notificada por `postgres_get_av_diag()` será diferente a "my_database". Si no se ha conectado a la base de datos correcta, se generará el siguiente mensaje tipo NOTICE:

```
NOTICE: You are not connected to the database with the age of oldest transaction
 ID. Connect to my_database database and run postgres_get_av_diag() for accurate
 reporting.
```

Conectarse a la base de datos con la antigüedad de transacción más antigua es importante por las siguientes razones:

- Identificar los bloqueadores de tablas temporales: dado que los metadatos de las tablas temporales son específicos de cada base de datos, normalmente se encuentran en la base de datos en la que se crearon. Sin embargo, si una tabla temporal resulta ser la que más bloquea y reside en la base de datos con la transacción más antigua, esta información podría resultar engañosa. La conexión a la base de datos correcta garantiza la identificación precisa del bloqueador de tablas temporal.
- Diagnóstico de vaciados lentos: los metadatos del índice y la información sobre el recuento de tablas son específicos de la base de datos y son necesarios para diagnosticar los problemas de vaciado lento.

La base de datos con la transacción más antigua se encuentra en una base de datos rdsadmin o template0

En algunos casos, las bases de datos `rdsadmin` o `template0` pueden identificarse como la base de datos con el ID de transacción más antiguo. Si esto ocurre, `postgres_get_av_diag()` emitirá el siguiente mensaje de tipo NOTICE:

```
NOTICE: The database with the age of oldest transaction ID is rdsadmin or template0,
 reach out to support if the reported blocker is in rdsadmin or template0.
```

Compruebe que el bloqueador de la lista no se haya originado en ninguna de estas dos bases de datos. Si se notifica que el bloqueador está presente en `rdsadmin` o `template0` de ellas, póngase en contacto con el servicio de asistencia, ya que estas bases de datos no son accesibles para el usuario y requieren intervención.

Es muy poco probable que las bases de datos `rdsadmin` o `template0` contengan un bloqueador principal.

Cuando ya está en curso un vaciado intensivo

La función `postgres_get_av_diag()` está diseñada para notificar si se está ejecutando un proceso de vaciado intensivo, pero solo activa esta salida después de que el vaciado haya estado activo durante al menos 1 minuto. Este retraso intencionado ayuda a reducir las probabilidades de que se produzcan falsos positivos. Mediante esta espera, la función garantiza que solo se registren los vaciados efectivos y significativos, lo que permite una supervisión más precisa y fiable de la actividad de vaciado.

La función `postgres_get_av_diag()` genera el siguiente mensaje de tipo NOTICE cuando detecta que se están realizando uno o varios vaciados intensivos.

```
NOTICE: Your database is currently running aggressive vacuum to prevent wraparound,
 monitor autovacuum performance.
```

Como se indica en el mensaje NOTICE, siga supervisando el rendimiento del vaciado. Para obtener más información acerca del vaciado intensivo, consulte Se está ejecutando un vaciado intensivo (para evitar el reinicio)

Cuando el vaciado intensivo está apagado

La función `postgres_get_av_diag()` genera el siguiente mensaje NOTICE si el autovacuum está deshabilitado en la instancia de la base de datos:

```
NOTICE: Autovacuum is OFF, we strongly recommend to enable it, no restart is
 necessary.
```

Autovacuum es una característica fundamental de la instancia de base de datos de RDS para PostgreSQL que garantiza un funcionamiento fluido de la base de datos. Elimina automáticamente las versiones de filas antiguas, recupera espacio de almacenamiento y evita que las tablas se sobrecarguen, lo que ayuda a mantener la eficiencia de las tablas y los índices

para lograr un rendimiento óptimo. Además, protege contra el reinicio de los identificadores de transacciones, lo que puede detener las transacciones en su instancia de Amazon RDS. La desactivación del autovacuum puede provocar una disminución a largo plazo del rendimiento y la estabilidad de la base de datos. Le sugerimos que lo mantenga activado todo el tiempo. Para obtener más información, consulte Descripción de autovacuum en entornos de RDS para PostgreSQL.

> **Note**
>
> La desactivación de autovacuum no detiene los vaciados intensivos. Seguirán produciéndose una vez que las tablas alcancen el umbral de `autovacuum_freeze_max_age`.

El número de transacciones pendientes es críticamente bajo

La función `postgres_get_av_diag()` genera el siguiente mensaje de tipo NOTICE cuando un vaciado previo al reinicio es inminente. Este mensaje NOTICE se emite cuando su instancia de Amazon RDS está a 100 millones de transacciones de la posibilidad de rechazar nuevas transacciones.

```
WARNING: Number of transactions remaining is critically low, resolve issues with
 autovacuum or perform manual VACUUM FREEZE before your instance stops accepting
 transactions.
```

Es necesario realizar acciones inmediatas para evitar el tiempo de inactividad de la base de datos. Debe supervisar de cerca sus operaciones de vaciado y considerar la posibilidad de iniciar manualmente un `VACUUM FREEZE` en la base de datos afectada para evitar errores en las transacciones.

Uso de mecanismos de registro admitidos por RDS for PostgreSQL

Hay varios parámetros, extensiones y otros elementos configurables que puede establecer para registrar actividades que ocurren en su instancia de base de datos de PostgreSQL. Estos incluyen los siguientes:

- El parámetro `log_statement` se puede usar para registrar la actividad del usuario en su base de datos de PostgreSQL. Para obtener más información sobre el registro de RDS for PostgreSQL

y cómo monitorear los registros, consulte Archivos de registro de bases de datos de RDS para PostgreSQL.

- El parámetro `rds.force_admin_logging_level` registra las acciones del usuario interno de Amazon RDS (rdsadmin) en las bases de datos de la instancia de base de datos. Escribe la salida en el registro de errores de PostgreSQL. Los valores permitidos son `disabled`, `debug5`, `debug4`, `debug3`, `debug2`, `debug1`, `info`, `notice`, `warning`, `error`, registro, `fatal`, y `panic`. El valor predeterminado es `disabled`.
- El parámetro `rds.force_autovacuum_logging_level` se puede configurar para capturar varias operaciones autovacuum en el registro de errores de PostgreSQL. Para obtener más información, consulte Registro de actividades de autovacuum y vacuum.
- La extensión PostgreSQL Audit (pgAudit) se puede instalar y configurar para capturar actividades a nivel de sesión o a nivel de objeto. Para obtener más información, consulte Uso de pgAudit para registrar la actividad de la base de datos.
- La extensión `log_fdw` le permite acceder al registro del motor de la base de datos mediante SQL. Para obtener más información, consulte Uso de la extensión log_fdw para acceder al registro de base de datos mediante SQL.
- La biblioteca `pg_stat_statements` se especifica como predeterminada para el parámetro `shared_preload_libraries` en la versión 10 y superiores de RDS for PostgreSQL. Es esta biblioteca la que puede usar para analizar consultas en ejecución. Asegúrese de que `pg_stat_statements` se establezca en el grupo de parámetros de base de datos. Para obtener más información sobre cómo supervisar su instancia de base de datos de RDS for PostgreSQL por medio de la información que proporciona esta biblioteca, consulte Estadísticas de SQL de RDS PostgreSQL.
- El parámetro `log_hostname` captura en el registro el nombre de host de cada conexión de cliente. Para RDS para PostgreSQL versión 12 y posteriores, este parámetro se establece como `off` de forma predeterminada. Si lo activa, asegúrese de supervisar los tiempos de conexión de las sesiones. Cuando está activado, el servicio utiliza la solicitud de búsqueda inversa del sistema de nombres de dominio (DNS) para obtener el nombre de host del cliente que realiza la conexión y agregarlo al registro de PostgreSQL. Esto tiene un impacto notable durante la conexión a la sesión. Le recomendamos que active este parámetro solo para resolver problemas.

En términos generales, el objetivo del registro es que el DBA pueda supervisar, ajustar el rendimiento y solucionar problemas. Muchos de los registros se cargan automáticamente en Amazon CloudWatch o en Información sobre rendimiento. Aquí, se ordenan y agrupan para proporcionar métricas completas para su instancia de base de datos. Para obtener más información sobre la

supervisión y las métricas de Amazon RDS, visite Supervisión de métricas en una instancia de Amazon RDS.

Administración de archivos temporales con PostgreSQL

En PostgreSQL, una consulta compleja puede realizar varias operaciones de ordenación y hash al mismo tiempo, y cada una de ellas utiliza memoria de la instancia para almacenar los resultados hasta el valor especificado en el parámetro `work_mem`. Cuando la memoria de la instancia no es suficiente, se crean archivos temporales para almacenar los resultados. Se escriben en el disco para completar la ejecución de la consulta. Posteriormente, una vez finalizada la consulta, estos archivos se eliminan automáticamente. En RDS para PostgreSQL, estos archivos se almacenan en Amazon EBS en el volumen de datos. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS. Puede monitorizar la métrica de `FreeStorageSpace` publicada en CloudWatch para asegurarse de que la instancia de base de datos tenga suficiente espacio de almacenamiento libre. Para obtener más información, consulte `FreeStorageSpace` ..

Recomendamos utilizar instancias de lecturas optimizadas para Amazon RDS para las cargas de trabajo que implican múltiples consultas simultáneas que aumentan el uso de archivos temporales. Estas instancias utilizan almacenamiento por bloques local basado en unidades de estado sólido (SSD) de memoria rápida no volátil (NVMe) para colocar los archivos temporales. Para obtener más información, consulte Mejora del rendimiento de las consultas de RDS para PostgreSQL con lecturas optimizadas para Amazon RDS.

Puede utilizar los siguientes parámetros y funciones para administrar los archivos temporales de la instancia.

- **`temp_file_limit`**: este parámetro cancela cualquier consulta que supere el tamaño de temp_files en KB. Este límite evita que cualquier consulta se ejecute de forma indefinida y consuma espacio en disco con archivos temporales. Puede calcular el valor utilizando los resultados del parámetro `log_temp_files`. Como práctica recomendada, examine el comportamiento de la carga de trabajo y establezca el límite de acuerdo con la estimación. En el siguiente ejemplo, se cancela una consulta cuando se supera el límite.

```
postgres=>select * from pgbench_accounts, pg_class, big_table;
```

```
ERROR: temporary file size exceeds temp_file_limit (64kB)
```

- **log_temp_files**: este parámetro envía mensajes a postgresql.log cuando se eliminan los archivos temporales de una sesión. Este parámetro produce registros después de que la consulta se complete correctamente. Por lo tanto, puede que no ayude a solucionar problemas de consultas activas y de larga ejecución.

  El ejemplo siguiente muestra que, cuando la consulta se completa correctamente, las entradas se registran en el archivo postgresql.log y se limpian los archivos temporales.

```
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:LOG:
 temporary file: path "base/pgsql_tmp/pgsql_tmp31236.5", size 140353536
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:STATEMENT:
  select a.aid from pgbench_accounts a, pgbench_accounts b where a.bid=b.bid order by
 a.bid limit 10;
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:LOG:
 temporary file: path "base/pgsql_tmp/pgsql_tmp31236.4", size 180428800
2023-02-06 23:48:35 UTC:205.251.233.182(12456):adminuser@postgres:[31236]:STATEMENT:
  select a.aid from pgbench_accounts a, pgbench_accounts b where a.bid=b.bid order by
 a.bid limit 10;
```

- **pg_ls_tmpdir**: esta función que está disponible desde RDS para PostgreSQL 13 y versiones posteriores proporciona visibilidad sobre el uso actual de los archivos temporales. La consulta completada no aparece en los resultados de la función. En el siguiente ejemplo, puede ver los resultados de esta función.

```
postgres=>select * from pg_ls_tmpdir();
```

```
      name       |    size    |      modification
-----------------+------------+------------------------
 pgsql_tmp8355.1 | 1072250880 | 2023-02-06 22:54:56+00
 pgsql_tmp8351.0 | 1072250880 | 2023-02-06 22:54:43+00
 pgsql_tmp8327.0 | 1072250880 | 2023-02-06 22:54:56+00
 pgsql_tmp8351.1 |  703168512 | 2023-02-06 22:54:56+00
 pgsql_tmp8355.0 | 1072250880 | 2023-02-06 22:54:00+00
 pgsql_tmp8328.1 |  835031040 | 2023-02-06 22:54:56+00
 pgsql_tmp8328.0 | 1072250880 | 2023-02-06 22:54:40+00
(7 rows)
```

```
postgres=>select query from pg_stat_activity where pid = 8355;

query
------------------------------------------------------------------------------------------
select a.aid from pgbench_accounts a, pgbench_accounts b where a.bid=b.bid order by
 a.bid
(1 row)
```

El nombre del archivo incluye el ID de procesamiento (PID) de la sesión que generó el archivo temporal. Una consulta más avanzada, como en el ejemplo siguiente, realiza una suma de los archivos temporales de cada PID.

```
postgres=>select replace(left(name, strpos(name, '.')-1),'pgsql_tmp','') as pid,
 count(*), sum(size) from pg_ls_tmpdir() group by pid;
```

```
 pid  | count |   sum
------+-------+------------------
 8355 |     2 | 2144501760
 8351 |     2 | 2090770432
 8327 |     1 | 1072250880
 8328 |     2 | 2144501760
(4 rows)
```

- **pg_stat_statements**: si activa el parámetro pg_stat_statements, puede ver el uso medio de archivos temporales por llamada. Puede identificar el query_id de la consulta y usarlo para examinar el uso de archivos temporales, como se muestra en el siguiente ejemplo.

```
postgres=>select queryid from pg_stat_statements where query like 'select a.aid from
 pgbench%';
```

```
       queryid
----------------------
 -7170349228837045701
(1 row)
```

```
postgres=>select queryid, substr(query,1,25), calls, temp_blks_read/calls
 temp_blks_read_per_call, temp_blks_written/calls temp_blks_written_per_call from
 pg_stat_statements where queryid = -7170349228837045701;
```

```
       queryid        |          substr           | calls | temp_blks_read_per_call |
 temp_blks_written_per_call
----------------------+---------------------------+-------+-------------------------
+---------------------------
 -7170349228837045701 | select a.aid from pgbench |    50 |                  239226 |
                     388678
(1 row)
```

- **Performance Insights**: en el panel de Información sobre el rendimiento, puede ver el uso temporal de los archivos activando las métricas temp_bytes y temp_files. A continuación, puede ver la media de estas dos métricas y cómo se corresponden con la carga de trabajo de la consulta. La vista de Información sobre el rendimiento no muestra específicamente las consultas que generan los archivos temporales. Sin embargo, al combinar Información sobre el rendimiento con la consulta que se muestra para `pg_ls_tmpdir`, puede solucionar problemas, realizar análisis y determinar los cambios en la carga de trabajo de la consulta.

  Para obtener más información sobre cómo analizar métricas y consultas con Información de rendimiento, consulte Análisis de métricas mediante el panel de Información sobre rendimiento.

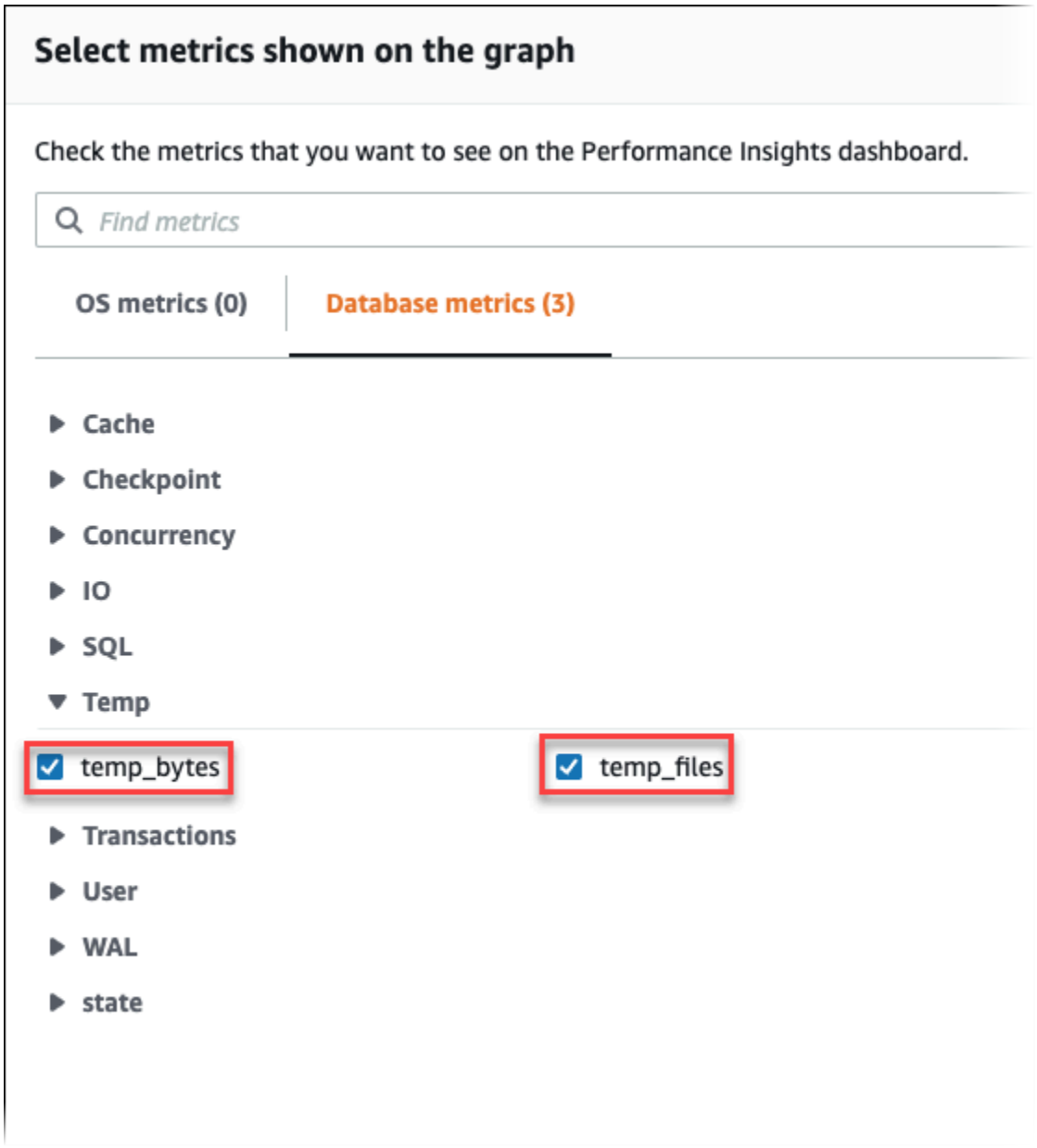
  Para ver un ejemplo sobre la visualización del uso de archivos temporales con Información de rendimiento, consulte Visualización del uso de archivos temporales con Información de rendimiento

Visualización del uso de archivos temporales con Información de rendimiento

Puede usar Información de rendimiento para consultar el uso de archivos temporales activando las métricas temp_bytes y temp_files. En Información de rendimiento, la vista no muestra las consultas específicas que generan archivos temporales; sin embargo, si combina Información de rendimiento con la consulta mostrada para `pg_ls_tmpdir`, puede solucionar problemas, realizar análisis y determinar cuáles son los cambios necesarios en la carga de trabajo de consultas.

1. En el panel de Información sobre el rendimiento, elija Administrar métricas.

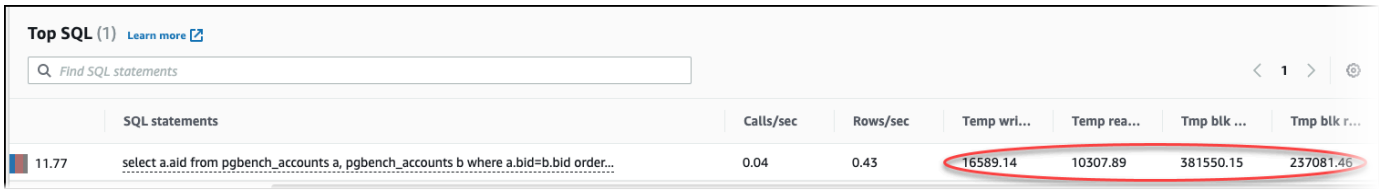
2. Elija las Métricas de la base de datos y seleccione las métricas temp_bytes y temp_files como se muestra en la siguiente captura de pantalla.



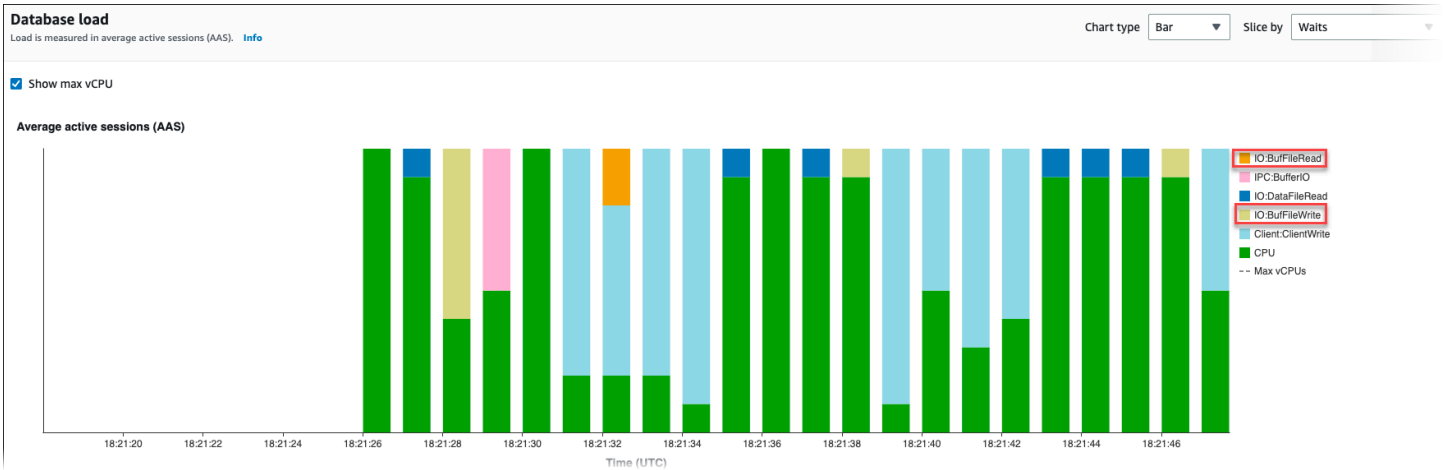
3. En la pestaña Principales SQL, seleccione el icono Preferencias.
4. En la ventana Preferencias, active las siguientes estadísticas para que aparezcan en la pestaña Principales SQL y seleccione Continuar.

   - Escrituras temporales por segundo
   - Lecturas temporales por segundo
   - Escritura temporal en bloque por llamada
   - Lectura temporal en bloque por llamada

5. El archivo temporal se divide cuando se combina con la consulta mostrada para `pg_ls_tmpdir`, como se observa en el siguiente ejemplo.



Los eventos `IO:BufFileRead` y `IO:BufFileWrite` se producen cuando las consultas principales de la carga de trabajo crean archivos temporales a menudo. Puede utilizar la Información de rendimiento para identificar las principales consultas pendientes en `IO:BufFileRead` e `IO:BufFileWrite` mediante la revisión del promedio de sesiones activas (AAS) en las secciones de carga de base de datos y SQL principales.



Para obtener más información sobre cómo analizar las consultas principales y cargar mediante eventos de espera con Información de Rendimiento, consulte Información general sobre la pestaña Top SQL (SQL principal). Debe identificar y ajustar las consultas que provocan el aumento del uso de archivos temporales y los eventos de espera relacionados. Para obtener más información sobre estos eventos de espera y su corrección, consulte IO:BufFileRead e IO:BufFileWrite.

> **Note**
>
> El parámetro `work_mem` controla cuándo se agota la memoria de la operación de ordenación y los resultados se escriben en archivos temporales. Se recomienda no cambiar la configuración de este parámetro por encima del valor predeterminado, ya que haría que cada sesión de base de datos consumiera más memoria. Además, una sola sesión que realiza combinaciones y ordenaciones complejas puede realizar operaciones paralelas en las que cada operación consume memoria.

Como práctica recomendada, cuando tenga un informe de gran tamaño con múltiples combinaciones y ordenaciones, defina este parámetro en el nivel de sesión mediante el comando `SET work_mem`. Por tanto, el cambio solo se aplica a la sesión actual y no cambia el valor globalmente.

Uso de pgBadger para el análisis de registros con PostgreSQL

Puede usar un analizador de registros como pgbadger para analizar los registros de PostgreSQL. La documentación de pgBadger establece que el patrón %l (la línea de registro para la sesión o el proceso) debe ser parte del prefijo. Sin embargo, si proporciona el RDS actual `log_line_prefix` como parámetro a pgBadger, aún debería generar un informe.

Por ejemplo, el siguiente comando asigna el formato correcto a un archivo de registro de Amazon RDS para PostgreSQL con fecha 04-02-2014 con pgbadger.

```
./pgbadger -f stderr -p '%t:%r:%u@%d:[%p]:' postgresql.log.2014-02-04-00
```

Uso de PGSnapper para supervisar PostgreSQL

Puede utilizar PGSnapper para facilitar la recopilación periódica de estadísticas y métricas relacionadas con el rendimiento de Amazon RDS para PostgreSQL. Para obtener más información, consulte Monitor Amazon RDS for PostgreSQL performance using PGSnapper (Supervise el rendimiento de Amazon RDS para PostgreSQL con PGSnapper).

Uso de parámetros en su instancia de base de datos de RDS for PostgreSQL

En algunos casos, puede crear una instancia de base de datos de RDS for PostgreSQL sin especificar un grupo de parámetros personalizado. De ser el caso, la instancia de base de datos se crea por medio del grupo de parámetros predeterminado para la versión de PostgreSQL que elija. Por ejemplo, suponga que crea una instancia de base de datos de RDS for PostgreSQL por medio de la versión 13.3 de PostgreSQL. En este caso, la instancia de base de datos se crea por medio de los valores del grupo de parámetros para las versiones 13 de PostgreSQL, `default.postgres13`.

También puede crear su propio grupo de parámetros de base de datos personalizado. Debe hacer esto si desea modificar cualquier configuración para la instancia de base de datos de RDS for

PostgreSQL a partir de sus valores predeterminados. Para aprender a hacerlo, consulte Grupos de parámetros para Amazon RDS.

Puede realizar un seguimiento de la configuración en su instancia de base de datos de RDS for PostgreSQL de varias maneras diferentes. Puede utilizar la AWS Management Console, la AWS CLI o la API de Amazon RDS. También puede consultar los valores de la tabla `pg_settings` de PostgreSQL de la instancia, como se muestra a continuación.

```
SELECT name, setting, boot_val, reset_val, unit
 FROM pg_settings
 ORDER BY name;
```

Para obtener más información sobre los valores que se muestran en esta consulta, consulte `pg_settings` en la documentación de PostgreSQL.

Tenga especial cuidado cuando cambie la configuración de `max_connections` y `shared_buffers` en la instancia de base de datos de RDS for PostgreSQL. Por ejemplo, suponga que modifica la configuración para `max_connections` o `shared_buffers` y utiliza valores que son demasiado altos para la carga de trabajo real. En este caso, su instancia de base de datos de RDS for PostgreSQL no se iniciará. Si esto ocurre, verá un error como el siguiente en el `postgres.log`.

```
2018-09-18 21:13:15 UTC::@:[8097]:FATAL:  could not map anonymous shared memory: Cannot
 allocate memory
2018-09-18 21:13:15 UTC::@:[8097]:HINT:  This error usually means that PostgreSQL's
 request for a shared memory segment
exceeded available memory or swap space. To reduce the request size (currently
 3514134274048 bytes), reduce
PostgreSQL's shared memory usage, perhaps by reducing shared_buffers or
 max_connections.
```

Sin embargo, no puede cambiar ningún valor de la configuración contenida en los grupos de parámetros de base de datos de RDS for PostgreSQL predeterminados. Para cambiar la configuración de cualquier parámetro, primero cree un grupo de parámetros de base de datos personalizado. Luego, cambie la configuración en ese grupo personalizado y, luego, aplique el grupo de parámetros personalizado a su instancia de base de datos de RDS for PostgreSQL. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

Hay dos tipos de parámetros en RDS para PostgreSQL.

- Parámetros estáticos: los parámetros estáticos requieren que la instancia de la base de datos RDS for PostgreSQL se reinicie después de un cambio para que el nuevo valor tenga efecto.
- Parámetros dinámicos: los parámetros dinámicos no requieren un reinicio después de cambiar su configuración.

> **Note**
>
> Si su instancia de base de datos de RDS for PostgreSQL utiliza su propio grupo de parámetros de base de datos personalizado, puede cambiar los valores de los parámetros dinámicos en la instancia de base de datos en ejecución. Puede hacerlo mediante la AWS Management Console, la AWS CLI o la API de Amazon RDS.

Si tiene privilegios para hacerlo, también puede cambiar los valores de los parámetros con los comandos `ALTER DATABASE`, `ALTER ROLE` y `SET`.

Lista de parámetros de la instancia de base de datos de RDS for PostgreSQL

La siguiente tabla enumera algunos de (pero no todos) los parámetros disponibles en una instancia de base de datos RDS for PostgreSQL. Para ver todos los parámetros disponibles, utilice el comando describe-db-parameters de AWS CLI. Por ejemplo, para obtener la lista de todos los parámetros disponibles en el grupo de parámetros predeterminado de RDS para PostgreSQL versión 13, ejecute lo siguiente.

```
aws rds describe-db-parameters --db-parameter-group-name default.postgres13
```

También puede usar la consola. Elija grupos de parámetros en el menú de Amazon RDS y, a continuación, elija el grupo de parámetros entre los disponibles en suRegión de AWS.

Nombre del parámetro	Apply_Type	Descripción
application_name	Dinámico	Define el nombre de la aplicación sobre la que informarán las estadísticas y los registros.
archive_command	Dinámico	Establece el comando del shell que se llamará para archivar un archivo WAL.
array_nulls	Dinámico	Permite la entrada de elementos NULL en matrices.
authentication_timeout	Dinámico	Establece el tiempo máximo permitido para completar una autenticación del cliente.
autovacuum	Dinámico	Inicia el subproceso de autovacuum.
autovacuum_analyze_scale_factor	Dinámico	Número de inserciones, actualizaciones o eliminaciones de tuplas previas al análisis como una fracción de reltuples.
autovacuum_analyze_threshold	Dinámico	Número mínimo de inserciones, actualizaciones o eliminaciones de tuplas previas al análisis.
autovacuum_freeze_max_age	Estático	Antigüedad con la que se debe aplicar autovacuum a una tabla para impedir el reinicio de los ID.

Nombre del parámetro	Apply_Type	Descripción
autovacuum_naptime	Dinámico	Tiempo de reposo entre ejecuciones de autovacuum.
autovacuum_max_workers	Estático	Define el número máximo de procesos de empleados de autovacuum que se ejecutan simultáneamente.
autovacuum_vacuum_cost_delay	Dinámico	Retardo del costo del vacío, en milisegundos, para autovacuum.
autovacuum_vacuum_cost_limit	Dinámico	Importe del costo del vacío disponible antes del periodo de reposo para autovacuum.
autovacuum_vacuum_scale_factor	Dinámico	Número de actualizaciones o eliminaciones de tuplas previas al vacío como una fracción de reltuples.
autovacuum_vacuum_threshold	Dinámico	Número mínimo de actualizaciones o eliminaciones de tuplas previas al vacío.
backslash_quote	Dinámico	Define si se admite una barra diagonal invertida (\) en el texto de las cadenas.
bgwriter_delay	Dinámico	Tiempo de reposo del escritor de segundo plano entre una ronda y la siguiente.
bgwriter_lru_maxpages	Dinámico	Número máximo de páginas de LRU del escritor de segundo plano que se deben vaciar en cada ronda.
bgwriter_lru_multiplier	Dinámico	Múltiplo del uso medio del búfer que se debe liberar en cada ronda.
bytea_output	Dinámico	Establece el formato de salida para bytes.

Nombre del parámetro	Apply_Type	Descripción
check_function_bodies	Dinámico	Comprueba los cuerpos de las funciones durante la ejecución de CREATE FUNCTION.
checkpoint_completion_target	Dinámico	Tiempo requerido para vaciar los búferes sucios durante el punto de comprobación expresado como una fracción del intervalo del punto de comprobación.
checkpoint_segments	Dinámico	Define la distancia máxima en los segmentos de registro entre los puntos de comprobación de registro previo a la lectura (WAL) automáticos.
checkpoint_timeout	Dinámico	Define el tiempo máximo entre los puntos de comprobación de WAL automáticos.
checkpoint_warning	Dinámico	Habilita las advertencias si los segmentos del punto de comprobación se rellenan con una frecuencia superior a esta.
client_connection_check_interval	Dinámico	Establece el intervalo de tiempo entre las comprobaciones de desconexión mientras se ejecutan las consultas.
client_encoding	Dinámico	Define la codificación del conjunto de caracteres del cliente.
client_min_messages	Dinámico	Define los niveles de los mensajes que se envían al cliente.
commit_delay	Dinámico	Define el retardo en microsegundos entre la confirmación de la transacción y el vaciado de WAL al disco.
commit_siblings	Dinámico	Define el número mínimo de transacciones abiertas concurrentes antes de ejecutar commit_delay.

Nombre del parámetro	Apply_Type	Descripción
constraint_exclusion	Dinámico	Habilita el planificador para que use restricciones con el fin de optimizar las consultas.
cpu_index_tuple_cost	Dinámico	Define la estimación del planificador del costo de procesar cada entrada de índice durante un examen del índice.
cpu_operator_cost	Dinámico	Define la estimación del planificador del costo de procesar cada llamada a operador o a función.
cpu_tuple_cost	Dinámico	Define la estimación del planificador del costo de procesar cada tupla (fila).
cursor_tuple_fraction	Dinámico	Define la estimación del planificador de la fracción de las filas de un cursor que se recuperarán.
datestyle	Dinámico	Define el formato de visualización para los valores de fecha y hora.
deadlock_timeout	Dinámico	Define el tiempo de espera de una interrupción antes de comprobar si se ha producido un bloqueo.
debug_pretty_print	Dinámico	Aplica una sangría a las visualizaciones del árbol de análisis y de planificación.
debug_print_parse	Dinámico	Registra el árbol de análisis de cada consulta.
debug_print_plan	Dinámico	Registra el plan de ejecución de cada consulta.
debug_print_rewritten	Dinámico	Registra el árbol de análisis reescrito de cada consulta.
default_statistics_target	Dinámico	Define el objetivo de estadística predeterminado.

Nombre del parámetro	Apply_Type	Descripción
default_tablespace	Dinámico	Define el espacio de tabla predeterminado en el que se deben crear las tablas y los índices.
default_transaction_deferrable	Dinámico	Define el estado diferible predeterminado de las nuevas transacciones.
default_transaction_isolation	Dinámico	Define el nivel de aislamiento de cada nueva transacción.
default_transaction_read_only	Dinámico	Define el estado de solo lectura predeterminado de las nuevas transacciones.
default_with_oids	Dinámico	Crea nuevas tablas con ID de objeto (OID) de forma predeterminada.
effective_cache_size	Dinámico	Define la suposición del planificador sobre el tamaño de la caché de disco.
effective_io_concurrency	Dinámico	Número de solicitudes simultáneas que el subsistema del disco puede gestionar de un modo eficiente.
enable_bitmapscan	Dinámico	Habilita el uso de planes de examen de mapas de bits por parte del planificador.
enable_hashagg	Dinámico	Habilita el uso de planes de agregación con hash por parte del planificador.
enable_hashjoin	Dinámico	Habilita el uso de planes de unión con hash por parte del planificador.
enable_indexscan	Dinámico	Habilita el uso de planes de examen de índice por parte del planificador.
enable_material	Dinámico	Habilita el uso de la materialización por parte del planificador.

Nombre del parámetro	Apply_Type	Descripción
enable_mergejoin	Dinámico	Habilita el uso de planes de unión de fusión por parte del planificador.
enable_nestloop	Dinámico	Habilita el uso de planes de unión de bucle anidado por parte del planificador.
enable_seqscan	Dinámico	Habilita el uso de planes de examen secuencial por parte del planificador.
enable_sort	Dinámico	Habilita el uso de pasos de ordenación explícitos por parte del planificador.
enable_tidscan	Dinámico	Habilita el uso de planes de examen de TID por parte del planificador.
escape_string_warning	Dinámico	Advierte sobre los caracteres de escape de barra diagonal invertida (\) en el texto de las cadenas ordinarias.
extra_float_digits	Dinámico	Define el número de dígitos que se muestran para los valores de punto flotante.
from_collapse_limit	Dinámico	Define el tamaño FROM-list por encima del cual las subconsultas no se contraen.
fsync	Dinámico	Fuerza la sincronización de las actualizaciones del disco.
full_page_writes	Dinámico	Escribe páginas completas en WAL la primera vez que se modifican después de un punto de comprobación.
geqo	Dinámico	Habilita la optimización genética de consultas.
geqo_effort	Dinámico	GEQO: effort se usa para definir el ajuste predeterminado de otros parámetros de GEQO.

Nombre del parámetro	Apply_Type	Descripción
geqo_generations	Dinámico	GEQO: número de iteraciones del algoritmo.
geqo_pool_size	Dinámico	GEQO: número de individuos de la población.
geqo_seed	Dinámico	GEQO: valor de inicialización para la selección de ruta aleatoria.
geqo_selection_bias	Dinámico	GEQO: presión selectiva dentro de la población.
geqo_threshold	Dinámico	Define el umbral de los elementos FROM por encima de los cuales se usa GEQO.
gin_fuzzy_search_limit	Dinámico	Define el resultado máximo permitido para la búsqueda exacta por GIN.
hot_standby_feedback	Dinámico	Determina si un servidor de espera en caliente envía mensajes de retroalimentación al servidor primario o de subida en espera.
intervalstyle	Dinámico	Define el formato de visualización para los valores de intervalo.
join_collapse_limit	Dinámico	Define el tamaño FROM-list por encima del cual las construcciones JOIN no se aplanan.
lc_messages	Dinámico	Define el idioma en el que se muestran los mensajes.
lc_monetary	Dinámico	Define la configuración regional para el formato de las cantidades monetarias.
lc_numeric	Dinámico	Define la configuración regional para el formato de los números.
lc_time	Dinámico	Define la configuración regional para el formato de los valores de fecha y hora.

Nombre del parámetro	Apply_Type	Descripción
log_autovacuum_min_duration	Dinámico	Define el tiempo de ejecución mínimo por encima del cual se registrarán las acciones de autovacuum.
log_checkpoints	Dinámico	Registra cada punto de comprobación.
log_connections	Dinámico	Registra cada conexión realizada correctamente.
log_disconnections	Dinámico	Registra el final de una sesión, incluida su duración.
log_duration	Dinámico	Registra la duración de cada declaración de SQL completada.
log_error_verbosity	Dinámico	Define el detalle de los mensajes registrados.
log_executor_stats	Dinámico	Escribe las estadísticas de rendimiento del ejecutor en el registro del servidor.
log_filename	Dinámico	Define el patrón del nombre de archivo para los archivos de registro.
log_file_mode	Dinámico	Establece los permisos de los archivos de registro. El valor predeterminado es 0644.
log_hostname	Dinámico	Registra el nombre del host en los registros de conexión. A partir de PostgreSQL 12 y versiones posteriores, este parámetro está desactivado de forma predeterminada. Cuando se activa, la conexión utiliza la búsqueda inversa de DNS para obtener el nombre de host que se captura en los registros de conexión. Si activa este parámetro, debe supervisar el impacto que tiene en el tiempo que se tarda en establecer las conexiones.

Nombre del parámetro	Apply_Type	Descripción
log_line_prefix	Dinámico	Controla la información prefijada en cada línea de registro.
log_lock_waits	Dinámico	Registra las esperas de bloqueo largas.
log_min_duration_statement	Dinámico	Define el tiempo de ejecución mínimo por encima del cual se registrarán las instrucciones.
log_min_error_statement	Dinámico	Hace que todas las declaraciones que generen un error en este nivel o por encima de él se registren.
log_min_messages	Dinámico	Define los niveles de los mensajes que se registran.
log_parser_stats	Dinámico	Escribe las estadísticas de desempeño del analizador en el registro del servidor.
log_planner_stats	Dinámico	Escribe las estadísticas de desempeño del planificador en el registro del servidor.
log_rotation_age	Dinámico	Se producirá una rotación automática del archivo de registro después de N minutos.
log_rotation_size	Dinámico	Se producirá una rotación automática del archivo de registro después de N kilobytes.
log_statement	Dinámico	Define el tipo de declaraciones que se deben registrar.
log_statement_stats	Dinámico	Escribe las estadísticas de desempeño acumulativas en el registro del servidor.
log_temp_files	Dinámico	Registra el uso de archivos temporales con un tamaño superior a este número de kilobytes.
log_timezone	Dinámico	Establece la zona horaria que se usará en los mensajes de registro.

Nombre del parámetro	Apply_Type	Descripción
log_truncate_on_rotation	Dinámico	Permite truncar los archivos de registro existentes con el mismo nombre durante la rotación del registro.
logging_collector	Estático	Inicia un subproceso para capturar el resultado de stderr o csvlogs en archivos de registro.
maintenance_work_mem	Dinámico	Define la memoria máxima que se debe usar para las operaciones de mantenimiento.
max_connections	Estático	Define el número máximo de conexiones simultáneas.
max_files_per_process	Estático	Define el número máximo de archivos abiertos simultáneamente para cada proceso del servidor.
max_locks_per_transaction	Estático	Define el número máximo de bloqueos por transacción.
max_pred_locks_per_transaction	Estático	Define el número máximo de bloqueos de predicado por transacción.
max_prepared_transactions	Estático	Define el número máximo de transacciones preparadas simultáneamente.
max_stack_depth	Dinámico	Define la profundidad máxima de la pila en kilobytes.
max_standby_archive_delay	Dinámico	Define el retardo máximo antes de la cancelación de consultas cuando un servidor de espera en caliente está procesando los datos de WAL archivados.

Nombre del parámetro	Apply_Type	Descripción
`max_standby_streaming_delay`	Dinámico	Define el retardo máximo antes de la cancelación de consultas cuando un servidor de espera en caliente está procesando los datos de WAL transmitidos.

`max_wal_size`	Dinámico	Establece el tamaño de WAL (MB) que lanza un punto de comprobación.
		• Para RDS para PostgreSQL 15 y versiones anteriores, es de 2 GB.
		• Para RDS para PostgreSQL 16 y versiones posteriores, RDS para PostgreSQL se configura automáticamente en función del tamaño de almacenamiento asignado a la instancia:
		  • 6 GB para instancias con almacenamiento asignado de 100 GB o más.
		  • 2 GB para instancias con almacenamiento asignado de menos de 100 GB.
		
		Use el comando siguiente en la instancia de base de datos de Amazon RDS para PostgreSQL para ver su valor actual:
		`SHOW max_wal_size;`

`min_wal_size`	Dinámico	Establece el tamaño mínimo al que reducir el WAL. Para la versión 9.6 de PostgreSQL y anteriores, `min_wal_size` está en unidades de 16 MB. Para la versión 10 de PostgreSQL y posteriores, `min_wal_size` está en unidades de 1 MB.

Nombre del parámetro	Apply_Type	Descripción
quote_all_identifiers	Dinámico	Añade comillas (") a todos los identificadores cuando se generan fragmentos SQL.
random_page_cost	Dinámico	Define la estimación del planificador del coste de una página de disco que no se recupera secuencialmente. Este parámetro no tiene valor a menos que la administración del plan de consultas (QPM) esté activada. Cuando QPM está activado, el valor predeterminado para este parámetro es 4.
rds.adaptive_autovacuum	Dinámico	Ajusta automáticamente los parámetros autovacuum cuando se superan los umbrales del identificador de transacción.
rds.force_ssl	Dinámico	Requiere el uso de conexiones SSL. El valor predeterminado se establece en 1 (activado) para RDS para la versión 15 de PostgreSQL. Todas las demás versiones de RDS para PostgreSQL 14 principal y anteriores tienen el valor predeterminado establecido en 0 (desactivado).
rds.local_volume_spill_enabled	Estático	Permite escribir archivos de vertidos lógicos en el volumen local.
rds.log_retention_period	Dinámico	Establece la retención de registros de manera que Amazon RDS elimina los registros de PostgreSQL que sobrepasan n minutos.
rds.rds_superuser_reserved_connections	Estático	Establece el número de ranuras de conexión reservadas para rds_superusers. Este parámetro solo está disponible en la versión 15 y anteriores. Para obtener más información, consulte la documentación de PostgreSQL sobre reserved_connections.

Nombre del parámetro	Apply_Type	Descripción
`rds.replica_identity_full`	Dinámico	Al establecer este parámetro en on, invalida la configuración de identidad de réplica a `FULL` para todas las tablas de la base de datos. Esto significa que todos los valores de las columnas se escriben en el registro de escritura anticipada (WAL), independientemente de la configuración de `REPLICA IDENTITY FULL`. **Note** La activación de este parámetro puede aumentar las IOPS de la instancia de base de datos debido al registro WAL adicional.
`rds.restrict_password_commands`	Estático	Restringe quién puede administrar contraseñas de los usuarios con el rol `rds_password` . Establezca este parámetro en 1 para habilitar la restricción de contraseñas. El valor predeterminado es 0.
`search_path`	Dinámico	Define el orden de búsqueda del esquema para los nombres que no cumplen los requisitos del esquema.
`seq_page_cost`	Dinámico	Define la estimación del planificador del costo de una página de disco que se recupera secuencialmente.
`session_replication_role`	Dinámico	Define el comportamiento de las sesiones para los desencadenadores y las reglas de reescritura.
`shared_buffers`	Estático	Define el número de búferes de memoria compartida utilizados por el servidor.

Nombre del parámetro	Apply_Type	Descripción
shared_preload_libraries	Estático	Enumera las bibliotecas compartidas para precargar en la instancia de base de datos de RDS para PostgreSQL. Los valores admitidos son: auto_explain, orafce, pgaudit, pglogical, pg_bigm, pg_cron, pg_hint_plan, pg_prewarm, pg_similarity, pg_stat_statements, pg_tle, pg_transport, plprofiler y plrust.
ssl	Dinámico	Habilita las conexiones SSL.
sql_inheritance	Dinámico	Hace que las subtablas se incluyan de manera predeterminada en varios comandos.
ssl_renegotiation_limit	Dinámico	Define la cantidad de tráfico que se debe enviar y recibir antes de renegociar las claves de cifrado.
standard_conforming_strings	Dinámico	Hace que las cadenas ... traten las barras diagonales invertidas literalmente.
statement_timeout	Dinámico	Establece la duración máxima permitida de cualquier declaración.
synchronize_seqscans	Dinámico	Habilita los exámenes secuenciales sincronizados.
synchronous_commit	Dinámico	Define el nivel de sincronización de las transacciones actuales.
tcp_keepalives_count	Dinámico	Número máximo de retransmisiones de keepalive de TCP.
tcp_keepalives_idle	Dinámico	Tiempo entre emisiones de keepalive de TCP.
tcp_keepalives_interval	Dinámico	Tiempo entre retransmisiones de keepalive de TCP.

Nombre del parámetro	Apply_Type	Descripción
`temp_buffers`	Dinámico	Define el número máximo de búferes temporales utilizados por cada sesión.
`temp_file_limit`	Dinámico	Establece el tamaño máximo en KB que pueden alcanzar los archivos temporales.
`temp_tablespaces`	Dinámico	Define los espacios de tabla que se deben usar para las tablas temporales y los archivos de ordenación.
`timezone`	Dinámico	Define la zona horaria para visualizar e interpretar las marcas temporales. Internet Assigned Numbers Authority (Autoridad de Números Asignados en Internet, IANA por sus siglas en inglés) publica nuevas zonas horarias en https://www.iana.org/time-zones varias veces al año. Cada vez que RDS publica una nueva versión secundaria de mantenimiento de PostgreSQL, incluye los datos de zona horaria más recientes en el momento de la publicación. Cuando utiliza las versiones más recientes de RDS para PostgreSQL, dispone de datos de zona horaria recientes de RDS. Para garantizar que la instancia de base de datos tenga datos de zona horaria recientes, se recomienda actualizar a una versión posterior del motor de base de datos. No puede modificar las tablas de zona horaria de las instancias de base de datos de PostgreSQL de forma manual. RDS no modifica ni restablece los datos de zona horaria de las instancias de base de datos en ejecución. Los nuevos datos de zona horaria solo se instalan cuando se actualiza la versión del motor de base de datos.

Nombre del parámetro	Apply_Type	Descripción
track_activities	Dinámico	Recopila información sobre la ejecución de comandos.
track_activity_query_size	Estático	Define el tamaño reservado para pg_stat_activity.current_query en bytes.
track_counts	Dinámico	Recopila estadísticas sobre la actividad de la base de datos.
track_functions	Dinámico	Recopila estadísticas de nivel de función sobre la actividad de la base de datos.
track_io_timing	Dinámico	Recopila estadísticas temporales sobre la actividad de E/S de la base de datos.
transaction_deferrable	Dinámico	Indica si se debe retrasar una transacción serializable de solo lectura hasta que se pueda comenzar sin posibles errores de serialización.
transaction_isolation	Dinámico	Define el nivel de aislamiento de las transacciones actuales.
transaction_read_only	Dinámico	Define el estado de solo lectura de las transacciones actuales.
transform_null_equals	Dinámico	Trata expr=NULL como expr IS NULL.
update_process_title	Dinámico	Actualiza el título del proceso para mostrar el comando SQL activo.
vacuum_cost_delay	Dinámico	Retardo del costo del vacío en milisegundos.
vacuum_cost_limit	Dinámico	Importe del costo del vacío disponible antes del periodo de reposo.

Nombre del parámetro	Apply_Type	Descripción
vacuum_cost_page_dirty	Dinámico	Costo del vacío para una página ensuciada por el vacío.
vacuum_cost_page_hit	Dinámico	Costo del vacío para una página encontrada en la caché del búfer.
vacuum_cost_page_miss	Dinámico	Costo del vacío para una página no encontrada en la caché del búfer.
vacuum_defer_cleanup_age	Dinámico	Número de transacciones para las que se deben retrasar el vacío y la limpieza en caliente, si los hay.
vacuum_freeze_min_age	Dinámico	Antigüedad mínima a la que el vacío debe inmovilizar una fila de una tabla.
vacuum_freeze_table_age	Dinámico	Antigüedad a la que el vacío debe examinar una tabla completa para inmovilizar tuplas.
wal_buffers	Estático	Define el número de búferes de página de disco de memoria compartida para WAL.
wal_writer_delay	Dinámico	Tiempo de reposo del escritor de WAL entre vaciados de WAL.
work_mem	Dinámico	Define la memoria máxima que se debe usar para los espacios de trabajo de consulta.
xmlbinary	Dinámico	Define cómo se deben codificar los valores binarios en XML.
xmloption	Dinámico	Define si los datos XML de las operaciones implícitas de análisis y serialización se deben considerar documentos o fragmentos de contenido .

Amazon RDS usa las unidades predeterminadas de PostgreSQL para todos los parámetros. En la tabla siguiente se muestra la unidad predeterminada de PostgreSQL para cada parámetro.

Nombre del parámetro	Unidad
archive_timeout	s
authentication_timeout	s
autovacuum_naptime	s
autovacuum_vacuum_cost_delay	ms
bgwriter_delay	ms
checkpoint_timeout	s
checkpoint_warning	s
deadlock_timeout	ms
effective_cache_size	8 KB
lock_timeout	ms
log_autovacuum_min_duration	ms
log_min_duration_statement	ms
log_rotation_age	minutos
log_rotation_size	KB
log_temp_files	KB
maintenance_work_mem	KB
max_stack_depth	KB
max_standby_archive_delay	ms
max_standby_streaming_delay	ms

Nombre del parámetro	Unidad
post_auth_delay	s
pre_auth_delay	s
segment_size	8 KB
shared_buffers	8 KB
statement_timeout	ms
ssl_renegotiation_limit	KB
tcp_keepalives_idle	s
tcp_keepalives_interval	s
temp_file_limit	KB
work_mem	KB
temp_buffers	8 KB
vacuum_cost_delay	ms
wal_buffers	8 KB
wal_receiver_timeout	ms
wal_segment_size	B
wal_sender_timeout	ms
wal_writer_delay	ms
wal_receiver_status_interval	s

Ajuste con eventos de espera de RDS para PostgreSQL

Los eventos de espera son una importante herramienta de ajuste para RDS para PostgreSQL. Si puede averiguar por qué las sesiones esperan recursos y qué están haciendo, podrá reducir mejor los cuellos de botella. Puede utilizar la información de esta sección para encontrar las posibles causas y acciones correctivas. En esta sección también se describen los conceptos básicos de ajuste de PostgreSQL.

Los eventos de espera en esta sección son específicos de RDS para PostgreSQL.

Temas

- Conceptos esenciales para el ajuste de RDS para PostgreSQL
- Eventos de espera de RDS para PostgreSQL
- Client:ClientRead
- Client:ClientWrite
- CPU
- IO:BufFileRead y IO:BufFileWrite
- IO:DataFileRead
- IO:WALWrite
- Eventos de espera IPC:parallel
- Lock:advisory
- Lock:extend
- Lock:Relation
- Lock:transactionid
- Lock:tuple
- LWLock:BufferMapping (LWLock:buffer_mapping)
- LWLock:BufferIO (IPC:BufferIO)
- LWLock:buffer_content (BufferContent)
- LWLock:lock_manager (LWLock:lockmanager)
- LWLock:pg_stat_statements
- Timeout:PgSleep
- Timeout:VacuumDelay

Conceptos esenciales para el ajuste de RDS para PostgreSQL

Antes de ajustar la base de datos de RDS para PostgreSQL, asegúrese de saber qué son los eventos de espera y por qué se producen. Revise también la arquitectura básica de memoria y disco de RDS para PostgreSQL. Para ver un diagrama de arquitectura útil, consulte el wikibook de PostgreSQL.

Temas

- Eventos de espera de RDS para PostgreSQL
- Memoria de RDS para PostgreSQL
- Procesos de RDS para PostgreSQL

Eventos de espera de RDS para PostgreSQL

Un evento de espera es una indicación de que la sesión espera un recurso. Por ejemplo, el evento de espera `Client:ClientRead` ocurre cuando RDS para PostgreSQL espera recibir datos del cliente. Por lo general, las sesiones esperan recursos como los siguientes.

- Acceso de subproceso único a un búfer, por ejemplo, cuando una sesión intenta modificar un búfer
- Una fila bloqueada actualmente por otra sesión
- Lectura de un archivo de datos
- Escritura de un archivo de registro

Por ejemplo, para satisfacer una consulta, la sesión podría hacer un escaneo de tabla completo. Si los datos ya no están en la memoria, la sesión espera a que se complete la E/S del disco. Cuando los búferes se leen en la memoria, es posible que la sesión tenga que esperar porque otras sesiones tienen acceso a los mismos búferes. La base de datos registra las esperas mediante un evento de espera predefinido. Estos eventos se agrupan en categorías.

Un evento de espera no significa por sí solo un problema de rendimiento. Por ejemplo, si los datos solicitados no están en memoria, es necesario leer los datos del disco. Si una sesión bloquea una fila para una actualización, otra sesión espera a que se desbloquee la fila para poder actualizarla. Una confirmación requiere un tiempo de espera para que se complete la escritura en un archivo de registro. Las esperas forman parte del funcionamiento normal de una base de datos.

Por otro lado, un gran número de eventos de espera suele ser indicativo de un problema de rendimiento. En estos casos, se pueden utilizar los datos de los eventos de espera para determinar

en qué se gastan las sesiones. Por ejemplo, si un informe que normalmente se ejecuta en minutos ahora se ejecuta durante horas, puede identificar los eventos de espera que más contribuyen al tiempo total de espera. Si puede determinar las causas de los principales eventos de espera, a veces puede hacer cambios que mejoren el rendimiento. Por ejemplo, si la sesión se encuentra a la espera de una fila que ha sido bloqueada por otra sesión, puede terminar la sesión de bloqueo.

Memoria de RDS para PostgreSQL

La memoria de RDS para PostgreSQL se divide en compartida y local.

Temas

- Memoria compartida en RDS para PostgreSQL
- Memoria local en RDS para PostgreSQL

Memoria compartida en RDS para PostgreSQL

RDS para PostgreSQL asigna memoria compartida cuando se inicia la instancia. La memoria compartida se divide en múltiples subáreas. En las siguientes secciones se proporcionan descripciones de las más importantes.

Temas

- Búferes compartidos
- Búferes de registro de escritura anticipada (WAL)

Búferes compartidos

El grupo de búferes compartidos es un área de memoria de RDS para PostgreSQL que contiene todas las páginas que utilizan o han utilizado las conexiones de la aplicación. Una página es la versión de memoria de un bloque de disco. El grupo de búferes compartidos almacena en caché los bloques de datos leídos desde el disco. El grupo reduce la necesidad de volver a leer los datos del disco, lo que hace que la base de datos funcione de forma más eficiente.

Cada tabla e índice se almacena como una matriz de páginas de tamaño fijo. Cada bloque contiene varias tuplas, que corresponden a filas. Una tupla se puede almacenar en cualquier página.

El grupo de búferes compartidos tiene memoria finita. Si una nueva solicitud requiere una página que no está en la memoria, y no hay más memoria, RDS para PostgreSQL desaloja una página que

se utiliza con menos frecuencia para satisfacer la solicitud. La política de expulsión se implementa mediante un algoritmo de barrido de reloj.

El parámetro `shared_buffers` determina la cantidad de memoria que el servidor dedica al almacenamiento en caché de los datos. El valor predeterminado se establece en `{DBInstanceClassMemory/32768}` bytes, en función de la memoria disponible para la instancia de base de datos.

Búferes de registro de escritura anticipada (WAL)

Un búfer del registro de escritura anticipada (WAL) contiene datos de transacciones que RDS para PostgreSQL escribe posteriormente en el almacenamiento persistente. Con el mecanismo WAL, RDS para PostgreSQL puede hacer lo siguiente:

- Recuperar datos después de un error
- Reducir la E/S del disco al evitar las escrituras frecuentes en el disco

Cuando un cliente cambia los datos, RDS para PostgreSQL escribe los cambios en el búfer de WAL. Cuando el cliente emite un `COMMIT`, el proceso de escritura WAL escribe los datos de la transacción en el archivo WAL.

El parámetro `wal_level` determina la cantidad de información que se escribe en el WAL, con posibles valores como `minimal`, `replica` y `logical`.

Memoria local en RDS para PostgreSQL

Cada proceso de backend asigna memoria local para el procesamiento de consultas.

Temas

- Área de memoria de trabajo
- Área de memoria de trabajo de mantenimiento
- Área de búfer temporal

Área de memoria de trabajo

El área de memoria de trabajo contiene datos temporales para las consultas que ejecutan ordenaciones y hashes. Por ejemplo, una consulta con una cláusula `ORDER BY` ejecuta una ordenación. Las consultas utilizan tablas hash en uniones hash y agregaciones.

El parámetro `work_mem` indica la cantidad de memoria que se utilizará en las operaciones internas de ordenación y en las tablas hash antes de escribir en los archivos temporales del disco, medido en megabytes. El valor predeterminado es 4 MB. Se pueden ejecutar varias sesiones simultáneamente, y cada sesión puede ejecutar operaciones de mantenimiento en paralelo. Por esta razón, la memoria de trabajo total utilizada puede ser múltiplo del parámetro `work_mem`.

Área de memoria de trabajo de mantenimiento

El área de memoria de trabajo de mantenimiento almacena en caché los datos de las operaciones de mantenimiento. Estas operaciones incluyen el vaciado, creación de un índice y adición de claves externas.

El parámetro `maintenance_work_mem` especifica la cantidad máxima de memoria que utilizarán las operaciones de mantenimiento, medido en megabytes. El valor predeterminado es 64 MB. Una sesión de base de datos solo puede ejecutar una operación de mantenimiento a la vez.

Área de búfer temporal

El área de búfer temporal almacena en caché las tablas temporales de cada sesión de la base de datos.

Cada sesión asigna búferes temporales según sea necesario hasta el límite que se especifique. Cuando finaliza la sesión, el servidor borra los búferes.

El parámetro `temp_buffers` establece el número máximo de búferes temporales utilizados por cada sesión, medido en megabytes. El valor predeterminado es 8 MB. Antes del primer uso de las tablas temporales dentro de una sesión, puede cambiar el valor de `temp_buffers`.

Procesos de RDS para PostgreSQL

RDS para PostgreSQL utiliza varios procesos.

Temas

- Proceso de administrador de correos
- Procesos de backend
- Procesos en segundo plano

Proceso de administrador de correos

El proceso de administrador de correos es el primer proceso que se ejecuta cuando se inicia RDS para PostgreSQL. El proceso de administrador de correos tiene las siguientes funciones principales:

- Bifurcar y monitorear los procesos en segundo plano
- Recibir solicitudes de autenticación de los procesos cliente, y autenticarlos antes de permitir que la base de datos atienda las solicitudes

Procesos de backend

Si el administrador de correos autentica una solicitud de cliente, el administrador de correos bifurca un nuevo proceso de backend, también llamado proceso postgres. Un proceso cliente se conecta exactamente a un proceso backend. El proceso cliente y el proceso backend se comunican directamente sin la intervención del proceso de administrador de correos.

Procesos en segundo plano

El proceso de administrador de correos bifurca varios procesos que ejecutan distintas tareas de backend. Algunas de las más importantes son las siguientes:

- Escritor de WAL

  RDS para PostgreSQL escribe datos en el búfer WAL (registro de escritura anticipada) en los archivos de registro. El principio del registro por adelantado es que la base de datos no puede escribir los cambios en los archivos de datos hasta que la base de datos escriba los registros que describen esos cambios en el disco. El mecanismo de WAL reduce la E/S del disco y permite a RDS para PostgreSQL utilizar los registros para recuperar la base de datos en caso de error.
- Escritor en segundo plano

  Este proceso escribe de forma periódica las páginas sucias (modificadas) desde los búferes de memoria a los archivos de datos. Una página se vuelve sucia cuando un proceso de backend la modifica en la memoria.
- Daemon de autovacuum

  El daemon consta de lo siguiente:

  - El iniciador de autovacuum
  - Los procesos de trabajo de autovacuum

Cuando autovacuum está activado busca las tablas en las que se ha insertado, actualizado o eliminado un número elevado de tuplas. El daemon tiene las siguientes responsabilidades:

- Recuperar o reutilizar el espacio de disco ocupado por las filas actualizadas o eliminadas
- Actualizar las estadísticas utilizadas por el planificador
- Proteger contra la pérdida de datos antiguos debido al reinicio del ID de transacción

La característica de autovacuum automatiza la ejecución de los comandos `VACUUM` y `ANALYZE`. `VACUUM` tiene las siguientes variantes: estándar y completo. El vacío estándar se ejecuta en paralelo con otras operaciones de la base de datos. `VACUUM FULL` requiere un bloqueo exclusivo sobre la tabla en la que se trabaja. Por lo tanto, no puede ejecutarse en paralelo con operaciones que acceden a la misma tabla. `VACUUM` crea una cantidad considerable de tráfico de E/S, lo que puede causar un bajo rendimiento para otras sesiones activas.

Eventos de espera de RDS para PostgreSQL

La siguiente tabla enumera los eventos de espera de RDS para PostgreSQL que suelen indicar problemas de rendimiento, y resume las causas más comunes y las acciones correctivas.

Evento de espera	Definición
Client:ClientRead	Este evento ocurre cuando RDS para PostgreSQL espera recibir datos del cliente.
Client:ClientWrite	Este evento ocurre cuando RDS para PostgreSQL espera escribir datos en el cliente.
CPU	Este evento ocurre cuando un subproceso está activo en la CPU o espera por la CPU.
IO:BufFileRead y IO:BufFileWrite	Los eventos ocurren cuando RDS para PostgreSQL crean archivos temporales.
IO:DataFileRead	Este evento ocurre cuando una conexión espera en un proceso backend para leer una página requerida desde el almacenamiento porque la página no está disponible en la memoria compartida.

Evento de espera	Definición
IO:WALWrite	Este evento ocurre cuando RDS para PostgreSQL está esperando a que se escriban los búferes del registro de escritura anticipada (WAL) en un archivo WAL.
Lock:advisory	Este evento ocurre cuando una aplicación PostgreSQL utiliza un bloqueo para coordinar la actividad en varias sesiones.
Lock:extend	Este evento ocurre cuando un proceso backend espera bloquear una relación para ampliarla mientras otro proceso tiene un bloqueo en esa relación para el mismo propósito.
Lock:Relation	Este evento ocurre cuando una consulta espera adquirir un bloqueo en una tabla o vista que está actualmente bloqueada por otra transacción.
Lock:transactionid	Este evento ocurre cuando una transacción espera un bloqueo a nivel de fila.
Lock:tuple	Este evento ocurre cuando un proceso de backend espera adquirir un bloqueo en una tupla.
LWLock:BufferMapping (LWLock:buffer_mapping)	Este evento se produce cuando una sesión espera asociar un bloque de datos con un búfer en el grupo de búferes compartidos.
LWLock:BufferIO (IPC:BufferIO)	El evento ocurre cuando RDS para PostgreSQL espera que otros procesos terminen sus operaciones de entrada/salida (E/S) cuando intentan acceder a una página de forma simultánea.

Evento de espera	Definición
LWLock:buffer_content (BufferContent)	Este evento ocurre cuando una sesión espera leer o escribir una página de datos en la memoria mientras otra sesión bloquea esa página para la escritura.
LWLock:lock_manager (LWLock:lockmanager)	Este evento ocurre cuando el motor de RDS para PostgreSQL mantiene el área de memoria del bloqueo compartido para asignar, verificar y desasignar un bloqueo cuando no es posible un bloqueo de ruta rápida.
Timeout:PgSleep	Este evento ocurre cuando un proceso del servidor llamó a la función `pg_sleep` y espera que el tiempo de espera expire.
Timeout:VacuumDelay	Este evento indica que el proceso de vacío está en reposo porque se ha alcanzado el límite de costo estimado.

Client:ClientRead

El evento `Client:ClientRead` ocurre cuando RDS para PostgreSQL espera recibir datos del cliente.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con RDS para PostgreSQL versión 10 y posteriores.

Context

Una instancia de base de datos de RDS para PostgreSQL espera recibir datos del cliente. La instancia de la base de datos de RDS para PostgreSQL tiene que recibir los datos del cliente antes de poder enviar más datos al cliente. El tiempo que la instancia espera antes de recibir los datos del cliente es un evento `Client:ClientRead`.

Causas probables del aumento del tiempo de espera

Las causas más comunes para que el evento `Client:ClientRead` aparezca en el máximo de esperas son las siguientes:

Aumento de la latencia de la red

Puede haber un aumento de la latencia de la red entre la instancia de la base de datos de RDS para PostgreSQL y el cliente. Una mayor latencia de la red aumenta el tiempo necesario para que la instancia de base de datos reciba los datos del cliente.

Aumento de la carga en el cliente

Puede haber presión de la CPU o saturación de la red en el cliente. Un aumento de la carga en el cliente puede retrasar la transmisión de datos desde el cliente a la instancia de la base de datos de RDS para PostgreSQL.

Excesivos viajes de ida y vuelta de la red

Un gran número de viajes de ida y vuelta de la red entre la instancia de la base de datos de RDS para PostgreSQL y el cliente puede retrasar la transmisión de datos del cliente a la instancia de la base de datos de RDS para PostgreSQL.

Operación de copia grande

Durante una operación de copia, los datos se transfieren desde el sistema de archivos del cliente a la instancia de la base de datos de RDS para PostgreSQL. El envío de una gran cantidad de datos a la instancia de la base de datos puede retrasar la transmisión de datos del cliente a la instancia de la base de datos.

Conexión de cliente inactivo

Cuando un cliente se conecta a la instancia de la base de datos de RDS para PostgreSQL en un estado `idle in transaction`, la instancia de la base de datos puede esperar a que el cliente envíe más datos o emita un comando. Una conexión en este estado puede conducir a un aumento de eventos `Client:ClientRead`.

PgBouncer se utiliza para la agrupación de conexiones

PgBouncer tiene un ajuste de configuración de red de bajo nivel llamado `pkt_buf`, que se establece en 4.096 de forma predeterminada. Si la carga de trabajo envía paquetes de consulta de más de 4096 bytes a través de PgBouncer, recomendamos aumentar la configuración de `pkt_buf` a 8192. Si la nueva configuración no disminuye el número de eventos `Client:ClientRead`, recomendamos aumentar la configuración de `pkt_buf` a valores mayores, como 16 384 o 32 768. Si el texto de la consulta es grande, el ajuste más grande puede ser particularmente útil.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Colocar los clientes en la misma zona de disponibilidad y subred VPC que el evento de espera
- Escalar el cliente
- Utilizar las instancias de generación actual
- Aumentar el ancho de banda de la red
- Monitorear los máximos de rendimiento de la red
- Monitorear las transacciones en el estado “inactivo en la transacción”

Colocar los clientes en la misma zona de disponibilidad y subred VPC que el evento de espera

Para reducir la latencia de la red y aumentar su rendimiento, coloque los clientes en la misma zona de disponibilidad y subred de nube privada virtual (VPC) que la instancia de la base de datos de RDS para PostgreSQL. Asegúrese de que los clientes estén lo más cerca posible desde el punto de vista geográfico de la instancia de la base de datos.

Escalar el cliente

Con Amazon CloudWatch u otras métricas del anfitrión, determine si su cliente está actualmente limitado por la CPU o el ancho de banda de la red, o ambos. Si el cliente está restringido, escale su cliente en forma adecuada.

Utilizar las instancias de generación actual

En algunos casos, es posible que no utilice una clase de instancia de base de datos que admita tramas gigantes. Si ejecuta la aplicación en Amazon EC2, considere la posibilidad de utilizar una instancia de generación actual para el cliente. Además, configure la unidad de transmisión máxima (MTU) en el sistema operativo del cliente. Esta técnica podría reducir el número de viajes de ida y vuelta de la red y aumentar el rendimiento de la red. Para obtener más información, consulte Tramas gigantes (MTU 9001) en la Guía del usuario de Amazon EC2.

Para obtener información acerca de las clases de instancia de base de datos, consulte Clases de instancia de base de datos de . Para determinar la clase de instancia de base de datos que equivale a un tipo de instancia de Amazon EC2, coloque `db.` antes del nombre del tipo de instancia de Amazon EC2. Por ejemplo, la instancia de Amazon EC2 `r5.8xlarge` equivale a la clase de instancia de base de datos `db.r5.8xlarge`.

Aumentar el ancho de banda de la red

Utilice las métricas de Amazon CloudWatch de `NetworkReceiveThroughput` y `NetworkTransmitThroughput` para monitorear el tráfico de red entrante y saliente en la instancia de la base de datos. Estas métricas pueden ayudarle a determinar si el ancho de banda de la red es suficiente para su carga de trabajo.

Si el ancho de banda de su red no es suficiente, auméntelo. Si el cliente de AWS o la instancia de base de datos alcanza los límites del ancho de banda de la red, la única forma de aumentar el ancho de banda es aumentar el tamaño de la instancia de base de datos. Para obtener más información, consulte Tipos de clase de instancia de base de datos.

Para obtener más información acerca de las métricas de CloudWatch, consulte Métricas de Amazon CloudWatch para Amazon RDS.

Monitorear los máximos de rendimiento de la red

Si utiliza clientes de Amazon EC2, Amazon EC2 proporciona límites máximos para las métricas de rendimiento de la red, incluido el ancho de banda de red entrante y saliente agregado. También proporciona un seguimiento de la conexión para garantizar que los paquetes se devuelven como se espera y el acceso a los servicios de enlace local para servicios como el sistema de nombres de dominio (DNS). Para monitorear estos máximos, utilice un controlador de red mejorado actual y monitoree el rendimiento de la red para su cliente.

Para obtener más información, consulte Monitorear el rendimiento de la red de la instancia de Amazon EC2 en la Guía del usuario de Amazon EC2 y Monitorear el rendimiento de la red de la instancia de Amazon EC2 en la Guía del usuario de Amazon EC2.

Monitorear las transacciones en el estado “inactivo en la transacción”

Verifique si tiene un número creciente de conexiones `idle in transaction`. Para ello, monitoree la columna `state` en la tabla `pg_stat_activity`. Es posible que pueda identificar el origen de la conexión si ejecuta una consulta similar a la siguiente.

```
select client_addr, state, count(1) from pg_stat_activity
where state like 'idle in transaction%'
group by 1,2
order by 3 desc
```

Client:ClientWrite

El evento `Client:ClientWrite` ocurre cuando RDS para PostgreSQL espera escribir datos en el cliente.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con RDS para PostgreSQL versión 10 y posteriores.

Context

Un proceso cliente debe leer todos los datos recibidos de un clúster de la base de datos de RDS para PostgreSQL antes de que el clúster pueda enviar más datos. El tiempo que el clúster espera antes de enviar más datos al cliente es un evento `Client:ClientWrite`.

La reducción del rendimiento de la red entre la instancia de base de datos de RDS para PostgreSQL y el cliente puede causar este evento. La presión de la CPU y la saturación de la red en el cliente

también pueden causar este evento. La presión de la CPU es cuando la CPU se utiliza por completo y hay tareas esperando por el tiempo de la CPU. La saturación de la red es cuando la red entre la base de datos y el cliente transporta más datos de los que puede manejar.

Causas probables del aumento de las esperas

Las causas más comunes para que el evento `Client:ClientWrite` aparezca en el máximo de esperas son las siguientes:

Aumento de la latencia de la red

Puede haber un aumento de la latencia de la red entre la instancia de la base de datos de RDS para PostgreSQL y el cliente. Una mayor latencia de la red aumenta el tiempo necesario para que el cliente reciba los datos.

Aumento de la carga en el cliente

Puede haber presión de la CPU o saturación de la red en el cliente. Un aumento de la carga en el cliente retrasa la recepción de los datos de la instancia de la base de datos de RDS para PostgreSQL.

Gran volumen de datos enviados al cliente

La instancia de la base de datos de RDS para PostgreSQL puede estar enviando una gran cantidad de datos al cliente. Es posible que el cliente no pueda recibir los datos tan rápido como el clúster los envía. Actividades como una copia de una tabla grande pueden resultar en un aumento de eventos `Client:ClientWrite`.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Coloque los clientes en la misma zona de disponibilidad y subred VPC que el clúster
- Utilizar las instancias de generación actual
- Reducir la cantidad de datos enviados al cliente
- Escale el cliente

Coloque los clientes en la misma zona de disponibilidad y subred VPC que el clúster

Para reducir la latencia de la red y aumentar su rendimiento, coloque los clientes en la misma zona de disponibilidad y subred de nube privada virtual (VPC) que la instancia de la base de datos de RDS para PostgreSQL.

Utilizar las instancias de generación actual

En algunos casos, es posible que no utilice una clase de instancia de base de datos que admita tramas gigantes. Si ejecuta la aplicación en Amazon EC2, considere la posibilidad de utilizar una instancia de generación actual para el cliente. Además, configure la unidad de transmisión máxima (MTU) en el sistema operativo del cliente. Esta técnica podría reducir el número de viajes de ida y vuelta de la red y aumentar el rendimiento de la red. Para obtener más información, consulte Tramas gigantes (MTU 9001) en la Guía del usuario de Amazon EC2.

Para obtener información acerca de las clases de instancia de base de datos, consulte Clases de instancia de base de datos de . Para determinar la clase de instancia de base de datos que equivale a un tipo de instancia de Amazon EC2, coloque `db.` antes del nombre del tipo de instancia de Amazon EC2. Por ejemplo, la instancia de Amazon EC2 `r5.8xlarge` equivale a la clase de instancia de base de datos `db.r5.8xlarge`.

Reducir la cantidad de datos enviados al cliente

Cuando sea posible, ajuste la aplicación para reducir la cantidad de datos que la instancia de la base de datos de RDS para PostgreSQL envía al cliente. Hacer estos ajustes reduce la contención de la CPU y de la red en el cliente.

Escale el cliente

Con Amazon CloudWatch u otras métricas del anfitrión, determine si su cliente está actualmente limitado por la CPU o el ancho de banda de la red, o ambos. Si el cliente está restringido, escale su cliente en forma adecuada.

CPU

Este evento ocurre cuando un subproceso está activo en la CPU o espera por la CPU.

Temas

- Versiones del motor admitidas
- Context

- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es relevante para todas las versiones de RDS para PostgreSQL.

Context

La unidad de procesamiento central (CPU) es el componente de un ordenador que ejecuta instrucciones. Por ejemplo, las instrucciones de la CPU hacen operaciones aritméticas e intercambian datos en la memoria. Si una consulta aumenta el número de instrucciones que ejecuta a través del motor de base de datos, aumenta el tiempo de ejecución de la consulta. La programación de la CPU consiste en dar tiempo de CPU a un proceso. La programación es orquestada por el núcleo del sistema operativo.

Temas

- Cómo saber cuándo se produce esta espera
- Métrica de DBloadCPU
- Métrica os.cpuUtilization
- Causa probable de la programación de la CPU

Cómo saber cuándo se produce esta espera

Este evento de espera de CPU indica que un proceso del backend se encuentra activo en la CPU o en espera de la misma. Se sabrá que sucede cuando una consulta muestre la siguiente información:

- La columna `pg_stat_activity.state` tiene el valor `active`.
- Las columnas `wait_event_type` y `wait_event` en `pg_stat_activity` son `null`.

Para ver los procesos del backend que se encuentran en uso o en espera de CPU, ejecute la siguiente consulta.

```
SELECT *
FROM   pg_stat_activity
```

```
WHERE  state = 'active'
AND    wait_event_type IS NULL
AND    wait_event IS NULL;
```

Métrica de DBloadCPU

La métrica de Información sobre rendimiento para la CPU es `DBLoadCPU`. El valor de `DBLoadCPU` puede diferir del valor de la métrica `CPUUtilization` de Amazon CloudWatch. Esta última métrica se recopila del hipervisor para una instancia de base de datos.

Métrica os.cpuUtilization

Las métricas del sistema operativo de Información sobre rendimiento proporcionan información detallada sobre la utilización de la CPU. Por ejemplo, puede mostrar las siguientes métricas:

- `os.cpuUtilization.nice.avg`
- `os.cpuUtilization.total.avg`
- `os.cpuUtilization.wait.avg`
- `os.cpuUtilization.idle.avg`

Información sobre rendimiento informa del uso de la CPU por parte del motor de base de datos como `os.cpuUtilization.nice.avg`.

Causa probable de la programación de la CPU

El núcleo del sistema operativo (SO) ejecuta la programación de la CPU. Cuando la CPU está activa, es posible que un proceso tenga que esperar para programarse. La CPU está activa mientras realiza los cálculos. También está activa mientras ejecuta un subproceso inactivo, es decir, un subproceso inactivo que espera la E/S de la memoria. Este tipo de E/S domina la carga de trabajo típica de una base de datos.

Es probable que los procesos esperen a que se programe una CPU cuando se cumplen las siguientes condiciones:

- La métrica CloudWatch `CPUUtilization` está cerca del 100 por ciento.
- La carga media es mayor que el número de vCPU, lo que indica una carga pesada. Puede encontrar la métrica `loadAverageMinute` en la sección de métricas del sistema operativo en Información sobre rendimiento.

Causas probables del aumento de las esperas

Cuando el evento de espera de la CPU ocurre más de lo normal, lo que posiblemente indica un problema de rendimiento, las causas típicas pueden ser las siguientes.

Temas

- Causas probables de picos repentinos
- Causas probables de alta frecuencia prolongada
- Casos aislados

Causas probables de picos repentinos

Las causas más probables de picos repentinos son las siguientes:

- La aplicación abrió demasiadas conexiones simultáneas a la base de datos. Este escenario se conoce como “tormenta de conexiones”
- La carga de trabajo de la aplicación ha cambiado de alguna de las siguientes maneras:
  - Nuevas consultas
  - Un aumento del tamaño del conjunto de datos
  - Mantenimiento o creación de índices
  - Nuevas funciones
  - Nuevos operadores
  - Aumento de la ejecución de consultas en paralelo
- Los planes de ejecución de sus consultas han cambiado. En algunos casos, un cambio puede provocar un aumento de los búferes. Por ejemplo, la consulta utiliza ahora un escaneo secuencial cuando antes utilizaba un índice. En este caso, las consultas necesitan más CPU para lograr el mismo objetivo.

Causas probables de alta frecuencia prolongada

Las causas más probables de eventos que se repiten durante un periodo prolongado:

- Demasiados procesos de backend se ejecutan de forma simultánea en la CPU. Estos procesos pueden llegar a ser procesos de trabajo paralelos.
- Las consultas tienen un rendimiento subóptimo porque necesitan un gran número de búferes.

Casos aislados

Si ninguna de las causas probables resulta ser la causa real, es posible que se produzcan las siguientes situaciones:

- La CPU está intercambiando procesos de entrada y salida.
- La CPU podría gestionar las entradas de la tabla de páginas si se ha desactivado la función de páginas enormes. Esta característica de administración de la memoria está habilitada de forma predeterminada para todas las clases de instancias de base de datos que no sean de la clase de instancia de base de datos micro, pequeña y mediana. Para obtener más información, consulte Páginas enormes para RDS for PostgreSQL .

Acciones

Si el evento de espera de CPU domina la actividad de la base de datos, no indica necesariamente un problema de rendimiento. Responda a este evento solo cuando el rendimiento se deteriore.

Temas

- Investigue si la base de datos es la causa del aumento de la CPU
- Determine si el número de conexiones aumentó
- Responder a los cambios en la carga de trabajo

Investigue si la base de datos es la causa del aumento de la CPU

Examine la métrica `os.cpuUtilization.nice.avg` en Información sobre rendimiento. Si este valor es mucho menor que el uso de la CPU, los procesos ajenos a la base de datos son los que más contribuyen a la CPU.

Determine si el número de conexiones aumentó

Examine la métrica `DatabaseConnections` en Amazon CloudWatch. La acción a tomar depende de si el número aumentó o disminuyó durante el periodo de aumento de los eventos de espera de la CPU.

Las conexiones aumentaron

Si el número de conexiones aumentó, compare el número de procesos de backend que consumen CPU con el número de vCPU. Los siguientes escenarios son posibles:

- El número de procesos de backend que consumen CPU es menor que el número de vCPU.

  En este caso, el número de conexiones no es un problema. Sin embargo, puede intentar reducir la utilización de la CPU.

- El número de procesos de backend que consumen CPU es mayor que el número de vCPU.

  En este caso, considere las siguientes opciones:

  - Disminuya el número de procesos backend conectados a la base de datos. Por ejemplo, implemente una solución de agrupación de conexiones, como el proxy RDS. Para obtener más información, consulte Amazon RDS Proxy .
  - Actualice el tamaño de su instancia para obtener un mayor número de vCPU.
  - Redirija algunas cargas de trabajo de solo lectura a nodos lectores, si procede.

Las conexiones no aumentaron

Examine las métricas de `blks_hit` en Información sobre rendimiento. Busque una correlación entre el aumento de `blks_hit` y el uso de la CPU. Los siguientes escenarios son posibles:

- El uso de la CPU y `blks_hit` están correlacionados.

  En este caso, encuentre las principales instrucciones SQL que están relacionadas con el uso de la CPU y busque los cambios de plan. Puede utilizar cualquiera de las siguientes técnicas:

  - Explicar los planes manualmente y compararlos con el plan de ejecución esperado.
  - Buscar un aumento en los aciertos de bloque por segundo y en los aciertos de bloque local por segundo. En la sección Top SQL (SQL principal) del panel de Información sobre rendimiento, elija Preferences (Preferencias).

- El uso de la CPU y `blks_hit` no están correlacionados.

  En este caso, determine si se produce alguna de las siguientes situaciones:

  - La aplicación se conecta y desconecta con rapidez de la base de datos.

    Diagnostique este comportamiento mediante la activación de `log_connections` y `log_disconnections`, y luego analice los registros de PostgreSQL. Considere utilizar el analizador de registros `pgbadger`. Para obtener más información, consulte https://github.com/darold/pgbadger.

  - El sistema operativo está sobrecargado.

En este caso, Información sobre rendimiento muestra que los procesos del backend consumen la CPU durante más tiempo del habitual. Busque pruebas en las métricas de Información sobre rendimiento `os.cpuUtilization` o en la métrica CloudWatch `CPUUtilization`. Si el sistema operativo está sobrecargado, consulte las métricas de Monitoreo mejorado para hacer un diagnóstico más profundo. Específicamente, observe la lista de procesos y el porcentaje de CPU que consume cada proceso.

- Las instrucciones SQL más importantes son las que consumen demasiada CPU.

  Examine las instrucciones que se relacionan con el uso de la CPU para ver si pueden utilizar menos CPU. Ejecute un comando `EXPLAIN`, y céntrese en los nodos del plan que tienen el mayor impacto. Considere utilizar un visualizador de planes de ejecución de PostgreSQL. Para probar esta herramienta, consulte http://explain.dalibo.com/.

Responder a los cambios en la carga de trabajo

Si la carga de trabajo cambió, busque los siguientes tipos de cambios:

Nuevas consultas

Verifique si las nuevas consultas son las esperadas. Si es así, asegúrese de que los planes de ejecución y el número de ejecuciones por segundo son los esperados.

Aumento del tamaño del conjunto de datos

Determine si la partición, si no se ha implementado todavía, podría ayudar. Esta estrategia podrá reducir el número de páginas que debe recuperar una consulta.

Mantenimiento o creación de índices

Verifique si el programa de mantenimiento es el previsto. Una práctica recomendada es programar las actividades de mantenimiento fuera de los picos de actividad.

Nuevas funciones

Verifique si estas funciones se comportan como se espera durante las pruebas. En concreto, verifique si el número de ejecuciones por segundo es el esperado.

Nuevos operadores

Verifique si su rendimiento es el esperado durante las pruebas.

Aumento de la ejecución de consultas paralelas

Determine si se ha producido alguna de las siguientes situaciones:

- Las relaciones o los índices implicados han crecido repentinamente en tamaño de modo que difieren significativamente de `min_parallel_table_scan_size` o `min_parallel_index_scan_size`.
- Se hicieron cambios recientes en `parallel_setup_cost` o `parallel_tuple_cost`.
- Se hicieron cambios recientes en `max_parallel_workers` o `max_parallel_workers_per_gather`.

IO:BufFileRead y IO:BufFileWrite

Los eventos `IO:BufFileRead` e `IO:BufFileWrite` ocurren cuando RDS para PostgreSQL crea archivos temporales. Cuando las operaciones requieren más memoria de la que los parámetros de la memoria de trabajo definen actualmente, escriben datos temporales en el almacenamiento persistente. Esta operación se llama a veces “derramamiento en el disco”

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

`IO:BufFileRead` e `IO:BufFileWrite` se relacionan con el área de memoria de trabajo y el área de memoria de trabajo de mantenimiento. Para obtener más información acerca de estas áreas de memoria locales, consulte el punto Resource Consumption (Consumo de recursos) en la documentación de PostgreSQL.

El valor predeterminado de `work_mem` es de 4 MB. Si una sesión ejecuta operaciones en paralelo, cada proceso de trabajo que maneja el paralelismo utiliza 4 MB de memoria. Por esta razón,

configure `work_mem` con cuidado. Si el valor es demasiado alto, una base de datos con muchas sesiones puede consumir demasiada memoria. Si establece el valor demasiado bajo, RDS para PostgreSQL crea archivos temporales en el almacenamiento local. La E/S del disco para estos archivos temporales puede reducir el rendimiento.

Si se observa la siguiente secuencia de eventos, es posible que la base de datos genere archivos temporales:

1. Disminución repentina y brusca de la disponibilidad
2. Recuperación rápida del espacio libre

También puede observar un patrón de “motosierra”. Este patrón puede indicar que la base de datos crea archivos pequeños de forma constante.

Causas probables del aumento de las esperas

En general, estos eventos de espera son causados por operaciones que consumen más memoria de la que asignan los parámetros `work_mem` o `maintenance_work_mem`. Para compensar, las operaciones se escriben en archivos temporales. Las causas más comunes de los eventos `IO:BufFileRead` y `IO:BufFileWrite` son las siguientes:

Consultas que necesitan más memoria de la que existe en la zona de memoria de trabajo

Las consultas con las siguientes características utilizan el área de memoria de trabajo:

- Combinaciones hash
- Cláusula `ORDER BY`
- `GROUP BY`Cláusula
- `DISTINCT`
- Funciones de ventana
- `CREATE TABLE AS SELECT`
- Actualización de la vista materializada

Instrucciones que necesitan más memoria de la que existe en el área de memoria de trabajo de mantenimiento

Las siguientes instrucciones utilizan el área de memoria de trabajo de mantenimiento:

- `CREATE INDEX`

- CLUSTER

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Identifique el problema
- Examine sus consultas de unión (join)
- Examinar las consultas ORDER BY y GROUP BY
- Evite utilizar la operación DISTINCT
- Considere la posibilidad de utilizar funciones de ventana en lugar de funciones GROUP BY
- Investigar las vistas materializadas y las instrucciones CTA
- Utilizar pg_repack al reconstruir índices
- Aumentar maintenance_work_mem al hacer un clúster de tablas
- Ajustar la memoria para evitar IO:BufFileRead e IO:BufFileWrite

Identifique el problema

Imagine una situación en la que Información sobre rendimiento no está activado y sospecha que `IO:BufFileRead` e `IO:BufFileWrite` se producen con más frecuencia de lo normal. Para identificar el origen del problema, puede configurar el parámetro `log_temp_files` para registrar todas las consultas que generen más KB de archivos temporales que el umbral especificado. De forma predeterminada, `log_temp_files` se establece en `-1`, lo que desactiva esta función de registro. Si establece este parámetro como `0`, RDS para PostgreSQL registra todos los archivos temporales. Si lo establece en `1024`, RDS para PostgreSQL registra todas las consultas que produzcan archivos temporales de más de 1 MB. Para más información sobre `log_temp_files`, consulte Error Reporting and Logging en la documentación de PostgreSQL.

Examine sus consultas de unión (join)

Es probable que la consulta utilice combinaciones. Por ejemplo, la siguiente consulta une cuatro tablas.

```
SELECT *
       FROM "order"
```

```
 INNER JOIN order_item
       ON (order.id = order_item.order_id)
 INNER JOIN customer
       ON (customer.id = order.customer_id)
 INNER JOIN customer_address
       ON (customer_address.customer_id = customer.id AND
           order.customer_address_id = customer_address.id)
 WHERE customer.id = 1234567890;
```

Una posible causa de los picos de uso de archivos temporales es un problema en la propia consulta. Por ejemplo, una cláusula rota podría no filtrar las uniones correctamente. Considere la segunda unión interna en el siguiente ejemplo.

```
SELECT *
       FROM "order"
 INNER JOIN order_item
       ON (order.id = order_item.order_id)
 INNER JOIN customer
       ON (customer.id = customer.id)
 INNER JOIN customer_address
       ON (customer_address.customer_id = customer.id AND
           order.customer_address_id = customer_address.id)
 WHERE customer.id = 1234567890;
```

La consulta anterior une por error `customer.id` con `customer.id`, lo que genera un producto cartesiano entre cada cliente y cada pedido. Este tipo de unión accidental genera grandes archivos temporales. Según el tamaño de las tablas, una consulta cartesiana puede incluso llenar el almacenamiento. Es posible que la aplicación tenga uniones cartesianas cuando se den las siguientes condiciones:

- Se observan grandes y bruscas disminuciones en la disponibilidad del almacenamiento, seguidas de una rápida recuperación.
- No se crean índices.
- No se emiten instrucciones `CREATE TABLE FROM SELECT`.
- No se actualizan las vistas materializadas.

Para ver si las tablas se unen con las claves adecuadas, inspeccione las directivas de consulta y de asignación objeto-relacional. Tenga en cuenta que algunas consultas de la aplicación no se llaman todo el tiempo, y algunas consultas se generan de forma dinámica.

Examinar las consultas ORDER BY y GROUP BY

En algunos casos, una cláusula `ORDER BY` puede dar lugar a un exceso de archivos temporales. Tenga en cuenta estas directrices:

- Incluya las columnas en una cláusula `ORDER BY` solo cuando sea necesario ordenarlas. Esta directriz es especialmente importante para las consultas que devuelven miles de filas y especifican muchas columnas en la cláusula `ORDER BY`.
- Considere la posibilidad de crear índices para acelerar las cláusulas `ORDER BY` cuando coincidan con columnas que tengan el mismo orden ascendente o descendente. Los índices parciales son preferibles porque son más pequeños. Los índices más pequeños se leen y recorren más rápidamente.
- Si crea índices para columnas que pueden aceptar valores nulos, considere si quiere que los valores nulos se almacenen al final o al principio de los índices.

  Si es posible, reduzca el número de filas que hay que ordenar, mediante el filtrado del conjunto de resultados. Si utiliza instrucciones de la cláusula `WITH` o subconsultas, recuerde que una consulta interna genera un conjunto de resultados y lo pasa a la consulta externa. Cuantas más filas pueda filtrar una consulta, menos tendrá que ordenar esta última.
- Si no necesita obtener el conjunto de resultados completo, utilice la cláusula `LIMIT`. Por ejemplo, si solo quiere las cinco primeras filas, una consulta que utilice la cláusula `LIMIT` no sigue generando resultados. De este modo, la consulta requiere menos memoria y archivos temporales.

Una consulta que utiliza una cláusula `GROUP BY` también puede requerir archivos temporales. Las consultas `GROUP BY` resumen los valores con funciones como las siguientes:

- `COUNT`
- `AVG`
- `MIN`
- `MAX`
- `SUM`
- `STDDEV`

Para ajustar las consultas `GROUP BY`, siga las recomendaciones para las consultas `ORDER BY`.

Evite utilizar la operación DISTINCT

Si es posible, evite utilizar la operación `DISTINCT` para eliminar las filas duplicadas. Cuantas más filas innecesarias y duplicadas devuelva la consulta, más cara será la operación `DISTINCT`. Si es posible, agregue filtros en la cláusula `WHERE`, incluso si utiliza los mismos filtros para diferentes tablas. Filtrar la consulta y unirla correctamente mejora su rendimiento y reduce el uso de recursos. Además, evita que los informes y resultados sean incorrectos.

Si necesita utilizar `DISTINCT` para varias filas de una misma tabla, considere la posibilidad de crear un índice compuesto. Agrupar varias columnas en un índice puede mejorar el tiempo de evaluación de las filas distintas. Además, si utiliza RDS para PostgreSQL versión 10 o posterior, puede correlacionar estadísticas entre varias columnas con el comando `CREATE STATISTICS`.

Considere la posibilidad de utilizar funciones de ventana en lugar de funciones GROUP BY

Al utilizar `GROUP BY`, se modifica el conjunto de resultados y luego se recupera el resultado agregado. Con las funciones de ventana, se agregan los datos sin cambiar el conjunto de resultados. Una función de ventana utiliza la cláusula `OVER` para efectuar cálculos a través de los conjuntos definidos por la consulta, correlacionando una fila con otra. Puede utilizar todas las funciones `GROUP BY` en las funciones de ventana, pero también puede utilizar funciones como las siguientes:

- `RANK`
- `ARRAY_AGG`
- `ROW_NUMBER`
- `LAG`
- `LEAD`

Para minimizar el número de archivos temporales generados por una función de ventana, elimine las duplicaciones para el mismo conjunto de resultados cuando necesite dos agregaciones distintas. Analice la siguiente consulta.

```
SELECT sum(salary) OVER (PARTITION BY dept ORDER BY salary DESC) as sum_salary
     , avg(salary) OVER (PARTITION BY dept ORDER BY salary ASC) as avg_salary
  FROM empsalary;
```

Puede volver a escribir la consulta con la cláusula `WINDOW` de la siguiente manera.

```
SELECT sum(salary) OVER w as sum_salary
```

```
        , avg(salary) OVER w as_avg_salary
    FROM empsalary
WINDOW w AS (PARTITION BY dept ORDER BY salary DESC);
```

De forma predeterminada, el planificador de ejecución de RDS para PostgreSQL consolida nodos similares para no duplicar operaciones. Sin embargo, al utilizar una declaración explícita para el bloque de la ventana, puede actualizar la consulta más fácilmente. También puede mejorar el rendimiento al evitar la duplicación.

Investigar las vistas materializadas y las instrucciones CTA

Cuando una vista materializada se actualiza, ejecuta una consulta. Esta consulta puede contener una operación como `GROUP BY`, `ORDER BY` o `DISTINCT`. Durante una actualización, es posible que observe un gran número de archivos temporales y los eventos de espera `IO:BufFileWrite` e `IO:BufFileRead`. Del mismo modo, cuando se crea una tabla basada en una instrucción `SELECT`, la instrucción `CREATE TABLE` ejecuta una consulta. Para reducir los archivos temporales necesarios, optimice la consulta.

Utilizar pg_repack al reconstruir índices

Cuando se crea un índice, el motor ordena el conjunto de resultados. A medida que las tablas aumentan de tamaño y los valores de la columna indexada se diversifican, los archivos temporales requieren más espacio. En la mayoría de los casos, no se puede evitar la creación de archivos temporales para tablas grandes sin modificar el área de memoria de trabajo de mantenimiento. Para obtener más información acerca de `maintenance_work_mem`, consulte https://www.postgresql.org/docs/current/runtime-config-resource.html en la documentación de PostgreSQL.

Una posible solución para recrear un índice grande es utilizar la extensión pg_repack. Para más información, consulte Reorganize tables in PostgreSQL databases with minimal locks en la documentación de pg_repack. Para obtener información sobre la configuración de la extensión en su instancia de base de datos de RDS para PostgreSQL, consulte Reducción de la sobrecarga en tablas e índices con la extensión pg_repack.

Aumentar maintenance_work_mem al hacer un clúster de tablas

El comando `CLUSTER` hace un clúster de la tabla especificada por table_name basado en un índice existente especificado por index_name. RDS para PostgreSQL recrea físicamente la tabla para que coincida con el orden de un índice determinado.

Cuando el almacenamiento magnético era frecuente, los clústeres eran comunes porque el rendimiento del almacenamiento era limitado. Ahora que el almacenamiento basado en SSD es

común, los clústeres son menos populares. Sin embargo, si se hacen clústeres en las tablas, se puede aumentar ligeramente el rendimiento en función del tamaño de la tabla, índice, consulta, etc.

Si ejecuta el comando `CLUSTER` y observa los eventos de espera `IO:BufFileWrite` e `IO:BufFileRead`, ajuste `maintenance_work_mem`. Aumente el tamaño de la memoria a una cantidad bastante grande. Un valor alto significa que el motor puede utilizar más memoria para la operación de clusterización.

Ajustar la memoria para evitar IO:BufFileRead e IO:BufFileWrite

En algunas situaciones, es necesario ajustar la memoria. Su objetivo es equilibrar la memoria en las siguientes áreas de consumo mediante los parámetros adecuados, de la siguiente manera.

- El valor `work_mem`
- La memoria restante después de descontar el valor `shared_buffers`
- El máximo de conexiones abiertas y en uso, que está limitado por `max_connections`

Para obtener más información sobre el ajuste de la memoria, consulte el punto Resource Consumption (Consumo de recursos) en la documentación de PostgreSQL.

Aumentar el tamaño del área de memoria de trabajo

En algunas situaciones, la única opción es aumentar la memoria que utiliza la sesión. Si las consultas están correctamente escritas y se utilizan las claves correctas para las uniones, considere aumentar el valor `work_mem`.

Para saber cuántos archivos temporales genera una consulta, establezca `log_temp_files` en `0`. Si aumenta el valor de `work_mem` hasta el valor máximo identificado en los registros, evitará que la consulta genere archivos temporales. Sin embargo, `work_mem` establece el máximo por nodo del plan para cada conexión o proceso de trabajo paralelo. Si la base de datos tiene 5000 conexiones, y si cada una utiliza 256 MiB de memoria, el motor necesita 1.2 TiB de RAM. Esto significa que la instancia podría quedarse sin memoria.

Reservar suficiente memoria para el grupo de búferes compartidos

La base de datos utiliza áreas de memoria como el grupo de búferes compartidos, no solo el área de memoria de trabajo. Tenga en cuenta los requisitos de estas áreas de memoria adicionales antes de aumentar `work_mem`.

Por ejemplo, supongamos que su clase de instancia de RDS para PostgreSQL es db.r5.2xlarge. Esta clase tiene 64 GiB de memoria. De forma predeterminada, el 25 por ciento de la memoria se reserva para el grupo de búferes compartidos. Después de restar la cantidad asignada al área de memoria compartida, quedan 16 384 MB. No asigne la memoria restante exclusivamente al área de memoria de trabajo porque el sistema operativo y el motor también necesitan memoria.

La memoria que puedes asignar a `work_mem` depende de la clase de instancia. Si utiliza una clase de instancia más grande, habrá más memoria disponible. Sin embargo, en el ejemplo anterior, no puedes usar más de 16 GiB. De lo contrario, la instancia dejará de estar disponible cuando se agote la memoria. Para recuperar la instancia del estado no disponible, los servicios de automatización de RDS para PostgreSQL se reinician automáticamente.

Administrar el número de conexiones

Supongamos que la instancia de su base de datos tiene 5 000 conexiones simultáneas. Cada conexión utiliza al menos 4 MiB de `work_mem`. El alto consumo de memoria de las conexiones puede degradar el rendimiento. Para ello, tiene las siguientes opciones:

- Actualizar a una clase de instancia mayor.
- Disminuir el número de conexiones simultáneas a la base de datos mediante el uso de un proxy de conexión o un grupo de conexiones.

En el caso de los proxies, considere Amazon RDS Proxy, pgBouncer o un grupo de conexiones acorde con su aplicación. Esta solución alivia la carga de la CPU. También reduce el riesgo cuando todas las conexiones requieren el área de memoria de trabajo. Cuando hay menos conexiones a la base de datos, puede aumentar el valor de `work_mem`. De esta manera, se reduce la ocurrencia de los eventos de espera `IO:BufFileRead` y `IO:BufFileWrite`. Además, las consultas que esperan el área de memoria de trabajo se aceleran de forma significativa.

IO:DataFileRead

El evento `IO:DataFileRead` ocurre cuando una conexión espera en un proceso backend para leer una página requerida del almacenamiento porque la página no está disponible en la memoria compartida.

Temas

- Versiones del motor admitidas
- Context

- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

Todas las consultas y operaciones de manipulación de datos (DML) acceden a páginas en el grupo de búferes. Las instrucciones que pueden inducir lecturas incluyen `SELECT`, `UPDATE` y `DELETE`. Por ejemplo, un `UPDATE` puede leer páginas de tablas o índices. Si la página que se solicita o actualiza no está en el grupo de búferes compartidos, esta lectura puede provocar el evento `IO:DataFileRead`.

Dado que el grupo de búferes compartidos es finito, puede llenarse. En este caso, las solicitudes de páginas que no están en la memoria obligan a la base de datos a leer bloques del disco. Si el evento `IO:DataFileRead` se produce con frecuencia, es posible que el grupo de búferes compartidos sea demasiado pequeño para acomodar la carga de trabajo. Este problema se agudiza en las consultas `SELECT` que leen un gran número de filas que no caben en el grupo de búferes. Para obtener más información acerca del grupo de búferes, consulte el punto Resource Consumption (Consumo de recursos) en la documentación de PostgreSQL.

Causas probables del aumento del tiempo de espera

Las causas más comunes del evento `IO:DataFileRead` son las siguientes:

Picos de conexión

Es posible que varias conexiones generen el mismo número de eventos de espera IO:DataFileRead. En este caso, puede producirse un pico (aumento repentino y grande) en los eventos `IO:DataFileRead`.

Instrucciones SELECT y DML que hacen escaneos secuenciales

Es posible que la aplicación realice una nueva operación. O una operación existente podría cambiar debido a un nuevo plan de ejecución. En estos casos, busque las tablas (particularmente las tablas grandes) que tengan un valor de `seq_scan` mayor. Encuéntrelas mediante la consulta

de `pg_stat_user_tables`. Para rastrear las consultas que generan más operaciones de lectura, utilice la extensión `pg_stat_statements`.

CTAS y CREATE INDEX para grandes conjuntos de datos

Un CTAS es una instrucción `CREATE TABLE AS SELECT`. Si ejecuta un CTAS con un conjunto de datos grande como origen, o crea un índice en una tabla grande, puede producirse el evento `IO:DataFileRead`. Cuando se crea un índice, es posible que la base de datos tenga que leer todo el objeto mediante una exploración secuencial. Un CTAS genera lecturas `IO:DataFile` cuando las páginas no están en la memoria.

Varios procesos de trabajo de vacío que se ejecutan al mismo tiempo

Los procesos de trabajo de vacío pueden activarse de forma manual o automática. Se recomienda adoptar una estrategia de vacío agresiva. Sin embargo, cuando una tabla tiene muchas filas actualizadas o eliminadas, las esperas `IO:DataFileRead` aumentan. Una vez recuperado el espacio, el tiempo de vacío dedicado a `IO:DataFileRead` disminuye.

Ingesta de grandes cantidades de datos

Cuando la aplicación ingiere grandes cantidades de datos, las operaciones `ANALYZE` pueden producirse con mayor frecuencia. El proceso `ANALYZE` se puede activar mediante un desencadenador de autovacuum o invocarse de forma manual.

La operación `ANALYZE` lee un subconjunto de la tabla. El número de páginas que deben ser escaneadas se calcula al multiplicar 30 por el valor de `default_statistics_target`. Para obtener más información, consulte la documentación de PostgreSQL. El parámetro `default_statistics_target` acepta valores entre 1 y 10 000, siendo el valor por defecto 100.

Falta de recursos

Si el ancho de banda de la red de la instancia o la CPU se consumen, el evento `IO:DataFileRead` podría ocurrir con más frecuencia.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Verificar los filtros de predicado para las consultas que generan esperas
- Minimizar el efecto de las operaciones de mantenimiento

- Responder a un gran número de conexiones

Verificar los filtros de predicado para las consultas que generan esperas

Supongamos que identifica consultas específicas que generan eventos de espera `IO:DataFileRead`. Puede identificarlos con las siguientes técnicas:

- Información sobre rendimiento
- Vistas de catálogo como la que proporciona la extensión `pg_stat_statements`
- La vista de catálogo `pg_stat_all_tables`, si muestra de forma periódica un aumento del número de lecturas físicas
- La vista `pg_statio_all_tables`, si muestra que los contadores `_read` aumentan

Le recomendamos que determine qué filtros se utilizan en el predicado (cláusula `WHERE`) de estas consultas. Siga estas instrucciones:

- Ejecute el comando `EXPLAIN`. En la salida, identifique qué tipos de escaneos se utilizan. Un escaneo secuencial no indica necesariamente un problema. Las consultas que utilizan escaneos secuenciales producen naturalmente más eventos `IO:DataFileRead` en comparación con las consultas que utilizan filtros.

  Averigüe si la columna que aparece en la cláusula `WHERE` se encuentra en un índice. Si no es así, considere la posibilidad de crear un índice para esta columna. Este enfoque evita los escaneos secuenciales y reduce los eventos `IO:DataFileRead`. Si una consulta tiene filtros restrictivos y produce aún escaneos secuenciales, evalúe si se utilizan los índices adecuados.
- Verifique si la consulta tiene acceso a una tabla muy grande. En algunos casos, la partición de una tabla puede mejorar el rendimiento, ya que permite que la consulta solo lea las particiones necesarias.
- Examine la cardinalidad (número total de filas) de sus operaciones de unión. Tenga en cuenta lo restrictivos que son los valores que se pasan en los filtros de la cláusula `WHERE`. Si es posible, ajuste su consulta para reducir el número de filas que se pasan en cada paso del plan.

Minimizar el efecto de las operaciones de mantenimiento

Las operaciones de mantenimiento como `VACUUM` y `ANALYZE` son importantes. Le recomendamos que no las desactive ya que encontrará eventos de espera `IO:DataFileRead` relacionados con

estas operaciones de mantenimiento. Los siguientes enfoques pueden minimizar el efecto de estas operaciones:

- Ejecute las operaciones de mantenimiento de forma manual durante las horas de menor actividad. Esta técnica evita que la base de datos alcance el umbral de las operaciones automáticas.
- Para tablas muy grandes, considere la posibilidad de particionar la tabla. Esta técnica reduce la sobrecarga de las operaciones de mantenimiento. La base de datos solo accede a las particiones que requieren mantenimiento.
- Cuando capture grandes cantidades de datos, considere la posibilidad de desactivar la característica de autoanálisis.

La característica de autovacuum se activa de forma automática para una tabla cuando la siguiente fórmula es verdadera.

```
pg_stat_user_tables.n_dead_tup > (pg_class.reltuples x autovacuum_vacuum_scale_factor)
 + autovacuum_vacuum_threshold
```

La vista `pg_stat_user_tables` y el catálogo `pg_class` tienen varias filas. Una fila puede corresponder a una fila de la tabla. Esta fórmula asume que las `reltuples` son para una tabla específica. Los parámetros `autovacuum_vacuum_scale_factor` (0,20 de forma predeterminada) y `autovacuum_vacuum_threshold` (50 tuplas de forma predeterminada) se suelen establecer de forma global para toda la instancia. Sin embargo, puede establecer valores diferentes para una tabla específica.

Temas

- Buscar tablas que consuman espacio de forma innecesaria
- Buscar índices que consuman espacio de forma innecesaria
- Buscar tablas aptas para autovacuum

Buscar tablas que consuman espacio de forma innecesaria

Para encontrar tablas que consuman espacio innecesariamente, puede utilizar funciones de la extensión `pgstattuple` de PostgreSQL. Esta extensión (módulo) está disponible de forma predeterminada en todas las instancias de base de datos de RDS para PostgreSQL y se puede instanciar en la instancia con el siguiente comando.

```
CREATE EXTENSION pgstattuple;
```

Para obtener más información sobre esta extensión, consulte pgstattuple en la documentación de PostgreSQL.

Puede comprobar si hay una sobrecarga de tablas e índices en su aplicación. Para obtener más información, consulte Diagnóstico de sobrecarga de tablas e índices.

Buscar índices que consuman espacio de forma innecesaria

Para encontrar índices sobrecargados y estimar la cantidad de espacio consumida innecesariamente en las tablas para las que tiene privilegios de lectura, puede ejecutar la siguiente consulta.

```
-- WARNING: rows with is_na = 't' are known to have bad statistics ("name" type is not
 supported).
-- This query is compatible with PostgreSQL 8.2 and later.

SELECT current_database(), nspname AS schemaname, tblname, idxname,
 bs*(relpages)::bigint AS real_size,
  bs*(relpages-est_pages)::bigint AS extra_size,
  100 * (relpages-est_pages)::float / relpages AS extra_ratio,
  fillfactor, bs*(relpages-est_pages_ff) AS bloat_size,
  100 * (relpages-est_pages_ff)::float / relpages AS bloat_ratio,
  is_na
  -- , 100-(sub.pst).avg_leaf_density, est_pages, index_tuple_hdr_bm,
  -- maxalign, pagehdr, nulldatawidth, nulldatahdrwidth, sub.reltuples, sub.relpages
  -- (DEBUG INFO)
FROM (
  SELECT coalesce(1 +
       ceil(reltuples/floor((bs-pageopqdata-pagehdr)/(4+nulldatahdrwidth)::float)), 0
       -- ItemIdData size + computed avg size of a tuple (nulldatahdrwidth)
    ) AS est_pages,
    coalesce(1 +
       ceil(reltuples/floor((bs-pageopqdata-pagehdr)*fillfactor/
(100*(4+nulldatahdrwidth)::float))), 0
    ) AS est_pages_ff,
    bs, nspname, table_oid, tblname, idxname, relpages, fillfactor, is_na
    -- , stattuple.pgstatindex(quote_ident(nspname)||'.'||quote_ident(idxname)) AS
 pst,
    -- index_tuple_hdr_bm, maxalign, pagehdr, nulldatawidth, nulldatahdrwidth,
 reltuples
    -- (DEBUG INFO)
  FROM (
```

```
   SELECT maxalign, bs, nspname, tblname, idxname, reltuples, relpages, relam,
table_oid, fillfactor,
     ( index_tuple_hdr_bm +
         maxalign - CASE -- Add padding to the index tuple header to align on MAXALIGN
           WHEN index_tuple_hdr_bm%maxalign = 0 THEN maxalign
           ELSE index_tuple_hdr_bm%maxalign
         END
       + nulldatawidth + maxalign - CASE -- Add padding to the data to align on
MAXALIGN
           WHEN nulldatawidth = 0 THEN 0
           WHEN nulldatawidth::integer%maxalign = 0 THEN maxalign
           ELSE nulldatawidth::integer%maxalign
         END
     )::numeric AS nulldatahdrwidth, pagehdr, pageopqdata, is_na
     -- , index_tuple_hdr_bm, nulldatawidth -- (DEBUG INFO)
   FROM (
     SELECT
       i.nspname, i.tblname, i.idxname, i.reltuples, i.relpages, i.relam, a.attrelid
AS table_oid,
       current_setting('block_size')::numeric AS bs, fillfactor,
       CASE -- MAXALIGN: 4 on 32bits, 8 on 64bits (and mingw32 ?)
         WHEN version() ~ 'mingw32' OR version() ~ '64-bit|x86_64|ppc64|ia64|amd64'
THEN 8
         ELSE 4
       END AS maxalign,
       /* per page header, fixed size: 20 for 7.X, 24 for others */
       24 AS pagehdr,
       /* per page btree opaque data */
       16 AS pageopqdata,
       /* per tuple header: add IndexAttributeBitMapData if some cols are null-able */
       CASE WHEN max(coalesce(s.null_frac,0)) = 0
         THEN 2 -- IndexTupleData size
         ELSE 2 + (( 32 + 8 - 1 ) / 8)
         -- IndexTupleData size + IndexAttributeBitMapData size ( max num filed per
index + 8 - 1 /8)
       END AS index_tuple_hdr_bm,
       /* data len: we remove null values save space using it fractionnal part from
stats */
       sum( (1-coalesce(s.null_frac, 0)) * coalesce(s.avg_width, 1024)) AS
nulldatawidth,
       max( CASE WHEN a.atttypid = 'pg_catalog.name'::regtype THEN 1 ELSE 0 END ) > 0
AS is_na
     FROM pg_attribute AS a
       JOIN (
```

```
          SELECT nspname, tbl.relname AS tblname, idx.relname AS idxname,
            idx.reltuples, idx.relpages, idx.relam,
            indrelid, indexrelid, indkey::smallint[] AS attnum,
            coalesce(substring(
              array_to_string(idx.reloptions, ' ')
               from 'fillfactor=([0-9]+)')::smallint, 90) AS fillfactor
          FROM pg_index
            JOIN pg_class idx ON idx.oid=pg_index.indexrelid
            JOIN pg_class tbl ON tbl.oid=pg_index.indrelid
            JOIN pg_namespace ON pg_namespace.oid = idx.relnamespace
          WHERE pg_index.indisvalid AND tbl.relkind = 'r' AND idx.relpages > 0
        ) AS i ON a.attrelid = i.indexrelid
        JOIN pg_stats AS s ON s.schemaname = i.nspname
          AND ((s.tablename = i.tblname AND s.attname =
 pg_catalog.pg_get_indexdef(a.attrelid, a.attnum, TRUE))
          -- stats from tbl
          OR  (s.tablename = i.idxname AND s.attname = a.attname))
          -- stats from functional cols
        JOIN pg_type AS t ON a.atttypid = t.oid
      WHERE a.attnum > 0
      GROUP BY 1, 2, 3, 4, 5, 6, 7, 8, 9
    ) AS s1
  ) AS s2
    JOIN pg_am am ON s2.relam = am.oid WHERE am.amname = 'btree'
) AS sub
-- WHERE NOT is_na
ORDER BY 2,3,4;
```

Buscar tablas aptas para autovacuum

Para buscar tablas que se puedan vaciar automáticamente, ejecute la siguiente consulta.

```
--This query shows tables that need vacuuming and are eligible candidates.
--The following query lists all tables that are due to be processed by autovacuum.
-- During normal operation, this query should return very little.
WITH  vbt AS (SELECT setting AS autovacuum_vacuum_threshold
              FROM pg_settings WHERE name = 'autovacuum_vacuum_threshold')
    , vsf AS (SELECT setting AS autovacuum_vacuum_scale_factor
              FROM pg_settings WHERE name = 'autovacuum_vacuum_scale_factor')
    , fma AS (SELECT setting AS autovacuum_freeze_max_age
              FROM pg_settings WHERE name = 'autovacuum_freeze_max_age')
    , sto AS (SELECT opt_oid, split_part(setting, '=', 1) as param,
                split_part(setting, '=', 2) as value
              FROM (SELECT oid opt_oid, unnest(reloptions) setting FROM pg_class) opt)
```

```
SELECT
    '"'||ns.nspname||'"."'||c.relname||'"' as relation
    , pg_size_pretty(pg_table_size(c.oid)) as table_size
    , age(relfrozenxid) as xid_age
    , coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
 autovacuum_freeze_max_age
    , (coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
         coalesce(cvsf.value::float,autovacuum_vacuum_scale_factor::float) *
 c.reltuples)
         as autovacuum_vacuum_tuples
    , n_dead_tup as dead_tuples
FROM pg_class c
JOIN pg_namespace ns ON ns.oid = c.relnamespace
JOIN pg_stat_all_tables stat ON stat.relid = c.oid
JOIN vbt on (1=1)
JOIN vsf ON (1=1)
JOIN fma on (1=1)
LEFT JOIN sto cvbt ON cvbt.param = 'autovacuum_vacuum_threshold' AND c.oid =
 cvbt.opt_oid
LEFT JOIN sto cvsf ON cvsf.param = 'autovacuum_vacuum_scale_factor' AND c.oid =
 cvsf.opt_oid
LEFT JOIN sto cfma ON cfma.param = 'autovacuum_freeze_max_age' AND c.oid = cfma.opt_oid
WHERE c.relkind = 'r'
AND nspname <> 'pg_catalog'
AND (
    age(relfrozenxid) >= coalesce(cfma.value::float, autovacuum_freeze_max_age::float)
    or
    coalesce(cvbt.value::float, autovacuum_vacuum_threshold::float) +
      coalesce(cvsf.value::float,autovacuum_vacuum_scale_factor::float) * c.reltuples
 <= n_dead_tup
    -- or 1 = 1
)
ORDER BY age(relfrozenxid) DESC;
```

Responder a un gran número de conexiones

Cuando se monitorea Amazon CloudWatch, se puede encontrar que la métrica `DatabaseConnections` se dispara. Este aumento indica un mayor número de conexiones a su base de datos. Se recomienda el siguiente enfoque:

- Limite el número de conexiones que la aplicación puede abrir con cada instancia. Si la aplicación tiene una característica de grupo de conexiones integrada, establezca un número razonable de

conexiones. Base el número en lo que las vCPU de su instancia puedan paralelizar de forma efectiva.

Si su aplicación no utiliza una característica de grupo de conexiones, considere utilizar Amazon RDS Proxy o una alternativa. Este enfoque permite que su aplicación abra varias conexiones con el equilibrador de carga. El equilibrador puede entonces abrir un número restringido de conexiones con la base de datos. Como se ejecutan menos conexiones en paralelo, la instancia de base de datos hace menos cambios de contexto en el núcleo. Las consultas deberían progresar más rápido, lo que provocaría menos eventos de espera. Para obtener más información, consulte Amazon RDS Proxy .

- Siempre que sea posible, aproveche las réplicas de lectura para RDS para PostgreSQL. Cuando la aplicación ejecute una operación de solo lectura, envíe estas solicitudes a la(s) réplica(s) de lectura. Esta técnica reduce la presión de E/S en el nodo principal (de escritura).
- Considere la posibilidad de escalar verticalmente su instancia de base de datos. Una clase de instancia de mayor capacidad proporciona más memoria, lo que le da a RDS para PostgreSQL un grupo de búferes compartidos mayor para mantener las páginas. El tamaño más grande también le da a la instancia de base de datos más vCPU para manejar las conexiones. Más vCPU son especialmente útiles cuando las operaciones que generan eventos de espera `IO:DataFileRead` se escriben.

IO:WALWrite

Temas

- Versiones del motor admitidas
- Contexto
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL 10 y posteriores.

Contexto

La actividad de la base de datos que genera datos de registro de escritura anticipada llena primero los búferes de WAL y, a continuación, los escribe en el disco de forma asincrónica. El evento de espera `IO:WALWrite` se genera cuando la sesión de SQL espera a que los datos de WAL terminen de escribirse en el disco para poder lanzar la llamada COMMIT de la transacción.

Causas probables del aumento del tiempo de espera

Si este evento de espera se produce con frecuencia, debe revisar su carga de trabajo, el tipo de actualizaciones que realiza y su frecuencia. En particular, busque los siguientes tipos de actividad.

Actividad intensa de DML

El cambio de datos en las tablas de bases de datos no se produce de forma instantánea. Es posible que una inserción en una tabla deba esperar a que otro cliente inserte o actualice la misma tabla. Las instrucciones del lenguaje de manipulación de datos (DML) para cambiar los valores de los datos (INSERT, UPDATE, DELETE, COMMIT, ROLLBACK TRANSACTION) pueden generar disputas que hagan que el archivo de registro de escritura anticipada espere a que se vacíen los búferes. Esta situación se refleja en las siguientes métricas de Información de rendimiento de Amazon RDS, que indican una actividad de DML intensa.

- `tup_inserted`
- `tup_updated`
- `tup_deleted`
- `xact_rollback`
- `xact_commit`

Para obtener más información sobre estas métricas, consulte Contadores de Información sobre rendimiento para Amazon RDS para PostgreSQL.

Actividad de puntos de comprobación frecuente

Los puntos de control frecuentes contribuyen a aumentar el número de archivos WAL. En RDS para PostgreSQL, la escritura de páginas completas siempre está «activada». La escritura de páginas completas ayuda a proteger contra la pérdida de datos. Sin embargo, cuando los puntos de comprobación se realizan con demasiada frecuencia, el sistema puede sufrir problemas de rendimiento general. Esto es especialmente cierto en sistemas con una actividad intensa de DML.

En algunos casos, es posible que encuentres mensajes de error en tel `postgresql.log` que indiquen que «los puntos de comprobación se producen con demasiada frecuencia».

Le recomendamos que, al ajustar los puntos de comprobación, equilibre cuidadosamente el rendimiento con el tiempo esperado de recuperación en caso de que se produzca un cierre anormal.

Acciones

Le recomendamos que realice las siguientes acciones para reducir los números de este evento de espera.

Temas

- Reducir el número de confirmaciones
- Monitorear los puntos de comprobación
- Escalar la E/S verticalmente
- Volumen de registro específico (DLV)

Reducir el número de confirmaciones

Para reducir el número de confirmaciones, combine las instrucciones en bloques de transacciones. Utilice Información de rendimiento de Amazon RDS para examinar el tipo de consultas que se está ejecutando. También puede trasladar las grandes operaciones de mantenimiento a las horas de menor actividad. Por ejemplo, cree índices o utilice operaciones `pg_repack` durante las horas que no sean de producción.

Monitorear los puntos de comprobación

Hay dos parámetros que puede monitorear para ver con qué frecuencia su instancia de base de datos de RDS para PostgreSQL escribe puntos de comprobación en el archivo WAL.

- `log_checkpoints`: este parámetro está activado de forma predeterminada. Hace que se envíe un mensaje al registro de PostgreSQL para cada punto de comprobación. Estos mensajes de registro incluyen la cantidad de búferes escritos, el tiempo dedicado a escribirlos y la cantidad de archivos WAL agregados, eliminados o reciclados para un punto de comprobación determinado.

  Para más información sobre este parámetro, consulte Error Reporting and Logging (Registro y notificación de errores) en la documentación de PostgreSQL.

- `checkpoint_warning`: este parámetro establece un valor umbral (en segundos) para la frecuencia del punto de comprobación por encima del cual se genera una advertencia. De forma predeterminada, este parámetro no está configurado en RDS para PostgreSQL. Puede establecer el valor de este parámetro de modo que reciba una advertencia cuando los cambios en la base de datos de su instancia de base de datos de RDS para PostgreSQL se escriban a una velocidad para la que los archivos WAL no tengan el tamaño adecuado. Por ejemplo, supongamos que establece este parámetro en 30. Si su instancia de RDS para PostgreSQL necesita escribir cambios con mayor frecuencia que cada 30 segundos, se envía la advertencia «los puntos de comprobación se producen con demasiada frecuencia» al registro de PostgreSQL. Esto puede indicar que su valor `max_wal_size` debe aumentarse.

  Para obtener más información, consulte Write Ahead Log (Registro de escritura anticipada) en la documentación de PostgreSQL.

Escalar la E/S verticalmente

Este tipo de evento de espera de entrada/salida (E/S) se puede solucionar escalando las operaciones de entrada/salida por segundo (IOPS) para proporcionar una E/S más rápida. Es preferible escalar la E/S a escalar la CPU, ya que escalar la CPU puede generar aún más contención de E/S, ya que el aumento de la CPU puede soportar más trabajo y, por lo tanto, agravar aún más el cuello de botella de E/S. En general, recomendamos que considere ajustar la carga de trabajo antes de realizar las operaciones de escalado.

Volumen de registro específico (DLV)

Puede utilizar un volumen de registro específico (DLV) para una instancia de base de datos que utilice el almacenamiento de IOPS aprovisionadas (PIOPS) mediante la consola de Amazon RDS, la AWS CLI o la API de Amazon RDS. Un DLV transporta los registros de transacciones de la base de datos PostgreSQL a un volumen de almacenamiento independiente del volumen que contiene las tablas de la base de datos. Para obtener más información, consulte Volumen de registro específico (DLV).

Eventos de espera IPC:parallel

Los siguientes `IPC:parallel wait events` indican que una sesión está esperando una comunicación entre procesos relacionada con operaciones de ejecución de consultas en paralelo.

- `IPC:BgWorkerStartup`: un proceso está esperando a que un proceso de trabajo paralelo complete la secuencia de inicio. Esto sucede al inicializar los procesos de trabajo para la ejecución de consultas en paralelo.
- `IPC:BgWorkerShutdown`: un proceso está esperando a que un proceso de trabajo paralelo complete la secuencia de apagado. Esto sucede durante la fase de limpieza de la ejecución de consultas en paralelo.
- `IPC:ExecuteGather`: un proceso está esperando recibir datos de procesos de trabajo paralelos durante la ejecución de consultas. Esto ocurre cuando el proceso líder necesita recopilar resultados de los procesos de trabajo.
- `IPC:ParallelFinish`: un proceso está esperando a que los procesos de trabajo paralelos finalicen la ejecución y comuniquen los resultados finales. Esto sucede durante la fase de finalización de la ejecución de consultas en paralelo.

Temas

- Versiones del motor admitidas
- Contexto
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de Aurora PostgreSQL.

Contexto

La ejecución de consultas en paralelo en PostgreSQL implica que varios procesos trabajan juntos para procesar una sola consulta. Cuando se determina que una consulta es adecuada para la paralelización, un proceso líder coordina uno o varios procesos de trabajo paralelos en función de la configuración del parámetro `max_parallel_workers_per_gather`. El proceso líder divide el trabajo entre los procesos de trabajo, cada proceso de trabajo procesa la parte de los datos de forma independiente y los resultados se recopilan de nuevo en el proceso líder.

> **Note**
>
> Cada proceso de trabajo paralelo funciona como un proceso independiente con requisitos de recursos similares a los de una sesión de usuario completa. Esto significa que una consulta en paralelo con cuatro procesos de trabajo puede consumir hasta cinco veces más recursos (CPU, memoria y ancho de banda de E/S) que una consulta que no sea en paralelo, ya que tanto el proceso líder como cada proceso de trabajo mantienen las asignaciones de recursos propias. Por ejemplo, la configuración como `work_mem` se aplica individualmente a cada proceso de trabajo, lo que puede multiplicar el uso total de memoria en todos los procesos.

La arquitectura de consulta en paralelo consta de tres componentes principales:

- Proceso líder: el proceso principal que inicia la operación paralela, divide la carga de trabajo y coordina los procesos de trabajo.
- Procesos de trabajo: procesos en segundo plano que ejecutan partes de la consulta en paralelo.
- Recopilación/combinación de recopilaciones: operaciones que combinan los resultados de varios procesos de trabajo y los devuelven al líder

Durante la ejecución en paralelo, los procesos deben comunicarse entre sí a través de mecanismos de comunicación entre procesos (IPC). Estos eventos de espera IPC se producen durante diferentes fases:

- Inicio de procesos de trabajo: cuando se inicializan los procesos de trabajo paralelos
- Intercambio de datos: cuando los procesos de trabajo procesan datos y envían los resultados al líder
- Cierre de procesos de trabajo: cuando finaliza la ejecución paralela y se terminan los procesos de trabajo
- Puntos de sincronización: cuando los procesos necesitan coordinarse o esperar a que otros procesos completen las tareas

Comprender estos eventos de espera es fundamental para diagnosticar problemas de rendimiento relacionados con la ejecución de consultas en paralelo, sobre todo en entornos de alta simultaneidad en los que pueden ejecutarse varias consultas en paralelo al mismo tiempo.

Causas probables del aumento del tiempo de espera

Hay varios factores que pueden contribuir a un aumento de los eventos de espera IPC relacionados con la ejecución en paralelo:

Alta simultaneidad de consultas en paralelo

Cuando se ejecutan muchas consultas en paralelo al mismo tiempo, puede producirse un conflicto de recursos y un aumento de los tiempos de espera para las operaciones IPC. Esto es muy habitual en sistemas con grandes volúmenes de transacciones o cargas de trabajo de análisis.

Planes de consultas en paralelo poco óptimos

Si el planificador de consultas elige planes paralelos ineficientes, puede dar lugar a una paralelización innecesaria o a una distribución deficiente del trabajo entre los procesos de trabajo. Esto puede provocar un aumento de las esperas de IPC, sobre todo para los eventos `IPC:ExecuteGather` e `IPC:ParallelFinish`. Estos problemas de planificación suelen deberse a estadísticas obsoletas y a la saturación de tablas e índices.

Inicio y apagado frecuentes de procesos de trabajo paralelos

Las consultas de corta duración que inician y terminan con frecuencia procesos de trabajo paralelos pueden provocar un aumento de los eventos `IPC:BgWorkerStartup` y `IPC:BgWorkerShutdown`. Esto se observa a menudo en cargas de trabajo OLTP con muchas consultas pequeñas y paralelizables.

Limitaciones de recursos

La capacidad limitada de CPU, memoria o E/S puede provocar cuellos de botella en la ejecución paralela, lo que aumenta los tiempos de espera en todos los eventos IPC. Por ejemplo, si la CPU está saturada, los procesos de trabajo pueden tardar más en iniciarse o en procesar la parte del trabajo.

Estructuras de consultas complejas

Las consultas con varios niveles de paralelismo (por ejemplo, uniones paralelas seguidas de agregaciones paralelas) pueden dar lugar a patrones IPC más complejos y a un aumento de los tiempos de espera, sobre todo para eventos `IPC:ExecuteGather`.

Grandes conjuntos de resultados

Las consultas que producen conjuntos de resultados grandes pueden provocar un aumento de los tiempos de espera de `IPC:ExecuteGather`, ya que el proceso líder dedica más tiempo a recopilar y procesar los resultados de los procesos de trabajo.

Comprender estos factores puede ayudar a diagnosticar y resolver problemas de rendimiento relacionados con la ejecución de consultas paralelas en Aurora PostgreSQL.

Acciones

Cuando ve esperas relacionadas con consultas en paralelo, normalmente significa que un proceso backend está coordinando o esperando procesos de trabajo paralelos. Estas esperas son comunes durante la ejecución de planes paralelos. Puede investigar y mitigar el impacto de estas esperas mediante la supervisión del uso de procesos de trabajo paralelos, la revisión de la configuración de los parámetros y el ajuste de la ejecución de las consultas y asignación de recursos.

Temas

- Análisis de los planes de consulta en busca de paralelismo ineficiente
- Supervisión del uso de consultas en paralelo
- Revisión y ajuste de la configuración de consultas en paralelo
- Optimización de la asignación de recursos
- Investigación de la administración de conexiones
- Revisión y optimización de las operaciones de mantenimiento

Análisis de los planes de consulta en busca de paralelismo ineficiente

La ejecución de consultas en paralelo a menudo puede provocar inestabilidad del sistema, picos de CPU y variaciones impredecibles en el rendimiento de las consultas. Es fundamental analizar a fondo si el paralelismo mejora realmente la carga de trabajo específica. Utilice EXPLAIN ANALYZE para revisar los planes de ejecución de consultas en paralelo.

Deshabilite temporalmente el paralelismo de la sesión para comparar la eficiencia del plan:

```
SET max_parallel_workers_per_gather = 0;
EXPLAIN ANALYZE <your_query>;
```

Vuelva a habilitar el paralelismo y compare:

```
RESET max_parallel_workers_per_gather;
EXPLAIN ANALYZE <your_query>;
```

Si al deshabilitar el paralelismo se obtienen resultados mejores o más coherentes, considere la posibilidad de deshabilitarlo para consultas específicas de sesión mediante comandos SET. Para lograr un impacto más amplio, es posible que desee deshabilitar el paralelismo de instancia mediante el ajuste de los parámetros pertinentes en el grupo de parámetros de base de datos. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Supervisión del uso de consultas en paralelo

Utilice las siguientes consultas para obtener visibilidad de la actividad y la capacidad de las consultas en paralelo:

Compruebe los procesos de trabajo paralelos activos:

```
SELECT
    COUNT(*)
FROM
    pg_stat_activity
WHERE
    backend_type = 'parallel worker';
```

Esta consulta muestra el número de procesos de trabajo paralelos activos. Un valor alto puede indicar que “max_parallel_workers” se ha configurado con un valor alto y es recomendable que considere la posibilidad de reducirlo.

Compruebe las consultas en paralelo simultáneas:

```
SELECT
    COUNT(DISTINCT leader_pid)
```

```
FROM
    pg_stat_activity
WHERE
    leader_pid IS NOT NULL;
```

Esta consulta devuelve el número de procesos líderes distintos que han iniciado consultas en paralelo. Un número alto indica que varias sesiones están ejecutando consultas en paralelo simultáneamente, lo que puede aumentar la demanda de CPU y memoria.

Revisión y ajuste de la configuración de consultas en paralelo

Revise los siguientes parámetros para asegurarse de que se ajustan a la carga de trabajo:

- `max_parallel_workers`: número total de procesos de trabajo paralelos en todas las sesiones.
- `max_parallel_workers_per_gather`: número máximo de procesos de trabajo por consulta.

Para cargas de trabajo OLAP, aumentar estos valores puede mejorar el rendimiento. Para cargas de trabajo OLTP, por lo general, se prefieren valores más bajos.

```
SHOW max_parallel_workers;
SHOW max_parallel_workers_per_gather;
```

Optimización de la asignación de recursos

Supervise la utilización de la CPU y considere la posibilidad de ajustar el número de vCPU si es coherentemente alto y si la aplicación se beneficia de las consultas en paralelo. Asegúrese de que haya memoria suficiente para las operaciones paralelas.

- Utilice las métricas de Información de rendimiento para determinar si el sistema está limitado por la CPU.
- Cada proceso de trabajo paralelo utiliza un `work_mem` propio. Asegúrese de que el uso total de memoria se encuentra dentro de los límites de la instancia.

Las consultas en paralelo pueden consumir muchos más recursos que las consultas que no son en paralelo, ya que cada proceso de trabajo es un proceso completamente independiente que tiene aproximadamente el mismo impacto en el sistema que una sesión de usuario adicional. Esto

debe tenerse en cuenta al elegir un valor para esta configuración, así como al configurar otras opciones que controlan la utilización de recursos, como `work_mem`. Para obtener más información, consulte la documentación de PostgreSQL. Los límites de recursos, como `work_mem`, se aplican individualmente a cada proceso de trabajo, lo que significa que la utilización total puede ser mucho mayor en todos los procesos de lo que sería normalmente para un solo proceso.

Considere la posibilidad de aumentar las vCPU o ajustar los parámetros de memoria si la carga de trabajo está muy paralelizada.

Investigación de la administración de conexiones

Si se agota la conexión, revise las estrategias de agrupación de conexiones de la aplicación. Considere la posibilidad de implementar la agrupación de conexiones de aplicación si aún no se utiliza.

Revisión y optimización de las operaciones de mantenimiento

Coordine la creación de índices y otras tareas de mantenimiento para evitar la contienda por los recursos. Considere la posibilidad de programar estas operaciones durante las horas de menor actividad. Evite programar tareas de mantenimiento intensas (por ejemplo, creaciones de índices en paralelo) durante periodos de alta carga de consultas de los usuarios. Estas operaciones pueden consumir procesos de trabajo paralelos y afectar al rendimiento de las consultas habituales.

Lock:advisory

El evento `Lock:advisory` ocurre cuando una aplicación PostgreSQL utiliza un bloqueo para coordinar la actividad entre varias sesiones.

Temas

- Versiones del motor relevantes
- Context
- Causas
- Acciones

Versiones del motor relevantes

La información de eventos de espera es relevante para RDS para PostgreSQL versión 9.6 y posteriores.

Context

Los bloqueos consultivos de PostgreSQL son bloqueos cooperativos a nivel de aplicación, bloqueados y desbloqueados explícitamente por el código de la aplicación del usuario. Una aplicación puede usar los bloqueos consultivos de PostgreSQL para coordinar la actividad a través de varias sesiones. A diferencia de los bloqueos regulares a nivel de objeto o de fila, la aplicación tiene control total sobre el tiempo de vida del bloqueo. Para más información, consulte Advisory Locks en la documentación de PostgreSQL.

Los bloqueos consultivos se pueden liberar antes de que finalice una transacción o mantenerse en una sesión a través de las transacciones. Esto no es verdadero para los bloqueos implícitos, forzados por el sistema, como un bloqueo de acceso exclusivo a una tabla adquirido por una instrucción `CREATE INDEX`.

Para una descripción de las funciones que se utilizan para adquirir (bloquear) y liberar (desbloquear) los bloqueos de asesoramiento, consulte Advisory Lock Functions en la documentación de PostgreSQL.

Los bloqueos consultivos se implementan sobre el sistema de bloqueo regular de PostgreSQL y son visibles en la vista del sistema `pg_locks`.

Causas

Este tipo de bloqueo es controlado exclusivamente por una aplicación que lo utiliza de forma explícita. Los bloqueos consultivos que se adquieren para cada fila como parte de una consulta pueden causar un pico de bloqueos o una acumulación a largo plazo.

Estos efectos se producen cuando la consulta se ejecuta de forma que adquiere bloqueos en más filas de las que devuelve la consulta. La aplicación debe liberar finalmente todos los bloqueos, pero si se adquieren bloqueos en filas que no se devuelven, la aplicación no puede encontrar todos los bloqueos.

El siguiente ejemplo proviene de Advisory Locks en la documentación de PostgreSQL.

```
SELECT pg_advisory_lock(id) FROM foo WHERE id > 12345 LIMIT 100;
```

En este ejemplo, la cláusula `LIMIT` solo puede detener la salida de la consulta después de que las filas se hayan seleccionado internamente y sus valores de ID se hayan bloqueado. Esto puede ocurrir de forma repentina cuando un volumen de datos creciente hace que el planificador elija un

plan de ejecución diferente que no fue probado durante el desarrollo. La acumulación en este caso ocurre porque la aplicación llama explícitamente a `pg_advisory_unlock` para cada valor de ID que fue bloqueado. Sin embargo, en este caso no se puede encontrar el conjunto de bloqueos adquiridos en las filas que no fueron devueltas. Como los bloqueos se adquieren a nivel de sesión, no se liberan automáticamente al final de la transacción.

Otra posible causa de los picos de intentos de bloqueo son los conflictos involuntarios. En estos conflictos, partes no relacionadas de la aplicación comparten el mismo espacio de ID de bloqueo por error.

Acciones

Revisar el uso de la aplicación de los bloqueos consultivos y detallar dónde y cuándo en el flujo de la aplicación se adquiere y libera cada tipo de bloqueo consultivo.

Determine si una sesión adquiere demasiados bloqueos o si una sesión de larga duración no libera los bloqueos con suficiente antelación, lo que provoca una acumulación lenta de bloqueos. Puede corregir una acumulación lenta de bloqueos de sesión si finaliza la sesión con `pg_terminate_backend(pid)`.

Un cliente en espera de un bloqueo consultivo aparece en `pg_stat_activity` con `wait_event_type=Lock` y `wait_event=advisory`. Puede obtener valores de bloqueo específicos al consultar la vista del sistema `pg_locks` para el mismo `pid`, buscando `locktype=advisory` y `granted=f`.

A continuación, puede identificar la sesión de bloqueo al consultar `pg_locks` para el mismo bloqueo consultivo con `granted=t`, como se muestra en el siguiente ejemplo.

```
SELECT blocked_locks.pid AS blocked_pid,
         blocking_locks.pid AS blocking_pid,
         blocked_activity.usename AS blocked_user,
         blocking_activity.usename AS blocking_user,
         now() - blocked_activity.xact_start AS blocked_transaction_duration,
         now() - blocking_activity.xact_start AS blocking_transaction_duration,
         concat(blocked_activity.wait_event_type,':',blocked_activity.wait_event) AS
 blocked_wait_event,
         concat(blocking_activity.wait_event_type,':',blocking_activity.wait_event) AS
 blocking_wait_event,
         blocked_activity.state AS blocked_state,
         blocking_activity.state AS blocking_state,
```

```
         blocked_locks.locktype AS blocked_locktype,
         blocking_locks.locktype AS blocking_locktype,
         blocked_activity.query AS blocked_statement,
         blocking_activity.query AS blocking_statement
   FROM pg_catalog.pg_locks blocked_locks
   JOIN pg_catalog.pg_stat_activity blocked_activity ON blocked_activity.pid =
blocked_locks.pid
   JOIN pg_catalog.pg_locks blocking_locks
       ON blocking_locks.locktype = blocked_locks.locktype
       AND blocking_locks.DATABASE IS NOT DISTINCT FROM blocked_locks.DATABASE
       AND blocking_locks.relation IS NOT DISTINCT FROM blocked_locks.relation
       AND blocking_locks.page IS NOT DISTINCT FROM blocked_locks.page
       AND blocking_locks.tuple IS NOT DISTINCT FROM blocked_locks.tuple
       AND blocking_locks.virtualxid IS NOT DISTINCT FROM blocked_locks.virtualxid
       AND blocking_locks.transactionid IS NOT DISTINCT FROM
blocked_locks.transactionid
       AND blocking_locks.classid IS NOT DISTINCT FROM blocked_locks.classid
       AND blocking_locks.objid IS NOT DISTINCT FROM blocked_locks.objid
       AND blocking_locks.objsubid IS NOT DISTINCT FROM blocked_locks.objsubid
       AND blocking_locks.pid != blocked_locks.pid
   JOIN pg_catalog.pg_stat_activity blocking_activity ON blocking_activity.pid =
blocking_locks.pid
   WHERE NOT blocked_locks.GRANTED;
```

Todas las funciones de la API de bloqueo consultivo tienen dos conjuntos de argumentos, un argumento `bigint` o dos argumentos `integer`:

- Para las funciones API con un argumento `bigint`, los 32 bits superiores están en `pg_locks.classid` y los 32 bits inferiores están en `pg_locks.objid`.
- Para las funciones de la API con dos argumentos `integer`, el primer argumento es `pg_locks.classid` y el segundo argumento es `pg_locks.objid`.

El valor de `pg_locks.objsubid` indica qué forma de la API se utilizó: 1 significa un argumento `bigint`; 2 significa dos argumentos `integer`.

Lock:extend

El evento `Lock:extend` se produce cuando un proceso del backend espera bloquear una relación para extenderla mientras otro proceso tiene un bloqueo en esa relación con el mismo propósito.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

El evento `Lock:extend` indica que un proceso backend se encuentra a la espera de extender una relación sobre la que otro proceso backend tiene un bloqueo mientras está extendiendo esa relación. Debido a que solo un proceso a la vez puede extender una relación, el sistema genera un evento de espera `Lock:extend`. Las operaciones `INSERT`, `COPY` y `UPDATE` pueden generar este evento.

Causas probables del aumento de las esperas

Cuando el evento `Lock:extend` aparece más de lo normal, lo que posiblemente indica un problema de rendimiento, las causas típicas son las siguientes:

Aumento de las inserciones o actualizaciones concurrentes en la misma tabla

Puede haber un aumento en el número de sesiones concurrentes con consultas que insertan o actualizan la misma tabla.

Ancho de banda de red insuficiente

El ancho de banda de la red en la instancia de base de datos puede ser insuficiente para las necesidades de comunicación del almacenamiento de la carga de trabajo actual. Esto puede contribuir a la latencia del almacenamiento que provoca un aumento de los eventos `Lock:extend`.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Reducir las inserciones y actualizaciones concurrentes en la misma relación
- Aumentar el ancho de banda de la red

Reducir las inserciones y actualizaciones concurrentes en la misma relación

En primer lugar, determine si hay un aumento de las métricas `tup_inserted` y `tup_updated` y un aumento de este evento de espera. Si es así, verifique qué relaciones están en alta contención para las operaciones de inserción y actualización. Para determinar esto, consulte la vista `pg_stat_all_tables` para los valores de los campos `n_tup_ins` y `n_tup_upd`. Para obtener información sobre la vista `pg_stat_all_tables`, consulte pg_stat_all_tables en la documentación de PostgreSQL.

Para obtener más información acerca de las consultas bloqueadas y no bloqueadas, consulte `pg_stat_activity` como en el siguiente ejemplo:

```
SELECT
    blocked.pid,
    blocked.usename,
    blocked.query,
    blocking.pid AS blocking_id,
    blocking.query AS blocking_query,
    blocking.wait_event AS blocking_wait_event,
    blocking.wait_event_type AS blocking_wait_event_type
FROM pg_stat_activity AS blocked
JOIN pg_stat_activity AS blocking ON blocking.pid = ANY(pg_blocking_pids(blocked.pid))
where
blocked.wait_event = 'extend'
and blocked.wait_event_type = 'Lock';

   pid  | usename  |            query             | blocking_id |
            blocking_query                          | blocking_wait_event |
 blocking_wait_event_type
  ------+----------+------------------------------+-------------
+-------------------------------------------------------------------
+---------------------+--------------------------
   7143 |  myuser  | insert into tab1 values (1); |        4600 | INSERT INTO tab1 (a)
 SELECT s FROM generate_series(1,1000000) s; | DataFileExtend      | IO
```

Después de identificar las relaciones que contribuyen a aumentar los eventos `Lock:extend`, utilice las siguientes técnicas para reducir la contención:

- Compruebe si puede utilizar el particionamiento para reducir la contención para la misma tabla. Separar las tuplas insertadas o actualizadas en diferentes particiones puede reducir la contención. Para obtener información sobre las particiones, consulte Administración de las particiones de PostgreSQL con la extensión pg_partman.
- Si el evento de espera se debe principalmente a la actividad de actualización, considere reducir el valor de fillfactor de la relación. Esto puede reducir las solicitudes de nuevos bloques durante la actualización. El fillfactor es un parámetro de almacenamiento para una tabla que determina la cantidad máxima de espacio para empaquetar una página de la tabla. Se expresa como un porcentaje del espacio total de una página. Para más información sobre el parámetro fillfactor, consulte CREATE TABLE en la documentación de PostgreSQL.

  > **Important**
  >
  > Recomendamos ampliamente que pruebe su sistema si cambia el fillfactor porque cambiar este valor puede impactar negativamente en el rendimiento, de acuerdo a su carga de trabajo.

Aumentar el ancho de banda de la red

Para ver si hay un aumento en la latencia de escritura, verifique la métrica `WriteLatency` en CloudWatch. Si lo hay, utilice las métricas `WriteThroughput` y `ReadThroughput` de Amazon CloudWatch para monitorear el tráfico relacionado con el almacenamiento en la instancia de base de datos. Estas métricas pueden ayudarle a determinar si el ancho de banda de la red es suficiente para la actividad de almacenamiento de su carga de trabajo.

Si el ancho de banda de su red no es suficiente, auméntelo. Si la instancia de base de datos alcanza los límites del ancho de banda de la red, la única forma de aumentar el ancho de banda es aumentar el tamaño de la instancia de base de datos.

Para obtener más información acerca de las métricas de CloudWatch, consulte Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS. Para obtener información sobre el rendimiento de la red para cada clase de instancia de base de datos, consulte Métricas de nivel de instancia de Amazon CloudWatch para Amazon RDS.

Lock:Relation

El evento `Lock:Relation` ocurre cuando una consulta espera adquirir un bloqueo en una tabla o vista (relación) que se encuentra bloqueada por otra transacción.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

La mayoría de los comandos de PostgreSQL utilizan implícitamente bloqueos para controlar el acceso concurrente a los datos de las tablas. También puede utilizar estos bloqueos explícitamente en su código de aplicación con el comando `LOCK`. Muchos modos de bloqueo no son compatibles entre sí, y pueden bloquear las transacciones cuando intentan acceder al mismo objeto. Cuando esto sucede, RDS para PostgreSQL genera un evento `Lock:Relation`. Algunos ejemplos comunes son los siguientes:

- Los bloqueos exclusivos como `ACCESS EXCLUSIVE` pueden bloquear todos los accesos concurrentes. Las operaciones del lenguaje de definición de datos (DDL) como `DROP TABLE`, `TRUNCATE`, `VACUUM FULL` y `CLUSTER` adquieren bloqueos `ACCESS EXCLUSIVE` implícitamente. `ACCESS EXCLUSIVE` es también el modo de bloqueo por defecto para las instrucciones `LOCK TABLE` que no especifican un modo explícitamente.
- El uso de `CREATE INDEX (without CONCURRENT)` en una tabla entra en conflicto con las instrucciones de lenguaje de manipulación de datos (DML) `UPDATE`, `DELETE` e `INSERT`, que adquieren bloqueos `ROW EXCLUSIVE`.

Para más información sobre los bloqueos a nivel de tabla y los modos de bloqueo conflictivos, consulte Explicit Locking en la documentación de PostgreSQL.

Las consultas y transacciones que se bloquean normalmente se desbloquean de una de las siguientes maneras:

- Consulta de bloqueo: la aplicación puede cancelar la consulta o el usuario puede terminar el proceso. El motor también puede forzar la finalización de la consulta debido al tiempo de espera de una sesión o a un mecanismo de detección de bloqueos.
- Transacción bloqueada: una transacción deja de bloquearse cuando se ejecuta una instrucción `ROLLBACK` o `COMMIT`. Las restauraciones también ocurren de forma automática cuando las sesiones se desconectan por un cliente o por problemas de red, o se terminan. Las sesiones se pueden terminar cuando el motor de base de datos se apaga, cuando el sistema se queda sin memoria, etc.

Causas probables del aumento del tiempo de espera

Cuando el evento `Lock:Relation` se produce con más frecuencia de lo normal, puede indicar un problema de rendimiento. Las causas típicas son las siguientes:

Aumento de las sesiones concurrentes con bloqueos de tablas en conflicto

Puede haber un aumento en el número de sesiones concurrentes con consultas que bloquean la misma tabla con modos de bloqueo conflictivos.

Operaciones de mantenimiento

Las operaciones de mantenimiento de estado como `VACUUM` y `ANALYZE` pueden aumentar significativamente el número de bloqueos conflictivos. `VACUUM FULL` adquiere un bloqueo `ACCESS EXCLUSIVE`, y `ANALYSE` adquiere un bloqueo `SHARE UPDATE EXCLUSIVE`. Ambos tipos de bloqueos pueden causar un evento de espera `Lock:Relation`. Las operaciones de mantenimiento de datos de la aplicación, como la actualización de una vista materializada, también pueden aumentar las consultas y transacciones bloqueadas.

Bloqueos en instancias de lectura

Puede haber un conflicto entre los bloqueos de relaciones que mantienen el escritor y los lectores. En la actualidad, solo los bloqueos de relaciones de `ACCESS EXCLUSIVE` se replican en instancias de lector. Sin embargo, el bloqueo de relaciones `ACCESS EXCLUSIVE` entrará en conflicto con cualquier bloqueo de relaciones `ACCESS SHARE` que mantenga el lector. Esto puede provocar un aumento de los eventos de espera de las relaciones de bloqueo en el lector.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Reducir el impacto de las instrucciones SQL que se bloquean
- Minimizar el efecto de las operaciones de mantenimiento

Reducir el impacto de las instrucciones SQL que se bloquean

Para reducir el impacto de las instrucciones SQL que se bloquean, modifique el código de su aplicación cuando sea posible. A continuación se presentan dos técnicas comunes para reducir los bloqueos:

- Utilizar la opción `NOWAIT`: algunos comandos SQL, como las instrucciones `SELECT` y `LOCK`, admiten esta opción. La directiva `NOWAIT` cancela la consulta que solicita el bloqueo si éste no puede adquirirse inmediatamente. Esta técnica puede ayudar a evitar que una sesión bloqueada provoque una acumulación de sesiones bloqueadas detrás de ella.

  Por ejemplo: Supongamos que la transacción A espera un bloqueo que tiene la transacción B. Ahora, si B solicita un bloqueo en una tabla que está bloqueada por la transacción C, la transacción A podría quedar bloqueada hasta que la transacción C finalice. Pero si la transacción B utiliza un `NOWAIT` cuando solicita el bloqueo en C, puede fallar rápido y asegurar que la transacción A no tenga que esperar de forma indefinida.
- Utilice `SET lock_timeout`: establezca un valor de `lock_timeout` para limitar el tiempo que una sentencia SQL espera para adquirir un bloqueo en una relación. Si el bloqueo no se adquiere dentro del tiempo de espera especificado, la transacción que solicita el bloqueo se cancela. Establezca este valor en la sesión.

Minimizar el efecto de las operaciones de mantenimiento

Las operaciones de mantenimiento como `VACUUM` y `ANALYZE` son importantes. Le recomendamos que no las desactive ya que encontrará eventos de espera `Lock:Relation` relacionados con estas operaciones de mantenimiento. Los siguientes enfoques pueden minimizar el efecto de estas operaciones:

- Ejecute las operaciones de mantenimiento de forma manual durante las horas de menor actividad.
- Para reducir las esperas de `Lock:Relation` causadas por las tareas de autovacuum, realice los ajustes de autovacuum necesarios. Para obtener información sobre el ajuste de autovacuum, consulte Trabajo con Autovacuum de PostgreSQL en Amazon RDS en la Guía del usuario de Amazon RDS.

Lock:transactionid

El evento `Lock:transactionid` se produce cuando una transacción espera un bloqueo a nivel de fila.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

El evento `Lock:transactionid` ocurre cuando una transacción intenta adquirir un bloqueo a nivel de fila que ya fue otorgado a una transacción que se está ejecutando al mismo tiempo. La sesión que muestra el evento de espera `Lock:transactionid` se encuentra bloqueada debido a este bloqueo. Después de que la transacción bloqueada termine con una instrucción `COMMIT` o `ROLLBACK`, la transacción bloqueada puede continuar.

La semántica de control de concurrencia multiversión de RDS para PostgreSQL garantiza que los lectores no bloqueen a los escritores y que los escritores no bloqueen a los lectores. ara que se produzcan conflictos en las filas, las transacciones bloqueantes y bloqueadas deben emitir instrucciones conflictivas de los siguientes tipos:

- `UPDATE`
- `SELECT … FOR UPDATE`
- `SELECT … FOR KEY SHARE`

La instrucción `SELECT … FOR KEY SHARE` es un caso especial. La base de datos utiliza la cláusula `FOR KEY SHARE` para optimizar el rendimiento de la integridad referencial. Un bloqueo en una fila puede bloquear los comandos `INSERT`, `UPDATE` y `DELETE` en otras tablas que hacen referencia a la fila.

Causas probables del aumento de las esperas

Cuando este evento aparece más de lo normal, la causa suele ser instrucciones `UPDATE`, `SELECT … FOR UPDATE` o `SELECT … FOR KEY SHARE` combinadas con las siguientes condiciones.

Temas

- Gran concurrencia
- Inactividad en la transacción
- Transacciones de larga duración

Gran concurrencia

RDS para PostgreSQL puede utilizar una semántica de bloqueo pormenorizada por filas. La probabilidad de conflictos entre filas aumenta cuando se cumplen las siguientes condiciones:

- Una carga de trabajo de gran concurrencia compite por las mismas filas.
- Aumenta la concurrencia.

Inactividad en la transacción

A veces la columna `pg_stat_activity.state` muestra el valor `idle in transaction`. Este valor aparece para las sesiones que iniciaron una transacción, pero aún no han emitido un `COMMIT` o `ROLLBACK`. Si el valor de `pg_stat_activity.state` no se encuentra `active`, la consulta mostrada en `pg_stat_activity` es la más reciente en terminar de ejecutarse. La sesión de bloqueo no se encuentra en proceso activo de una consulta porque una transacción abierta está manteniendo un bloqueo.

Si una transacción inactiva adquirió un bloqueo entre filas, puede impedir que otras sesiones lo adquieran. Esta condición conduce a la aparición frecuente del evento de espera `Lock:transactionid`. Para diagnosticar el problema, examine la salida de `pg_stat_activity` y `pg_locks`.

Transacciones de larga duración

Las transacciones que se ejecutan durante mucho tiempo obtienen bloqueos durante mucho tiempo. Estos bloqueos de larga duración pueden bloquear la ejecución de otras transacciones.

Acciones

El bloqueo de filas es un conflicto entre las instrucciones `UPDATE`, `SELECT … FOR UPDATE`, o `SELECT … FOR KEY SHARE`. Antes de intentar una solución, averigüe cuándo se están ejecutando estas instrucciones en la misma fila. Utilice esta información para elegir una estrategia descrita en las siguientes secciones.

Temas

- Responder a la alta concurrencia
- Responder a las transacciones inactivas
- Responder a las transacciones de larga duración

Responder a la alta concurrencia

Si el problema es la concurrencia, pruebe una de las siguientes técnicas:

- Reduzca la concurrencia en la aplicación. Por ejemplo, disminuya el número de sesiones activas.
- Implemente un grupo de conexiones. Para saber cómo agrupar conexiones con RDS Proxy, consulte Amazon RDS Proxy .
- Diseñe la aplicación o el modelo de datos para evitar las instrucciones `UPDATE` y `SELECT … FOR UPDATE` en conflicto. También puede disminuir el número de claves foráneas a las que se accede mediante instrucciones `SELECT … FOR KEY SHARE`.

Responder a las transacciones inactivas

Si `pg_stat_activity.state` muestra una transacción `idle in transaction`, utilice las siguientes estrategias:

- Active la confirmación automática siempre que sea posible. Este enfoque evita que las transacciones bloqueen otras transacciones mientras esperan un `COMMIT` o `ROLLBACK`.
- Busque rutas de código en las que falten `COMMIT`, `ROLLBACK` o `END`.
- Asegúrese de que la lógica de manejo de excepciones en su aplicación siempre tiene una ruta hacia `end of transaction` válido.
- Asegúrese de que su aplicación procesa los resultados de la consulta después de finalizar la transacción con `COMMIT` o `ROLLBACK`.

Responder a las transacciones de larga duración

Si las transacciones de larga duración provocan la aparición frecuente de `Lock:transactionid`, pruebe las siguientes estrategias:

- Mantenga los bloqueos de filas fuera de las transacciones de larga duración.
- Limite la longitud de las consultas mediante la implementación de confirmación automática siempre que sea posible.

Lock:tuple

El evento `Lock:tuple` se produce cuando un proceso backend espera adquirir un bloqueo sobre una tupla.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

El evento `Lock:tuple` indica que un backend espera adquirir un bloqueo sobre una tupla mientras otro backend mantiene un bloqueo conflictivo sobre la misma tupla. La siguiente tabla ilustra un escenario en el que las sesiones generan el evento `Lock:tuple`.

Tiem	Sesión 1	Sesión 2	Sesión 3
t1	Inicia una transacción.		
t2	Actualiza la fila 1.		

Tiem	Sesión 1	Sesión 2	Sesión 3
t3		Actualiza la fila 1. La sesión adquiere un bloqueo exclusivo sobre la tupla y luego espera a que la sesión 1 libere el bloqueo mediante la confirmación o reversión.	
t4			Actualiza la fila 1. La sesión espera a que la sesión 2 libere el bloqueo exclusivo en la tupla.

También puede simular este evento de espera con la herramienta de punto de referencia `pgbench`. Configure un alto número de sesiones concurrentes para actualizar la misma fila en una tabla con un archivo SQL personalizado.

Para obtener más información sobre los modos de bloqueo conflictivos, consulte E en la documentación de PostgreSQL. Para más información sobre `pgbench`, consulte pgbench en la documentación de PostgreSQL.

Causas probables del aumento de las esperas

Cuando este evento aparece más de lo normal, lo que posiblemente indica un problema de rendimiento, las causas típicas son las siguientes:

- Un gran número de sesiones concurrentes están intentando adquirir un bloqueo conflictivo para la misma tupla al ejecutar instrucciones `UPDATE` o `DELETE`.
- Las sesiones altamente concurrentes se encuentran en ejecución con una instrucción `SELECT` que utiliza los modos de bloqueo `FOR UPDATE` o `FOR NO KEY UPDATE`.
- Varios factores hacen que la aplicación o los grupos de conexión abran más sesiones para ejecutar las mismas operaciones. A medida que nuevas sesiones intentan modificar las mismas filas, la carga de la base de datos puede aumentar y puede aparecer `Lock:tuple`.

Para más información, consulte Row-Level Locks en la documentación de PostgreSQL.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Investigue la lógica de su aplicación
- Encontrar la sesión bloqueadora
- Reducir la concurrencia cuando es alta
- Solucionar los cuellos de botella

Investigue la lógica de su aplicación

Verifique si una sesión del bloqueador se encuentra en el estado `idle in transaction` por mucho tiempo. Si es así, considere la posibilidad de finalizar la sesión del bloqueador como una solución a corto plazo. Puede utilizar la función `pg_terminate_backend`. Para más información sobre esta función, consulte Server Signaling Functions en la documentación de PostgreSQL.

Para una solución a largo plazo, haga lo siguiente:

- Ajuste la lógica de la aplicación.
- Utilice el parámetro `idle_in_transaction_session_timeout`. Este parámetro finaliza cualquier sesión con una transacción abierta que haya estado inactiva durante más tiempo del especificado. Para más información, consulte Client Connection Defaults en la documentación de PostgreSQL.
- Utilice la confirmación automática en la medida de lo posible. Para más información, consulte SET AUTOCOMMIT en la documentación de PostgreSQL.

Encontrar la sesión bloqueadora

Mientras se produce el evento de espera `Lock:tuple`, identifique el bloqueador y la sesión bloqueada mediante la búsqueda de los bloqueos que dependen unos de otros. Para más información, consulte la Información sobre dependencia de bloqueos en el wiki de PostgreSQL.

El siguiente ejemplo muestra todas las sesiones, con un filtro `tuple` y ordenadas por `wait_time`.

```
SELECT blocked_locks.pid AS blocked_pid,
         blocking_locks.pid AS blocking_pid,
```

```
        blocked_activity.usename AS blocked_user,
        blocking_activity.usename AS blocking_user,
        now() - blocked_activity.xact_start AS blocked_transaction_duration,
        now() - blocking_activity.xact_start AS blocking_transaction_duration,
        concat(blocked_activity.wait_event_type,':',blocked_activity.wait_event) AS
blocked_wait_event,
        concat(blocking_activity.wait_event_type,':',blocking_activity.wait_event) AS
blocking_wait_event,
        blocked_activity.state AS blocked_state,
        blocking_activity.state AS blocking_state,
        blocked_locks.locktype AS blocked_locktype,
        blocking_locks.locktype AS blocking_locktype,
        blocked_activity.query AS blocked_statement,
        blocking_activity.query AS blocking_statement
   FROM pg_catalog.pg_locks blocked_locks
   JOIN pg_catalog.pg_stat_activity blocked_activity ON blocked_activity.pid =
blocked_locks.pid
   JOIN pg_catalog.pg_locks blocking_locks
       ON blocking_locks.locktype = blocked_locks.locktype
       AND blocking_locks.DATABASE IS NOT DISTINCT FROM blocked_locks.DATABASE
       AND blocking_locks.relation IS NOT DISTINCT FROM blocked_locks.relation
       AND blocking_locks.page IS NOT DISTINCT FROM blocked_locks.page
       AND blocking_locks.tuple IS NOT DISTINCT FROM blocked_locks.tuple
       AND blocking_locks.virtualxid IS NOT DISTINCT FROM blocked_locks.virtualxid
       AND blocking_locks.transactionid IS NOT DISTINCT FROM
blocked_locks.transactionid
       AND blocking_locks.classid IS NOT DISTINCT FROM blocked_locks.classid
       AND blocking_locks.objid IS NOT DISTINCT FROM blocked_locks.objid
       AND blocking_locks.objsubid IS NOT DISTINCT FROM blocked_locks.objsubid
       AND blocking_locks.pid != blocked_locks.pid
   JOIN pg_catalog.pg_stat_activity blocking_activity ON blocking_activity.pid =
blocking_locks.pid
   WHERE NOT blocked_locks.GRANTED;
```

Reducir la concurrencia cuando es alta

El evento `Lock:tuple` puede producirse de manera frecuente, especialmente en un momento de carga de trabajo elevada. En esta situación, considere reducir la alta concurrencia para las filas muy ocupadas. A menudo, solo unas pocas filas controlan una cola o la lógica booleana, lo que hace que estas filas estén muy ocupadas.

Puede reducir la concurrencia mediante el uso de diferentes enfoques basados en los requisitos de la empresa, lógica de la aplicación y tipo de carga de trabajo. Por ejemplo, puede hacer lo siguiente:

- Rediseñar la lógica de la tabla y los datos para reducir la alta concurrencia.
- Cambiar la lógica de la aplicación para reducir la alta concurrencia entre filas.
- Aprovechar y rediseñar las consultas con bloqueos entre filas.
- Utilizar la cláusula `NOWAIT` con operaciones de reintento.
- Considerar el uso de control de concurrencia optimista y de lógica de bloqueo híbrida.
- Considerar la posibilidad de cambiar el nivel de aislamiento de la base de datos.

Solucionar los cuellos de botella

La `Lock:tuple` producirse con cuellos de botella, como el agotamiento de la CPU o el uso máximo del ancho de banda de Amazon EBS. Para reducir los cuellos de botella, considere los siguientes enfoques:

- Escalar verticalmente el tipo de clase de instancia.
- Optimizar las consultas que consumen muchos recursos.
- Cambiar la lógica de la aplicación.
- Archivar los datos a los que rara vez se accede.

LWLock:BufferMapping (LWLock:buffer_mapping)

Este evento se produce cuando una sesión espera asociar un bloque de datos con un búfer en el grupo de búferes compartidos.

> **Note**
>
> Para la versión 13 y posteriores de RDS para PostgreSQL, el nombre de este evento es `LWLock:BufferMapping`. Para la versión 12 y posteriores de RDS para PostgreSQL, el nombre de este evento es `LWLock:buffer_mapping`.

Temas

- Versiones del motor admitidas
- Context
- Causas
- Acciones

Versiones del motor admitidas

La información del evento de espera es relevante para RDS para PostgreSQL versión 9.6 y posteriores.

Context

El grupo de búferes compartidos es un área de memoria de PostgreSQL que contiene todas las páginas que utilizan o utilizaban los procesos. Cuando un proceso necesita una página, lee la página en el grupo de búferes compartidos. El parámetro `shared_buffers` establece el tamaño del búfer compartido y reserva un área de memoria para almacenar las páginas de tablas e índices. Si cambia este parámetro, asegúrese de reiniciar la base de datos.

El evento de espera `LWLock:buffer_mapping` ocurre en los siguientes escenarios:

- Un proceso busca una página en la tabla de búferes y adquiere un bloqueo de asignación de búferes compartidos.
- Un proceso carga una página en el grupo de búferes y adquiere un bloqueo de asignación de búferes exclusivo.
- Un proceso elimina una página del grupo y adquiere un bloqueo de asignación de búferes exclusivo.

Causas

Cuando este evento aparece más de lo normal, lo que puede indicar un problema de rendimiento, la base de datos entra y sale del grupo de búferes compartidos. Las causas típicas son las siguientes:

- Consultas grandes
- Índices y tablas sobrecargados
- Escaneos completos de tablas
- Un tamaño del grupo compartido menor que el conjunto de trabajo

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera.

Temas

- Monitorear las métricas relacionadas con el buffer
- Evaluar la estrategia de indexación
- Reducir el número de búferes que deben ser asignados rápidamente

Monitorear las métricas relacionadas con el buffer

Cuando las esperas de `LWLock:buffer_mapping` se disparan, hay que investigar la tasa de aciertos del búfer. Puede utilizar estas métricas para comprender mejor lo que ocurre en la caché del búfer. Examina las siguientes métricas:

`blks_hit`

Esta métrica del contador de Información sobre rendimiento indica el número de bloques que se recuperaron del grupo de búferes compartidos. Después de que aparezca el evento de espera `LWLock:buffer_mapping`, se puede observar un pico en `blks_hit`.

`blks_read`

Esta métrica del contador de Información sobre rendimiento indica el número de bloques que requirieron E/S para leerse en el grupo de búferes compartidos. Puede observar un pico en `blks_read` en el periodo previo al evento de espera `LWLock:buffer_mapping`.

Evaluar la estrategia de indexación

Para confirmar que la estrategia de indexación no disminuye el rendimiento, verifique lo siguiente:

Sobrecarga del índice

Asegúrese de que el índice y la sobrecarga de la tabla no provocan la lectura de páginas innecesarias en el búfer compartido. Si las tablas contienen filas que no se utilizan, considere la posibilidad de archivar los datos y eliminar las filas de las tablas. A continuación, puede reconstruir los índices para las tablas redimensionadas.

Índices para consultas de uso frecuente

Para determinar si cuenta con los índices óptimos, monitoree las métricas del motor de base de datos en Información sobre rendimiento. La métrica `tup_returned` muestra el número de filas leídas. La métrica `tup_fetched` muestra el número de filas devueltas al cliente. Si `tup_returned` es mucho mayor que `tup_fetched`, es posible que los datos no estén bien indexados. Además, es posible que las estadísticas de la tabla no se encuentren actualizadas.

Reducir el número de búferes que deben ser asignados rápidamente

Para reducir los eventos de espera de `LWLock:buffer_mapping`, intente reducir el número de búferes que se deben asignar de forma rápida. Una estrategia es hacer operaciones por lotes más pequeños. Se pueden conseguir lotes más pequeños por medio de la partición de las tablas.

LWLock:BufferIO (IPC:BufferIO)

El evento `LWLock:BufferIO` ocurre cuando RDS para PostgreSQL espera que otros procesos terminen sus operaciones de entrada/salida (E/S) cuando intentan acceder a una página de forma simultánea. Su propósito es que la misma página se lea en el búfer compartido.

Temas

- Versiones del motor relevantes
- Context
- Causas
- Acciones

Versiones del motor relevantes

Esta información de eventos de espera es relevante para todas las versiones de RDS para PostgreSQL. Para RDS para PostgreSQL 12 y versiones anteriores, este evento de espera se denomina lwlock:buffer_io, mientras que en la versión 13 de RDS para PostgreSQL se denomina lwlock:bufferio. A partir de la versión 14 de RDS para PostgreSQL, el evento de espera BufferIO se movió de tipo de evento de espera `LWLock` a `IPC` (IPC:bufferIO).

Context

Cada búfer compartido tiene un bloqueo de E/S que está asociado con el evento de espera `LWLock:BufferIO`, cada vez que un bloque (o una página) se tiene que recuperar fuera del grupo de búferes compartidos.

Este bloqueo se utiliza para manejar múltiples sesiones que requieren acceso al mismo bloque. Este bloque se tiene que leer desde fuera del grupo de búferes compartidos, que se define con el parámetro `shared_buffers`.

Tan pronto como la página se lee dentro del grupo de búferes compartidos, el bloqueo `LWLock:BufferIO` se libera.

> **Note**
>
> El evento de espera `LWLock:BufferIO` precede al evento de espera IO:DataFileRead. El evento de espera `IO:DataFileRead` se produce mientras se leen datos del almacenamiento.

Para obtener más información sobre los bloqueos ligeros, consulte Información general sobre los bloqueos.

Causas

Las causas más comunes para que el evento `LWLock:BufferIO` aparezca en el máximo de esperas son las siguientes:

- Varios backends o conexiones que intentan acceder a la misma página que también tiene pendiente una operación de E/S
- La relación entre el tamaño del grupo de búferes compartidos (definido por el parámetro `shared_buffers`) y el número de búferes que necesita la carga de trabajo actual
- El tamaño del grupo de búferes compartidos no está bien equilibrado con el número de páginas que se desalojan por otras operaciones
- Índices grandes o sobrecargados que requieren que el motor lea más páginas de las necesarias en el grupo de búferes compartidos
- La falta de índices obliga al motor de la base de datos a leer más páginas de las necesarias en las tablas
- Puntos de control que se producen con demasiada frecuencia o que necesitan vaciar demasiadas páginas modificadas
- Picos repentinos de conexiones a la base de datos que intentan hacer operaciones en la misma página

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera:

- Observe las métricas de Amazon CloudWatch en busca de una correlación entre los descensos bruscos de los eventos de espera `BufferCacheHitRatio` y `LWLock:BufferIO`. Este efecto

a veces significa que tiene una configuración de búferes compartidos pequeña. Puede que tenga que aumentarla o escalar verticalmente la clase de instancia de base de datos. Puede dividir su carga de trabajo en más nodos de lectura.

- Ajuste `max_wal_size` y `checkpoint_timeout` en función del tiempo de pico de su carga de trabajo si ve que `LWLock:BufferIO` coincide con las caídas de la métrica `BufferCacheHitRatio`. A continuación, identifique qué consulta puede ser la causa.
- Verifique si tiene índices sin utilizar y elimínelos.
- Utilice tablas particionadas (que también tengan índices particionados). Esto ayuda a mantener un bajo nivel de reordenación de índices y reduce su impacto.
- Evite indexar columnas innecesariamente.
- Evite los picos repentinos de conexión a la base de datos, utilice un grupo de conexiones.
- Limite el número máximo de conexiones a la base de datos como práctica recomendada.

LWLock:buffer_content (BufferContent)

El evento `LWLock:buffer_content` ocurre cuando una sesión espera para leer o escribir una página de datos en memoria mientras otra sesión tiene esa página bloqueada para escribir. En RDS para PostgreSQL 13 y versiones posteriores, este evento de espera se llama `BufferContent`.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento de las esperas
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

Para leer o manipular datos, PostgreSQL accede a ellos a través de búferes de memoria compartida. Para leer del búfer, un proceso obtiene un bloqueo ligero (LWLock) sobre el contenido del búfer en modo compartido. Para escribir en el búfer, obtiene ese bloqueo en modo exclusivo. Los bloqueos

compartidos permiten a otros procesos adquirir simultáneamente bloqueos compartidos sobre ese contenido. Los bloqueos exclusivos impiden que otros procesos obtengan cualquier tipo de bloqueo sobre él.

El evento `LWLock:buffer_content` (`BufferContent`) indica que varios procesos intentan obtener un bloqueo sobre el contenido de un búfer específico.

Causas probables del aumento de las esperas

Cuando el evento `LWLock:buffer_content` (`BufferContent`) aparece más de lo normal, lo que posiblemente indica un problema de rendimiento, las causas típicas son las siguientes:

Aumento de las actualizaciones simultáneas de los mismos datos

Puede haber un aumento en el número de sesiones concurrentes con consultas que actualizan el mismo contenido del búfer. Esta contención puede ser más pronunciada en tablas con muchos índices.

Los datos de carga de trabajo no están en la memoria

Cuando los datos que la carga de trabajo activa está procesando no están en memoria, estos eventos de espera pueden aumentar. Este efecto se debe a que los procesos que mantienen bloqueos pueden mantenerlos durante más tiempo mientras hacen operaciones de E/S en disco.

Uso excesivo de restricciones de clave externa

Las restricciones de clave externa pueden aumentar el tiempo que un proceso mantiene un bloqueo de contenido de búfer. Este efecto se debe a que las operaciones de lectura requieren un bloqueo de contenido de búfer compartido en la clave referenciada mientras se actualiza dicha clave.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera. Puede identificar los eventos `LWLock:buffer_content` (`BufferContent`) mediante Información sobre rendimiento de Amazon RDS o consultar la vista `pg_stat_activity`.

Temas

- Mejorar la eficiencia en memoria
- Reducir el uso de restricciones de clave externa

- Eliminar los índices que no se utilizan
- Aumentar el tamaño de la memoria caché al utilizar secuencias

Mejorar la eficiencia en memoria

Para aumentar la posibilidad de que los datos de la carga de trabajo activa estén en memoria, particione las tablas o escale verticalmente su clase de instancia. Para obtener información acerca de las clases de instancia de base de datos, consulte Clases de instancia de base de datos de .

Reducir el uso de restricciones de clave externa

Examine las cargas de trabajo que experimentan un elevado número de eventos de espera `LWLock:buffer_content` (`BufferContent`) para comprobar el uso de las restricciones de clave externa. Elimine las restricciones de clave externa innecesarias.

Eliminar los índices que no se utilizan

Para las cargas de trabajo que experimentan un gran número de eventos de espera `LWLock:buffer_content` (`BufferContent`), identifique los índices que no se utilizan y elimínelos.

Aumentar el tamaño de la memoria caché al utilizar secuencias

Si las tablas usan secuencias, aumente el tamaño de la memoria caché para eliminar la contención en las páginas de secuencias y las páginas de índice. Cada secuencia es una página individual en la memoria compartida. La memoria caché predefinida es por conexión. Es posible que esto no sea suficiente para gestionar la carga de trabajo cuando muchas sesiones simultáneas reciben un valor de secuencia.

LWLock:lock_manager (LWLock:lockmanager)

Este evento ocurre cuando el motor de RDS para PostgreSQL mantiene el área de memoria del bloqueo compartido para asignar, verificar y desasignar un bloqueo cuando no es posible un bloqueo de ruta rápida.

Temas

- Versiones del motor admitidas
- Contexto
- Causas probables del aumento de las esperas

- Acciones

Versiones del motor admitidas

La información del evento de espera es relevante para RDS para PostgreSQL versión 9.6 y posteriores. Para las versiones de RDS para PostgreSQL anteriores a la 13, el nombre de este evento de espera es `LWLock:lock_manager`. Para la versión 13 de RDS para PostgreSQL y posteriores, el nombre de este evento de espera es `LWLock:lockmanager`.

Contexto

Cuando se emite una instrucción SQL, RDS para PostgreSQL registra bloqueos para proteger la estructura, los datos y la integridad de la base de datos durante las operaciones simultáneas. El motor puede lograr este objetivo con un bloqueo de ruta rápido o con un bloqueo de ruta que no es rápido. Un bloqueo de ruta que no es rápido es más caro y crea más sobrecarga que un bloqueo de ruta rápido.

Bloqueo rápido de la ruta

Para reducir la sobrecarga de los bloqueos que se toman y liberan con frecuencia, pero que rara vez entran en conflicto, los procesos del backend pueden utilizar el bloqueo de ruta rápido. La base de datos utiliza este mecanismo para los bloqueos que cumplen los siguientes criterios:

- Utilizan el método de bloqueo DEFAULT.
- Representan un bloqueo en una relación de la base de datos y no en una relación compartida.
- Son bloqueos débiles que probablemente no entren en conflicto.
- El motor puede verificar rápidamente que no pueden existir bloqueos conflictivos.

El motor no puede utilizar el bloqueo de ruta rápida cuando se cumple alguna de las siguientes condiciones:

- El bloqueo no cumple los criterios anteriores.
- No hay más ranuras disponibles para el proceso de backend.

Para ajustar las consultas para que se bloqueen rápidamente, puede utilizar la siguiente consulta.

```
SELECT count(*), pid, mode, fastpath
```

```
  FROM pg_locks
 WHERE fastpath IS NOT NULL
 GROUP BY 4,3,2
 ORDER BY pid, mode;
 count | pid  |      mode       | fastpath
-------+------+-----------------+----------
16 | 9185 | AccessShareLock | t
336 | 9185 | AccessShareLock | f
1 | 9185 | ExclusiveLock   | t
```

La siguiente consulta muestra solo el total de la base de datos.

```
SELECT count(*), mode, fastpath
  FROM pg_locks
 WHERE fastpath IS NOT NULL
 GROUP BY 3,2
 ORDER BY mode,1;
count |      mode       | fastpath
-------+-----------------+----------
16 | AccessShareLock | t
337 | AccessShareLock | f
1 | ExclusiveLock   | t
(3 rows)
```

Para más información sobre el bloqueo de ruta rápida, consulte fast path en el README del administrador de bloqueos de PostgreSQL y pg-locks en la documentación de PostgreSQL.

Ejemplo de un problema de escalado para el administrador de bloqueos

En este ejemplo, una tabla con el nombre `purchases` almacena cinco años de datos, particionados por día. Cada partición tiene dos índices. Se produce la siguiente secuencia de eventos:

1. Se consultan los datos de muchos días, lo que requiere que la base de datos lea muchas particiones.
2. La base de datos crea una entrada de bloqueo para cada partición. Si los índices de las particiones forman parte de la ruta de acceso del optimizador, la base de datos también crea una entrada de bloqueo para ellos.
3. Cuando el número de entradas de bloqueo solicitadas para el mismo proceso backend es superior a 16, que es el valor `FP_LOCK_SLOTS_PER_BACKEND`, el administrador de bloqueos utiliza el método de bloqueo de ruta no rápida.

Las aplicaciones modernas pueden tener cientos de sesiones. Si las sesiones simultáneas consultan la base de datos principal sin una poda adecuada de las particiones, la base de datos puede crear cientos o incluso miles de bloqueos de ruta no rápida. Normalmente, cuando esta simultaneidad es mayor que el número de vCPU, aparece el evento de espera `LWLock:lock_manager`.

> **Note**
>
> El evento de espera `LWLock:lock_manager` no está relacionado con el número de particiones o índices en un esquema de base de datos. En cambio, está relacionado con el número de bloqueos de rutas no rápidas que la base de datos debe controlar.

Causas probables del aumento de las esperas

Cuando el evento de espera `LWLock:lock_manager` ocurre más de lo normal, lo que posiblemente indica un problema de rendimiento, las causas más probables de los picos repentinos son las siguientes:

- Las sesiones activas simultáneas ejecutan consultas que no utilizan bloqueos de ruta rápida. Estas sesiones también exceden el máximo de vCPU.
- Un gran número de sesiones activas simultáneas acceden a una tabla con muchas particiones. Cada partición tiene múltiples índices.
- La base de datos está experimentando una tormenta de conexiones. De forma predeterminada, algunas aplicaciones y software de grupo de conexiones crean más conexiones cuando la base de datos es lenta. Esta práctica empeora el problema. Ajuste el software de grupo de conexiones para que no se produzcan tormentas de conexiones.
- Un gran número de sesiones consultan una tabla principal sin borrar particiones.
- Un lenguaje de definición de datos (DDL), un lenguaje de manipulación de datos (DML) o un comando de mantenimiento bloquea exclusivamente una relación ocupada o tuplas a las que se accede o modifica con frecuencia.

Acciones

Si se produce el evento de espera `CPU`, no indica necesariamente un problema de rendimiento. Responda a este evento solo cuando el rendimiento disminuya y este evento de espera domine la carga de la base de datos.

Temas

- Utilizar la poda de particiones
- Eliminar índices innecesarios
- Ajustar sus consultas para el bloqueo rápido de rutas
- Ajustar otros eventos de espera
- Reducir los cuellos de botella del hardware
- Utilizar un grupo de conexiones
- Actualización de la versión de RDS para PostgreSQL

Utilizar la poda de particiones

La poda de particiones es una estrategia de optimización de consultas para tablas partidas de forma declarativa que excluye las particiones innecesarias de los escaneos de tablas, lo que mejora el rendimiento. La poda de particiones está activada de forma predeterminada. Si está desactivada, actívela de la siguiente manera.

```
SET enable_partition_pruning = on;
```

Las consultas pueden aprovechar la poda de particiones cuando la cláusula `WHERE` contiene la columna que se utiliza para la partición. Para más información, consulte Partition Pruningc en la documentación de PostgreSQL.

Eliminar índices innecesarios

Es posible que la base de datos contenga índices que no se utilicen o que se utilicen muy poco. Si es así, considere eliminarlos. Haga una de estas dos operaciones:

- Aprenda a encontrar índices innecesarios al leer Índices no utilizados en el wiki de PostgreSQL.
- Ejecute PG Collector. Este script SQL recopila información de la base de datos y la presenta en un informe HTML consolidado. Verifique la sección “Índices no utilizados”. Para más información, consulte pg-collector en el repositorio GitHub de AWS Labs.

Ajustar sus consultas para el bloqueo rápido de rutas

Para averiguar si las consultas utilizan el bloqueo de ruta rápida, consulte la columna `fastpath` en la tabla `pg_locks`. Si las consultas no utilizan el bloqueo de ruta rápida, intente reducir el número de relaciones por consulta a menos de 16.

Ajustar otros eventos de espera

Si `LWLock:lock_manager` es el primero o el segundo en la lista de esperas principales, verifique si los siguientes eventos de espera también aparecen en la lista:

- `Lock:Relation`
- `Lock:transactionid`
- `Lock:tuple`

Si los eventos anteriores aparecen en primer lugar en la lista, considere la posibilidad de ajustar estos eventos de espera en primer lugar. Estos eventos pueden ser un controlador para `LWLock:lock_manager`.

Reducir los cuellos de botella del hardware

Es posible que tenga un cuello de botella en el hardware, como el agotamiento de la CPU o el uso máximo de su ancho de banda de Amazon EBS. En estos casos, considere la posibilidad de reducir los cuellos de botella de hardware. Considere las siguientes acciones:

- Escalar verticalmente la clase de instancia.
- Optimizar las consultas que consumen grandes cantidades de CPU y memoria.
- Cambiar la lógica de su aplicación.
- Archivar los datos.

Para más información sobre la CPU, memoria y ancho de banda de red de EBS, consulte Tipos de instancias de Amazon RDS.

Utilizar un grupo de conexiones

Si el número total de conexiones activas supera el máximo de vCPU, más procesos del sistema operativo requieren CPU de lo que su tipo de instancia puede admitir. En este caso, considere la posibilidad de utilizar o ajustar un grupo de conexiones. Para más información sobre las vCPU de su tipo de instancia, consulte Tipos de instancias de Amazon RDS.

Para más información sobre la agrupación de conexiones, consulte los siguientes recursos:

- Amazon RDS Proxy
- pgbouncer

- Connection Pools and Data Sources en la documentación de PostgreSQL

Actualización de la versión de RDS para PostgreSQL

Si la versión actual de RDS para PostgreSQL es inferior a la 12, actualice a la versión 12 o posterior. Las versiones 12 y posteriores de PostgreSQL tienen un mecanismo de partición mejorado. Para más información sobre la versión 12, consulte las Notas de la versión 12.0 de PostgreSQL. Para más información sobre la actualización de RDS para PostgreSQL, consulte Actualizaciones del motor de base de datos de RDS para PostgreSQL.

LWLock:pg_stat_statements

El evento de espera LWLock:pg_stat_statements se produce cuando la extensión `pg_stat_statements` toma un bloqueo exclusivo en la tabla hash que rastrea las instrucciones SQL. Esto ocurre en las siguientes situaciones:

- Cuando el número de instrucciones rastreadas alcanza el valor del parámetro `pg_stat_statements.max` configurado y es necesario dejar espacio para más entradas, la extensión realiza una clasificación del número de llamadas, elimina el 5 % de las instrucciones menos ejecutadas y vuelve a rellenar el hash con las entradas restantes.
- Cuando `pg_stat_statements` realiza una operación de `garbage collection` en el archivo `pgss_query_texts.stat` del disco y lo vuelve a escribir.

Temas

- Versiones del motor admitidas
- Contexto
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Contexto

Descripción de la extensión pg_stat_statements: la extensión pg_stat_statements rastrea las estadísticas de ejecución de instrucción SQL en una tabla hash. La extensión rastrea las instrucciones SQL hasta el límite definido por el parámetro `pg_stat_statements.max`. Este parámetro determina el número máximo de instrucciones que se pueden rastrear, lo que corresponde al número máximo de filas en la vista de pg_stat_statements.

Persistencia de las estadísticas de las instrucciones: la extensión mantiene las estadísticas de las instrucciones a través de reinicios de instancia mediante:

- Escritura de datos en un archivo llamado pg_stat_statements.stat
- Uso del parámetro pg_stat_statements.save para controlar el comportamiento de persistencia

Cuando pg_stat_statements.save se establece en:

- activado (predeterminado): las estadísticas se guardan al apagar el servidor y se vuelven a cargar al iniciar el servidor
- desactivado (predeterminado): las estadísticas no se guardan al apagar el servidor ni se vuelven a cargar al iniciar el servidor

Almacenamiento de texto de consulta: la extensión almacena el texto de las consultas rastreadas en un archivo denominado `pgss_query_texts.stat`. Este archivo puede crecer hasta duplicar el tamaño medio de todas las instrucciones SQL rastreadas antes de que se produzca la recopilación de elementos no utilizados. La extensión requiere un bloqueo exclusivo en la tabla de hash durante las operaciones de limpieza y reescritura del archivo `pgss_query_texts.stat`.

Proceso de desasignación de instrucciones: cuando el número de instrucciones rastreadas alcanza el límite `pg_stat_statements.max` y es necesario realizar un seguimiento de las nuevas, la extensión:

- Toma un bloqueo exclusivo (LWLock:pg_stat_statements) en la tabla de hash.
- Carga los datos existentes en la memoria local.
- Realiza una clasificación rápida en función del número de llamadas.
- Elimina las instrucciones menos solicitadas (el 5 % inferior).
- Vuelve a rellenar la tabla hash con las entradas restantes.

Supervisión de la desasignación de instrucciones: en PostgreSQL 14 y versiones posteriores, puede supervisar la desasignación de las instrucciones mediante la vista pg_stat_statements_info. Esta vista incluye una columna dealloc que muestra cuántas veces se desasignaron las instrucciones para dejar espacio a otras nuevas

Si la desasignación de las instrucciones se produce con frecuencia, se realizará con más frecuencia la recopilación de elementos no utilizados del archivo `pgss_query_texts.stat` en el disco.

Causas probables del aumento del tiempo de espera

Entre las causas típicas del aumento de las esperas de `LWLock:pg_stat_statements` se incluyen las siguientes:

- Un aumento en el número de consultas únicas utilizadas por la aplicación.
- El valor del parámetro `pg_stat_statements.max` es pequeño en comparación con el número de consultas únicas que se utilizan.

Acciones

Recomendamos diferentes acciones en función de las causas del evento de espera. Puede identificar los eventos de `LWLock:pg_stat_statements` mediante Información de rendimiento de Amazon RDS o consultando la vista de `pg_stat_activity`.

Ajuste los siguientes parámetros `pg_stat_statements` para controlar el comportamiento de seguimiento y reducir los eventos de espera de las instrucciones LWLock:pg_stat_statements.

Temas

- Desactivación del parámetro pg_stat_statements.track
- Aumento del parámetro pg_stat_statements.max
- Desactivación del parámetro pg_stat_statements.track_utility

Desactivación del parámetro pg_stat_statements.track

Si el evento de espera de LWLock:pg_stat_statements está afectando negativamente al rendimiento de la base de datos y se requiere una solución rápida antes de continuar con el análisis de la vista de `pg_stat_statements` para identificar la causa raíz, el parámetro `pg_stat_statements.track` se puede desactivar configurándolo en `none`. Esto desactivará la recopilación de estadísticas de instrucciones.

Aumento del parámetro pg_stat_statements.max

Para reducir la desasignación y minimizar la recopilación de elementos no utilizados del archivo `pgss_query_texts.stat` en el disco, aumente el valor del parámetro `pg_stat_statements.max`. El valor predeterminado es `5,000`.

> **Note**
>
> El parámetro `pg_stat_statements.max` está estático. Debe reiniciar la instancia de base de datos para aplicar los cambios a este parámetro.

Desactivación del parámetro pg_stat_statements.track_utility

Puede analizar la vista de pg_stat_statements para determinar qué comandos de utilidad consumen la mayor cantidad de recursos rastreados por `pg_stat_statements`.

El parámetro `pg_stat_statements.track_utility` controla si el módulo realiza un seguimiento de los comandos de utilidad, que incluyen todos los comandos excepto SELECT, INSERT, UPDATE, DELETE y MERGE. Este parámetro está establecido en on de forma predeterminada.

Por ejemplo, cuando la aplicación utiliza muchas consultas de puntos de guardado, que son intrínsecamente únicas, puede aumentar la desasignación de instrucciones. Para abordar este problema, puede desactivar el parámetro `pg_stat_statements.track_utility` para impedir que `pg_stat_statements` realice un seguimiento de las consultas de puntos de guardado.

> **Note**
>
> El parámetro `pg_stat_statements.track_utility` es un parámetro dinámico. Puede cambiar su valor sin necesidad de reiniciar la instancia de la base de datos.

Example Ejemplo de consultas de punto de guardado únicas en pg_stat_statements

```
                    query                         |       queryid
--------------------------------------------------+---------------------
 SAVEPOINT JDBC_SAVEPOINT_495701                  | -7249565344517699703
 SAVEPOINT JDBC_SAVEPOINT_1320                    | -1572997038849006629
 SAVEPOINT JDBC_SAVEPOINT_26739                   |  54791337410474486
```

```
SAVEPOINT JDBC_SAVEPOINT_1294466                | 8170064357463507593
ROLLBACK TO SAVEPOINT JDBC_SAVEPOINT_65016      | -33608214779996400
SAVEPOINT JDBC_SAVEPOINT_14185                  | -2175035613806809562
SAVEPOINT JDBC_SAVEPOINT_45837                  | -6201592986750645383
SAVEPOINT JDBC_SAVEPOINT_1324                   | 6388797791882029332
```

PostgreSQL 17 presenta varias mejoras para el seguimiento de comandos de utilidades:

- Los nombres de los puntos de guardado ahora se muestran como constantes.
- Los ID de transacción globales (GID) de los comandos de confirmación de dos fases ahora se muestran como constantes.
- Los nombres de las instrucciones DEALLOCATE se muestran como constantes.
- Los parámetros CALL ahora se muestran como constantes.

Timeout:PgSleep

El evento `Timeout:PgSleep` ocurre cuando un proceso del servidor llama a la función `pg_sleep` y espera a que el tiempo de espera expire.

Temas

- Versiones del motor admitidas
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Causas probables del aumento del tiempo de espera

Este evento de espera ocurre cuando una aplicación, función almacenada o usuario emite una sentencia SQL que llama a una de las siguientes funciones:

- `pg_sleep`
- `pg_sleep_for`
- `pg_sleep_until`

Las funciones anteriores retrasan la ejecución hasta que transcurra el número de segundos especificado. Por ejemplo, `SELECT pg_sleep(1)` hace una pausa de 1 segundo. Para más información, consulte Delaying Execution en la documentación de PostgreSQL.

Acciones

Identifique la sentencia que estaba ejecutando la función `pg_sleep`. Determine si el uso de la función es adecuado.

Timeout:VacuumDelay

El evento `Timeout:VacuumDelay` indica que se ha superado el límite de costo de las E/S de vacío y que el proceso de vacío está en reposo. Las operaciones de aspiración se detienen durante el tiempo especificado en el parámetro de retraso de coste correspondiente y, a continuación, reanudan su trabajo. Para el comando de limpieza manual, el retraso se especifica en el parámetro `vacuum_cost_delay`. Para el deamon autovacuum, el retraso se especifica en `autovacuum_vacuum_cost_delay parameter.`.

Temas

- Versiones del motor admitidas
- Context
- Causas probables del aumento del tiempo de espera
- Acciones

Versiones del motor admitidas

Esta información de eventos de espera es compatible con todas las versiones de RDS para PostgreSQL.

Context

PostgreSQL tiene un daemon autovaccum y un comando de limpieza manual. El proceso de autovacuum está “activado” de forma predeterminada para las instancias de base de datos de RDS para PostgreSQL. El comando de limpieza manual se usa según sea necesario, por ejemplo, para purgar tablas de tuplas muertas o para generar nuevas estadísticas.

Cuando se realiza la limpieza, PostgreSQL utiliza un contador interno para realizar un seguimiento de los costos estimados a medida que el sistema realiza diversas operaciones de E/S. Cuando el contador alcanza el valor especificado en el parámetro de límite de costo, el proceso que realiza la

operación permanece en reposo durante el breve período especificado en el parámetro de retraso de costo. A continuación, reinicia el contador y continúa con las operaciones.

El proceso de vacío tiene parámetros que se pueden utilizar para regular el consumo de recursos. El vacío automático y el comando de vacío manual tienen sus propios parámetros para establecer el valor de límite de costo. También tienen sus propios parámetros para especificar un retraso en el costo, una cantidad de tiempo para poner la limpieza en reposo cuando se alcanza el límite. De esta manera, el parámetro de retraso de costos funciona como un mecanismo de limitación del consumo de recursos. En las siguientes listas encontrará las descripciones de estos parámetros.

Parámetros que afectan a la limitación del daemon autovacuum

- `autovacuum_vacuum_cost_limit`: especifica el valor límite de costo que se utilizará en las operaciones de vacío automático. El aumento de la configuración de este parámetro permite que el proceso de vacío utilice más recursos y reduce el evento de espera `Timeout:VacuumDelay`.
- `autovacuum_vacuum_cost_delay`: especifica el valor retardo de costo que se utilizará en las operaciones de vacío automático. El valor predeterminado es de 2 milisegundos. Al establecer el parámetro de retardo en 0, se desactiva el mecanismo de limitación y, por lo tanto, el evento de espera `Timeout:VacuumDelay` no aparecerá.

Para más información, visite Automatic Vacuuming (Vacío automático) en la documentación de PostgreSQL.

Parámetros que afectan a la limitación del proceso de vacío manual

- `vacuum_cost_limit`: umbral en el que el proceso de limitación está en reposo. El límite predeterminado de es de 200. Este número representa las estimaciones de costos acumulados para las E/S adicionales que necesitan varios recursos. Al aumentar este valor, se reduce el número del evento de espera `Timeout:VacuumDelay`.
- `vacuum_cost_delay`: cantidad de tiempo que el proceso de vacío está en reposo cuando se ha alcanzado el límite de costo de vacío. La configuración predeterminada es 0, lo que significa que esta función está desactivada. Puede configurarla con un valor entero para especificar el número de milisegundos necesarios para activar esta función, pero le recomendamos que la deje como configuración predeterminada.

Para obtener más información acerca del parámetro `vacuum_cost_delay`, consulte el punto Resource Consumption (Consumo de recursos) en la documentación de PostgreSQL.

Para obtener más información acerca del uso del vacío automático con RDS para PostgreSQL, consulte Uso de autovacuum de PostgreSQL en Amazon RDS para PostgreSQL.

Causas probables del aumento del tiempo de espera

`Timeout:VacuumDelay` se ve afectado por el equilibrio entre la configuración de los parámetros del límite de costo (`vacuum_cost_limit`, `autovacuum_vacuum_cost_limit`) y los parámetros de retraso de costo (`vacuum_cost_delay`, `autovacuum_vacuum_cost_delay`) que controlan la duración del reposo del vacío. Al aumentar el valor de un parámetro de límite de costo, el vacío puede utilizar más recursos antes de que entre en reposo. Esto se traduce en menos eventos de espera `Timeout:VacuumDelay`. El aumento de cualquiera de los parámetros de retraso hace que el evento de espera `Timeout:VacuumDelay` se produzca con más frecuencia y durante períodos de tiempo más prolongados.

La configuración del parámetro `autovacuum_max_workers` también puede aumentar el número de `Timeout:VacuumDelay`. Cada proceso adicional de trabajo de autovacuum contribuye al mecanismo de contador interno y, por lo tanto, se puede alcanzar el límite más rápidamente que con un solo proceso de trabajo de autovacuum. A medida que se alcanza el límite de costo más rápidamente, el retraso en el costo se hace efectivo con más frecuencia, lo que resulta en más eventos de espera `Timeout:VacuumDelay`. Para más información, consulte autovacuum_max_workers en la documentación de PostgreSQL.

Los objetos grandes, como de 500 GB o más, también aumentan este evento de espera, ya que el vacío puede tardar algún tiempo en completar el procesamiento de objetos grandes.

Acciones

Si las operaciones de vacío se completan según lo previsto, no es necesario realizar ninguna corrección. En otras palabras, este evento de espera no significa necesariamente que se trate de un problema. Indica que el vacío está en reposo durante el período de tiempo especificado en el parámetro de retraso, de modo que los recursos se puedan aplicar a otros procesos que deben completarse.

Si desea que las operaciones de vacío se completen más rápido, puede reducir los parámetros de retardo. Esto acorta el tiempo que el vacío permanece inactivo.

Ajuste de RDS para PostgreSQL con información proactiva de Amazon DevOps Guru

La información proactiva de DevOps Guru detecta las condiciones en sus instancias de base de datos de RDS para PostgreSQL que pueden causar problemas y le permiten conocerlos antes de que se produzcan. La información proactiva puede alertarle sobre algún elemento que lleve tiempo inactivo en la conexión de la transacción. Para obtener más información sobre cómo resolver un problema relacionado con una inactividad prolongada en las conexiones de transacciones, consulte La base de datos lleva mucho tiempo inactiva en la conexión de la transacción.

DevOps Guru puede hacer lo siguiente:

- Evitar muchos problemas comunes en las bases de datos cotejando la configuración de la base de datos con la configuración habitual recomendada.
- Alertar sobre problemas críticos en su flota que, si no se comprueban, pueden provocar problemas mayores en el futuro.
- Avisarle de los problemas que acaban de descubrirse.

Cada información proactiva contiene un análisis de la causa del problema y recomendaciones para las acciones correctivas.

Para obtener más información sobre Amazon DevOps Guru para Amazon RDS, consulte Análisis de anomalías de rendimiento con Amazon DevOps Guru para Amazon RDS.

La base de datos lleva mucho tiempo inactiva en la conexión de la transacción

Una conexión a la base de datos lleva en el estado `idle in transaction` más de 1800 segundos.

Temas

- Versiones del motor admitidas
- Context
- Causas probables de este problema
- Acciones

- Métricas relevantes

Versiones del motor admitidas

Esta información es compatible con todas las versiones de RDS para PostgreSQL.

Context

Una transacción en el estado `idle in transaction` puede contener bloqueos que bloqueen otras consultas. También puede evitar que `VACUUM` (incluido autovacuum) limpie las filas inactivas, lo que provoca una sobrecarga de índices o tablas o un resumen de los ID de transacciones.

Causas probables de este problema

Una transacción iniciada en una sesión interactiva con BEGIN o START TRANSACTION no ha finalizado con los comandos COMMIT, ROLLBACK o END. Esto hace que la transacción pase al estado `idle in transaction`.

Acciones

Para encontrar transacciones inactivas, consulte `pg_stat_activity`.

En su cliente SQL, ejecute la siguiente consulta para ver todas las conexiones en el estado `idle in transaction` y ordenarlas por duración:

```
SELECT now() - state_change as idle_in_transaction_duration, now() - xact_start as
 xact_duration,*
FROM  pg_stat_activity
WHERE state  = 'idle in transaction'
AND   xact_start is not null
ORDER BY 1 DESC;
```

Recomendamos diferentes acciones en función de las causas.

Temas

- Finalización de la transacción
- Finalización de la conexión
- Configure el parámetro idle_in_transaction_session_timeout
- Compruebe el estado AUTOCOMMIT

- Compruebe la lógica de la transacción en el código de su aplicación

Finalización de la transacción

Al iniciar una transacción en una sesión interactiva con BEGIN o START TRANSACTION, esta pasa al estado `idle in transaction`. Permanecerá en este estado hasta que finalice la transacción al emitir los comandos COMMIT, ROLLBACK, END o hasta que finalice la conexión por completo para revertir la transacción.

Finalización de la conexión

Finalice la conexión con una transacción inactiva mediante la siguiente consulta:

```
SELECT pg_terminate_backend(pid);
```

pid es el ID del proceso de la conexión.

Configure el parámetro idle_in_transaction_session_timeout

Configure el parámetro `idle_in_transaction_session_timeout` en el grupo de parámetros. La ventaja de configurar este parámetro es que no requiere una intervención manual para finalizar el periodo de inactividad prolongado de la transacción. Para obtener más información sobre este parámetro, consulte la documentación de PostgreSQL.

El siguiente mensaje aparecerá en el archivo de registro de PostgreSQL una vez finalizada la conexión y cuando haya una transacción en el estado idle_in_transaction durante más tiempo del especificado.

```
FATAL: terminating connection due to idle in transaction timeout
```

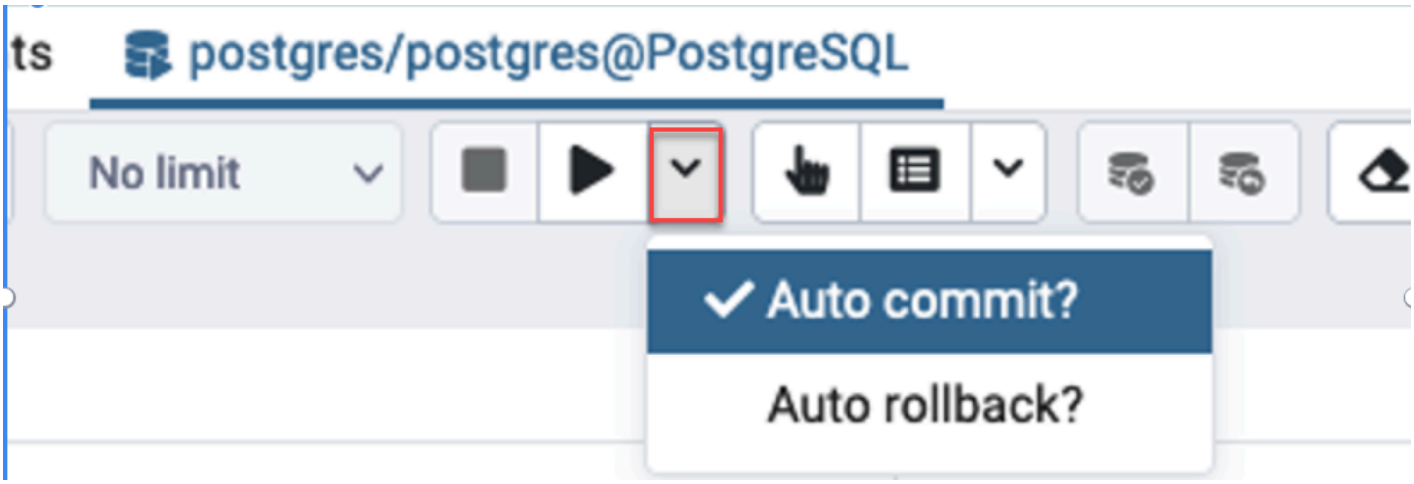
Compruebe el estado AUTOCOMMIT

AUTOCOMMIT está activado de forma predeterminada. Pero si se desactiva accidentalmente en el cliente, asegúrese de volver a activarlo.

- En su cliente psql, ejecute el siguiente comando:

```
postgres=> \set AUTOCOMMIT on
```

- En pgadmin, para activarlo, seleccione la opción AUTOCOMMIT en la flecha hacia abajo.



Compruebe la lógica de la transacción en el código de su aplicación

Investigue la lógica de su aplicación para detectar posibles problemas. Considere las siguientes acciones:

- Compruebe si la confirmación automática de JDBC está activada en su aplicación. Además, considere la posibilidad de usar comandos `COMMIT` explícitos en su código.
- Compruebe su lógica de gestión de errores para ver si cierra una transacción después de que se produzcan errores.
- Compruebe si su aplicación tarda mucho en procesar las filas devueltas por una consulta mientras la transacción está abierta. Si es así, considere la posibilidad de programar la aplicación para que cierre la transacción antes de procesar las filas.
- Compruebe si una transacción contiene muchas operaciones de larga duración. Si es así, divida una sola transacción en varias transacciones.

Métricas relevantes

Las siguientes métricas de PI están relacionadas con esta información:

- idle_in_transaction_count: número de sesiones en el estado `idle in transaction`.
- idle_in_transaction_max_time: la duración de la transacción en ejecución de más larga duración en el estado `idle in transaction`.

Uso de extensiones PostgreSQL con Amazon RDS para PostgreSQL

Puede ampliar la funcionalidad de PostgreSQL instalando una variedad de extensiones y módulos. Por ejemplo, para trabajar con datos espaciales, puede instalar y utilizar la extensión de PostGIS. Para obtener más información, consulte Administración de datos espaciales con la extensión PostGIS. Otro ejemplo, si desea mejorar la entrada de datos para tablas muy grandes, puede considerar la posibilidad de particionar los datos con la extensión `pg_partman`. Para obtener más información, consulte Administración de las particiones de PostgreSQL con la extensión pg_partman.

> **Note**
>
> RDS para PostgreSQL admite extensiones de lenguaje de confianza para PostgreSQL a través de la extensión `pg_tle`, que puede agregar a la instancia de base de datos. Con esta extensión, los desarrolladores pueden crear sus propias extensiones de PostgreSQL en un entorno seguro que simplifica los requisitos de instalación y configuración. Para obtener información sobre las versiones de RDS para PostgreSQL que admiten la extensión `pg_tle` y para más detalles, consulte Uso de Extensiones de lenguaje de confianza para PostgreSQL.

En algunos casos, en lugar de instalar una extensión, puede agregar un módulo específico a la lista de `shared_preload_libraries` en el grupo de parámetros de la base de datos personalizado de la instancia de base de datos de RDS para PostgreSQL. Por lo general, el grupo de parámetros del clúster de base de datos predeterminado solo carga las `pg_stat_statements`, pero hay varios otros módulos disponibles para agregarlos a la lista. Por ejemplo, puede añadir la capacidad de programación añadiendo el módulo`pg_cron`, tal como se detalla en Programación de mantenimiento con la extensión pg_cron de PostgreSQL. Como otro ejemplo, puede registrar los planes de ejecución de consultas cargando el módulo `auto_explain`. Para obtener más información, consulte Logging execution plans of queries (Registro de los planes de ejecución de las consultas) en el centro de conocimiento de AWS.

Según la versión de RDS para PostgreSQL, la instalación de una extensión podría requerir permisos `rds_superuser`, de la siguiente forma:

- Para versiones 12 y anteriores de RDS para PostgreSQL, la instalación de extensiones requiere privilegios de `rds_superuser`.

- Para la versión 13 y superiores de RDS para PostgreSQL , los usuarios (roles) con permisos de creación en una instancia de base de datos determinada pueden instalar y utilizar cualquier extensión de confianza. Para obtener una lista de las extensiones de confianza, consulte Extensiones de confianza de PostgreSQL.

También puede especificar con precisión qué extensiones se pueden instalar en la instancia de base de datos de RDS para PostgreSQL, enumerándolas en el parámetro `rds.allowed_extensions`. Para obtener más información, consulte Restringir la instalación de extensiones de PostgreSQL.

Para obtener más información acerca del rol `rds_superuser`, consulte Descripción de los roles y permisos de PostgreSQL.

Temas

- Uso de las funciones de la extensión orafce
- Uso de la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL
- Administración de las particiones de PostgreSQL con la extensión pg_partman
- Uso de pgAudit para registrar la actividad de la base de datos
- Programación de mantenimiento con la extensión pg_cron de PostgreSQL
- Uso de pglogical para sincronizar datos entre instancias
- Uso de pgactive para admitir la replicación activa-activa
- Reducción de la sobrecarga en tablas e índices con la extensión pg_repack
- Actualización y uso de la extensión PLV8
- Uso de PL/Rust para escribir funciones de PostgreSQL en lenguaje Rust
- Administración de datos espaciales con la extensión PostGIS

Uso de las funciones de la extensión orafce

La extensión orafce brinda funciones y operadores que emulan un subconjunto de funciones y paquetes de una base de datos de Oracle. La extensión orafce facilita la realización de la portabilidad de una aplicación Oracle a PostgreSQL. Esta extensión es compatible con la versión 9.6.6 y posteriores de RDS for PostgreSQL. Para obtener más información sobre orafce, consulte orafce en GitHub.

> **Note**
>
> RDS for PostgreSQL no admite el paquete `utl_file` que forma parte de la extensión orafce. Esto se debe a que las funciones del esquema `utl_file` proporcionan operaciones de lectura y escritura con archivos de texto del sistema operativo, lo que requiere el acceso de los superusuarios al host subyacente. Como servicio administrado, RDS for PostgreSQL no brinda acceso al host.

Para usar la extensión orafce

1. Conéctese a la instancia de base de datos con el nombre de usuario principal que utilizó para crear la instancia de base de datos.

   Si desea activar orafce para una base de datos diferente en la misma instancia de base de datos, utilice el comando psql `/c dbname`. Con este comando, cambia de la base de datos principal después de iniciar la conexión.
2. Active la extensión orafce con la instrucción `CREATE EXTENSION`.

   ```
   CREATE EXTENSION orafce;
   ```
3. Transfiera la propiedad del esquema de Oracle al rol rds_superuser con la instrucción `ALTER SCHEMA`.

   ```
   ALTER SCHEMA oracle OWNER TO rds_superuser;
   ```

   Si desea ver la lista de propietarios del esquema de Oracle, utilice el comando `\dn` de psql.

Uso de la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL

Al utilizar la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL, puede delegar la administración de la extensión a un usuario que no necesita ser un `rds_superuser`. Con esta compatibilidad de extensiones delegadas, se crea un nuevo rol denominado `rds_extension` que debe asignarse a un usuario para que administre otras extensiones. Este rol puede crear, actualizar y eliminar extensiones.

Puede especificar qué extensiones se pueden instalar en la instancia de base de datos de RDS enumerándolas en el parámetro `rds.allowed_extensions`. Para obtener más información, consulte Uso de extensiones PostgreSQL con Amazon RDS para PostgreSQL.

Puede restringir la lista de extensiones disponibles que el usuario puede administrar con el rol `rds_extension` utilizando el parámetro `rds.allowed_delegated_extensions`.

La compatibilidad de extensiones delegadas está disponible en las siguientes versiones:

- Todas las versiones superiores
- Versión 16.4 y otras versiones 16 superiores
- Versión 15.8 y otras versiones 15 superiores
- Versión 14.13 y otras versiones 14 superiores
- Versión 13.16 y otras versiones 13 superiores
- Versión 12.20 y otras versiones 12 superiores

Temas

- Activación de la compatibilidad con extensiones delegadas a un usuario
- Configuración utilizada en la compatibilidad de extensiones delegadas de RDS para PostgreSQL
- Desactivar la compatibilidad para la extensión delegada
- Ventajas del uso de la compatibilidad de extensiones delegadas de Amazon RDS
- Limitación de la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL
- Permisos necesarios para determinadas extensiones
- Consideraciones de seguridad
- Eliminación de extensión en cascada deshabilitada

- Ejemplos de extensiones que se pueden agregar mediante la compatibilidad de extensiones delegadas

Activación de la compatibilidad con extensiones delegadas a un usuario

Debe realizar lo siguiente para habilitar la compatibilidad con extensiones delegadas en un usuario:

1. Otorgar el rol **`rds_extension`** a un usuario: conéctese a la base de datos como `rds_superuser` y ejecute el siguiente comando:

```
Postgres => grant rds_extension to user_name;
```

2. Defina la lista de extensiones disponibles para que las administren los usuarios delegados: `rds.allowed_delegated_extensions` permite especificar un subconjunto de las extensiones disponibles utilizando `rds.allowed_extensions` en el parámetro del clúster de base de datos. Puede realizar esto en uno de los siguientes niveles:

   - En el clúster o en el grupo de parámetros de la instancia, a través de la AWS Management Console o la API. Para obtener más información, consulte Grupos de parámetros para Amazon RDS.
   - Use el siguiente comando en el nivel de la base de datos:

```
alter database database_name set rds.allowed_delegated_extensions =
 'extension_name_1,
                   extension_name_2,...extension_name_n';
```

   - Use el siguiente comando en el nivel de usuario:

```
alter user user_name set rds.allowed_delegated_extensions = 'extension_name_1,
                   extension_name_2,...extension_name_n';
```

   > **Note**
   >
   > No es necesario reiniciar la base de datos después de cambiar el parámetro dinámico `rds.allowed_delegated_extensions`.

3. Permita el acceso del usuario delegado a los objetos creados durante el proceso de creación de la extensión: algunas extensiones crean objetos que requieren la concesión de permisos

adicionales antes de que el usuario con el rol `rds_extension` pueda acceder a ellos. El `rds_superuser` debe conceder al usuario delegado acceso a esos objetos. Una de las opciones es utilizar un desencadenador de eventos para conceder automáticamente el permiso al usuario delegado. Para obtener más información, consulte el ejemplo de desencadenador de eventos en Desactivar la compatibilidad para la extensión delegada.

Configuración utilizada en la compatibilidad de extensiones delegadas de RDS para PostgreSQL

Nombre de la configuración	Descripción	Valor predeterminado	Notas	Quién puede modificar o conceder el permiso
`rds.allowed_delegated_extensions`	Este parámetro limita las extensiones que un rol de rds_extension puede administrar en una base de datos. Debe ser un subconjunto de rds.allowed_extensions.	empty string	• De forma predeterminada, este parámetro es una cadena vacía, lo que significa que no se ha delegado ninguna extensión a los usuarios con `rds_extension` . • Se puede agregar cualquier extensión compatible si el usuario tiene permisos para hacerlo. Para ello, establezca el parámetro `rds.allow`	rds_superuser

Nombre de la configuración	Descripción	Valor predeterminado	Notas	Quién puede modificar o conceder el permiso
			`ed_delegated_extensions` en una cadena de nombres de extensión separados por comas. Al agregar una lista de extensiones a este parámetro, identifica explícitamente las extensiones que puede instalar el usuario con el rol `rds_extension`. • Si se establece en `*`, significa que todas las extensiones que aparecen en `rds_allowed_extensions` se delegan a los usuarios con el rol `rds_extension`.	

Nombre de la configuración	Descripción	Valor predeterminado	Notas	Quién puede modificar o conceder el permiso
			Para obtener más información sobre la configuración de este parámetro, consulte Activación de la compatibilidad con extensiones delegadas a un usuario.	
`rds.allowed_extensions`	Este parámetro permite que un cliente limite las extensiones que se pueden instalar en la instancia de base de datos de RDS. Para obtener más información, consulte Restringir la instalación de extensiones de PostgreSQL.	"*"	De forma predeterminada, este parámetro está establecido en “*”, lo que significa que los usuarios con los privilegios necesarios pueden crear todas las extensiones compatibles con RDS para PostgreSQL y Aurora PostgreSQL. Vacío significa que no se pueden instalar extensiones en la instancia de base de datos de RDS.	administrator

Nombre de la configuración	Descripción	Valor predeterminado	Notas	Quién puede modificar o conceder el permiso
`rds.delegated_extension_allow_drop_cascade`	Este parámetro controla la capacidad del usuario con `rds_extension` de eliminar la extensión mediante una opción en cascada.	off	De forma predeterminada, `rds.delegated_extension_allow_drop_cascade` está establecido en `off`. Esto significa que los usuarios con `rds_extension` no pueden eliminar una extensión mediante la opción en cascada. Para otorgar esa habilidad, el parámetro `rds.delegated_extension_allow_drop_cascade` debe configurarse como on.	rds_superuser

Desactivar la compatibilidad para la extensión delegada

Desactivación parcial

Los usuarios delegados no pueden crear nuevas extensiones, pero sí pueden actualizar las existentes.

- Restablece `rds.allowed_delegated_extensions` al valor predeterminado en el grupo de parámetros del clúster de base de datos.
- Use el siguiente comando en el nivel de la base de datos:

```
alter database database_name reset rds.allowed_delegated_extensions;
```

- Use el siguiente comando en el nivel de usuario:

```
alter user user_name reset rds.allowed_delegated_extensions;
```

Desactivación completa

Al revocar el rol `rds_extension` de un usuario, el usuario recuperará los permisos estándar. El usuario ya no puede crear, actualizar ni eliminar extensiones.

```
postgres => revoke rds_extension from user_name;
```

Ejemplo de desencadenador de eventos

Si desea permitir que un usuario delegado con `rds_extension` utilice extensiones que requieran configurar permisos en los objetos creados al crear la extensión, puede personalizar el siguiente ejemplo de un desencadenador de eventos y agregar solo las extensiones para las que desee que los usuarios delegados tengan acceso a todas las funciones. Este activador de eventos se puede crear en la plantilla 1 (la plantilla predeterminada), por lo que todas las bases de datos creadas a partir de la plantilla 1 tendrán ese desencadenador de eventos. Cuando un usuario delegado instala la extensión, este desencadenador otorgará automáticamente la propiedad de los objetos creados por la extensión.

```
CREATE OR REPLACE FUNCTION create_ext()

  RETURNS event_trigger AS $$

DECLARE

  schemaname TEXT;
  databaseowner TEXT;

  r RECORD;
```

```
BEGIN

  IF tg_tag = 'CREATE EXTENSION' and current_user != 'rds_superuser' THEN
    RAISE NOTICE 'SECURITY INVOKER';
    RAISE NOTICE 'user: %', current_user;
    FOR r IN SELECT * FROM pg_event_trigger_ddl_commands()
    LOOP
        CONTINUE WHEN r.command_tag != 'CREATE EXTENSION' OR r.object_type !=
 'extension';

        schemaname = (
            SELECT n.nspname
            FROM pg_catalog.pg_extension AS e
            INNER JOIN pg_catalog.pg_namespace AS n
            ON e.extnamespace = n.oid
            WHERE e.oid = r.objid
        );

        databaseowner = (
            SELECT pg_catalog.pg_get_userbyid(d.datdba)
            FROM pg_catalog.pg_database d
            WHERE d.datname = current_database()
        );
        RAISE NOTICE 'Record for event trigger %, objid: %,tag: %, current_user: %,
 schema: %, database_owenr: %', r.object_identity, r.objid, tg_tag, current_user,
 schemaname, databaseowner;
        IF r.object_identity = 'address_standardizer_data_us' THEN
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE %I.us_gaz TO
 %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE %I.us_lex TO
 %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE %I.us_rules
 TO %I WITH GRANT OPTION;', schemaname, databaseowner);
        ELSIF r.object_identity = 'dict_int' THEN
            EXECUTE format('ALTER TEXT SEARCH DICTIONARY %I.intdict OWNER TO %I;',
 schemaname, databaseowner);
        ELSIF r.object_identity = 'pg_partman' THEN
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE
 %I.part_config TO %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE
 %I.part_config_sub TO %I WITH GRANT OPTION;', schemaname, databaseowner);
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON TABLE
 %I.custom_time_partitions TO %I WITH GRANT OPTION;', schemaname, databaseowner);
```

```
        ELSIF r.object_identity = 'postgis_topology' THEN
            EXECUTE format('GRANT SELECT, UPDATE, INSERT, DELETE ON ALL TABLES IN
 SCHEMA topology TO %I WITH GRANT OPTION;', databaseowner);
            EXECUTE format('GRANT USAGE, SELECT ON ALL SEQUENCES IN SCHEMA topology TO
 %I WITH GRANT OPTION;', databaseowner);
            EXECUTE format('GRANT EXECUTE ON ALL FUNCTIONS IN SCHEMA topology TO %I
 WITH GRANT OPTION;', databaseowner);
            EXECUTE format('GRANT USAGE ON SCHEMA topology TO %I WITH GRANT OPTION;',
 databaseowner);
        END IF;
    END LOOP;
  END IF;
END;
$$ LANGUAGE plpgsql SECURITY DEFINER;

CREATE EVENT TRIGGER log_create_ext ON ddl_command_end EXECUTE PROCEDURE create_ext();
```

Ventajas del uso de la compatibilidad de extensiones delegadas de Amazon RDS

Al utilizar la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL, delega de forma segura la administración de la extensión a los usuarios que no tengan el rol `rds_superuser`. Esta característica proporciona los siguientes beneficios:

- Puede delegar fácilmente la administración de extensiones a los usuarios de su elección.
- Esto no requiere el rol `rds_superuser`.
- Ofrece la posibilidad de admitir diferentes conjuntos de extensiones para diferentes bases de datos en el mismo clúster de base de datos.

Limitación de la compatibilidad de extensiones delegadas de Amazon RDS para PostgreSQL

- Los objetos creados durante el proceso de creación de la extensión pueden requerir privilegios adicionales para que la extensión funcione correctamente.
- De forma predeterminada, hay algunas extensiones que el usuario de la extensión delegada no puede administrar, como `log_fdw`, `pg_cron`, `pg_tle`, `pgactive`, `pglogical`, `postgis_raster`, `postgis_tiger_geocoder`, `postgis_topology`.

Permisos necesarios para determinadas extensiones

Para crear, usar o actualizar las siguientes extensiones, el usuario delegado debe tener los privilegios necesarios en las siguientes funciones, tablas y esquemas.

Exter es que nece propi o perm	Función	Tablas	Esquema	Diccionario de búsqueda de texto	Comentario
addre tanda er_da s	Ninguno	us_gaz, us_lex, us_lex, l.us_rules	Ninguno	Ninguno	Ninguno
amch	bt_index_check, bt_index_ parent_check	Ninguno	Ninguno	Ninguno	Ninguno
dict_i	Ninguno	Ninguno	Ninguno	intdict	Ninguno
pg_p n	Ninguno	custom_ti me_partitions, part_config, part_config_sub	Ninguno	Ninguno	Ninguno
pg_st tatem	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
Post(	st_tileenvelope	spatial_ref_sys	Ninguno	Ninguno	Ninguno
postg aster	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
postg opolo	Ninguno	topology, layer	topology	Ninguno	el usuario delegado debe

Exter es que nece propi o perm	Función	Tablas	Esquema	Diccionario de búsqueda de texto	Comentario
					ser el propietar io de la base de datos
log_f	create_fo reign_tab le_for_log_file	Ninguno	Ninguno	Ninguno	Ninguno
rds_t	role_pass word_encr yption_type	Ninguno	Ninguno	Ninguno	Ninguno
postg iger_ oder	Ninguno	geocode_s ettings_default, geocode_s ettings	tiger	Ninguno	Ninguno
pg_fr acem	pg_freespace	Ninguno	Ninguno	Ninguno	Ninguno
pg_vi lity	pg_visibility	Ninguno	Ninguno	Ninguno	Ninguno

Consideraciones de seguridad

Tenga en cuenta que un usuario con el rol `rds_extension` podrá administrar las extensiones en todas las bases de datos en las que tenga el privilegio de conexión. Si la intención es que un usuario delegado administre la extensión en una única base de datos, una práctica recomendada consiste en revocar todos los privilegios del público en cada base de datos y, a continuación, conceder de forma explícita el privilegio de conexión para esa base de datos específica al usuario delegado.

Existen varias extensiones que permiten a un usuario acceder a la información de varias bases de datos. Asegúrese de que los usuarios a los que conceda `rds_extension` tengan capacidades para múltiples bases de datos antes de agregar estas extensiones a `rds.allowed_delegated_extensions`. Por ejemplo, `postgres_fdw` y `dblink` proporcionan la funcionalidad de realizar consultas en todas las bases de datos de la misma instancia o de instancias remotas. `log_fdw` lee los archivos de registro del motor postgres, que son de todas las bases de datos de la instancia, y pueden contener consultas lentas o mensajes de error de varias bases de datos. `pg_cron` permite ejecutar trabajos en segundo plano programados en la instancia de base de datos y puede configurar los trabajos para que se ejecuten en una base de datos diferente.

Eliminación de extensión en cascada deshabilitada

La posibilidad de eliminar la extensión con la opción en cascada por parte de un usuario con el rol `rds_extension` la controla el parámetro `rds.delegated_extension_allow_drop_cascade`. De forma predeterminada, `rds-delegated_extension_allow_drop_cascade` está establecido en `off`. Esto significa que los usuarios con el tol `rds_extension` no pueden eliminar una extensión mediante la opción en cascada como se muestra en la siguiente consulta.

```
DROP EXTENSION CASCADE;
```

Esto eliminará automáticamente los objetos que dependan de la extensión y, a su vez, todos los objetos que dependan de esos objetos. El intento de utilizar la opción en cascada generará un error.

Para otorgar esa habilidad, el parámetro `rds.delegated_extension_allow_drop_cascade` debe configurarse como on.

Cambiar el parámetro dinámico `rds.delegated_extension_allow_drop_cascade` no requiere un reinicio de la base de datos. Puede realizar esto en uno de los siguientes niveles:

- En el clúster o en el grupo de parámetros de la instancia, a través de la AWS Management Console o la API.
- Con el siguiente comando en el nivel de la base de datos:

  ```
  alter database database_name set rds.delegated_extension_allow_drop_cascade = 'on';
  ```

- Con el siguiente comando en el nivel de usuario:

  ```
  alter role tenant_user set rds.delegated_extension_allow_drop_cascade = 'on';
  ```

Ejemplos de extensiones que se pueden agregar mediante la compatibilidad de extensiones delegadas

- rds_tools

```
extension_test_db=> create extension rds_tools;
CREATE EXTENSION
extension_test_db=> SELECT * from rds_tools.role_password_encryption_type() where
 rolname = 'pg_read_server_files';
ERROR: permission denied for function role_password_encryption_type
```

- amcheck

```
extension_test_db=> CREATE TABLE amcheck_test (id int);
CREATE TABLE
extension_test_db=> INSERT INTO amcheck_test VALUES (generate_series(1,100000));
INSERT 0 100000
extension_test_db=> CREATE INDEX amcheck_test_btree_idx ON amcheck_test USING btree
 (id);
CREATE INDEX
extension_test_db=> create extension amcheck;
CREATE EXTENSION
extension_test_db=> SELECT bt_index_check('amcheck_test_btree_idx'::regclass);
ERROR: permission denied for function bt_index_check
extension_test_db=> SELECT bt_index_parent_check('amcheck_test_btree_idx'::regclass);
ERROR: permission denied for function bt_index_parent_check
```

- pg_freespacemap

```
extension_test_db=> create extension pg_freespacemap;
CREATE EXTENSION
extension_test_db=> SELECT * FROM pg_freespace('pg_authid');
ERROR: permission denied for function pg_freespace
extension_test_db=> SELECT * FROM pg_freespace('pg_authid',0);
ERROR: permission denied for function pg_freespace
```

- pg_visibility

```
extension_test_db=> create extension pg_visibility;
CREATE EXTENSION
extension_test_db=> select * from pg_visibility('pg_database'::regclass);
ERROR: permission denied for function pg_visibility
```

- postgres_fdw

```
extension_test_db=> create extension postgres_fdw;
CREATE EXTENSION
extension_test_db=> create server myserver foreign data wrapper postgres_fdw options
 (host 'foo', dbname 'foodb', port '5432');
ERROR: permission denied for foreign-data wrapper postgres_fdw
```

Administración de las particiones de PostgreSQL con la extensión pg_partman

Las particiones de tablas de PostgreSQL proporcionan un marco para el manejo de alto rendimiento de la entrada de datos y la generación de informes. Utilice particiones para bases de datos que requieren una entrada muy rápida de grandes cantidades de datos. Las particiones también proporcionan consultas más rápidas de tablas grandes. Las particiones ayudan a mantener los datos sin afectar la instancia de base de datos porque requiere menos recursos de E/S.

Mediante el uso de particiones, puede dividir los datos en fragmentos de tamaño personalizado para su procesamiento. Por ejemplo, puede dividir datos de series temporales para rangos como por hora, por día, por semana, por mes, por trimestre, por año, personalizados o cualquier combinación de estos. Para un ejemplo de datos de series temporales, si divide la tabla por hora, cada partición contiene una hora de datos. Si divide la tabla de series temporales por día, las particiones contienen datos de un día, y así sucesivamente. La clave de partición controla el tamaño de una partición.

Cuando se utiliza un comando `INSERT` o `UPDATE` de SQL en una tabla particionada, el motor de base de datos enruta los datos a la partición adecuada. Las particiones de tablas de PostgreSQL que almacenan los datos son tablas secundarias de la tabla principal.

Durante las lecturas de consultas de la base de datos, el optimizador de PostgreSQL analiza la cláusula `WHERE` de la consulta y, si es posible, dirige el análisis de la base de datos solo a las particiones relevantes.

A partir de la versión 10, PostgreSQL utiliza particiones declarativas para implementar particiones de tablas. Esto también se conoce como particionado PostgreSQL nativo. Antes de PostgreSQL versión 10, usaba desencadenadores para implementar particiones.

Las particiones de tablas de PostgreSQL proporcionan las siguientes características:

- Creación de nuevas particiones en cualquier momento.
- Rangos de particiones variables.
- Particiones desmontables y reconectables mediante instrucciones de lenguaje de definición de datos (DDL).

  Por ejemplo, las particiones desmontables son útiles para eliminar datos históricos de la partición principal, pero mantienen los datos históricos para su análisis.
- Las nuevas particiones heredan las propiedades de la tabla de base de datos principal, incluidas las siguientes:

  - Índices
  - Claves principales, que deben incluir la columna de la clave de partición
  - Claves externas
  - Restricciones de comprobación
  - Referencias
- creación de índices para la tabla completa o cada partición específica

No se puede modificar el esquema de una partición individual. Sin embargo, se puede modificar la tabla principal (como agregar una nueva columna), que se propaga a las particiones.

Temas

- Información general de la extensión pg_partman de PostgreSQL
- Habilitación de la extensión pg_partman
- Configuración de particiones mediante la función create_parent
- Configuración del mantenimiento de particiones mediante la función run_maintenance_proc

Información general de la extensión pg_partman de PostgreSQL

Puede utilizar la extensión `pg_partman` de PostgreSQL para automatizar la creación y el mantenimiento de las particiones de tablas. Para obtener más información general, consulte PG Partition Manager en la documentación de `pg_partman`.

> **Note**
>
> La extensión `pg_partman` es compatible con las versiones 12.5 y posteriores de RDS for PostgreSQL.

En lugar de tener que crear manualmente cada partición, configure `pg_partman` con las siguientes opciones:

- Tabla que se dividirá
- Tipo de partición
- Clave de partición
- Grado de detalle de la partición

- Opciones de precreación y administración de particiones

Después de crear una tabla con particiones de PostgreSQL, la registra con `pg_partman` al llamar a la función `create_parent`. Al hacerlo, se crean las particiones necesarias en función de los parámetros que pase a la función.

La extensión `pg_partman` también proporciona la función `run_maintenance_proc`, que puede ejecutarse de forma programada para administrar automáticamente las particiones. Para asegurarse de que se creen las particiones apropiadas según sea necesario, programe esta función para que se ejecute periódicamente (por ejemplo, por hora). También puede asegurarse de que las particiones se eliminen automáticamente.

Habilitación de la extensión pg_partman

Si tiene varias bases de datos dentro de la misma instancia de base de dato de PostgreSQL para la que desea administrar particiones, debe habilitar la extensión `pg_partman` por separado para cada base de datos. Para habilitar la extensión `pg_partman` para una base de datos específica, cree el esquema de mantenimiento de particiones y, después, cree la extensión `pg_partman` de la siguiente manera:

```
CREATE SCHEMA partman;
CREATE EXTENSION pg_partman WITH SCHEMA partman;
```

> **Note**
>
> Para crear la extensión `pg_partman`, asegúrese de tener privilegios `rds_superuser`.

Si recibe un error como el siguiente, conceda los privilegios `rds_superuser` a la cuenta o utilice su cuenta de superusuario.

```
ERROR: permission denied to create extension "pg_partman"
HINT: Must be superuser to create this extension.
```

Para conceder privilegios `rds_superuser`, conéctese con su cuenta de superusuario y ejecute el siguiente comando:

```
GRANT rds_superuser TO user-or-role;
```

Para los ejemplos que muestran el uso de la extensión pg_partman, utilizamos la siguiente tabla de base de datos y partición de muestra. Esta base de datos utiliza una tabla particionada basada en una marca temporal. Un esquema `data_mart` contiene una tabla denominada `events` con una columna denominada `created_at`. En la `events` tabla se incluyen los siguientes ajustes:

- Claves primarias `event_id` y `created_at`, que deben tener la columna utilizada para guiar la partición.
- Una restricción de comprobación `ck_valid_operation` para aplicar los valores para una columna de la tabla `operation`.
- Dos claves externas, donde una (`fk_orga_membership`) apunta a la tabla externa `organization` y la otra (`fk_parent_event_id`) es una clave externa con referencia propia.
- Dos índices, donde uno (`idx_org_id`) es para la clave externa y el otro (`idx_event_type`) es para el tipo de evento.

Las siguientes instrucciones DDL crean estos objetos, que se incluyen automáticamente en cada partición.

```
CREATE SCHEMA data_mart;
CREATE TABLE data_mart.organization ( org_id BIGSERIAL,
        org_name TEXT,
        CONSTRAINT pk_organization PRIMARY KEY (org_id)
    );

CREATE TABLE data_mart.events(
        event_id        BIGSERIAL,
        operation       CHAR(1),
        value           FLOAT(24),
        parent_event_id BIGINT,
        event_type      VARCHAR(25),
        org_id          BIGSERIAL,
        created_at      timestamp,
        CONSTRAINT pk_data_mart_event PRIMARY KEY (event_id, created_at),
        CONSTRAINT ck_valid_operation CHECK (operation = 'C' OR operation = 'D'),
        CONSTRAINT fk_orga_membership
            FOREIGN KEY(org_id)
            REFERENCES data_mart.organization (org_id),
        CONSTRAINT fk_parent_event_id
            FOREIGN KEY(parent_event_id, created_at)
            REFERENCES data_mart.events (event_id,created_at)
    ) PARTITION BY RANGE (created_at);
```

```
CREATE INDEX idx_org_id     ON  data_mart.events(org_id);
CREATE INDEX idx_event_type ON  data_mart.events(event_type);
```

Configuración de particiones mediante la función create_parent

Después de habilitar la extensión `pg_partman`, utilice la función `create_parent` para configurar las particiones dentro del esquema de mantenimiento de particiones. En este ejemplo se utiliza el ejemplo de la tabla `events` creado en Habilitación de la extensión pg_partman. Ejecute la función `create_parent` de la siguiente manera:

```
SELECT partman.create_parent(
 p_parent_table => 'data_mart.events',
 p_control      => 'created_at',
 p_type         => 'range',
 p_interval     => '1 day',
 p_premake      => 30);
```

Los parámetros son los siguientes:

- `p_parent_table` – La tabla principal particionada. Esta tabla ya debe existir y estar totalmente cualificada, incluido el esquema.
- `p_control` – La columna en la que se basará la partición. El tipo de datos debe ser entero o basado en el tiempo.
- `p_type`: el tipo es `'range'` o `'list'`.
- `p_interval` – El intervalo de tiempo o intervalo de enteros para cada partición. Los valores de ejemplo incluyen `1 day`, `1 hour`, etc.
- `p_premake` – La cantidad de particiones que se debe crear de antemano para admitir nuevas inserciones.

Para obtener una descripción completa de la función `create_parent`, consulte Funciones de creación en la documentación de `pg_partman`.

Configuración del mantenimiento de particiones mediante la función run_maintenance_proc

Puede ejecutar operaciones de mantenimiento de particiones para crear automáticamente nuevas particiones, desasociar particiones o eliminar particiones antiguas. El mantenimiento de particiones

se basa en la función `run_maintenance_proc` de la extensión `pg_partman` y la extensión `pg_cron`, que inicia un programador interno. El programador `pg_cron` ejecuta automáticamente instrucciones SQL, funciones y procedimientos definidos en las bases de datos.

En el ejemplo siguiente se utiliza el ejemplo de la tabla `events` creado en Habilitación de la extensión pg_partman para establecer que las operaciones de mantenimiento de particiones se ejecuten automáticamente. Como requisito previo, agregue `pg_cron` al parámetro `shared_preload_libraries` en el grupo de parámetros de la instancia de base de datos.

```
CREATE EXTENSION pg_cron;

UPDATE partman.part_config
SET infinite_time_partitions = true,
    retention = '3 months',
    retention_keep_table=true
WHERE parent_table = 'data_mart.events';
SELECT cron.schedule('@hourly', $$CALL partman.run_maintenance_proc()$$);
```

A continuación, puede encontrar una explicación paso a paso del ejemplo anterior:

1. Modifique el grupo de parámetros asociado a la instancia de base de datos y agregue `pg_cron` al valor del parámetro `shared_preload_libraries`. Este cambio requiere un reinicio de la instancia de base de datos para que surta efecto. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.
2. Ejecute el comando `CREATE EXTENSION pg_cron;` con una cuenta que tenga los permisos `rds_superuser`. Esto habilita la extensión `pg_cron`. Para obtener más información, consulte Programación de mantenimiento con la extensión pg_cron de PostgreSQL.
3. Ejecute el comando `UPDATE partman.part_config` para ajustar la configuración de `pg_partman` para la tabla `data_mart.events`.
4. Ejecute el comando `SET . . .` para configurar la tabla `data_mart.events`, con estas cláusulas:
   a. `infinite_time_partitions = true,` – Configura la tabla para que pueda crear automáticamente nuevas particiones sin ningún límite.
   b. `retention = '3 months',` – Configura la tabla para que tenga una retención máxima de tres meses.
   c. `retention_keep_table=true` – Configura la tabla para que cuando venza el periodo de retención, la tabla no se elimine automáticamente. En su lugar, las particiones que son anteriores al periodo de retención solo se separan de la tabla principal.

5. Ejecute el comando `SELECT cron.schedule . . .` para hacer una llamada a la función `pg_cron`. Esta llamada define la frecuencia con la que el programador ejecuta el procedimiento de mantenimiento de `pg_partman`, `partman.run_maintenance_proc`. Para este ejemplo, el procedimiento se ejecuta cada hora.

Para obtener una descripción completa de la función `run_maintenance_proc`, consulte Funciones de mantenimiento en la documentación de `pg_partman`.

Uso de pgAudit para registrar la actividad de la base de datos

Las instituciones financieras, las agencias gubernamentales y muchas industrias necesitan mantener registros de auditoría para cumplir con los requisitos reglamentarios. Al utilizar la extensión de auditoría de PostgreSQL (PGAudit) con su Instancia de base de datos de RDS for PostgreSQL, puede capturar los registros detallados que suelen necesitar los auditores o para cumplir con los requisitos reglamentarios. Por ejemplo, puede configurar la extensión pgAudit para realizar un seguimiento de los cambios realizados en bases de datos y tablas específicas, para registrar el usuario que realizó el cambio y muchos otros detalles.

La extensión pgAudit se basa en la funcionalidad de la infraestructura de registro nativa de PostgreSQL ampliando los mensajes de registro con más detalle. En otras palabras, utiliza el mismo método para ver el registro de auditoría que para ver cualquier mensaje de registro. Para obtener más información sobre los registros de PostgreSQL, consulte Archivos de registro de bases de datos de RDS para PostgreSQL.

La extensión PGAudit elimina los datos confidenciales, como las contraseñas de texto no cifrado, de los registros. Si su instancia de base de datos de RDS for PostgreSQL está configurado para registrar las instrucciones del lenguaje de manipulación de datos (DML) tal como se detalla en Activación de registro de consultas para su instancia de base de datos de RDS para PostgreSQL, puede evitar el problema de la contraseña de texto sin cifrar mediante la extensión de auditoría de PostgreSQL.

Puede configurar la auditoría en las instancias de la base de datos con un alto grado de especificidad. Puede auditar todas las bases de datos y todos los usuarios. O bien, puede optar por auditar solo determinadas bases de datos, usuarios y otros objetos. También puede excluir explícitamente a determinados usuarios y bases de datos de la auditoría. Para obtener más información, consulte Exclusión de usuarios o bases de datos del registro de auditoría.

Dada la cantidad de detalles que se pueden capturar, le recomendamos que, si usa pgAudit, controle su consumo de almacenamiento.

La extensión pgAudit es compatible con todas las Versiones de RDS para PostgreSQL: Para obtener una lista de las versiones de pgAudit compatibles con la versión de RDS para PostgreSQL, consulte Versiones de extensión para Amazon RDS for PostgreSQL en las Notas de la versión de Amazon RDS for PostgreSQL.

Temas

- Configuración de la extensión pgAudit

- Auditoría de objetos de base de datos
- Exclusión de usuarios o bases de datos del registro de auditoría
- Referencia para la extensión pgAudit

Configuración de la extensión pgAudit

Para configurar la extensión pgAudit en la instancia de base de datos de RDS for PostgreSQL , primero hay que añadir pgAudit a las bibliotecas compartidas en el grupo de parámetros de base de datos personalizado para su instancia de base de datos RDS for PostgreSQL. Para obtener información acerca de cómo crear el grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS. A continuación, instale la extensión pgAudit. Por último, especifique las bases de datos y objetos que desea auditar. Los procedimientos de esta sección le muestran cómo hacerlo. Puede utilizar la AWS Management Console o la AWS CLI.

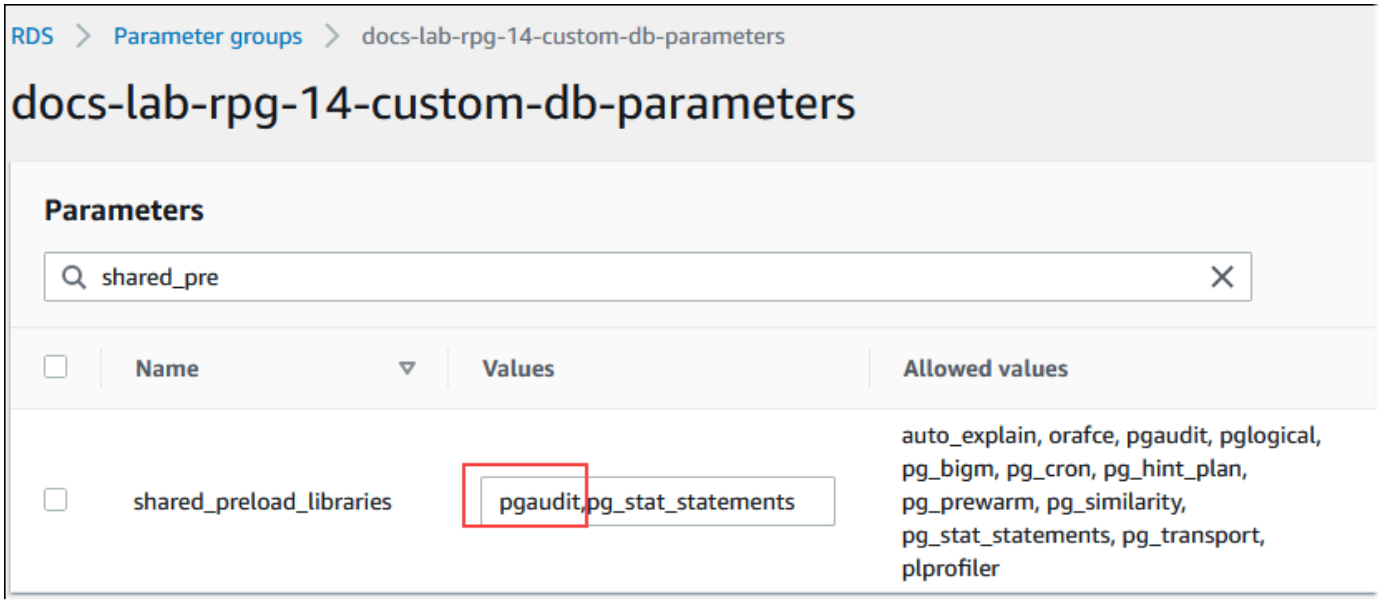
Debe tener permisos como el rol `rds_superuser` para realizar todas estas tareas.

En los pasos siguientes se supone que la instancia de base de datos de RDS for PostgreSQL está asociada a un grupo de parámetros de DB.

Consola

Para configurar la extensión pgAudit

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija la instancia de base de datos de RDS for PostgreSQL.
3. Abra la pestaña Configuration (Configuración) para su Instancia de base de datos RDS para PostgreSQL. Entre los detalles de la instancia, busque el enlace del grupo de parámetros.
4. Elija el enlace para abrir los parámetros personalizados asociados al Instancia de base de datos RDS para PostgreSQL.
5. En el campo de búsqueda Parametes (Parámetros), escriba `shared_pre` para buscar el parámetro `shared_preload_libraries`.
6. Seleccione Edit parameters (Editar parámetros) para acceder a los valores de las propiedades.
7. Añada `pgaudit` a la lista en el campo Values (Valores). Utilice una coma para separar los elementos de la lista de valores.



8. Reinicie la instancia de base de datos de RDS for PostgreSQL para que surta efecto el cambio en el parámetro `shared_preload_libraries`.
9. Cuando la instancia esté disponible, compruebe que pgAudit se haya inicializado. Use `psql` para conectarse a la instancia de base de datos de RDS for PostgreSQL y, a continuación, ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pgaudit
(1 row)
```

10. Con pgAudit inicializado, ahora puede crear la extensión. Debe crear la extensión después de inicializar la biblioteca, ya que la extensión `pgaudit` instala activadores de eventos para auditar las sentencias del lenguaje de definición de datos (DDL).

```
CREATE EXTENSION pgaudit;
```

11. Cierre la sesión de `psql`.

```
labdb=> \q
```

12. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

13. Busque el parámetro `pgaudit.log` en la lista y configúrelo con el valor adecuado para su caso de uso. Por ejemplo, al establecer el parámetro `pgaudit.log` en `write` como se muestra en la siguiente imagen, se capturan las inserciones, las actualizaciones, las eliminaciones y algunos otros tipos de cambios en el registro.



También puede elegir uno de los siguientes valores para el parámetro `pgaudit.log`.

- none: es el valor predeterminado. No se registran cambios en la base de datos.
- all: registra todo (read, write, function, role, ddl, misc).
- ddl: registra todas las instrucciones del lenguaje de definición de datos (DDL) que no están incluidas en la clase `ROLE`.
- function: registra llamadas a funciones y bloques `DO`.
- misc: registra comandos variados como, por ejemplo, `DISCARD`, `FETCH`, `CHECKPOINT`, `VACUUM` y `SET`.
- read: registra `SELECT` y `COPY` cuando el origen es una relación (como una tabla) o una consulta.
- role: registra instrucciones relacionadas con roles y privilegios, como `GRANT`, `REVOKE`, `CREATE ROLE`, `ALTER ROLE` y `DROP ROLE`.
- write: registra `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE` y `COPY` cuando el destino es una relación (tabla).

14. Elija Guardar cambios.
15. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
16. Elija su instancia de base de datos de RDS para PostgreSQL desde la lista de bases de datos.

AWS CLI

Para configurar pgAudit

Para configurar pgAudit mediante AWS CLI, llame a la operación modify-db-parameter-group para modificar los parámetros del registro de auditoría de su grupo de parámetros personalizado, como se muestra en el siguiente procedimiento.

1. Utilice el siguiente comando AWS CLI para añadir `pgaudit` al parámetro `shared_preload_libraries`.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pgaudit,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Utilice el siguiente comando AWS CLI para reiniciar la instancia de base de datos de RDS for PostgreSQL para que se inicialice la biblioteca pgaudit.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

3. Cuando la instancia esté disponible, puede verificar si `pgaudit` se ha inicializado. Use `psql` para conectarse a la instancia de base de datos de RDS for PostgreSQL y, a continuación, ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pgaudit
(1 row)
```

   Con pgAudit inicializado, ahora puede crear la extensión.

```
CREATE EXTENSION pgaudit;
```

4. Cierre la sesión de `psql` para poder utilizar AWS CLI.

```
labdb=> \q
```

5. Utilice el siguiente comando AWS CLI para especificar las clases de instrucciones que desea registrar con el registro de auditoría de sesión. El ejemplo establece el parámetro `pgaudit.log` en`write`, que captura las inserciones, las actualizaciones y las eliminaciones del registro.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=pgaudit.log,ParameterValue=write,ApplyMethod=pending-reboot" \
   --region aws-region
```

También puede elegir uno de los siguientes valores para el parámetro `pgaudit.log`.

- none: es el valor predeterminado. No se registran cambios en la base de datos.
- all: registra todo (read, write, function, role, ddl, misc).
- ddl: registra todas las instrucciones del lenguaje de definición de datos (DDL) que no están incluidas en la clase `ROLE`.
- function: registra llamadas a funciones y bloques `DO`.
- misc: registra comandos variados como, por ejemplo, `DISCARD`, `FETCH`, `CHECKPOINT`, `VACUUM` y `SET`.
- read: registra `SELECT` y `COPY` cuando el origen es una relación (como una tabla) o una consulta.
- role: registra instrucciones relacionadas con roles y privilegios, como `GRANT`, `REVOKE`, `CREATE ROLE`, `ALTER ROLE` y `DROP ROLE`.
- write: registra `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE` y `COPY` cuando el destino es una relación (tabla).

Reinicie la instancia de base de datos de RDS for PostgreSQL mediante el siguiente comando AWS CLI.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

Auditoría de objetos de base de datos

Con PGAudit configurado en su instancia de base de datos de RDS for PostgreSQL y configurado según sus requisitos, se captura información más detallada en el registro de PostgreSQL. Por ejemplo, si bien la configuración de registro predeterminada de PostgreSQL identifica la fecha y la hora en que se realizó un cambio en una tabla de base de datos, con la extensión pgAudit la entrada de registro puede incluir el esquema, el usuario que realizó el cambio y otros detalles, según cómo estén configurados los parámetros de la extensión. Puede configurar la auditoría para realizar un seguimiento de los cambios de las siguientes maneras.

- Para cada sesión, por usuario. Para el nivel de sesión, puede capturar el texto completo del comando.
- Para cada objeto, por usuario y por base de datos.

La capacidad de auditoría de objetos se activa cuando se crea el rol `rds_pgaudit` en el sistema y, a continuación, se agrega este rol al parámetro `pgaudit.role` del grupo de parámetros personalizados. De forma predeterminada, el parámetro `pgaudit.role` no está configurado y el único valor permitido es `rds_pgaudit`. En los siguientes pasos se asume que `pgaudit` se ha inicializado y que ha se ha creado la extensión `pgaudit` siguiendo el procedimiento descrito en Configuración de la extensión pgAudit.

```
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:LOG: statement: SELECT feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:LOG: AUDIT: SESSION,2,1,READ,SELECT,TABLE,public.support,"SELECT
feedback, s.sentiment,s.confidence
FROM support,aws_comprehend.detect_sentiment(feedback, 'en') s
ORDER BY s.confidence DESC;",<none>
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:LOG: QUERY STATISTICS
2022-10-07 23:36:51 UTC:52.95.4.10(14410):postgres@labdb:[1374]:DETAIL: ! system usage stats:
! 0.009494 s user, 0.007442 s system, 0.141985 s elapsed
! [0.022327 s user, 0.007442 s system total]
```

Como se muestra en este ejemplo, la línea «LOG: AUDIT: SESSION» proporciona información sobre la tabla y su esquema, entre otros detalles.

Para configurar la auditoría de objetos

1. Use `psql` para conectarse a la insancia de base de tos de RDS for PostgreSQL.

   ```
   psql --host=your-instance-name.aws-region.rds.amazonaws.com --port=5432 --
   username=postgrespostgres --password --dbname=labdb
   ```

2. Cree un rol de base de datos llamado `rds_pgaudit` mediante el siguiente comando.

```
labdb=> CREATE ROLE rds_pgaudit;
CREATE ROLE
labdb=>
```

3. Cierre la sesión de `psql`.

```
labdb=> \q
```

En los siguientes pasos, use elAWS CLI para modificar los parámetros del registro de auditoría en el grupo de parámetros personalizado.

4. Utilice el siguiente comando AWS CLI para establecer el parámetro `pgaudit.role` en `rds_pgaudit`. De forma predeterminada, este parámetro está vacío y `rds_pgaudit` es el único valor permitido.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=pgaudit.role,ParameterValue=rds_pgaudit,ApplyMethod=pending-reboot"
 \
   --region aws-region
```

5. Reinicie AWS CLIla instancia de la instancia de base de datos de RDS for PostgreSQL para que sus cambios en los parámetros surtan efecto.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

6. Ejecute el siguiente comando para confirmar que `pgaudit.role` se establece en `rds_pgaudit`.

```
SHOW pgaudit.role;
pgaudit.role
------------------
rds_pgaudit
```

Para probar el registro de pgAudit, puede ejecutar varios comandos de ejemplo que desee auditar. Por ejemplo, podría ejecutar los siguientes comandos.

```
CREATE TABLE t1 (id int);
GRANT SELECT ON t1 TO rds_pgaudit;
SELECT * FROM t1;
id
----
(0 rows)
```

Los registros de base de datos contendrán una entrada similar a la siguiente.

```
...
2017-06-12 19:09:49 UTC:...:rds_test@postgres:[11701]:LOG: AUDIT:
OBJECT,1,1,READ,SELECT,TABLE,public.t1,select * from t1;
...
```

Para obtener información acerca de la visualización de los registros, consulte Supervisión de archivos de registro de Amazon RDS.

Para obtener más información sobre la extensión pgAudit, consulte pgAudit en GitHub.

Exclusión de usuarios o bases de datos del registro de auditoría

Como se explica en Archivos de registro de bases de datos de RDS para PostgreSQL, los registros de PostgreSQL consumen espacio de almacenamiento. El uso de la extensión pgAudit aumenta el volumen de datos recopilados en los registros en diversos grados, según los cambios de los que realice un seguimiento. Es posible que no necesite auditar todos los usuarios o bases de datos de su Instancia de base de datos RDS para PostgreSQL.

Para minimizar los impactos en el almacenamiento y evitar la captura innecesaria de registros de auditoría, puede excluir a los usuarios y las bases de datos de la auditoría. También puede cambiar el registro dentro de una sesión determinada. Los siguientes ejemplos muestran cola forma de hacerlo.

> **Note**
>
> La configuración de los parámetros a nivel de sesión tiene prioridad sobre la configuración del grupo de parámetros del grupo de parámetros de la base de datos personalizada para la instancia de la base de datos de RDS for PostgreSQL. Si no desea que los usuarios de la base de datos omitan los ajustes de configuración del registro de auditoría, asegúrese de cambiar sus permisos.

Supongamos que su instancia de base de datos de RDS for PostgreSQL está configurado para auditar el mismo nivel de actividad para todos los usuarios y bases de datos. A continuación, decide que no desea auditar al usuario `myuser`. Puede desactivar la auditoría de `myuser` con el siguiente comando de SQL.

```
ALTER USER myuser SET pgaudit.log TO 'NONE';
```

A continuación, puede utilizar la siguiente consulta para comprobar la columna `user_specific_settings` de `pgaudit.log` para confirmar que el parámetro está establecido en `NONE`.

```
SELECT
    usename AS user_name,
    useconfig AS user_specific_settings
FROM
    pg_user
WHERE
    usename = 'myuser';
```

Debería ver una salida como la siguiente.

```
 user_name | user_specific_settings
-----------+------------------------
 myuser    | {pgaudit.log=NONE}
(1 row)
```

Puede desactivar el registro de un usuario determinado en medio de su sesión con la base de datos con el siguiente comando.

```
ALTER USER myuser IN DATABASE mydatabase SET pgaudit.log TO 'none';
```

Utilice la siguiente consulta para comprobar la columna de configuración de pgaudit.log para una combinación específica de usuario y base de datos.

```
SELECT
    usename AS "user_name",
    datname AS "database_name",
    pg_catalog.array_to_string(setconfig, E'\n') AS "settings"
FROM
    pg_catalog.pg_db_role_setting s
```

```
    LEFT JOIN pg_catalog.pg_database d ON d.oid = setdatabase
    LEFT JOIN pg_catalog.pg_user r ON r.usesysid = setrole
WHERE
    usename = 'myuser'
    AND datname = 'mydatabase'
ORDER BY
    1,
    2;
```

Se muestra una salida similar a la siguiente.

```
  user_name | database_name |     settings
-----------+---------------+-----------------
 myuser    | mydatabase    | pgaudit.log=none
(1 row)
```

Tras desactivar la auditoría de `myuser`, decide que no desea realizar un seguimiento de los cambios en `mydatabase`. Puede desactivar la auditoría de esa base de datos específica mediante el siguiente comando.

```
ALTER DATABASE mydatabase SET pgaudit.log to 'NONE';
```

A continuación, utilice la siguiente consulta para comprobar la columna database_specific_settings y confirmar que pgaudit.log tiene el valor NONE.

```
SELECT
a.datname AS database_name,
b.setconfig AS database_specific_settings
FROM
pg_database a
FULL JOIN pg_db_role_setting b ON a.oid = b.setdatabase
WHERE
a.datname = 'mydatabase';
```

Debería ver una salida como la siguiente.

```
 database_name | database_specific_settings
---------------+----------------------------
 mydatabase    | {pgaudit.log=NONE}
(1 row)
```

Para restablecer la configuración predeterminada de myuser, use el siguiente comando:

```
ALTER USER myuser RESET pgaudit.log;
```

Para restablecer la configuración predeterminada de una base de datos, use el siguiente comando:

```
ALTER DATABASE mydatabase RESET pgaudit.log;
```

Para restablecer el usuario y la base de datos a la configuración por defecto, utilice el siguiente comando.

```
ALTER USER myuser IN DATABASE mydatabase RESET pgaudit.log;
```

También puede capturar eventos específicos en el registro configurando `pgaudit.log` en uno de los otros valores permitidos para el parámetro `pgaudit.log`. Para obtener más información, consulte Lista de ajustes permitidos para el parámetro `pgaudit.log`.

```
ALTER USER myuser SET pgaudit.log TO 'read';
ALTER DATABASE mydatabase SET pgaudit.log TO 'function';
ALTER USER myuser IN DATABASE mydatabase SET pgaudit.log TO 'read,function'
```

Referencia para la extensión pgAudit

Puede especificar el nivel de detalle que desea para el registro de auditoría cambiando uno o más de los parámetros que se enumeran en esta sección.

Control del comportamiento de pgAudit

Puede controlar el registro de auditoría cambiando uno o más de los parámetros que aparecen en la tabla siguiente.

Parámetro	Descripción
`pgaudit.log`	Especifica las clases de instrucciones que se registrarán mediante el registro de auditoría de sesión. Los valores permitidos incluyen ddl, function, misc, read, role, write, none, all. Para obtener más información, consulte Lista de ajustes permitidos para el parámetro `pgaudit.log` .

Parámetro	Descripción
`pgaudit.log_catalog`	Cuando se activa (se establece en 1), agrega instrucciones al registro de auditoría si todas las relaciones de una instrucción se encuentran en pg_catalog.
`pgaudit.log_level`	Especifica el nivel de registro que se usará para las entradas de registro. Valores permitidos, debug5, debug4, debug3, debug2, debug1, info, notice, warning, log.
`pgaudit.log_parameter`	Cuando se activa (se establece en 1), los parámetros transmitidos con la instrucción se capturan en el registro de auditoría.
`pgaudit.log_relation`	Cuando se activa (se establece en 1), el registro de auditoría de la sesión crea una entrada de registro separada para cada relación (TABLE, VIEW, etc.) referenciada en una instrucción SELECT o DML.
`pgaudit.log_statement_once`	Especifica si el registro incluirá el texto de la instrucción y los parámetros con la primera entrada de registro para una combinación de instrucción o subinstrucción o con cada entrada.
`pgaudit.role`	Especifica el rol maestro que se usará para el registro de auditoría de objetos. La única entrada permitida es `rds_pgaudit` .

Lista de ajustes permitidos para el parámetro **`pgaudit.log`**

Valor	Descripción
Ninguno	Esta es la opción predeterminada. No se registran cambios en la base de datos.
Todos	Registra todo (read, write, function, role, ddl, misc).
ddl	Registra todas las instrucciones del lenguaje de definición de datos (DDL) que no están incluidas en la clase `ROLE`.

Valor	Descripción
función	Registra llamadas a funciones y bloques `DO`.
misc	Registra comandos variados como, por ejemplo, `DISCARD`, `FETCH`, `CHECKPOINT` , `VACUUM` y `SET`.
leer	Registra `SELECT` y `COPY` cuando el origen es una relación (como una tabla) o una consulta.
role	Registra instrucciones relacionadas con roles y privilegios, como, por ejemplo, `GRANT`, `REVOKE`, `CREATE ROLE`, `ALTER ROLE` y `DROP ROLE`.
write	Registra `INSERT`, `UPDATE`, `DELETE`, `TRUNCATE` y `COPY` cuando el destino es una relación (tabla).

Para registrar varios tipos de eventos con auditorías de sesiones, utilice una lista separada por comas. Para registrar todos los tipos de eventos, establezca `pgaudit.log` en `ALL`. Reinicie la instancia de base de datos para aplicar los cambios.

Con la auditoría de objetos, puede mejorar los registros de auditoría para que funcionen con algunas relaciones específicas. Por ejemplo, puede especificar que desea crear registros de auditoría para las operaciones `READ` en una o más tablas.

Programación de mantenimiento con la extensión pg_cron de PostgreSQL

Puede utilizar la extensión `pg_cron` de PostgreSQL para programar comandos de mantenimiento dentro de una base de datos de PostgreSQL. Para obtener más información sobre la extensión, consulte ¿Qué es pg_cron? en la documentación de pg_cron.

La extensión `pg_cron` es compatible con las versiones 12.5 y posteriores del motor de RDS para PostgreSQL.

Para obtener más información acerca del uso de `pg_cron`, consulte Programación de mantenimiento con la extensión pg_cron de PostgreSQL para sus bases de datos de RDS para PostgreSQL o las bases de datos de Aurora PostgreSQL-Compatible Edition

Temas

- Configuración de la extensión pg_cron
- Concesión de permisos para usuarios de base de datos para usar pg_cron
- Programación de trabajos pg_cron
- Referencia para la extensión pg_cron

Configuración de la extensión pg_cron

Habilite la extensión de `pg_cron` de la siguiente manera:

1. Modifique el grupo de parámetros personalizado asociado a la instancia de base de datos de PostgreSQL agregando `pg_cron` al valor del parámetro `shared_preload_libraries`.
   - Si su instancia de base de datos de RDS para PostgreSQL utiliza el parámetro `rds.allowed_extensions` para enumerar de forma explícita las extensiones que se pueden instalar, debe añadir la extensión `pg_cron` a la lista. Solo ciertas versiones de RDS para PostgreSQL admiten el parámetro `rds.allowed_extensions`. De forma predeterminada, se permiten todas las extensiones disponibles. Para obtener más información, consulte Restringir la instalación de extensiones de PostgreSQL.

   Reinicie la instancia de base de datos de PostgreSQL para que se apliquen los cambios en el grupo de parámetros. Para obtener más información acerca de cómo trabajar con grupos de parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

2. Una vez reiniciada la instancia de base de datos de PostgreSQL, ejecute el siguiente comando con una cuenta que tenga permisos `rds_superuser`. Por ejemplo, si utilizó la configuración predeterminada al crear la instancia de base de datos RDS para PostgreSQL, conéctese como usuario `postgres` y cree la extensión.

   ```
   CREATE EXTENSION pg_cron;
   ```

   El programador `pg_cron` se establece en la base de datos de PostgreSQL predeterminada que se denomina `postgres`. Los objetos `pg_cron` se crean en esta base de datos `postgres` y todas las acciones de programación se ejecutan en esta base de datos.

3. Puede utilizar la configuración predeterminada o programar trabajos que ejecutar en otras bases de datos en la instancia de base de datos de PostgreSQL. Para programar trabajos de otras bases de datos en la instancia de base de datos de PostgreSQL, consulte el ejemplo en Programación de un trabajo cron para una base de datos que no sea la predeterminada.

Concesión de permisos para usuarios de base de datos para usar pg_cron

La instalación de la extensión `pg_cron` requiere privilegios de `rds_superuser`. Sin embargo, los permisos para usar `pg_cron` se pueden conceder (los concede un miembro del grupo/rol `rds_superuser`) a otros usuarios de la base de datos para que puedan programar sus propios trabajos. Es recomendable que conceda permisos al esquema `cron` solo según sea necesario si mejora las operaciones en su entorno de producción.

Para conceder permiso a un usuario de base de datos en el esquema `cron`, ejecute el siguiente comando:

```
postgres=> GRANT USAGE ON SCHEMA cron TO db-user;
```

Esto da permiso *`db-user`* para acceder al esquema de `cron` para programar trabajos cron para los objetos a los que tienen permiso de acceso. Si el usuario de la base de datos no tiene permisos, se produce un error en el trabajo tras publicar el mensaje de error en el `postgresql.log`, como se muestra a continuación:

```
2020-12-08 16:41:00 UTC::@:[30647]:ERROR: permission denied for table table-name
2020-12-08 16:41:00 UTC::@:[27071]:LOG: background worker "pg_cron" (PID 30647) exited
 with exit code 1
```

En otras palabras, asegúrese de que los usuarios de bases de datos a los que se les conceden permisos en el esquema de `cron` también tengan permisos sobre los objetos (tablas, esquemas, etc.) que tienen pensado programar.

Los detalles del trabajo cron y su éxito o fracaso también se capturan en la tabla `cron.job_run_details`. Para obtener más información, consulte Tablas para programar trabajos y capturar estado .

Programación de trabajos pg_cron

En las secciones que siguen se muestra cómo programar varias tareas de administración con trabajos `pg_cron`.

> **Note**
>
> Al crear trabajos `pg_cron`, compruebe que el valor `max_worker_processes` sea mayor que el número de `cron.max_running_jobs`. Se producirá un error en el trabajo `pg_cron` si se queda sin procesos de trabajo en segundo plano. El número predeterminado de trabajos `pg_cron` es 5. Para obtener más información, consulte Parámetros para administrar la extensión pg_cron.

Temas

- Limpieza de tablas
- Depuración de la tabla del historial pg_cron
- Registrar errores únicamente en el archivo postgresql.log
- Programación de un trabajo cron para una base de datos que no sea la predeterminada

Limpieza de tablas

En la mayoría de los casos, autovacuum maneja el mantenimiento de limpieza. Sin embargo, se recomienda programar una limpieza de una tabla específica en el momento que lo desee.

Véase también, Uso de autovacuum de PostgreSQL en Amazon RDS para PostgreSQL.

A continuación, se muestra un ejemplo del uso de la función `cron.schedule` para configurar un trabajo para usar `VACUUM FREEZE` en una tabla específica todos los días a las 22:00 (GMT).

```
SELECT cron.schedule('manual vacuum', '0 22 * * *', 'VACUUM FREEZE pgbench_accounts');
```

```
 schedule
----------
1
(1 row)
```

Una vez ejecutado el ejemplo anterior, puede comprobar del siguiente modo el historial de la `cron.job_run_details` tabla.

```
postgres=> SELECT * FROM cron.job_run_details;
jobid  | runid | job_pid | database | username | command                        |
 status    | return_message | start_time                    | end_time
-------+-------+---------+----------+----------+--------------------------------
+-----------+----------------+--------------------------------
+-------------------------------
 1     | 1     | 3395    | postgres | adminuser| vacuum freeze pgbench_accounts
 | succeeded | VACUUM         | 2020-12-04 21:10:00.050386+00 | 2020-12-04
 21:10:00.072028+00
(1 row)
```

A continuación, se presenta una consulta de la tabla `cron.job_run_details` para ver los trabajos fallidos.

```
postgres=> SELECT * FROM cron.job_run_details WHERE status = 'failed';
jobid | runid | job_pid | database | username | command                          | status
 | return_message                                | start_time                    |
 end_time
------+-------+---------+----------+----------+----------------------------------+--------
+-----------------------------------------------+--------------------------------
+-------------------------------
 5    | 4     | 30339   | postgres | adminuser| vacuum freeze pgbench_account | failed
 | ERROR: relation "pgbench_account" does not exist | 2020-12-04 21:48:00.015145+00 |
 2020-12-04 21:48:00.029567+00
(1 row)
```

Para obtener más información, consulte Tablas para programar trabajos y capturar estado .

Depuración de la tabla del historial pg_cron

La tabla `cron.job_run_details` contiene un historial de los trabajos cron que con el tiempo pueden volverse muy grandes. Se recomienda programar un trabajo que depure esta tabla. Por ejemplo, mantener entradas de una semana podría ser suficiente para solucionar problemas.

En el siguiente ejemplo se utiliza la función cron.schedule para programar un trabajo que se ejecuta todos los días a la medianoche para depurar la tabla `cron.job_run_details`. El trabajo mantiene solo los últimos siete días. Utilice su cuenta de `rds_superuser` para programar el trabajo de la siguiente manera:

```
SELECT cron.schedule('0 0 * * *', $$DELETE
    FROM cron.job_run_details
    WHERE end_time < now() - interval '7 days'$$);
```

Para obtener más información, consulte Tablas para programar trabajos y capturar estado .

Registrar errores únicamente en el archivo postgresql.log

Para evitar escribir en la tabla `cron.job_run_details`, modifique el grupo de parámetros asociado a la instancia de base de datos de PostgreSQL y establezca el parámetro `cron.log_run` en Off (Desactivado). La extensión `pg_cron` ya no escribe en la tabla y captura errores solo en el archivo `postgresql.log`. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

Utilice el siguiente comando para comprobar el valor del parámetro `cron.log_run`.

```
postgres=> SHOW cron.log_run;
```

Para obtener más información, consulte Parámetros para administrar la extensión pg_cron.

Programación de un trabajo cron para una base de datos que no sea la predeterminada

Todos los metadatos de `pg_cron` se mantienen en la base de datos predeterminada de PostgreSQL que se denomina `postgres`. Dado que los trabajadores en segundo plano se utilizan para ejecutar los trabajos cron de mantenimiento, puede programar un trabajo en cualquiera de sus bases de datos dentro de la instancia de base de datos de PostgreSQL:

> **Note**
>
> Solo los usuarios con el rol `rds_superuser` o los privilegios `rds_superuser` pueden mostrar todos los trabajos cron en la base de datos. Los demás usuarios solo pueden ver sus propios trabajos en la tabla `cron.job`.

1. En la base de datos cron, programe el trabajo como lo hace normalmente mediante el uso de cron.schedule.

```
postgres=> SELECT cron.schedule('database1 manual vacuum', '29 03 * * *', 'vacuum
 freeze test_table');
```

2. Como usuario con el rol `rds_superuser`, actualice la columna de base de datos para el trabajo que acaba de crear a fin de que se ejecute en otra base de datos dentro de la instancia de base de datos de PostgreSQL.

```
postgres=> UPDATE cron.job SET database = 'database1' WHERE jobid = 106;
```

3. Verifique consultando la tabla `cron.job`.

```
postgres=> SELECT * FROM cron.job;
jobid | schedule    | command                         | nodename  | nodeport |
 database | username  | active | jobname
------+-------------+---------------------------------+-----------+----------
+----------+-----------+--------+-------------------------
106   | 29 03 * * * | vacuum freeze test_table        | localhost | 8192     |
 database1| adminuser | t      | database1 manual vacuum
  1   | 59 23 * * * | vacuum freeze pgbench_accounts | localhost | 8192     |
 postgres | adminuser | t      | manual vacuum
(2 rows)
```

> **Note**
>
> En algunas situaciones, puede agregar un trabajo cron que desea ejecutar en otra base de datos. En tales casos, el trabajo podría intentar ejecutarse en la base de datos predeterminada (`postgres`) antes de actualizar la columna de la base de datos correcta. Si el nombre de usuario tiene permisos, el trabajo se ejecuta correctamente en la base de datos predeterminada.

Referencia para la extensión pg_cron

Con la extensión `pg_cron`, puede utilizar los siguientes parámetros, funciones y tablas. Para obtener más información, consulte ¿Qué es pg_cron? en la documentación de pg_cron.

Temas

- Parámetros para administrar la extensión pg_cron
- Referencia de función: cron.schedule
- Referencia de función: cron.unschedule
- Tablas para programar trabajos y capturar estado

Parámetros para administrar la extensión pg_cron

A continuación, aparece la lista de parámetros para controlar el comportamiento de la extensión `pg_cron`.

Parámetro	Descripción
cron.database_name	La base de datos en la que se conservan los metadatos de `pg_cron`.
`cron.host`	El nombre de host que se va a conectar a PostgreSQL. No se puede modificar este valor.
`cron.log_run`	Registre todos los trabajos que se ejecutan en la tabla `job_run_details` . Los valores son on o `off`. Para obtener más informaci ón, consulte Tablas para programar trabajos y capturar estado .
`cron.log_statement`	Registre todas las instrucciones cron antes de ejecutarlas. Los valores son on o `off`.
`cron.max_running_jobs`	La cantidad máxima de trabajos que se pueden ejecutar simultáneamente.
`cron.use_background_workers`	Utilice procesos de trabajo secundarios en lugar de sesiones de cliente. No se puede modificar este valor.

Utilice el siguiente comando SQL para mostrar estos parámetros y sus valores:

```
postgres=> SELECT name, setting, short_desc FROM pg_settings WHERE name LIKE 'cron.%'
 ORDER BY name;
```

Referencia de función: cron.schedule

Esta función programa un trabajo cron. El trabajo se programa inicialmente en la base de datos predeterminada `postgres`. La función devuelve un valor `bigint` que representa el identificador del trabajo. Para programar trabajos para que se ejecuten en otras bases de datos dentro de la instancia de base de datos de PostgreSQL, consulte el ejemplo en Programación de un trabajo cron para una base de datos que no sea la predeterminada.

La función presenta dos formatos de sintaxis.

Sintaxis

```
cron.schedule (job_name,
    schedule,
    command
);

cron.schedule (schedule,
    command
);
```

Parámetros

Parámetro	Descripción
`job_name`	El nombre del trabajo cron.
`schedule`	Texto que indica la programación del trabajo cron. El formato es el formato cron estándar.
`command`	Texto del comando que se va a ejecutar.

Ejemplos

```
postgres=> SELECT cron.schedule ('test','0 10 * * *', 'VACUUM pgbench_history');
 schedule
```

```
----------
      145
(1 row)

postgres=> SELECT cron.schedule ('0 15 * * *', 'VACUUM pgbench_accounts');
 schedule
----------
      146
(1 row)
```

Referencia de función: cron.unschedule

Esta función elimina un trabajo cron. Puede especificar `job_name` o `job_id`. Una política se asegura de que usted es el propietario para quitar la programación del trabajo. La función devuelve un valor booleano que indica éxito o error.

La función tiene los siguientes formatos de sintaxis.

Sintaxis

```
cron.unschedule (job_id);

cron.unschedule (job_name);
```

Parámetros

Parámetro	Descripción
`job_id`	El identificador de trabajo que se devolvió desde la función `cron.schedule` cuando se programó el trabajo cron.
`job_name`	El nombre de un trabajo cron que se programó con la función `cron.schedule` .

Ejemplos

```
postgres=> SELECT cron.unschedule(108);
 unschedule
```

```
------------
 t
(1 row)

postgres=> SELECT cron.unschedule('test');
 unschedule
------------
 t
(1 row)
```

Tablas para programar trabajos y capturar estado

Las siguientes tablas se crean y utilizan para programar los trabajos cron y registrar la forma en la que se completaron.

Tabla	Descripción
`cron.job`	Contiene los metadatos de cada trabajo programado. La mayoría de las interacciones con esta tabla se deben hacer mediante el uso de las funciones `cron.schedule` y `cron.unschedule` . **Important** No recomendamos conceder privilegios de actualización o inserción directamente a esta tabla. Al hacerlo, el usuario podría actualizar la columna `username` para que se ejecute como `rds-superuser` .
`cron.job_run_details`	Contiene información histórica sobre ejecuciones de trabajos programados anteriores. Esto resulta útil para investigar el estado, los mensajes devueltos y la hora de inicio y finalización de la ejecución del trabajo.

Tabla	Descripción
	Note Para evitar que esta tabla crezca indefinidamente, púrguela regularmente. Para ver un ejemplo, consulte Depuración de la tabla del historial pg_cron.

Uso de pglogical para sincronizar datos entre instancias

Todas las versiones de RDS para PostgreSQL disponibles actualmente admiten la extensión `pglogical`. La extensión pglogical es anterior a la función de replicación lógica funcionalmente similar que se introdujo en la versión 10 de PostgreSQL. Para obtener más información, consulte Replicación lógica para Amazon RDS para PostgreSQL.

La extensión `pglogical` admite la replicación lógica entre dos o más Instancias de base de datos de RDS para PostgreSQL. También admite la replicación entre diferentes versiones de PostgreSQL y entre bases de datos que se ejecutan en instancias de base de datos de RDS para PostgreSQL y clústeres de bases de datos de Aurora PostgreSQL. La extensión `pglogical` utiliza un modelo de publicación y suscripción para replicar los cambios en las tablas y otros objetos, como secuencias, de un publicador a un suscriptor. Se basa en una ranura de replicación para garantizar que los cambios se sincronicen de un nodo publicador a un nodo suscriptor, que se define de la siguiente manera.

- El nodo publicador es la instancia de base de datos de RDS para PostgreSQL, que es la fuente de datos que se van a replicar en otros nodos. El nodo publicador define las tablas que se van a replicar en un conjunto de publicaciones.
- El nodo suscriptor es la instancia de base de datos de RDS para PostgreSQL que recibe las actualizaciones WAL del publicador. El suscriptor crea una suscripción para conectarse al publicador y obtener los datos WAL decodificados. Cuando el suscriptor crea la suscripción, se crea la ranura de replicación en el nodo del publicador.

A continuación, encontrará información sobre cómo configurar la extensión `pglogical`.

Temas

- Requisitos y limitaciones de la extensión pglogical
- Configuración de la extensión pglogical
- Configuración de la replicación lógica para la instancia de base de datos de RDS para PostgreSQL
- Restablecimiento de la replicación lógica después de una actualización principal
- Administración de ranuras de replicación lógica para RDS para PostgreSQL
- Referencia de parámetros para la extensión pglogical

Requisitos y limitaciones de la extensión pglogical

Todas las versiones disponibles actualmente de RDS para PostgreSQL admiten la extensión `pglogical`.

Tanto el nodo publicador como el nodo suscriptor deben estar configurados para la replicación lógica.

Las tablas que desee replicar desde un publicador a un suscriptor deben tener los mismos nombres y el mismo esquema. Estas tablas también deben contener las mismas columnas y las columnas deben utilizar los mismos tipos de datos. Tanto las tablas de los publicadores como las de suscriptores deben tener las mismas claves principales. Se recomienda utilizar únicamente la PRIMARY KEY como restricción única.

Las tablas del nodo suscriptor pueden tener restricciones más permisivas que las del nodo publicador para las restricciones CHECK y NOT NULL.

La extensión `pglogical` proporciona funciones como la replicación bidireccional que no son compatibles con la función de replicación lógica integrada en PostgreSQL (versión 10 y posteriores). Para obtener más información, consulte PostgreSQL bi-directional replication using pglogical (Replicación bidireccional de PostgreSQL mediante pglogical).

Configuración de la extensión pglogical

Para configurar la extensión `pglogical` en la instancia de base de datos de RDS para PostgreSQL , añada `pglogical` a las bibliotecas compartidas en el grupo de parámetros de base de datos personalizado para su instancia de base de datos de RDS para PostgreSQL. También debe establecer el valor del parámetro `rds.logical_replication` en 1 para activar la descodificación lógica. Por último, cree la extensión en la base de datos. Puede utilizar la AWS Management Console o la AWS CLI para estas tareas.

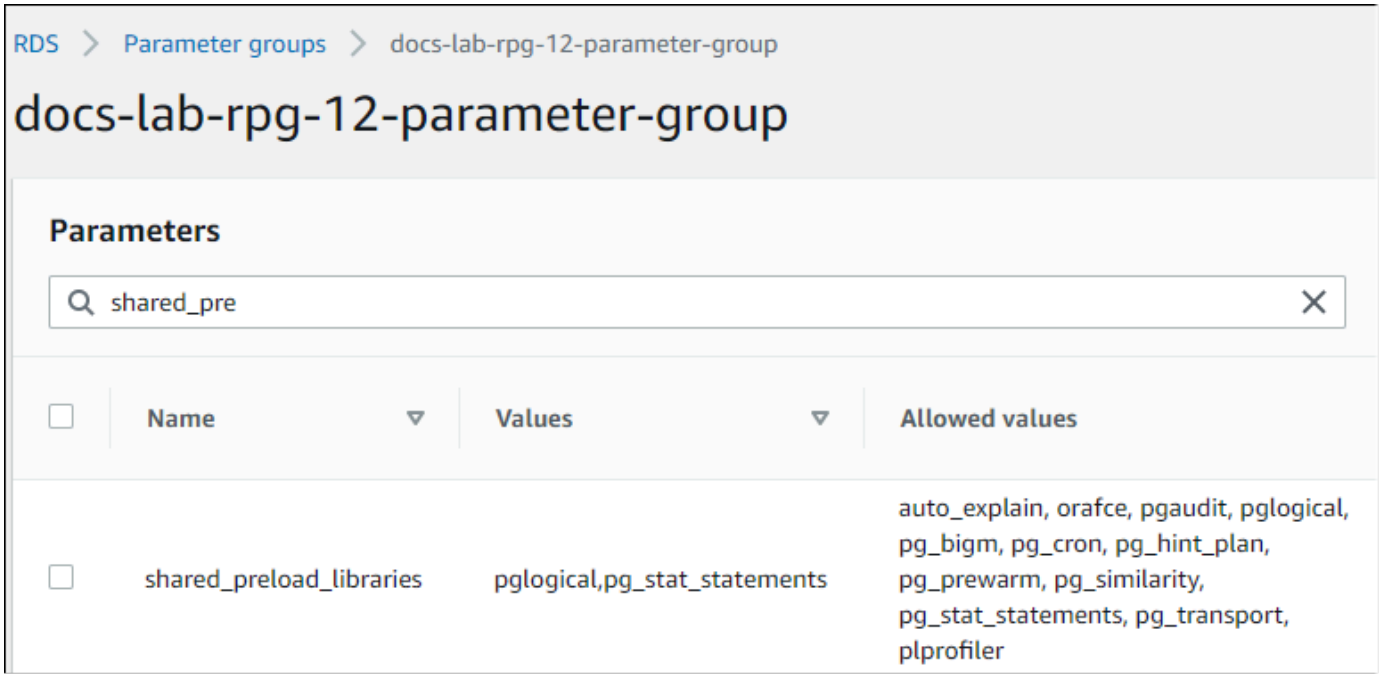
Debe tener permisos como el rol `rds_superuser` para realizar estas tareas.

En los pasos siguientes se supone que la instancia de base de datos de RDS for PostgreSQL está asociada a un grupo de parámetros de DB. Para obtener información acerca de cómo crear el grupo de parámetros de base de datos, consulte Grupos de parámetros para Amazon RDS.

Consola

Para configurar la extensión pglogical

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija la instancia de base de datos de RDS for PostgreSQL.
3. Abra la pestaña Configuration (Configuración) para su Instancia de base de datos RDS para PostgreSQL. Entre los detalles de la instancia, busque el enlace del grupo de parámetros.
4. Elija el enlace para abrir los parámetros personalizados asociados al Instancia de base de datos RDS para PostgreSQL.
5. En el campo de búsqueda Parametes (Parámetros), escriba `shared_pre` para buscar el parámetro `shared_preload_libraries`.
6. Seleccione Edit parameters (Editar parámetros) para acceder a los valores de las propiedades.
7. Añada `pglogical` a la lista en el campo Values (Valores). Utilice una coma para separar los elementos de la lista de valores.



8. Busque el parámetro `rds.logical_replication` y configúrelo en 1 para activar la replicación lógica.
9. Reinicie la instancia de base de datos de RDS para PostgreSQL para que surtan efecto los cambios.

10. Cuando la instancia esté disponible, puede usar `psql` (o pgAdmin) para conectarse a la instancia de base de datos de RDS para PostgreSQL.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

11. Para comprobar que pglogical esté inicializado, ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pglogical
(1 row)
```

12. Compruebe la configuración que permite la descodificación lógica, de la siguiente manera.

```
SHOW wal_level;
wal_level
-----------
 logical
(1 row)
```

13. Cree la extensión de la siguiente manera.

```
CREATE EXTENSION pglogical;
EXTENSION CREATED
```

14. Elija Guardar cambios.
15. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
16. Elija instancia de base de datos de RDS for PostgreSQL en la lista de bases de datos para seleccionarla y, a continuación, elija Reboot (Reiniciar) en el menú Actions (Acciones).

AWS CLI

Para configurar la extensión pglogical

Para configurar pglogical mediante la AWS CLI, llame a la operación modify-db-parameter-group para modificar determinados parámetros de su grupo de parámetros personalizado, tal como se muestra en el siguiente procedimiento.

1. Utilice el siguiente comando AWS CLI para añadir `pglogical` al parámetro `shared_preload_libraries`.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pglogical,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Utilice el siguiente comando AWS CLI para configurar `rds.logical_replication` en 1 y activar la función de descodificación lógica para la Instancia de base de datos RDS para PostgreSQL.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=rds.logical_replication,ParameterValue=1,ApplyMethod=pending-
reboot" \
   --region aws-region
```

3. Utilice el siguiente comando AWS CLI para reiniciar la instancia de base de datos de RDS para PostgreSQL para que se inicialice la biblioteca de pglogical.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

4. Cuando la instancia esté disponible, use `psql` para conectarse a la instancia de base de datos de RDS para PostgreSQL.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

5. Cree la extensión de la siguiente manera.

```
CREATE EXTENSION pglogical;
EXTENSION CREATED
```

6. Reinicie la instancia de base de datos de RDS for PostgreSQL mediante el siguiente comando AWS CLI.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

Configuración de la replicación lógica para la instancia de base de datos de RDS para PostgreSQL

En el siguiente procedimiento, se muestra cómo iniciar la replicación lógica entre dos instancias de base de datos de RDS para PostgreSQL. En los pasos, se asume que tanto el origen (publicador) como el destino (suscriptor) tienen la extensión `pglogical` configurada como se detalla en Configuración de la extensión pglogical.

> **Note**
>
> El `node_name` de un nodo de suscriptor no puede empezar por `rds`.

Para crear el nodo publicador y definir las tablas que se van a replicar

En estos pasos se asume que la instancia de base de datos de RDS para PostgreSQL tiene una base de datos que tiene una o más tablas que desea replicar en otro nodo. Debe volver a crear la estructura de tablas del publicador en el suscriptor, así que primero debe obtener la estructura de la tabla si es necesario. Para ello, utilice el metacomando de `psql \d` *`tablename`* y, a continuación, cree la misma tabla en la instancia del suscriptor. El siguiente procedimiento crea una tabla de ejemplo en el publicador (origen) con fines de demostración.

1. Utilice `psql` para conectarse a la instancia que tiene la tabla que desea usar como origen para los suscriptores.

   ```
   psql --host=source-instance.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password --dbname=labdb
   ```

   Si no dispone de una tabla existente que desee replicar, puede crear una tabla de ejemplo de la siguiente manera.

   a. Cree una tabla de ejemplo con la siguiente instrucción SQL.

```
CREATE TABLE docs_lab_table (a int PRIMARY KEY);
```

b. Rellene la tabla con los datos generados mediante la siguiente instrucción SQL.

```
INSERT INTO docs_lab_table VALUES (generate_series(1,5000));
INSERT 0 5000
```

c. Compruebe que los datos existen en la tabla mediante la siguiente instrucción SQL.

```
SELECT count(*) FROM docs_lab_table;
```

2. Identifique esta instancia de base de datos de RDS para PostgreSQL como nodo publicador de la siguiente manera.

```
SELECT pglogical.create_node(
    node_name := 'docs_lab_provider',
    dsn := 'host=source-instance.aws-region.rds.amazonaws.com port=5432
 dbname=labdb');
 create_node
-------------
   3410995529
(1 row)
```

3. Añada la tabla que desea replicar al conjunto de replicación predeterminado. Para obtener más información sobre los conjuntos de replicación, consulte Replication sets (Conjuntos de replicación) en la documentación de pglogical.

```
SELECT pglogical.replication_set_add_table('default', 'docs_lab_table', 'true',
 NULL, NULL);
 replication_set_add_table
  --------------------------
  t
  (1 row)
```

Se ha completado la configuración del nodo publicador. Ahora puede configurar el nodo suscriptor para recibir las actualizaciones del publicador.

Para configurar el nodo suscriptor y crear una suscripción para recibir actualizaciones

En estos pasos se asume que la instancia de base de datos de RDS para PostgreSQL se ha configurado con la extensión `pglogical`. Para obtener más información, consulte Configuración de la extensión pglogical.

1. Utilice `psql` para conectarse a la instancia en la que desea recibir actualizaciones del publicador.

```
psql --host=target-instance.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

2. En , la instancia de base de datos de RDS para PostgreSQL del suscriptor, cree la misma tabla que existe en el publicador. En este ejemplo, la tabla es `docs_lab_table`. Puede crear la tabla tal y como se indica a continuación.

```
CREATE TABLE docs_lab_table (a int PRIMARY KEY);
```

3. Compruebe que esta tabla esté vacía.

```
SELECT count(*) FROM docs_lab_table;
 count
-------
  0
(1 row)
```

4. Identifique esta instancia de base de datos de RDS para PostgreSQL como nodo suscriptor de la siguiente manera.

```
SELECT pglogical.create_node(
    node_name := 'docs_lab_target',
    dsn := 'host=target-instance.aws-region.rds.amazonaws.com port=5432
 sslmode=require dbname=labdb user=postgres password=********');
 create_node
-------------
   2182738256
(1 row)
```

5. Cree la suscripción.

```
SELECT pglogical.create_subscription(
   subscription_name := 'docs_lab_subscription',
```

```
   provider_dsn := 'host=source-instance.aws-region.rds.amazonaws.com port=5432
 sslmode=require dbname=labdb user=postgres password=*******',
   replication_sets := ARRAY['default'],
   synchronize_data := true,
   forward_origins := '{}' );
 create_subscription
---------------------
1038357190
(1 row)
```

Al completar este paso, los datos de la tabla del publicador se crean en la tabla del suscriptor. Para comprobar que ha ocurrido esto, utilice la siguiente consulta SQL.

```
SELECT count(*) FROM docs_lab_table;
 count
-------
  5000
(1 row)
```

A partir de este momento, los cambios realizados en la tabla del publicador se replicarán en la tabla del suscriptor.

Restablecimiento de la replicación lógica después de una actualización principal

Para poder realizar una actualización de una versión principal de un instancia de base de datos de RDS para PostgreSQL que se haya configurado como nodo publicador para la replicación lógica, debe eliminar todas las ranuras de replicación, incluso las que no estén activas. Se recomienda desviar temporalmente las transacciones de la base de datos del nodo publicador, eliminar las ranuras de replicación, actualizar la instancia de base de datos de RDS para PostgreSQL y, a continuación, restablecer y reiniciar la replicación.

Las ranuras de replicación se alojan únicamente en el nodo publicador. El nodo suscriptor de RDS para PostgreSQL en un escenario de replicación lógica no tiene espacios que eliminar, pero no se puede actualizar a una versión principal mientras esté designado como nodo suscriptor con una suscripción al publicador. Antes de actualizar el nodo suscriptor de RDS para PostgreSQL, elimine la suscripción y el nodo. Para obtener más información, consulte Administración de ranuras de replicación lógica para RDS para PostgreSQL.

Determinación de que la replicación lógica se ha interrumpido

Puede determinar que el proceso de replicación se ha interrumpido consultando el nodo publicador o el nodo suscriptor de la siguiente manera.

Para comprobar el nodo publicador

- Utilice `psql` para conectarse al nodo publicador y, a continuación, consulte la función `pg_replication_slots`. Anote el valor de la columna activa. Normalmente, esto devolverá `t` (true) y mostrará que la replicación está activa. Si la consulta devuelve `f` (false), indica que la replicación en el suscriptor se ha detenido.

```
SELECT slot_name,plugin,slot_type,active FROM pg_replication_slots;
                    slot_name              |      plugin      | slot_type | active
-------------------------------------------+------------------+-----------+--------
 pgl_labdb_docs_labcb4fa94_docs_lab3de412c | pglogical_output | logical   | f
(1 row)
```

Para comprobar el nodo suscriptor

En el nodo suscriptor, puede comprobar el estado de la replicación de tres maneras diferentes.

- Revise los registros de PostgreSQL en el nodo suscriptor para encontrar los mensajes de error. El registro identifica el error con mensajes que incluyen el código de salida 1, como se muestra a continuación.

```
2022-07-06 16:17:03 UTC::@:[7361]:LOG: background worker "pglogical apply
 16404:2880255011" (PID 14610) exited with exit code 1
2022-07-06 16:19:44 UTC::@:[7361]:LOG: background worker "pglogical apply
 16404:2880255011" (PID 21783) exited with exit code 1
```

- Consulte la función `pg_replication_origin`. Conéctese a la base de datos en el nodo suscriptor mediante `psql` y consulte la función `pg_replication_origin` de la siguiente manera.

```
SELECT * FROM pg_replication_origin;
 roident | roname
---------+--------
(0 rows)
```

Un conjunto de resultados vacío significa que la replicación se ha interrumpido. Debería ver una salida como la siguiente.

```
 roident |                      roname
---------+---------------------------------------------------
       1 | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

- Consulte la función `pglogical.show_subscription_status` tal y como se muestra en el siguiente ejemplo.

```
SELECT subscription_name,status,slot_name FROM pglogical.show_subscription_status();
     subscription_name | status |              slot_name
-------+----------------+--------+-----------------------------------
 docs_lab_subscription | down   | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

Este resultado muestra que la replicación se ha interrumpido. Su estado es `down`. Normalmente, la salida muestra el estado como `replicating`.

Si el proceso de replicación lógica se ha interrumpido, puede restablecerla siguiendo estos pasos.

Para restablecer la replicación lógica entre los nodos publicador y suscriptor

Para restablecer la replicación, primero debe desconectar el suscriptor del nodo publicador y, a continuación, restablecer la suscripción, tal como se describe en estos pasos.

1. Conéctese al nodo suscriptor con `psql` de la siguiente manera.

```
psql --host=222222222222.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=labdb
```

2. Desactive la suscripción mediante la función `pglogical.alter_subscription_disable`.

```
SELECT pglogical.alter_subscription_disable('docs_lab_subscription',true);
 alter_subscription_disable
----------------------------
 t
(1 row)
```

3. Obtenga el identificador del nodo publicador consultando el `pg_replication_origin` de la siguiente manera.

```
SELECT * FROM pg_replication_origin;
 roident |               roname
---------+-------------------------------------
       1 | pgl_labdb_docs_labcb4fa94_docs_lab3de412c
(1 row)
```

4. Utilice la respuesta del paso anterior con el comando `pg_replication_origin_create` para asignar el identificador que podrá utilizar la suscripción cuando se restablezca.

```
SELECT pg_replication_origin_create('pgl_labdb_docs_labcb4fa94_docs_lab3de412c');
  pg_replication_origin_create
------------------------------
                            1
(1 row)
```

5. Para activar la suscripción, introduzca su nombre con un estado de `true`, tal como se muestra en el ejemplo siguiente.

```
SELECT pglogical.alter_subscription_enable('docs_lab_subscription',true);
  alter_subscription_enable
---------------------------
 t
(1 row)
```

Compruebe el estado del nodo. Su estado debería ser `replicating`, tal y como se muestra en este ejemplo.

```
SELECT subscription_name,status,slot_name
  FROM pglogical.show_subscription_status();
            subscription_name |   status    |              slot_name
------------------------------+-------------+-------------------------------------
 docs_lab_subscription         | replicating |
 pgl_labdb_docs_lab98f517b_docs_lab3de412c
(1 row)
```

Compruebe el estado de la ranura de replicación del suscriptor en el nodo publicador. La columna `active` de la ranura debe devolver `t` (true), lo que indica que se ha restablecido la replicación.

```
SELECT slot_name,plugin,slot_type,active
  FROM pg_replication_slots;
                   slot_name              |      plugin      | slot_type | active
------------------------------------------+------------------+-----------+--------
 pgl_labdb_docs_lab98f517b_docs_lab3de412c | pglogical_output | logical   | t
(1 row)
```

Administración de ranuras de replicación lógica para RDS para PostgreSQL

Para poder realizar una actualización de una versión principal en instancia de base de datos de RDS para PostgreSQL que se utilice como nodo publicador en un escenario de replicación lógica, debe eliminar todas las ranuras de replicación de la instancia. El proceso de comprobación previa de la actualización de la versión principal le indica que la actualización no puede continuar hasta que se eliminen las ranuras disponibles.

Para eliminar ranuras de su instancia de base de datos de RDS para PostgreSQL, primero elimine la suscripción y, a continuación, elimine la ranura.

Para identificar las ranuras de replicación que se crearon con la extensión `pglogical`, inicie sesión en cada base de datos y obtenga el nombre de los nodos. Al consultar el nodo suscriptor, aparecen los nodos publicador y suscriptor en el resultado, tal como se muestra en este ejemplo.

```
SELECT * FROM pglogical.node;
node_id   |     node_name
------------+-------------------
 2182738256 | docs_lab_target
 3410995529 | docs_lab_provider
(2 rows)
```

Puede obtener los detalles de la suscripción con la siguiente consulta.

```
SELECT sub_name,sub_slot_name,sub_target
  FROM pglogical.subscription;
 sub_name |         sub_slot_name          | sub_target
----------+--------------------------------+------------
  docs_lab_subscription     | pgl_labdb_docs_labcb4fa94_docs_lab3de412c | 2182738256
(1 row)
```

Ahora puede eliminar la suscripción de la siguiente manera.

```
SELECT pglogical.drop_subscription(subscription_name := 'docs_lab_subscription');
```

```
 drop_subscription
------------------
                 1
(1 row)
```

Después de eliminar la suscripción, puede eliminar el nodo.

```
SELECT pglogical.drop_node(node_name := 'docs-lab-subscriber');
 drop_node
-----------
 t
(1 row)
```

Puede comprobar que el nodo ya no existe de la siguiente manera.

```
SELECT * FROM pglogical.node;
 node_id | node_name
---------+-----------
(0 rows)
```

Referencia de parámetros para la extensión pglogical

En la tabla verá los parámetros asociados a la extensión `pglogical`. Parámetros como `pglogical.conflict_log_level` y `pglogical.conflict_resolution` se utilizan para gestionar los conflictos de actualización. Pueden surgir conflictos cuando los cambios se realizan localmente en las mismas tablas que están suscritas a los cambios del publicador. Los conflictos también pueden producirse en varios escenarios, como la replicación bidireccional o cuando varios suscriptores replican desde el mismo publicador. Para obtener más información, consulte PostgreSQL bi-directional replication using pglogical (Replicación bidireccional de PostgreSQL mediante pglogical).

Parámetro	Descripción
pglogical.batch_inserts	Inserciones por lotes si es posible. No establecido de manera predeterminada. Se cambia a 1 para activarlo y a 0 para desactivarlo.
pglogical.conflict_log_level	Establece el nivel de registro utilizado para registrar los conflicto s resueltos. Los valores permitidos son debug5, debug4,

Parámetro	Descripción
	debug3, debug2, debug1, info, notice, warning, error, log, fatal y panic.
pglogical.conflict_resolution	Establece el método que se utilizará para resolver conflictos si es posible resolverlos. Los valores de cadena admitidos son error, apply_remote, keep_local, last_update_wins y first_update_wins.
pglogical.extra_connection_options	Opciones de conexión a añadir a todas las conexiones de los nodos pares.
pglogical.synchronous_commit	valor de confirmación sincrónica específico de pglogical
pglogical.use_spi	Utilice la SPI (interfaz de programación de servidores) en lugar de la API de nivel inferior para aplicar los cambios. Se establece en 1 para activarlo y en 0 para desactivarlo. Para obtener más información acerca de la SPI, consulte Server Programming Interface (Interfaz de programación de servidores) en la documentación de PostgreSQL.

Uso de pgactive para admitir la replicación activa-activa

La extensión `pgactive` utiliza la replicación activa-activa para admitir y coordinar las operaciones de escritura en varias bases de datos de RDS para PostgreSQL. Amazon RDS para PostgreSQL admite la extensión `pgactive` en las siguientes versiones:

- RDS para PostgreSQL, versiones 17.0 y todas las posteriores
- RDS para PostgreSQL 16.1 y versiones 16 posteriores
- RDS para PostgreSQL 15.2-R2 y versiones 15 posteriores
- RDS para PostgreSQL 14.10 y versiones 14 posteriores
- RDS para PostgreSQL 13.13 y versiones 13 posteriores
- RDS para PostgreSQL 12.17 y versiones 12 posteriores
- RDS para PostgreSQL 11.22

> **Note**
>
> Cuando hay operaciones de escritura en más de una base de datos en una configuración de replicación, es posible que surjan conflictos. Para obtener más información, consulte Gestión de conflictos en la replicación activa-activa

Temas

- Limitaciones de la extensión pgactive
- Inicialización de la capacidad de la extensión pgactive
- Configuración de la replicación activa-activa para las instancias de base de datos de RDS para PostgreSQL
- Medición del retraso de réplica entre miembros de pgactive
- Configuración de los ajustes de parámetros para la extensión pgactive
- Comprensión de conflictos activo-activo
- Descripción del esquema de pgactive
- Referencia de funciones de pgactive
- Gestión de conflictos en la replicación activa-activa
- Gestión de secuencias en la replicación activa-activa

Limitaciones de la extensión pgactive

- Todas las tablas requieren una clave principal; de lo contrario, no se permiten operaciones para actualizar ni eliminar. Los valores de la columna de clave principal no deberían actualizarse.
- Las secuencias pueden tener huecos y, a veces, es posible que no sigan un orden. Las secuencias no se replican. Para obtener más información, consulte Gestión de secuencias en la replicación activa-activa.
- Los DDL y los objetos grandes no se replican.
- Los índices únicos secundarios pueden provocar divergencias en los datos.
- La intercalación debe ser idéntica en todos los nodos del grupo.
- El equilibrador de carga entre los nodos es un antipatrón.
- Las transacciones grandes pueden provocar retardos en la replicación.

Inicialización de la capacidad de la extensión pgactive

Para inicializar la capacidad de la extensión `pgactive` en la instancia de base de datos de RDS para PostgreSQL, defina el valor del parámetro `rds.enable_pgactive` en `1` y, a continuación, cree la extensión en la base de datos. Al hacerlo, se activan automáticamente los parámetros `rds.logical_replication` `track_commit_timestamp` y se establece el valor de `wal_level` en `logical`.

Debe tener permisos como el rol `rds_superuser` para realizar estas tareas.

Puede usar la AWS Management Console o la AWS CLI para crear las instancias de base de datos de RDS para PostgreSQL necesarias. En los pasos siguientes, se supone que la instancia de base de datos de RDS para PostgreSQL está asociada a un grupo de parámetros de base de datos personalizado. Para obtener información sobre la creación de un grupo de parámetros de base de datos personalizado, consulte Grupos de parámetros para Amazon RDS.

Consola

Para inicializar la capacidad de la extensión pgactive

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija su instancia de base de datos de RDS para PostgreSQL.

3. Abra la pestaña Configuración para su instancia de base de datos de RDS para PostgreSQL. En los detalles de la instancia, busque el enlace Grupo de parámetros de instancia de base de datos.
4. Elija el enlace para abrir los parámetros personalizados asociados a la instancia de base de datos de RDS para PostgreSQL.
5. Busque el parámetro `rds.enable_pgactive` y configúrelo en 1 para inicializar la capacidad `pgactive`.
6. Seleccione Save changes (Guardar cambios).
7. En el panel de navegación de la consola de Amazon RDS, elija Bases de datos.
8. Seleccione su instancia de base de datos de RDS para PostgreSQL y, a continuación, seleccione Reinicio en el menú Acciones.
9. Confirme el reinicio de la instancia de base de datos para que sus cambios se apliquen.
10. Cuando la instancia de base de datos esté disponible, podrá utilizar `psql` o cualquier otro cliente de PostgreSQL para conectarse a la instancia de base de datos de RDS para PostgreSQL.

    En el siguiente ejemplo, se asume que su instancia de base de datos de RDS para PostgreSQL tiene una base de datos predeterminada llamada *`postgres`*.

    ```
    psql --host=mydb.111122223333.aws-region.rds.amazonaws.com --port=5432 --
    username=postgres --password=PASSWORD --dbname=postgres
    ```

11. Para comprobar que pgactive esté inicializado, ejecute el siguiente comando.

    ```
    postgres=>SELECT setting ~ 'pgactive'
    FROM pg_catalog.pg_settings
    WHERE name = 'shared_preload_libraries';
    ```

    Si `pgactive` está en `shared_preload_libraries`, el comando anterior devolverá lo siguiente:

    ```
    ?column?
    ----------
     t
    ```

AWS CLI

Para inicializar la capacidad de la extensión pgactive

Para inicializar `pgactive` utilizando la AWS CLI, llame a la operación modify-db-parameter-group para modificar determinados parámetros de su grupo de parámetros personalizado, tal como se muestra en el siguiente procedimiento.

1. Utilice el siguiente comando de la AWS CLI para configurar `rds.enable_pgactive` en 1 para inicializar la capacidad `pgactive` de la instancia de base de datos de RDS para PostgreSQL.

```
postgres=>aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=rds.enable_pgactive,ParameterValue=1,ApplyMethod=pending-reboot" \
   --region aws-region
```

2. Utilice el siguiente comando de la AWS CLI para reiniciar la instancia de base de datos de RDS para PostgreSQL para que se inicialice la biblioteca de `pgactive`.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

3. Cuando la instancia esté disponible, use `psql` para conectarse a la instancia de base de datos de RDS para PostgreSQL.

```
psql --host=mydb.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=master user --password=PASSWORD --dbname=postgres
```

4. Para comprobar que pgactive esté inicializado, ejecute el siguiente comando.

```
postgres=>SELECT setting ~ 'pgactive'
FROM pg_catalog.pg_settings
WHERE name = 'shared_preload_libraries';
```

   Si `pgactive` está en `shared_preload_libraries`, el comando anterior devolverá lo siguiente:

```
?column?
```

```
----------
 t
```

Configuración de la replicación activa-activa para las instancias de base de datos de RDS para PostgreSQL

En el siguiente procedimiento, se muestra cómo iniciar la replicación activo-activo entre dos instancias de base de datos de RDS para PostgreSQL donde `pgactive` esté disponible. Para ejecutar el ejemplo de alta disponibilidad multirregión, debe implementar instancias de Amazon RDS para PostgreSQL en dos regiones diferentes y configurar la interconexión de VPC. Para obtener más información, consulte Interconexión de VPC.

> **Note**
>
> El envío de tráfico entre varias regiones puede conllevar costes adicionales.

En estos pasos, se asume que la instancia de base de datos de RDS para PostgreSQL se ha habilitado con la extensión `pgactive`. Para obtener más información, consulte Inicialización de la capacidad de la extensión pgactive.

Para configurar la primera instancia de base de datos de RDS para PostgreSQL con la extensión **`pgactive`**

En el siguiente ejemplo, se ilustra cómo se crea el grupo `pgactive`, junto con otros pasos necesarios para crear la extensión `pgactive` en la instancia de base de datos de RDS para PostgreSQL.

1. Utilice `psql` u otra herramienta de cliente para conectarse a su primera instancia de base de datos de RDS para PostgreSQL.

   ```
   psql --host=firstinstance.111122223333.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password=PASSWORD --dbname=postgres
   ```

2. Cree una base de datos en la instancia de RDS para PostgreSQL mediante el siguiente comando:

   ```
   postgres=> CREATE DATABASE app;
   ```

3. Cambie la conexión a la nueva base de datos mediante el siguiente comando:

```
\c app
```

4. Cree y rellene una tabla de ejemplo utilizando las siguientes instrucciones SQL:

   a. Cree una tabla de ejemplo con la siguiente instrucción SQL.

```
app=> CREATE SCHEMA inventory;
CREATE TABLE inventory.products (
id int PRIMARY KEY, product_name text NOT NULL,
created_at timestamptz NOT NULL DEFAULT CURRENT_TIMESTAMP);
```

   b. Rellene la tabla con algunos datos de ejemplo mediante la siguiente instrucción SQL.

```
app=> INSERT INTO inventory.products (id, product_name)
VALUES (1, 'soap'), (2, 'shampoo'), (3, 'conditioner');
```

   c. Compruebe que los datos existen en la tabla mediante la siguiente instrucción SQL.

```
 app=>SELECT count(*) FROM inventory.products;

 count
-------
 3
```

5. Cree la extensión `pgactive` en la base de datos existente.

```
app=> CREATE EXTENSION pgactive;
```

6. Para crear e inicializar el grupo pgactive use los siguientes comandos:

```
app=>
-- connection info for endpoint1
CREATE SERVER pgactive_server_endpoint1
    FOREIGN DATA WRAPPER pgactive_fdw
    OPTIONS (host '<endpoint1>', dbname 'app');
CREATE USER MAPPING FOR postgres
    SERVER pgactive_server_endpoint1
    OPTIONS (user 'postgres', password '<password>');
      -- connection info for endpoint2
CREATE SERVER pgactive_server_endpoint2
```

```
    FOREIGN DATA WRAPPER pgactive_fdw
    OPTIONS (host '<endpoint2>', dbname 'app');
CREATE USER MAPPING FOR postgres
    SERVER pgactive_server_endpoint2
    OPTIONS (user 'postgres', password '<password>');
```

Ahora puede inicializar el grupo de replicación y agregar esta primera instancia:

```
SELECT pgactive.pgactive_create_group(
    node_name := 'endpoint1-app',
    node_dsn := 'user_mapping=postgres
 pgactive_foreign_server=pgactive_server_endpoint1'

);
```

Utilice los siguientes comandos como método alternativo, aunque menos seguro, para crear e inicializar el grupo pgactive:

```
app=> SELECT pgactive.pgactive_create_group(
    node_name := 'node1-app',
    node_dsn := 'dbname=app host=firstinstance.111122223333.aws-
region.rds.amazonaws.com user=postgres password=PASSWORD');
```

node1-app es el nombre que se asigna para identificar de forma exclusiva un nodo del grupo `pgactive`.

> **Note**
>
> Para realizar este paso correctamente en una instancia de base de datos de acceso público, debe activar el parámetro `rds.custom_dns_resolution` configurándolo en 1.

7. Para comprobar si la instancia de base de datos está lista, utilice el siguiente comando:

```
app=> SELECT pgactive.pgactive_wait_for_node_ready();
```

Si el comando se ejecuta correctamente, verá el siguiente resultado:

```
pgactive_wait_for_node_ready
-----------------------------
(1 row)
```

Para configurar la segunda instancia de RDS para PostgreSQL y unirla al grupo **`pgactive`**

En el siguiente ejemplo, se ilustra cómo puede unir una instancia de base de datos de RDS para PostgreSQL al grupo `pgactive`, junto con otros pasos necesarios para crear la extensión `pgactive` en la instancia de base de datos.

En estos pasos se asume que otras instancias de base de datos de RDS para PostgreSQL se han configurado con la extensión `pgactive`. Para obtener más información, consulte Inicialización de la capacidad de la extensión pgactive.

1. Utilice `psql` para conectarse a la instancia en la que desea recibir actualizaciones del publicador.

```
psql --host=secondinstance.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password=PASSWORD --dbname=postgres
```

2. Cree una base de datos en la segunda instancia de base de datos de RDS para PostgreSQL mediante el siguiente comando:

```
postgres=> CREATE DATABASE app;
```

3. Cambie la conexión a la nueva base de datos mediante el siguiente comando:

```
\c app
```

4. Cree la extensión `pgactive` en la base de datos existente.

```
app=> CREATE EXTENSION pgactive;
```

5. Una la segunda instancia de base de datos de RDS para PostgreSQL al grupo `pgactive` de una forma más segura mediante los siguientes comandos:

```
-- connection info for endpoint1
```

```
CREATE SERVER pgactive_server_endpoint1
    FOREIGN DATA WRAPPER pgactive_fdw
    OPTIONS (host '<endpoint1>', dbname 'app');
CREATE USER MAPPING FOR postgres
    SERVER pgactive_server_endpoint1
    OPTIONS (user 'postgres', password '<password>');

-- connection info for endpoint2
CREATE SERVER pgactive_server_endpoint2
    FOREIGN DATA WRAPPER pgactive_fdw
    OPTIONS (host '<endpoint2>', dbname 'app');
CREATE USER MAPPING FOR postgres
    SERVER pgactive_server_endpoint2
    OPTIONS (user 'postgres', password '<password>');
```

```
SELECT pgactive.pgactive_join_group(
    node_name := 'endpoint2-app',
    node_dsn := 'user_mapping=postgres
 pgactive_foreign_server=pgactive_server_endpoint2',
    join_using_dsn := 'user_mapping=postgres
 pgactive_foreign_server=pgactive_server_endpoint1'
);
```

Utilice los siguientes comandos como método alternativo, aunque menos seguro, para unir la segunda instancia de base de datos de RDS para PostgreSQL al grupo `pgactive`

```
app=> SELECT pgactive.pgactive_join_group(
node_name := 'node2-app',
node_dsn := 'dbname=app host=secondinstance.111122223333.aws-
region.rds.amazonaws.com user=postgres password=PASSWORD',
join_using_dsn := 'dbname=app host=firstinstance.111122223333.aws-
region.rds.amazonaws.com user=postgres password=PASSWORD');
```

node2-app es el nombre que se asigna para identificar de forma exclusiva un nodo del grupo `pgactive`.

6. Para comprobar si la instancia de base de datos está lista, utilice el siguiente comando:

```
app=> SELECT pgactive.pgactive_wait_for_node_ready();
```

Si el comando se ejecuta correctamente, verá el siguiente resultado:

```
pgactive_wait_for_node_ready
-----------------------------
(1 row)
```

Si la primera base de datos de RDS para PostgreSQL es relativamente grande, puede ver que `pgactive.pgactive_wait_for_node_ready()`emite el informe de progreso de la operación de restauración. El resultado tiene un aspecto similar al siguiente:

```
NOTICE:  restoring database 'app', 6% of 7483 MB complete
NOTICE:  restoring database 'app', 42% of 7483 MB complete
NOTICE:  restoring database 'app', 77% of 7483 MB complete
NOTICE:  restoring database 'app', 98% of 7483 MB complete
NOTICE:  successfully restored database 'app' from node node1-app in
 00:04:12.274956
 pgactive_wait_for_node_ready
-----------------------------
(1 row)
```

A partir de este momento, `pgactive` sincroniza los datos entre las dos instancias de base de datos.

7. Puede utilizar el siguiente comando para comprobar si la base de datos de la segunda instancia de base de datos contiene los datos:

```
app=> SELECT count(*) FROM inventory.products;
```

Si los datos se sincronizan correctamente, verá el siguiente resultado:

```
 count
-------
 3
```

8. Ejecute el siguiente comando para insertar nuevos valores:

```
app=> INSERT INTO inventory.products (id, product_name) VALUES (4, 'lotion');
```

9. Conéctese a la base de datos de la primera instancia de base de datos y ejecute la siguiente consulta:

   ```
   app=> SELECT count(*) FROM inventory.products;
   ```

   Si se inicializa la replicación activa-activa, el resultado es similar al siguiente:

   ```
   count
   -------
    4
   ```

Para separar y eliminar una instancia de base de datos del grupo **`pgactive`**

Para separar y eliminar una instancia de base de datos del grupo `pgactive`, siga estos pasos:

1. Puede separar la segunda instancia de base de datos de la primera instancia de base de datos mediante el siguiente comando:

   ```
   app=> SELECT * FROM pgactive.pgactive_detach_nodes(ARRAY['node2-app']);
   ```

2. Elimine la extensión `pgactive` de la segunda instancia de base de datos mediante el siguiente comando:

   ```
   app=> SELECT * FROM pgactive.pgactive_remove();
   ```

   Para eliminar la extensión a la fuerza:

   ```
   app=> SELECT * FROM pgactive.pgactive_remove(true);
   ```

3. Suelte la extensión con el siguiente comando:

   ```
   app=> DROP EXTENSION pgactive;
   ```

Medición del retraso de réplica entre miembros de pgactive

Puede utilizar la siguiente consulta para ver el retraso de réplica entre los miembros de `pgactive`. Ejecute esta consulta en todos los nodos de `pgactive` para obtener una idea completa.

```
app=> SELECT * FROM pgactive.pgactive_get_replication_lag_info();
#-[ RECORD 1 ]--------+---------------------------------------------
#node_name            | node2-app
#node_sysid           | 7481018224801653637
#application_name     | pgactive:7481018224801653637:send
#slot_name            | pgactive_16385_7481018224801653637_0_16385__
#active               | t
#active_pid           | 783486
#pending_wal_decoding | 0
#pending_wal_to_apply | 0
#restart_lsn          | 0/2108150
#confirmed_flush_lsn  | 0/2154690
#sent_lsn             | 0/2154690
#write_lsn            | 0/2154690
#flush_lsn            | 0/2154690
#replay_lsn           | 0/2154690
#-[ RECORD 2 ]--------+---------------------------------------------
#node_name            | node1-app
#node_sysid           | 7481018033434600853
#application_name     | pgactive:7481018033434600853:send
#slot_name            | pgactive_16385_7481018033434600853_0_16385__
#active               | t
#active_pid           | 783488
#pending_wal_decoding | 0
#pending_wal_to_apply | 0
#restart_lsn          | 0/20F5AD0
#confirmed_flush_lsn  | 0/214EF68
#sent_lsn             | 0/214EF68
#write_lsn            | 0/214EF68
#flush_lsn            | 0/214EF68
#replay_lsn           | 0/214EF68
```

Supervise los siguientes diagnósticos como mínimo:

activa

Configure alertas cuando el valor activo sea falso, lo que indica que la ranura no está en uso actualmente (la instancia del suscriptor se ha desconectado del publicador).

pending_wal_decoding

En la replicación lógica de PostgreSQL, los archivos WAL se almacenan en formato binario. El publicador debe decodificar estos cambios de WAL y convertirlos en cambios lógicos (como operaciones de inserción, actualización o eliminación).

La métrica pending_wal_decoding muestra el número de archivos WAL que esperan que los descodifique el publicador.

Este número puede aumentar debido a estos factores:

- Cuando el suscriptor no esté conectado, el estado activo será falso y pending_wal_decoding aumentará
- La ranura está activa, pero el publicador no puede mantenerse al día con el volumen de cambios de WAL

pending_wal_to_apply

La métrica pending_wal_apply indica el número de archivos WAL que esperan aplicarse en el suscriptor.

Varios factores pueden impedir que el suscriptor aplique los cambios y potencialmente causar un escenario de disco lleno:

- Diferencias de esquema: por ejemplo, cuando hay cambios en el flujo de WAL de una tabla llamada ejemplo, pero esa tabla no existe en el suscriptor
- Se actualizaron los valores en las columnas de la clave principal
- Los índices únicos secundarios pueden provocar divergencias en los datos

Configuración de los ajustes de parámetros para la extensión pgactive

Puede utilizar la siguiente consulta para ver todos los parámetros asociados a la extensión `pgactive`.

```
app=> SELECT * FROM pg_settings WHERE name LIKE 'pgactive.%';
```

Puede configurar la extensión `pgactive` mediante varios parámetros. Estos parámetros se pueden configurar mediante AWS Management Console o la interfaz de la CLI de AWS.

Parámetros de extensión de pgactive principales

La siguiente tabla proporciona una referencia para los principales parámetros de la extensión `pgactive`:

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.conflict_logging_include_tuples`	`boolean`	–	Registra la información completa de la tupla de la extensión `pgactive`. **Note** Es necesario reiniciar el servidor para que se apliquen los cambios.
`pgactive.log_conflicts_to_table`	`boolean`	–	Determina si la extensión `pgactive` registra los conflictos detectados

Parámetro	Unidad	Predeterminado/a	Descripción
			en la tabla `pgactive.pgactive_conflict_history` . Para obtener más información, consulte registro de conflictos. **Note** Es necesario reiniciar el servidor para que se apliquen los cambios.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.log_conflicts_to_logfile`	`boolean`	–	Determina si la extensión `pgactive` registra los conflictos detectados en el archivo de registro de PostgreSQL. Para obtener más información, consulte registro de conflictos. **Note** Es necesario reiniciar el servidor para que se apliquen los cambios.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.synchronous_commit`	`boolean`	off	Determina el comportamiento de confirmación de los trabajadores de aplicación de pgactive. Cuando está desactivado, los trabajadores de aplicación realizan confirmaciones asíncronas, lo que mejora el rendimiento de PostgreSQL durante las operaciones de aplicación, pero retrasa las confirmaciones de reproducción hacia el nodo ascendente. Establecerlo en `off` siempre es seguro y no provocará pérdidas ni omisiones de transacciones. Esta configuración solo afecta

Parámetro	Unidad	Predeterminado/a	Descripción
			al momento de las descargas a disco en el nodo descendente y cuándo se envían las confirmaciones al nodo ascendente. El sistema retrasa el envío de las confirmaciones de vaciado de reproducción hasta que las confirmaciones se vuelcan al disco mediante operaciones no relacionadas, como puntos de control o trabajos periódicos. Sin embargo, si el nodo ascendente tiene el nodo descendente en `synchronous_standby_names`, establecerlo en `off` hace que las confirmaciones sincrónic

Parámetro	Unidad	Predeterminado/a	Descripción
			as en el nodo ascendente tarden más en informar del éxito al cliente. En este caso, establezca el parámetro en on. **Note** Incluso cuando este parámetro se establece en on con nodos en `synchronous_standby_names`, pueden producirse conflictos de replicación en las configuraciones activo-activo. Esto

Parámetro	Unidad	Predeterminado/a	Descripción
			se debe a que el sistema carece de bloqueo entre nodos y de gestión global de instantáneas, lo que permite que las transacciones concurrentes en distintos nodos modifiquen la misma tupla. Además, las transacciones solo comienzan a replicars

Parámetro	Unidad	Predeterminado/a	Descripción
			e después de confirmarse en el nodo ascendente. La habilitación de la confirmación sincrónica no transforma la extensión pgactive en un sistema siempre coherente.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.temp_dump_directory`	`string`	–	Define la ruta de almacenamiento temporal necesaria para las operaciones de clonación de bases de datos durante la configuración inicial. En este directorio debe poder escribir el usuario de postgres y debe tener suficiente espacio de almacenamiento para contener un volcado completo de la base de datos. El sistema utiliza esta ubicación solo durante la configuración inicial de la base de datos con operaciones de copia lógica. Este parámetro no lo usa `pgactive_`

Parámetro	Unidad	Predeterminado/a	Descripción
			`init_copy command`.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.max_ddl_lock_delay`	`milliseconds`	`-1`	Especifica el tiempo máximo de espera para el bloqueo DDL antes de interrumpir por la fuerza las transacciones de escritura simultáneas. El valor predeterminado es `-1`, que adopta el valor establecido en `max_standby_streaming_delay` . Este parámetro acepta unidades de tiempo. Por ejemplo, puede configurarlo en 10 s para 10 segundos. Durante este periodo de espera, el sistema intenta adquirir bloqueos DDL mientras espera a que las transacciones de escritura

Parámetro	Unidad	Predeterminado/a	Descripción
			en curso se confirmen o se reviertan. Para obtener más información, consulte Bloqueos DDL.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.ddl_lock_timeout`	`milliseconds`	`-1`	Especifica cuánto tiempo espera un intento de bloqueo DDL para obtener el bloqueo. El valor predeterminado es `-1`, que utiliza el valor especificado en lock_timeout. Puede configurar este parámetro mediante unidades de tiempo como 10 s para 10 segundos. Este temporizador solo controla el periodo de espera para obtener un bloqueo DDL. Una vez que el sistema obtiene el bloqueo e inicia la operación DDL, el temporizador se detiene. Este parámetro no

Parámetro	Unidad	Predeterminado/a	Descripción
			limita la duración total que puede mantenerse un bloqueo DDL ni el tiempo total de la operación DDL. Para controlar la duración total de la operación, utilice `statement_timeout` en su lugar. Para obtener más información, consulte Bloqueos DDL.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.debug_trace_ddl_locks_level`	`boolean`	–	Invalida el nivel de registro de depuración predeterminado para las operaciones de bloqueo DDL en la extensión `pgactive`. Cuando se configura, esta configuración hace que los mensajes relacionados con el bloqueo DDL se emitan en el nivel de depuración LOG en lugar de en su nivel predeterminado. Utilice este parámetro para supervisar la actividad de bloqueo DDL sin activar los niveles de registro detallados `DEBUG1` o `DEBUG2` en todo el servidor.

Parámetro	Unidad	Predeterminado/a	Descripción
			Niveles de registro disponibles, en orden creciente de detalle: • none: los mensajes de bloqueo DDL aparecen solo en los niveles de registro del servidor DEBUG1 e inferiores. • statement: agrega la salida LOG para los intentos de adquisición de bloqueos DDL. • acquire_release: registra los eventos de adquisición, liberación y rechazo de bloqueos, y las aplicaciones de nodos del mismo nivel de

Parámetro	Unidad	Predeterminado/a	Descripción
			bloqueos DDL remotos. • peers: proporciona detalles adicionales sobre las negociaciones de bloqueos DDL entre nodos del mismo nivel. • debug: registra todas las actividades relacionadas con los bloqueos DDL en el nivel de LOG. Para obtener más información acerca de las opciones de supervisión, consulte Supervisión de bloqueos DDL globales.

Parámetro	Unidad	Predeterminado/a	Descripción
			Note Los cambios en esta configuración surten efecto al volver a cargar la configuración. No es necesario reiniciar el servidor.

Parámetros de extensión de pgactive adicionales

La siguiente tabla presenta las opciones de configuración interna y las que se utilizan con menos frecuencia disponibles para la extensión `pgactive`.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.debug_apply_delay`	`integer`	–	Establece un retraso de aplicación (en milisegundos) para las conexiones

Parámetro	Unidad	Predeterminado/a	Descripción
			configuradas que no tienen un retraso de aplicación explícito en su entrada `pgactive.pgactive_connections`. Este retraso se establece durante la creación o la unión del nodo, y pgactive no reproducirá una transacción en los nodos del mismo nivel hasta que hayan transcurrido al menos el número especificado de milisegundos desde que se confirmó. Se utiliza principalmente para simular redes de alta latencia en entornos de

Parámetro	Unidad	Predeterminado/a	Descripción
			prueba para facilitar la creación de conflictos. Por ejemplo, con un retraso de 500 ms en los nodos A y B, dispone de al menos 500 ms para realizar una inserción conflictiva en el nodo B tras insertar un valor en el nodo A. **Note** Requiere una recarga del servidor o un reinicio de los trabajadores de aplicación para que surta efecto.

Parámetro	Unidad	Predeterminado/a	Descripción
pgactive.connectability_check_duration	integer	–	Especifica la duración (en segundos) durante la cual un trabajador de base de datos intenta establecer conexiones durante los intentos erróneos. El trabajador realiza un intento de conexión por segundo hasta que tiene éxito o alcanza este valor de tiempo de espera. Esta configuración resulta útil cuando el motor de base de datos se inicia antes de que el trabajador esté preparado para establecer conexiones.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.skip_ddl_replication`	`boolean`	on	Controla cómo se replican o gestionan los cambios de DDL en Amazon RDS con `pgactive` habilitado. Cuando se establece en on, el nodo procesa los cambios de DDL como un nodo no pgactive. Los siguientes requisitos se aplican al trabajar con este parámetro: • Los nodos nuevos no pueden unirse a un grupo pgactive si su valor de `skip_ddl_replication` difiere del nodo ascendente. • Los nodos existentes no pueden iniciar

Parámetro	Unidad	Predeterminado/a	Descripción
			trabajadores de pgactive si el valor de los parámetros no coincide con el nodo ascendente. • Todos los miembros de pgactive deben usar el mismo valor de parámetro. Puede modificar este parámetro de dos formas con privilegios de superusuario: de forma global o local (nivel de sesión). **Note** Si se cambia este parámetro de forma incorrecta, se pueden interrump

Parámetro	Unidad	Predeterminado/a	Descripción
			ir las configuraciones de replicación.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.do_not_replicate`	`boolean`	–	Este parámetro es solo para uso interno. Cuando se establece este parámetro en una transacción, los cambios no se replican en otros nodos del clúster de base de datos. **Note** Si se cambia este parámetro de forma incorrecta, se pueden interrumpir las configuraciones de replicación.

Parámetro	Unidad	Predeterminado/a	Descripción
pgactive.discard_mismatched_row_attributes	boolean	–	Este parámetro está destinado solo a uso especializado. Recomendamos usar este parámetro solo para solucionar problemas de replicación específicos. Utilice este parámetro cuando: • El flujo de replicación entrante contiene filas con más columnas que la tabla local. • Estas filas remotas contienen valores que no son nulos. Esta configuración invalida el siguiente mensaje de error y permite

Parámetro	Unidad	Predeterminado/a	Descripción
			que surja una divergencia de datos para permitir que la replicación continúe: `cannot right-pad mismatched attributes; attno %u is missing in local table and remote row has non-null, non-dropped value for this attribute` **Note** Si se cambia este parámetro de forma incorrecta, se pueden interrumpir las configura

Parámetro	Unidad	Predeterminado/a	Descripción
			ciones de replicación.

Parámetro	Unidad	Predeterminado/a	Descripción
pgactive.debug_trace_replay	boolean	–	Cuando se establece en on, emite un mensaje de registro para cada acción remota que se aplique posteriormente al proceso de los trabajadores. Los registros incluyen: • Cambio de tipo • Nombre de la tabla afectada • Número de cambios desde el inicio de la transacción • LSN de confirmación de transacción • Marca temporal de confirmación • Identificador de nodo ascendente • Identificador de nodo de

Parámetro	Unidad	Predeterminado/a	Descripción
			reenvío (si corresponde) Los registros también capturan los comandos DDL en cola y las tablas descartadas. para> De forma predeterminada, los registros no incluyen el contenido de los campos de fila. Para incluir valores de fila en los registros, debe volver a compilarlos con los siguientes indicadores habilitados: • VERBOSE_INSERT • VERBOSE_UPDATE • VERBOSE_DELETE

Parámetro	Unidad	Predeterminado/a	Descripción
			Note La habilitación de esta configuración de registro puede afectar al rendimiento. Recomendamos habilitarla solo cuando sea necesario para solucionar problemas. Los cambios en esta configuración surten efecto al volver a cargar la configura

Parámetro	Unidad	Predeterminado/a	Descripción
			ción. No es necesario reiniciar el servidor.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.extra_apply_connection_options`		–	Puede configurar los parámetros de conexión para todas las conexiones de nodos del mismo nivel con los nodos de pgactive. Estos parámetros controlan ajustes como keepalive y los modos SSL. De forma predeterminada, pgactive utiliza los siguientes parámetros de conexión: • connect_timeout=30 • keepalives=1 • keepalives_idle=20 • keepalives_interval=20 • keepalives_count=5 Para invalidar los parámetros predeterm

Parámetro	Unidad	Predeterminado/a	Descripción
			inados, utilice el siguiente comando similar: `pgactive.extra_apply_connection_options = 'keepalives=0'` Las cadenas de conexión de los nodos individuales tienen prioridad sobre estas configuraciones y sobre las opciones de conexión integradas de pgactive. Para obtener más información acerca de los formatos de cadenas de conexión, consulte cadenas de conexión libpq. Recomendamos mantener

Parámetro	Unidad	Predeterminado/a	Descripción
			habilitada la configuración predeterminada de keepalive . Desactive keepalive solo si tiene problemas al realizar grandes transacciones a través de redes poco fiables. **Note** Recomendamos mantener habilitada la configuración predeterminada de keepalive . Desactive keepalive solo si tiene problemas al realizar grandes

Parámetro	Unidad	Predeterminado/a	Descripción
			transacciones a través de redes poco fiables. Los cambios en esta configuración surten efecto al volver a cargar la configuración. No es necesario reiniciar el servidor.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.init_node_parallel_jobs (int)`		–	Especifica el número de trabajos paralelos que `pg_dump` y `pg_restore` pueden utilizar durante las uniones de nodos lógicos con la función `pgactive.pgactive_join_group` . Los cambios en esta configuración surten efecto al volver a cargar la configuración. No es necesario reiniciar el servidor.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.max_nodes`	`int`	4	Especifica el número máximo de nodos permitidos en un grupo de extensiones de pgactive. El valor predeterminado es 4 nodos. Debe tener en cuenta lo siguiente al configurar el valor de este parámetro: • Todos los nodos de un grupo de extensión de pgactive deben usar el mismo valor de parámetro. • Un nodo nuevo no se puede unir si el valor de su parámetro es diferente al del nodo ascendente.

Parámetro	Unidad	Predeterminado/a	Descripción
			• Los nodos existentes no pueden iniciar los trabajadores de extensión de pgactive si el valor de sus parámetros es diferente al del nodo ascendente. • Los grupos más grandes requieren un esfuerzo adicional de supervisión y mantenimiento, por lo que debe establecer el valor de este parámetro con prudencia. Puede configurar este parámetro de dos maneras: en el archivo de configuración, mediante el

Parámetro	Unidad	Predeterminado/a	Descripción
			comando `ALTER SYSTEM SET` El valor predeterminado de este parámetro es `4`, lo que significa que puede haber un máximo de 4 nodos permitidos en el grupo de extensiones de `pgactive` en cualquier momento. **Note** El cambio surtirá efecto después de reiniciar el servidor.

Parámetro	Unidad	Predeterminado/a	Descripción
`pgactive.permit_node_identifier_getter_function_creation`	`boolean`	–	Este parámetro está destinado solo a uso interno. Cuando está habilitada, la extensión `pgactive` permite la creación de la función de obtención del identificador de nodo de pgactive.

Comprensión de conflictos activo-activo

Cuando se utiliza pgactive en el modo activo-activo, escribir en las mismas tablas desde varios nodos puede crear conflictos de datos. Aunque algunos sistemas de agrupación en clústeres utilizan bloqueos distribuidos para evitar el acceso simultáneo, pgactive adopta un enfoque optimista que se adapta mejor a las aplicaciones distribuidas geográficamente.

Algunos sistemas de agrupación en clústeres de bases de datos impiden el acceso simultáneo a los datos mediante el uso de bloqueos distribuidos. Aunque este enfoque funciona cuando los servidores están muy cerca, no admite aplicaciones distribuidas geográficamente porque requiere una latencia extremadamente baja para lograr un buen rendimiento. En lugar de utilizar bloqueos distribuidos (un enfoque pesimista), la extensión pgactive utiliza un enfoque optimista. Esto significa que:

- Ayuda a evitar conflictos cuando es posible.
- Permite que se produzcan determinados tipos de conflictos.
- Proporciona resolución de conflictos cuando se producen conflictos.

Este enfoque le proporciona más flexibilidad a la hora de crear aplicaciones distribuidas.

Cómo se producen los conflictos

Los conflictos entre nodos surgen de secuencias de eventos que no podrían ocurrir si todas las transacciones implicadas se produjeran simultáneamente en el mismo nodo. Como los nodos solo intercambian cambios una vez confirmadas las transacciones, cada transacción es válida individualmente en el nodo en el que se ha confirmado, pero no lo sería si se ejecutara en otro nodo que haya realizado otras tareas mientras tanto. Dado que la aplicación de pgactive básicamente reproduce la transacción en los demás nodos, la operación de reproducción puede producir un error si hay un conflicto entre una transacción que se está aplicando y una transacción que se ha confirmado en el nodo receptor.

La razón por la que la mayoría de los conflictos no se producen cuando todas las transacciones se ejecutan en un único nodo es que PostgreSQL cuenta con mecanismos de comunicación entre transacciones para evitarlos, entre los que se incluyen:

- Índices UNIQUE
- SEQUENCE
- Bloqueo de filas y relaciones
- Seguimiento de dependencias SERIALIZABLE

Todos estos mecanismos son formas de comunicarse entre transacciones para evitar problemas de concurrencia no deseados

pgactive logra una baja latencia y maneja bien las particiones de la red porque no utiliza un administrador de transacciones distribuido o un administrador de bloqueos. Sin embargo, esto significa que las transacciones en diferentes nodos se ejecutan completamente aisladas unas de otras. Aunque el aislamiento suele mejorar la coherencia de la base de datos, en este caso es necesario reducir el aislamiento para evitar conflictos.

Tipos de conflictos

Los conflictos que se pueden producir son:

Temas

- Conflictos de PRIMARY KEY o UNIQUE
- Conflictos INSERT/INSERT
- INSERT que infringen múltiples restricciones UNIQUE

- Conflictos UPDATE/UPDATE
- Conflictos UPDATE en la PRIMARY KEY
- UPDATE que infringen varias restricciones UNIQUE
- Conflictos UPDATE/DELETE
- Conflictos INSERT/UPDATE
- Conflictos DELETE/DELETE
- Conflictos de restricciones de clave externa
- Conflictos de restricciones de exclusión
- Conflictos de datos globales
- Conflictos de bloqueo y anulaciones de bloqueo
- Conflictos divergentes

Conflictos de PRIMARY KEY o UNIQUE

Los conflictos de filas se producen cuando varias operaciones intentan modificar la misma clave de fila de formas que no son posibles en un solo nodo. Estos conflictos representan el tipo más común de conflictos de datos.

pgactive resuelve los conflictos detectados mediante el manejo de last-update-wins o el gestor de conflictos personalizado.

Los conflictos de filas incluyen:

- INSERT frente a INSERT
- INSERT frente a UPDATE
- UPDATE frente a DELETE
- INSERT frente a DELETE
- DELETE frente a DELETE
- INSERT frente a DELETE

Conflictos INSERT/INSERT

El conflicto más común se produce cuando los INSERT en dos nodos diferentes crean una tupla con los mismos valores de PRIMARY KEY (o valores de restricción UNIQUE idénticos cuando no existe ninguna PRIMARY KEY).

pgactivelink resuelve los conflictos de INSERT utilizando la marca temporal del host de origen para conservar la tupla más reciente. Puede invalidar este comportamiento predeterminado con el controlador de conflictos personalizado. Aunque este proceso no requiere ninguna acción especial del administrador, tenga en cuenta que pgactivelink descarta una de las operaciones INSERT en todos los nodos. No se produce una fusión automática de datos a menos que el controlador personalizado la implemente.

pgactivelink solo puede resolver conflictos que impliquen una única violación de restricción. Si un INSERT infringe varias restricciones UNIQUE, debe implementar estrategias adicionales de resolución de conflictos.

INSERT que infringen múltiples restricciones UNIQUE

Un conflicto INSERT/INSERT puede infringir varias restricciones UNIQUE, incluida la PRIMARY KEY. pgactivelink solo puede gestionar conflictos que impliquen una única restricción UNIQUE. Cuando los conflictos infringen varias restricciones UNIQUE, el trabajador de aplicación produce un error y devuelve el siguiente error:

```
multiple unique constraints violated by remotely INSERTed tuple.
```

En versiones anteriores, esta situación generaba un error de "conflicto de unicidad divergente" en su lugar.

Para resolver estos conflictos, debe tomar medidas manuales. O bien DELETE las tuplas locales en conflicto o UPDATE las mismas para eliminar los conflictos con la nueva tupla remota. Tenga en cuenta que puede que tenga que abordar varias tuplas conflictivas. Actualmente, pgactivelink no proporciona ninguna funcionalidad integrada para ignorar, descartar o fusionar las tuplas que infringen múltiples restricciones únicas.

> **Note**
>
> Para obtener más información, consulte UPDATE que infringen varias restricciones UNIQUE.

Conflictos UPDATE/UPDATE

Este conflicto se produce cuando dos nodos modifican simultáneamente la misma tupla sin cambiar su PRIMARY KEY. pgactivelink resuelve estos conflictos mediante la lógica last-update-wins o el controlador de conflictos personalizado, si está definido. Una PRIMARY KEY es esencial para la

coincidencia de tuplas y la resolución de conflictos. En el caso de las tablas sin una PRIMARY KEY, pgactivelink rechaza las operaciones UPDATE con el siguiente error:

```
Cannot run UPDATE or DELETE on table (tablename) because it does not have a primary key.
```

Conflictos UPDATE en la PRIMARY KEY

Pgactive tiene limitaciones a la hora de gestionar las actualizaciones de PRIMARY KEY. Aunque puede realizar la operación UPDATE en una PRIMARY KEY, pgactive no puede resolver automáticamente los conflictos utilizando la lógica last-update-wins para estas operaciones. Debe asegurarse de que las actualizaciones de la PRIMARY KEY no entren en conflicto con los valores existentes. Si se producen conflictos durante las actualizaciones de PRIMARY KEY, se convierten en conflictos divergentes que requieren su intervención manual. Para obtener más información acerca de cómo manejar estas situaciones, consulte Conflictos divergentes.

UPDATE que infringen varias restricciones UNIQUE

pgactivelink no puede aplicar la resolución de conflictos last-update-wins cuando una UPDATE entrante infringe varias restricciones UNIQUE o valores de PRIMARY KEY. Este comportamiento es similar a las operaciones INSERT con múltiples infracciones de restricciones. Estas situaciones crean conflictos divergentes que requieren su intervención manual. Para obtener más información, consulte Conflictos divergentes.

Conflictos UPDATE/DELETE

Estos conflictos se producen cuando un nodo realiza una UPDATE en una fila mientras que otro nodo la DELETE simultáneamente. En este caso, se produce un conflicto UPDATE/DELETE durante la reproducción. La solución consiste en descartar cualquier UPDATE que llegue después de una DELETE, a menos que el gestor de conflictos personalizado especifique lo contrario.

pgactivelink requiere una PRIMARY KEY para hacer coincidir las tuplas y resolver los conflictos. Para las tablas sin una PRIMARY KEY, rechaza las operaciones DELETE con el siguiente error:

```
Cannot run UPDATE or DELETE on table (tablename) because it does not have a primary key.
```

> **Note**
>
> pgactivelink no puede distinguir entre los conflictos de UPDATE/DELETE e INSERT/UPDATE. En ambos casos, una UPDATE afecta a una fila que no existe. Debido a la

replicación asíncrona y a la falta de orden de reproducción entre los nodos, pgactivelink no puede determinar si la UPDATE es para una fila nueva (aún no se ha recibido INSERT) o para una fila eliminada. En ambos casos, pgactivelink descarta la UPDATE.

Conflictos INSERT/UPDATE

Este conflicto se puede producir en entornos de varios nodos. Ocurre cuando un nodo INSERT una fila, un segundo nodo la UPDATE y un tercer nodo recibe la UPDATE antes que el INSERT original. De forma predeterminada, pgactivelink resuelve estos conflictos descartando la UPDATE, a menos que el desencadenador de conflictos personalizado especifique lo contrario. Tenga en cuenta que este método de resolución puede provocar incoherencias en los datos entre los nodos. Para obtener más información acerca de escenarios similares y su manejo, consulte Conflictos UPDATE/DELETE.

Conflictos DELETE/DELETE

Este conflicto se produce cuando dos nodos diferentes eliminan simultáneamente la misma tupla. pgactivelink considera que estos conflictos son inofensivos porque ambas operaciones DELETE tienen el mismo resultado final. En este escenario, pgactivelink ignora de forma segura una de las operaciones DELETE sin afectar a la coherencia de datos.

Conflictos de restricciones de clave externa

Las restricciones de FOREIGN KEY pueden provocar conflictos al aplicar transacciones remotas a los datos locales existentes. Estos conflictos suelen producirse cuando las transacciones se aplican en una secuencia diferente a su orden lógico en los nodos de origen.

De forma predeterminada, pgactive aplica los cambios con session_replication_role como `replica`, lo que evita las comprobaciones de claves externas durante la replicación. En las configuraciones activo-activo, esto puede provocar infracciones de claves externas. La mayoría de las infracciones son temporales y se resuelven una vez que la replicación se pone al día. Sin embargo, pueden producirse claves externas huérfanas porque pgactive no admite el bloqueo de filas entre nodos.

Este comportamiento es inherente a los sistemas activo-activo asíncronos tolerantes a las particiones. Por ejemplo, el nodo A puede insertar una nueva fila secundaria mientras que el nodo B elimina simultáneamente su fila principal. El sistema no puede impedir este tipo de modificación concurrente entre nodos.

Para minimizar los conflictos de claves externas, recomendamos lo siguiente:

- Limitar las relaciones de claves externas a entidades estrechamente relacionadas.

- Modificar las entidades relacionadas desde un solo nodo cuando sea posible.
- Elegir entidades que rara vez requieran modificación.
- Implementar un control de concurrencia en el nivel de aplicación para las modificaciones.

Conflictos de restricciones de exclusión

pgactive link no admite restricciones de exclusión y restringe su creación.

> **Note**
>
> Si convierte una base de datos independiente existente en una base de datos de pgactivelink, elimine manualmente todas las restricciones de exclusión.

En un sistema asíncrono distribuido, no es posible garantizar que ningún conjunto de filas infrinja la restricción. Esto se debe a que todas las transacciones en los distintos nodos están completamente aisladas. Las restricciones de exclusión pueden provocar bloqueos de reproducción, donde la reproducción no puede avanzar de un nodo a otro debido a infracciones de las restricciones de exclusión.

Si obliga a pgactive Link a crear una restricción de exclusión o si no elimina las existentes al convertir una base de datos independiente en pgactive Link, es probable que la replicación se interrumpa. Para restaurar el progreso de la replicación, elimine o modifique las tuplas locales que entren en conflicto con una tupla remota entrante para poder aplicar la transacción remota.

Conflictos de datos globales

Cuando se utiliza pgactivelink, se pueden producir conflictos cuando los nodos tienen diferentes datos globales de todo el sistema PostgreSQL, como los roles. Estos conflictos pueden provocar que las operaciones (principalmente DDL) se ejecuten correctamente en un nodo, pero que no se apliquen a otros nodos.

Si un usuario existe en un nodo pero no en otro, pueden producirse problemas de replicación:

- Node1 tiene un nombre de usuario `fred`, pero este usuario no existe en Node2
- Cuando `fred` crea una tabla en Node1, la tabla se replica con `fred` como el propietario
- Cuando este comando DDL se aplica al Node2, se produce un error porque el usuario `fred` no existe

- Este error genera un ERROR en los registros de PostgreSQL en Node2 e incrementa el contador `pgactive.pgactive_stats.nr_rollbacks`

Solución: cree el usuario `fred` en Node2. El usuario no necesita permisos idénticos, sino que debe existir en ambos nodos.

Si existe una tabla en un nodo pero no en otro, las operaciones de modificación de datos producirán un error:

- Node1 tiene una tabla llamada `foo` que no existe en Node2
- Cualquier operación DML en la tabla `foo` en el Node1 producirá un error cuando se replique en Node2

Resolución: cree la tabla `foo` en el Node2 con la misma estructura.

> **Note**
>
> Actualmente, pgactivelink no replica los comandos CREATE USER ni las operaciones DDL. La replicación de DDL está prevista para una versión futura.

Conflictos de bloqueo y anulaciones de bloqueo

Como los procesos de aplicación de pgactive funcionan como sesiones de usuario normales, siguen las reglas estándar de bloqueo de filas y tablas. Esto puede provocar que los procesos de aplicación de pgactivelink esperen por bloqueos mantenidos por transacciones de usuarios o por otros procesos de aplicación.

Los siguientes tipos de bloqueos pueden afectar a los procesos de aplicación:

- Bloqueo explícito en el nivel de tabla (LOCK TABLE...) por sesiones de usuario
- Bloqueo explícito en el nivel de fila (SELECT ... FOR UPDATE/FOR SHARE) por sesiones de usuario
- Bloqueo desde claves foráneas
- Bloqueo implícito debido a UPDATE, INSERT o DELETE de filas, ya sea por actividad local o aplicación desde otros servidores

Los bloqueos pueden ocurrir entre:

- Un proceso de aplicación de pgactivelink y una transacción de usuario
- Dos procesos de aplicación

Cuando se producen bloqueos, el detector de bloqueos de PostgreSQL finaliza una de las transacciones problemáticas. Si se termina el proceso del trabajador de aplicación de pgactivelink, este reintenta automáticamente y normalmente tiene éxito.

> **Note**
>
> - Estos problemas son temporales y generalmente no requieren la intervención del administrador. Si un proceso de aplicación está bloqueado durante un periodo prolongado por un bloqueo en una sesión de usuario inactiva, puede terminar la sesión de usuario para reanudar la replicación. Esta situación es similar a cuando un usuario mantiene un bloqueo prolongado que afecta a la sesión de otro usuario.
> - Para identificar los retrasos en la reproducción relacionados con el bloqueo, habilite la instalación `log_lock_waits` en PostgreSQL.

Conflictos divergentes

Los conflictos divergentes se producen cuando los datos que deberían ser idénticos en todos los nodos difieren inesperadamente. Aunque estos conflictos no se deberían producir, no todos se pueden prevenir de forma fiable con la implementación actual.

> **Note**
>
> La modificación de PRIMARY KEY de una fila puede provocar conflictos divergentes si otro nodo cambia la clave de la misma fila antes de que todos los nodos procesen el cambio. Evite cambiar las claves principales o restrinja los cambios a un nodo designado. Para obtener más información, consulte the section called “Conflictos UPDATE en la PRIMARY KEY ”.

Los conflictos divergentes relacionados con los datos de las filas suelen requerir la intervención del administrador. Para resolver estos conflictos, debe ajustar manualmente los datos de un

nodo para que coincidan con otro mientras desactiva temporalmente la replicación mediante `pgactive.pgactive_do_not_replicate`. Estos conflictos no se deberían producir cuando se utiliza pgactive tal como se ha documentado y se evitan las configuraciones o funciones marcadas como inseguras.

Como administrador, debe resolver estos conflictos manualmente. En función del tipo de conflicto, necesitará utilizar opciones avanzadas como `pgactive.pgactive_do_not_replicate`. Use estas opciones con precaución, ya que un uso incorrecto puede empeorar la situación. Debido a la variedad de posibles conflictos, no podemos proporcionar instrucciones de resolución universales.

Los conflictos divergentes se producen cuando los datos que deberían ser idénticos en diferentes nodos difieren inesperadamente. Aunque estos conflictos no deberían producirse, no todos se pueden prevenir de forma fiable con la implementación actual.

Evitar o tolerar los conflictos

En la mayoría de los casos, puede utilizar un diseño de aplicación adecuado para evitar conflictos o hacer que la aplicación tolere los conflictos.

Los conflictos solo se producen cuando se realizan operaciones simultáneas en varios nodos. Para evitar conflictos:

- Escriba solo en un nodo
- Escriba en subconjuntos de bases de datos independientes en cada nodo (por ejemplo, asigne a cada nodo un esquema independiente)

Para conflictos entre INSERT e INSERT, utilice secuencias globales para evitar conflictos por completo.

Si los conflictos no son aceptables para su caso de uso, considere implementar el bloqueo distribuido a nivel de aplicación. A menudo, el mejor enfoque es diseñar la aplicación para que funcione con los mecanismos de resolución de conflictos de pgactive en lugar de intentar prevenir todos los conflictos. Para obtener más información, consulte the section called “Tipos de conflictos”.

Registro de conflictos

pgactivelink registra los incidentes de conflicto en la tabla `pgactive.pgactive_conflict_history` para ayudarle a diagnosticar y gestionar los conflictos activo-activo. El registro de conflictos en esta tabla solo se produce cuando se establece

`pgactive.log_conflicts_to_table` en verdadero. La extensión pgactive también registra los conflictos en el archivo de registro de PostgreSQL cuando log_min_messages se establece en `LOG` o `lower`, independientemente de la configuración de `pgactive.log_conflicts_to_table`.

Utilice la tabla del historial de conflictos para:

- Medir la frecuencia con la que la aplicación crea conflictos
- Identificar dónde se producen los conflictos
- Mejorar la aplicación para reducir las tasas de conflictos
- Detectar casos en los que las resoluciones de conflictos no producen los resultados deseados
- Determinar dónde necesita desencadenantes de conflictos definidos por el usuario o cambios en el diseño de la aplicación

Para los conflictos de filas, puede registrar opcionalmente los valores de las filas. Esto se controla mediante la configuración de `pgactive.log_conflicts_to_table`. Tenga en cuenta que:

- Esta es una opción global para toda la base de datos
- No hay ningún control por tabla sobre el registro de valores de fila
- No se aplican límites a los números de campo, los elementos de matriz o las longitudes de los campos
- Puede que no sea recomendable activar esta característica si trabaja con filas de varios megabytes que podrían desencadenar conflictos

Como la tabla del historial de conflictos contiene datos de todas las tablas de la base de datos (cada una con posibles esquemas diferentes), los valores de las filas registradas se almacenan como campos JSON. El JSON se crea mediante `row_to_json`, de forma similar a llamarlo directamente desde SQL. PostgreSQL no proporciona una función `json_to_row`, por lo que necesitará código específico de tabla (en PL/pgSQL, PL/Python, PL/Perl, etc.) para reconstruir una tupla de tipo compuesto a partir del JSON registrado.

> **Note**
>
> La compatibilidad para conflictos definidos por el usuario está planificada como una característica de extensión futura.

Descripción del esquema de pgactive

El esquema de pgactive administra la replicación activo-activo en RDS para PostgreSQL. Este esquema contiene tablas que almacenan información sobre la configuración y el estado de la replicación.

> **Note**
>
> El esquema de pgactive está en evolución y está sujeto a cambios. No modifique los datos de estas tablas directamente.

Las tablas de claves del esquema de pgactive incluyen:

- `pgactive_nodes`: almacena información sobre los nodos del grupo de replicación activo-activo.
- `pgactive_connections`: almacena los detalles de conexión de cada nodo.

pgactive_nodes

pgactive_nodes almacena información sobre los nodos que participan en el grupo de replicación activo-activo.

Columna	Tipo	Collation (Intercalación)	Nullable	Predeterminado/a
node_sysid	texto	–	not null	–
node_timeline	oid	–	not null	–
node_dboid	oid	–	not null	–
node_status	char	–	not null	–
node_name	texto	–	not null	–
node_dsn	texto	–	not null	–

Columna	Tipo	Collation (Intercalación)	Nullable	Predeterminado/a
node_init_from_dsn	texto	–	not null	–
node_read_only	valor booleano	–	–	false
node_seq_id	smallint	–	not null	–

node_sysid

ID único para un nodo, generado durante `pgactive_create_group` o `pgactive_join_group`

node_status

Preparación del nodo:

- b: configuración inicial
- i: inicio
- c: recuperación
- o: creación de ranuras de salida
- r: listo
- k: interrumpido

> **Note**
>
> Esta columna no indica si un nodo está conectado o desconectado.

node_name

Nombre de nodo único proporcionado por el usuario.

node_dsn

Cadena de conexión o nombre de mapeo de usuario

node_init_from_dsn

DSN a partir del cual se creó este nodo.

pgactive_connection

pgactive_connections almacena los detalles de conexión de cada nodo.

Columna	Tipo	Collation (Intercalación)	Nullable	Predeterminado/a	
conn_sysid	texto	none	not null	none	
conn_timeline	oid	none	not null	none	
conn_dboid	oid	none	not null	none	
conn_dsn	texto	none	not null	none	
conn_apply_delay	entero	none	none	none	
conn_replication_sets	texto	none	none	none	

conn_sysid

Identificador de nodo del nodo al que hace referencia esta entrada.

conn_dsn

Igual que pgactive.pgactive_nodes `node_dsn`.

conn_apply_delay

Si se establece, milisegundos que hay que esperar antes de aplicar cada transacción desde el nodo remoto. Principalmente para depurar. Si es nulo, se aplica el valor predeterminado global.

Uso de conjuntos de replicación

Los conjuntos de replicación determinan qué tablas incluir o excluir de las operaciones de replicación. De forma predeterminada, todas las tablas se replican a menos que especifique lo contrario mediante las siguientes funciones:

- `pgactive_exclude_table_replication_set()`: excluye las tablas especificadas de la replicación
- `pgactive_include_table_replication_set()`: incluye las tablas especificadas en la replicación

> **Note**
>
> Antes de configurar los conjuntos de replicación, tenga en cuenta lo siguiente:
>
> - Puede configurar la inclusión o exclusión de tablas solo después de ejecutar `pgactive_create_group()` pero antes de `pgactive_join_group()`.
> - Después de usar `pgactive_exclude_table_replication_set()`, no puede usar `pgactive_include_table_replication_set()`.
> - Después de usar `pgactive_include_table_replication_set()`, no puede usar `pgactive_exclude_table_replication_set()`.

El sistema gestiona las tablas recién creadas de forma diferente en función de la configuración inicial:

- Si excluyó las tablas: todas las tablas nuevas que se creen después de `pgactive_join_group()` se incluyen automáticamente en la replicación
- Si incluyó las tablas: todas las tablas nuevas que se creen después de `pgactive_join_group()` se excluyen automáticamente de la replicación.

Para ver la configuración del conjunto de réplicas de una tabla específica, utilice la función `pgactive.pgactive_get_table_replication_sets()`.

Referencia de funciones de pgactive

A continuación, puede encontrar una lista de funciones de pgactive con sus parámetros, valores de devolución y notas prácticas de uso para ayudarle a utilizarlas de forma eficaz:

get_last_applied_xact_info

Recupera la información de la última transacción aplicada a un nodo específico.

Arguments

- sysid (texto): OID de línea temporal
- dboid (OID)

Tipo de devolución

Hace lo siguiente:

- last_applied_xact_id (OID)
- last_applied_xact_committs (marca temporal con zona horaria)
- last_applied_xact_at (marca temporal con zona horaria)

Notas de uso

Use esta función para recuperar la información de la última transacción aplicada a un nodo específico.

pgactive_apply_pause

Pausa el proceso de aplicación de la replicación.

Arguments

Ninguno

Tipo de devolución

booleano

Notas de uso

Llame a esta función para pausar el proceso de aplicación de la replicación.

pgactive_apply_resume

Reanuda el proceso de aplicación de la replicación.

Arguments

Ninguno

Tipo de devolución

void

Notas de uso

Llame a esta función para reanudar el proceso de aplicación de la replicación.

pgactive_is_apply_paused

Comprueba si la aplicación de la replicación está actualmente en pausa.

Arguments

Ninguno

Tipo de devolución

booleano

Notas de uso

Use esta función para comprobar si la aplicación de la replicación está actualmente en pausa.

pgactive_create_group

Crea un grupo pgactive convirtiendo una base de datos independiente en el nodo inicial.

Arguments

- node_name (texto)
- node_dsn (texto)
- apply_delay integer DEFAULT NULL::integer - replication_sets text[] DEFAULT ARRAY[‘default’::text]

Tipo de devolución

void

Notas de uso

Crea un grupo pgactive convirtiendo una base de datos independiente en el nodo inicial. La función realiza comprobaciones de integridad antes de transformar el nodo en un nodo

de pgactive. Antes de usar esta función, asegúrese de que el clúster de PostgreSQL tenga suficientes `max_worker_processes` disponibles para admitir los trabajadores en segundo plano de pgactive.

pgactive_detach_nodes

Elimina los nodos especificados del grupo pgactive.

Arguments

- p_nodes (text[])

Tipo de devolución

void

Notas de uso

Use esta función para eliminar los nodos especificados del grupo pgactive.

pgactive_exclude_table_replication_set

Excluye una tabla específica de la replicación.

Arguments

- p_relation (regclass)

Tipo de devolución

void

Notas de uso

Utilice esta función para excluir una tabla específica de la replicación.

pgactive_get_replication_lag_info

Recupera información detallada sobre el retraso de la replicación, incluidos los detalles del nodo, el estado de WAL y los valores de LSN.

Arguments

Ninguno

Tipo de devolución

SETOF record - node_name text - node_sysid text - application_name text - slot_name text - active boolean - active_pid integer - pending_wal_decoding bigint - Tamaño aproximado de WAL en bytes que se decodificará en el nodo emisor - pending_wal_to_apply bigint - Tamaño aproximado del WAL en bytes que se aplicará en el nodo receptor - restart_lsn pg_lsn - confirmed_flush_lsn pg_lsn - sent_lsn pg_lsn - write_lsn pg_lsn - flush_lsn pg_lsn - replay_lsn pg_lsn

Notas de uso

Llame a esta función para recuperar información sobre el retraso de la replicación, incluidos los detalles del nodo, el estado de WAL y los valores de LSN.

pgactive_get_stats

Recupera las estadísticas de replicación de pgactive.

Arguments

Ninguno

Tipo de devolución

SETOF record - rep_node_id oid - rilocalid oid - riremoteid text - nr_commit bigint - nr_rollback bigint - nr_insert bigint - nr_insert_conflict bigint - nr_update bigint - nr_update_conflict bigint - nr_delete bigint - nr_delete_conflict bigint - nr_disconnect bigint

Notas de uso

Utilice esta función para recuperar las estadísticas de replicación de pgactive.

pgactive_get_table_replication_sets

Obtiene la configuración del conjunto de replicación de una relación específica.

Arguments

- relación (regclass)

Tipo de devolución

Registro SETOF

Notas de uso

Llame a esta función para obtener la configuración del conjunto de replicación de una relación específica.

pgactive_include_table_replication_set

Incluye una tabla específica en la replicación.

Arguments

- p_relation (regclass)

Tipo de devolución

void

Notas de uso

Utilice esta función para incluir una tabla específica en la replicación.

pgactive_join_group

Agrega un nodo a un grupo pgactive existente.

Arguments

- node_name (texto)
- node_dsn (texto)
- join_using_dsn (texto)
- apply_delay (entero, opcional)
- replication_sets (text[], predeterminado: ['default'])
- bypass_collation_check (booleano, predeterminado: falso)
- bypass_node_identifier_creation (booleano, predeterminado: falso)
- bypass_user_tables_check (booleano, predeterminado: falso)

Tipo de devolución

void

Notas de uso

Llame a esta función para agregar un nodo a un grupo pgactive existente. Asegúrese de que el clúster de PostgreSQL tenga suficientes max_worker_processes para los trabajadores en segundo plano de pgactive.

pgactive_remove

Elimina todos los componentes de pgactive del nodo local.

Arguments

- force (booleano, predeterminado: falso)

Tipo de devolución

void

Notas de uso

Llame a esta función para eliminar todos los componentes de pgactive del nodo local.

pgactive_snowflake_id_nextval

Genera valores de secuencia únicos específicos del nodo.

Arguments

- regclass

Tipo de devolución

bigint

Notas de uso

Utilice esta función para generar valores de secuencia únicos específicos del nodo.

pgactive_update_node_conninfo

Actualiza la información de conexión de un nodo de pgactive.

Arguments

- node_name_to_update (texto)

- node_dsn_to_update (texto)

Tipo de devolución

void

Notas de uso

Use esta función para actualizar la información de conexión de un nodo de pgactive.

pgactive_wait_for_node_ready

Supervisa el progreso de las operaciones de creación o unión de grupos.

Arguments

- timeout (entero, predeterminado: 0)
- progress_interval (entero, predeterminado: 60)

Tipo de devolución

void

Notas de uso

Llame a esta función para supervisar el progreso de las operaciones de creación o unión de grupos.

Gestión de conflictos en la replicación activa-activa

La extensión `pgactive` funciona por base de datos y no por clúster. Cada instancia de base de datos que utiliza `pgactive` es una instancia independiente y puede aceptar cambios de datos de cualquier fuente. Cuando se envía un cambio a una instancia de base de datos, PostgreSQL lo confirma localmente y, a continuación, utiliza `pgactive` para replicar el cambio de forma asíncrona en otras instancias de base de datos. Cuando dos instancias de base de datos de PostgreSQL actualizan el mismo registro prácticamente al mismo tiempo, puede producirse un conflicto.

La extensión `pgactive` proporciona mecanismos para la detección y la resolución automática de conflictos. Realiza un seguimiento de la marca de tiempo en que se confirmó la transacción en ambas instancias de base de datos y aplica automáticamente el cambio con la última marca de tiempo. La extensión `pgactive` también registra cuando se produce un conflicto en la tabla `pgactive.pgactive_conflict_history`.

El `pgactive.pgactive_conflict_history` seguirá creciendo. Puede definir una política de depuración. Esto se puede hacer borrando algunos registros de forma regular o definiendo un esquema de partición para esta relación (y, luego, separando, descartando o truncando las particiones de interés). Para implementar la política de depuración de forma regular, una opción es usar la extensión `pg_cron` Consulte la siguiente información con un ejemplo para la tabla de historial de `pg_cron` Programación de mantenimiento con la extensión pg_cron de PostgreSQL.

Gestión de secuencias en la replicación activa-activa

Una instancia de base de datos de RDS para PostgreSQL con la extensión `pgactive` utiliza dos mecanismos de secuencia diferentes para generar valores únicos.

Secuencias globales

Para usar una secuencia global, cree una secuencia local con la instrucción `CREATE SEQUENCE`. Utilice `pgactive.pgactive_snowflake_id_nextval(seqname)` en lugar de `usingnextval(seqname)` para obtener el siguiente valor único de la secuencia.

En el siguiente ejemplo se crea una secuencia global.

```
app=> CREATE TABLE gstest (
      id bigint primary key,
      parrot text
    );
```

```
app=>CREATE SEQUENCE gstest_id_seq OWNED BY gstest.id;
```

```
app=> ALTER TABLE gstest \
      ALTER COLUMN id SET DEFAULT \
      pgactive.pgactive_snowflake_id_nextval('gstest_id_seq');
```

Secuencias particionadas

En las secuencias divididas o particionadas, se utiliza una secuencia PostgreSQL normal en cada nodo. Cada secuencia se incrementa en la misma cantidad y comienza con diferentes desplazamientos. Por ejemplo, con el paso 100, el nodo 1 genera una secuencia como 101, 201, 301, etc., y el nodo 2 genera una secuencia como 102, 202, 302, etc. Este esquema funciona bien incluso si los nodos no pueden comunicarse durante períodos prolongados, pero requiere que

el diseñador especifique un número máximo de nodos al establecer el esquema y requiere una configuración por nodo. Los errores pueden provocar fácilmente la superposición de secuencias.

Es relativamente sencillo configurar este enfoque con `pgactive` creando la secuencia deseada en un nodo de la siguiente manera:

```
CREATE TABLE some_table (generated_value bigint primary key);
```

```
app=> CREATE SEQUENCE some_seq INCREMENT 100 OWNED BY some_table.generated_value;
```

```
app=> ALTER TABLE some_table ALTER COLUMN generated_value SET DEFAULT
 nextval('some_seq');
```

A continuación, llame a `setval` en cada nodo para dar un valor inicial de desplazamiento diferente, de la siguiente manera.

```
app=>
-- On node 1
SELECT setval('some_seq', 1);

-- On node 2
SELECT setval('some_seq', 2);
```

Reducción de la sobrecarga en tablas e índices con la extensión pg_repack

Puede usar la extensión `pg_repack` para eliminar el sobredimensionamiento de las tablas y los índices como alternativa a `VACUUM FULL`. Esta extensión es compatible con RDS para las versiones 9.6.3 y superiores de PostgreSQL. Para obtener más información acerca de la extensión `pg_repack` y el reempaquetado de tablas completo, consulte la documentación del proyecto de GitHub.

A diferencia de lo que ocurre con `VACUUM FULL`, la extensión `pg_repack` requiere un bloqueo exclusivo (AccessExclusiveLock) por un breve período de tiempo durante la operación de reconstrucción de la tabla en los siguientes casos:

- Creación inicial de la tabla de registro: se crea una tabla de registro para registrar los cambios que se producen durante la copia inicial de los datos, como se muestra en el siguiente ejemplo:

```
postgres=>\dt+ repack.log_*
List of relations
-[ RECORD 1 ]-+----------
Schema        | repack
Name          | log_16490
Type          | table
Owner         | postgres
Persistence   | permanent
Access method | heap
Size          | 65 MB
Description   |
```

- Fase final de intercambio y eliminación.

Para el resto de la operación de reconstrucción, solo se necesita un bloqueo `ACCESS SHARE` en la tabla original para copiar sus filas a la nueva tabla. Esto ayuda a que las operaciones INSERT, UPDATE y DELETE continúen como de costumbre.

Recomendaciones

Las siguientes recomendaciones se aplican al eliminar el sobredimensionamiento de las tablas e índices mediante la extensión `pg_repack`:

- Realice el reempaquetado fuera del horario laboral o durante un período de mantenimiento para minimizar su impacto en el rendimiento de otras actividades de la base de datos.

- Monitorice de cerca las sesiones de bloqueo durante la actividad de reconstrucción y asegúrese de que no haya ninguna actividad en la tabla original que pueda bloquear `pg_repack`, especialmente durante la fase final de intercambio y eliminación, cuando es necesario bloquear exclusivamente la tabla original. Para obtener más información, consulte Identificar qué bloquea una consulta.

  Si ve una sesión que bloquee, puede finalizarla mediante el siguiente comando tras estudiarla detenidamente. Esto ayuda a continuar con `pg_repack` para terminar la reconstrucción:

  ```
  SELECT pg_terminate_backend(pid);
  ```

- Al aplicar los cambios acumulados de la tabla de registro `pg_repack's` en sistemas con una tasa de transacciones muy alta, es posible que el proceso de solicitud no pueda mantener la tasa de cambios. En esos casos, `pg_repack` no podría completar el proceso de aplicación. Para obtener más información, consulte Monitorización de la nueva tabla durante el reempaquetado. Si los índices están muy sobredimensionados, una solución alternativa es volver a empaquetar únicamente los índices. Esto también ayuda a que los ciclos de limpieza de índices de VACUUM finalicen más rápido.

  Puede omitir la fase de limpieza de índices mediante el VACUUM manual de la versión 12 de PostgreSQL, y se omite automáticamente durante el autovacuum de emergencia de la versión 14 de PostgreSQL. Esto ayuda a que VACUUM se complete más rápido sin eliminar el sobredimensionamiento del índice y solo está diseñado para situaciones de emergencia, como evitar que el VACUUM se acumule. Para obtener más información, consulte Evitar la sobrecarga en los índices en la Guía del usuario de Amazon Aurora.

Requisitos previos

- La tabla debe tener una restricción de PRIMARY KEY o una UNIQUE que no sea null.
- La versión de la extensión debe ser la misma tanto para el cliente como para el servidor.
- Asegúrese de que la instancia de RDS tenga más `FreeStorageSpace` que el tamaño total de la tabla sin la sobrecarga. Como ejemplo, considere el tamaño total de la tabla, incluidos el TOAST y los índices, como de 2 TB, y el tamaño total de la tabla como 1 TB. El `FreeStorageSpace` requerido debe ser superior al valor devuelto por el siguiente cálculo:

  `2TB (Table size) - 1TB (Table bloat) = 1TB`

Puede utilizar la siguiente consulta para comprobar el tamaño total de la tabla y utilizar `pgstattuple` para derivar la sobrecarga. Para obtener más información, consulte Diagnóstico de sobrecarga de tablas e índices en la Guía del usuario de Amazon Aurora.

```
SELECT pg_size_pretty(pg_total_relation_size('table_name')) AS total_table_size;
```

Este espacio se recupera una vez finalizada la actividad.

- Asegúrese de que la instancia de RDS tenga suficiente capacidad de procesamiento y E/S para gestionar la operación de reempaquetado. Podría considerar la posibilidad de escalar verticalmente la clase de instancia para lograr un equilibrio óptimo del rendimiento.

Para usar la extensión **`pg_repack`**

1. Instale la extensión `pg_repack` en la instancia de base de datos de RDS for PostgreSQL con el siguiente comando.

   ```
   CREATE EXTENSION pg_repack;
   ```

2. Ejecute los siguientes comandos para conceder acceso de escritura a las tablas de registro temporales creadas por `pg_repack`.

   ```
   ALTER DEFAULT PRIVILEGES IN SCHEMA repack GRANT INSERT ON TABLES TO PUBLIC;
   ALTER DEFAULT PRIVILEGES IN SCHEMA repack GRANT USAGE, SELECT ON SEQUENCES TO
    PUBLIC;
   ```

3. Conéctese a la base de datos mediante la utilidad de cliente `pg_repack`. Utilice una cuenta que tenga privilegios `rds_superuser`. Por ejemplo, suponga que ese rol `rds_test` tiene privilegios `rds_superuser`. La siguiente sintaxis realiza `pg_repack` para tablas completas, incluidos todos los índices de tablas de la base de datos `postgres`.

   ```
   pg_repack -h db-instance-name.111122223333.aws-region.rds.amazonaws.com -U rds_test
    -k postgres
   ```

   > **Note**
   >
   > Debe conectarse usando la opción -k. La opción -a no se admite.

La respuesta del cliente pg_repack proporciona información relativa a las tablas de la instancia de base de datos que se han vuelto a empaquetar.

```
INFO: repacking table "pgbench_tellers"
INFO: repacking table "pgbench_accounts"
INFO: repacking table "pgbench_branches"
```

4. La siguiente sintaxis vuelve a empaquetar una sola tabla orders, incluidos los índices de la base de datos postgres.

```
pg_repack -h db-instance-name.111122223333.aws-region.rds.amazonaws.com -U rds_test
 --table orders -k postgres
```

La siguiente sintaxis reempaqueta solo los índices de la tabla orders de la base de datos postgres.

```
pg_repack -h db-instance-name.111122223333.aws-region.rds.amazonaws.com -U rds_test
 --table orders --only-indexes -k postgres
```

Monitorización de la nueva tabla durante el reempaquetado

- El tamaño de la base de datos se incrementa en función del tamaño total de la tabla, menos la sobrecarga, hasta la fase de intercambio y eliminación del reempaquetado. Puede monitorizar la tasa de crecimiento del tamaño de la base de datos, calcular la velocidad de reempaquetado y estimar aproximadamente el tiempo que se tarda en completar la transferencia inicial de datos.

  Como ejemplo, considere que el tamaño total de la tabla es de 2 TB, el tamaño de la base de datos es de 4 TB y la sobrecarga total de la tabla es de 1 TB. El valor del tamaño total de la base de datos devuelto por el cálculo al final de la operación de reempaquetado es el siguiente:

  `2TB (Table size) + 4 TB (Database size) - 1TB (Table bloat) = 5TB`

  Puede estimar aproximadamente la velocidad de la operación de reempaquetado muestreando la tasa de crecimiento en bytes entre dos puntos en el tiempo. Si la tasa de crecimiento es de 1 GB por minuto, la operación inicial de creación de la tabla puede tardar 1000 minutos o 16,6 horas aproximadamente en completarse. Además de la construcción inicial de la tabla, pg_repack

también necesita aplicar los cambios acumulados. El tiempo que tarda depende del ritmo de aplicación de los cambios continuos más los acumulados.

> **Note**
>
> Puede usar la extensión `pgstattuple` para calcular la sobrecarga en la tabla. Para obtener más información, consulte pgstattuple.

- El número de filas de la tabla de registro `pg_repack's`, según el esquema de reempaquetado, representa el volumen de cambios pendientes de aplicarse a la nueva tabla tras la carga inicial.

  Puede consultar la tabla de registro `pg_repack's` en `pg_stat_all_tables` para supervisar los cambios aplicados a la nueva tabla. `pg_stat_all_tables.n_live_tup` indica el número de registros pendientes de ser aplicados a la nueva tabla. Para obtener más información, consulte pg_stat_all_tables.

```
postgres=>SELECT relname,n_live_tup FROM pg_stat_all_tables WHERE schemaname =
 'repack' AND relname ILIKE '%log%';

-[ RECORD 1 ]---------
relname    | log_16490
n_live_tup | 2000000
```

- Puede utilizar la extensión `pg_stat_statements` para determinar el tiempo que tarda cada paso de la operación de reempaquetado. Esto es útil para prepararse para aplicar la misma operación de reempaque en un entorno de producción. Puede ajustar la cláusula `LIMIT` para ampliar aún más la salida.

```
postgres=>SELECT
     SUBSTR(query, 1, 100) query,
     round((round(total_exec_time::numeric, 6) / 1000 / 60),4)
 total_exec_time_in_minutes
 FROM
     pg_stat_statements
 WHERE
     query ILIKE '%repack%'
 ORDER BY
     total_exec_time DESC LIMIT 5;
```

```
 query                                                                |
 total_exec_time_in_minutes
----------------------------------------------------------------------
+---------------------------
 CREATE UNIQUE INDEX index_16493 ON repack.table_16490 USING btree (a) |
        6.8627
 INSERT INTO repack.table_16490 SELECT a FROM ONLY public.t1           |
        6.4150
 SELECT repack.repack_apply($1, $2, $3, $4, $5, $6)                    |
        0.5395
 SELECT repack.repack_drop($1, $2)                                     |
        0.0004
 SELECT repack.repack_swap($1)                                         |
        0.0004
(5 rows)
```

El reempaquetado es una operación completamente fuera de lugar, por lo que la tabla original no se ve afectada y no prevemos ningún problema inesperado que requiera la recuperación de la tabla original. Si el reempaquetado falla inesperadamente, debe inspeccionar la causa del error y resolverlo.

Una vez resuelto el problema, coloque y vuelva a crear la extensión `pg_repack` en la base de datos en la que se encuentre la tabla y vuelva a intentar el paso `pg_repack`. Además, la disponibilidad de los recursos de computación y la accesibilidad simultánea de la tabla desempeñan un papel crucial a la hora de completar a tiempo la operación de reempaquetado.

Actualización y uso de la extensión PLV8

PLV8 es una extensión de lenguaje Javascript de confianza para PostgreSQL Puede usarlo para procedimientos almacenados, desencadenadores y otro código de procedimiento que se puede llamar desde SQL. Esta extensión de lenguaje es compatible con todas las versiones actuales de PostgreSQL.

Si utiliza PLV8 y actualiza PostgreSQL a una nueva versión de PLV8, inmediatamente aprovecha la nueva extensión. Lleve a cabo los siguientes pasos para sincronizar los metadatos del catálogo con la nueva versión de PLV8. Estos pasos son opcionales, pero recomendamos que los complete para evitar advertencias de discrepancia de metadatos.

El proceso de actualización elimina todas las funciones PLV8 existentes. Por lo tanto, le recomendamos que cree una instantánea de su instancia de base de datos de RDS for PostgreSQL antes de la actualización. Para obtener más información, consulte Creación de una instantánea de base de datos para una instancia de base de datos single-AZ para Amazon RDS.

> **Important**
>
> A partir de la versión 18 de PostgreSQL, Amazon RDS para PostgreSQL dejará de utilizar las extensiones `plcoffee` y `plls` de PostgreSQL. Le recomendamos que deje de usar Coffeescript y LiveScript en sus aplicaciones para asegurarse de tener una ruta de actualización para futuras actualizaciones de las versiones del motor.

Para sincronizar los metadatos del catálogo con una nueva versión de PLV8

1. Verifique que necesita realizar la actualización. Para ello, ejecute el siguiente comando mientras está conectado a la instancia.

   ```
   SELECT * FROM pg_available_extensions WHERE name IN ('plv8','plls','plcoffee');
   ```

   Si los resultados contienen valores de una versión instalada con un número inferior a la versión predeterminada, continúe con este procedimiento para actualizar las extensiones. Por ejemplo, el siguiente conjunto de resultados indica que debería actualizar.

   ```
   name    | default_version | installed_version |                    comment
   --------+-----------------+-------------------
   +-------------------------------------------------
   ```

```
plls    | 2.1.0           | 1.5.3             | PL/LiveScript (v8) trusted
 procedural language
plcoffee| 2.1.0           | 1.5.3             | PL/CoffeeScript (v8) trusted
 procedural language
plv8    | 2.1.0           | 1.5.3             | PL/JavaScript (v8) trusted
 procedural language
(3 rows)
```

2. Cree una instantánea de la instancia de base de datos de RDS for PostgreSQL si aún no lo ha hecho. Puede continuar con los pasos siguientes mientras se crea la instantánea.
3. Obtenga un recuento del número de funciones de PLV8 de su instancia de base de datos para que pueda validar que se aplican todas después de la actualización. Por ejemplo, la siguiente consulta SQL devuelve el número de funciones escritas en plv8, plcoffee y plls.

```
SELECT proname, nspname, lanname
FROM pg_proc p, pg_language l, pg_namespace n
WHERE p.prolang = l.oid
AND n.oid = p.pronamespace
AND lanname IN ('plv8','plcoffee','plls');
```

4. Use pg_dump para crear un archivo de volcado solo de esquema. Por ejemplo, cree un archivo en el equipo cliente en el directorio `/tmp`.

```
./pg_dump -Fc --schema-only -U master postgres >/tmp/test.dmp
```

   En este ejemplo se utilizan las siguientes opciones:

   - `-Fc`: formato personalizado
   - --schema-only: vuelca solo los comandos necesarios para crear el esquema (funciones en este caso)
   - `-U`: el nombre de usuario maestro de RDS
   - `database`: el nombre de la base de datos para nuestra instancia de base de datos

   Para obtener más información sobre pg_dump, consulte pg_dump en la documentación de PostgreSQL.
5. Extraiga la instrucción DDL "CREATE FUNCTION" que se encuentra en el archivo de volcado. El siguiente ejemplo utiliza el comando `grep` para extraer la instrucción DDL que crea las

funciones y guardarlas en un archivo. Se utiliza en los pasos posteriores para volver a crear las funciones.

```
./pg_restore -l /tmp/test.dmp | grep FUNCTION > /tmp/function_list
```

Para obtener más información sobre pg_restore, consulte pg_restore en la documentación de PostgreSQL.

6. Borre las funciones y las extensiones. El siguiente ejemplo elimina cualquier objeto basado en PLV8. La opción cascade garantiza que se borren los dependientes.

```
DROP EXTENSION plv8 CASCADE;
```

Si su instancia de PostgreSQL contiene objetos basados en plcoffee o plls, repita este paso para dichas extensiones.

7. Cree las extensiones. El siguiente ejemplo crea las extensiones plv8, plcoffee y plls.

```
CREATE EXTENSION plv8;
CREATE EXTENSION plcoffee;
CREATE EXTENSION plls;
```

8. Cree las funciones con el archivo de volcado y el archivo "driver".

El siguiente ejemplo recrea las funciones que extrajo anteriormente.

```
./pg_restore -U master -d postgres -Fc -L /tmp/function_list /tmp/test.dmp
```

9. Verifique que todas las funciones se recrean con la siguiente consulta.

```
SELECT * FROM pg_available_extensions WHERE name IN ('plv8','plls','plcoffee');
```

La versión 2 de PLV8 agrega la siguiente fila adicional a su conjunto de resultados:

```
    proname    |  nspname   | lanname
---------------+------------+----------
 plv8_version  | pg_catalog | plv8
```

Uso de PL/Rust para escribir funciones de PostgreSQL en lenguaje Rust

PL/Rust es una extensión del lenguaje Rust de confianza para PostgreSQL. Puede usarlo para procedimientos almacenados, funciones y otro código de procedimiento que se pueda llamar desde SQL. La extensión de lenguaje PL/Rust está disponible en las siguientes versiones:

- RDS para PostgreSQL 17.1 y otras versiones 17 posteriores
- RDS para PostgreSQL 16.1 y versiones 16 posteriores
- RDS para PostgreSQL, 15.2-R2 y versiones 15 posteriores
- RDS para PostgreSQL, 14.9 y versiones 14 posteriores
- RDS para PostgreSQL, 13.12 y versiones 13 posteriores

Para obtener más información, consulte PL/Rust en GitHub.

Temas

- Configuración de PL/Rust
- Creación de funciones con PL/Rust
- Uso de cajas con PL/Rust
- Limitaciones de PL/Rust

Configuración de PL/Rust

Para instalar la extensión plrust en la instancia de base de datos, agregue plrust al parámetro `shared_preload_libraries` en el grupo de parámetros de base de datos asociado con la instancia de base de datos. Con la extensión plrust instalada, puede crear funciones.

Para modificar el parámetro `shared_preload_libraries`, la instancia de base de datos debe asociarse al grupo de parámetros personalizado. Para obtener información sobre la creación de un grupo de parámetros de base de datos personalizado, consulte Grupos de parámetros para Amazon RDS.

Puede instalar la extensión plrust mediante la AWS Management Console o la AWS CLI.

En los pasos siguientes se supone que la instancia de base de datos está asociada a un grupo de parámetros de base de datos personalizado.

Consola

Instalar la extensión plrust en el parámetro **`shared_preload_libraries`**

Realice los siguientes pasos con una cuenta que sea miembro del grupo `rds_superuser` (rol).

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija el nombre de la instancia de base de datos para ver los detalles.
4. Abra la pestaña Configuración de la instancia de base de datos y busque el enlace del grupo de parámetros de instancias de base de datos.
5. Elija el enlace para abrir los parámetros personalizados asociados a la instancia de base de datos.
6. En el campo de búsqueda Parametes (Parámetros), escriba `shared_pre` para buscar el parámetro **`shared_preload_libraries`**.
7. Seleccione Edit parameters (Editar parámetros) para acceder a los valores de las propiedades.
8. Añada plrust a la lista en el campo Valores. Utilice una coma para separar los elementos de la lista de valores.
9. Reinicie la instancia de base de datos para que los cambios en el parámetro `shared_preload_libraries` surtan efecto. El reinicio inicial puede requerir tiempo adicional para completarse.
10. Cuando la instancia esté disponible, compruebe si se ha inicializado plrust. Use `psql` para conectarse a la instancia de base de datos y ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
```

El resultado debería tener un aspecto similar al siguiente:

```
shared_preload_libraries
--------------------------
rdsutils,plrust
(1 row)
```

AWS CLI

Instale la extensión plrust en el parámetro shared_preload_libraries.

Realice los siguientes pasos con una cuenta que sea miembro del grupo `rds_superuser` (rol).

1. Use el comando modify-db-parameter-group de AWS CLI para añadir plrust al parámetro `shared_preload_libraries`.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=plrust,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Use el comando reboot-db-instance de AWS CLI para reiniciar la instancia de base de datos e inicializar la biblioteca plrust. El reinicio inicial puede requerir tiempo adicional para completarse.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

3. Cuando la instancia esté disponible, compruebe si se ha inicializado plrust. Use `psql` para conectarse a la instancia de base de datos y ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
```

   El resultado debería tener un aspecto similar al siguiente:

```
shared_preload_libraries
--------------------------
rdsutils,plrust
(1 row)
```

Creación de funciones con PL/Rust

PL/Rust compilará la función como biblioteca dinámica, la cargará y la ejecutará.

La siguiente función de Rust filtra los múltiplos de una matriz.

```
postgres=> CREATE LANGUAGE plrust;
CREATE EXTENSION
```

```
CREATE OR REPLACE FUNCTION filter_multiples(a BIGINT[], multiple BIGINT) RETURNS
 BIGINT[]
    IMMUTABLE STRICT
    LANGUAGE PLRUST AS
$$
    Ok(Some(a.into_iter().filter(|x| x.unwrap() % multiple != 0).collect()))
$$;

WITH gen_values AS (
SELECT ARRAY(SELECT * FROM generate_series(1,100)) as arr)
SELECT filter_multiples(arr, 3)
from gen_values;
```

Uso de cajas con PL/Rust

En RDS para PostgreSQL versiones 16.3-R2 y posteriores, 15.7-R2 y versiones 15 posteriores, 14.12-R2 y versiones 14 posteriores y 13.15-R2 y versiones 13 y posteriores, PL/Rust admite cajas adicionales:

- `url`
- `regex`
- `serde`
- `serde_json`

En RDS para PostgreSQL versiones 15.5-R2 y posteriores, 14.10-R2 y versiones 14 posteriores y 13.13-R2 y versiones 13 posteriores, PL/Rust admite dos cajas adicionales:

- `croaring-rs`
- `num-bigint`

A partir de las versiones 15.4, 14.9 y 13.12 de Amazon RDS para PostgreSQL, PL/Rust admite las siguientes cajas:

- `aes`
- `ctr`

- `rand`

Estas cajas solo admiten las funciones predeterminadas. Es posible que las nuevas versiones de RDS para PostgreSQL contengan versiones actualizadas de las cajas y que las versiones anteriores de las cajas ya no sean compatibles.

Siga las prácticas recomendadas para realizar una actualización de una versión principal y comprobar si las funciones de PL/Rust son compatibles con la nueva versión principal. Para obtener más información, consulte el blog Best practices for upgrading Amazon RDS to major and minor versions of PostgreSQL y Actualización del motor de base de datos de PostgreSQL para Amazon RDS en la Guía del usuario de Amazon RDS.

Encontrará ejemplos del uso de dependencias al crear una función de PL/Rust en Use dependencies.

Limitaciones de PL/Rust

De forma predeterminada, los usuarios de bases de datos no pueden usar PL/Rust. Para proporcionar acceso a PL/Rust, conéctese como usuario con el privilegio rds_superuser y ejecute el siguiente comando:

```
postgres=> GRANT USAGE ON LANGUAGE PLRUST TO user;
```

Administración de datos espaciales con la extensión PostGIS

PostGIS es una extensión de PostgreSQL para almacenar y administrar información espacial. Para obtener más información sobre PostGIS, consulte PostGIS.net.

A partir de la versión 10.5, PostgreSQL admite la biblioteca libprotobuf 1.3.0 utilizada por PostGIS para trabajar con datos de teselas vectoriales de Mapbox.

La configuración de la extensión PostGIS requiere privilegios de `rds_superuser`. Le recomendamos que cree un usuario (rol) para administrar instalar la extensión PostGIS y los datos espaciales. La extensión PostGIS y sus componentes relacionados añaden miles de funciones a PostgreSQL. Considere la posibilidad de crear la extensión PostGIS en su propio esquema si eso tiene sentido para su caso de uso. En el ejemplo siguiente, se muestra cómo instalar la extensión en su propia base de datos, pero esto no es obligatorio.

Temas

- Paso 1: cree un usuario (rol) para administrar la extensión PostGIS
- Paso 2: cargue las extensiones PostGIS
- Paso 3: transferir la propiedad de los esquemas de extensión
- Paso 4: transferir la propiedad de las tablas de PostGIS
- Paso 5: pruebe las extensiones
- Paso 6: Actualice la extensión de PostGIS
- Versiones de extensión PostGIS
- Actualización de PostGIS 2 a PostGIS 3

Paso 1: cree un usuario (rol) para administrar la extensión PostGIS

En primer lugar, conéctese a una instancia de base de datos de RDS para PostgreSQL como usuario con privilegios `rds_superuser`. Si mantuvo el nombre predeterminado al configurar la instancia, conéctese como `postgres`.

```
psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --username=postgres
 --password
```

Cree un rol independiente (usuario) para administrar la extensión PostGIS.

```
postgres=>  CREATE ROLE gis_admin LOGIN PASSWORD 'change_me';
```

```
CREATE ROLE
```

Conceda los privilegios `rds_superuser` de este rol para permitir que el rol instale la extensión.

```
postgres=> GRANT rds_superuser TO gis_admin;
GRANT
```

Cree una base de datos para utilizarla para sus artefactos de PostGIS. Este paso es opcional. O puede crear un esquema en la base de datos de usuarios para las extensiones de PostGIS, pero esto tampoco es obligatorio.

```
postgres=> CREATE DATABASE lab_gis;
CREATE DATABASE
```

Conceda todos los privilegios `gis_admin` en la base de datos `lab_gis`.

```
postgres=> GRANT ALL PRIVILEGES ON DATABASE lab_gis TO gis_admin;
GRANT
```

Salga de la sesión y vuelva a conectarse a una instancia de base de datos de RDS para PostgreSQL como `gis_admin`.

```
postgres=> psql --host=111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=gis_admin --password --dbname=lab_gis
Password for user gis_admin:...
lab_gis=>
```

Continúe configurando la extensión tal y como se detalla en los pasos siguientes.

Paso 2: cargue las extensiones PostGIS

La extensión de PostGIS incluye varias extensiones relacionadas que funcionan juntas para proporcionar funcionalidad geoespacial. Dependiendo de su caso de uso, es posible que no necesite todas las extensiones creadas en este paso.

Utilice instrucciones `CREATE EXTENSION` para cargar las extensiones de PostGIS.

```
CREATE EXTENSION postgis;
CREATE EXTENSION
CREATE EXTENSION postgis_raster;
```

```
CREATE EXTENSION
CREATE EXTENSION fuzzystrmatch;
CREATE EXTENSION
CREATE EXTENSION postgis_tiger_geocoder;
CREATE EXTENSION
CREATE EXTENSION postgis_topology;
CREATE EXTENSION
CREATE EXTENSION address_standardizer_data_us;
CREATE EXTENSION
```

Para verificar los resultados, puede ejecutar la consulta SQL que se muestra en el siguiente ejemplo, que enumera las extensiones y sus propietarios.

```
SELECT n.nspname AS "Name",
  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"
  FROM pg_catalog.pg_namespace n
  WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'
  ORDER BY 1;
List of schemas
     Name     |   Owner
--------------+-----------
 public       | postgres
 tiger        | rdsadmin
 tiger_data   | rdsadmin
 topology     | rdsadmin
(4 rows)
```

Paso 3: transferir la propiedad de los esquemas de extensión

Use las declaraciones de ALTER SCHEMA para transferir la propiedad de los esquemas al rol `gis_admin`.

```
ALTER SCHEMA tiger OWNER TO gis_admin;
ALTER SCHEMA
ALTER SCHEMA tiger_data OWNER TO gis_admin;
ALTER SCHEMA
ALTER SCHEMA topology OWNER TO gis_admin;
ALTER SCHEMA
```

Si desea confirmar el cambio de propiedad, ejecute la siguiente consulta SQL. O bien, puede utilizar el metacomando \dn de la línea de comandos psql.

```
SELECT n.nspname AS "Name",
  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"
  FROM pg_catalog.pg_namespace n
  WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'
  ORDER BY 1;

       List of schemas
     Name     |     Owner
--------------+---------------
 public       | postgres
 tiger        | gis_admin
 tiger_data   | gis_admin
 topology     | gis_admin
(4 rows)
```

Paso 4: transferir la propiedad de las tablas de PostGIS

> **Note**
>
> No cambie la propiedad de las funciones de PostGIS. Para que PostGIS funcione correctamente y reciba actualizaciones, estas funciones deben retener la propiedad original. Para obtener más información sobre los permisos de PostGIS, consulte PostgreSQL Security.

Use la siguiente función para transferir la propiedad de las tablas de PostGIS al rol `gis_admin`. Ejecute la siguiente declaración desde el símbolo del sistema psql para crear la función.

```
CREATE FUNCTION exec(text) returns text language plpgsql volatile AS $f$ BEGIN EXECUTE
 $1; RETURN $1; END; $f$;
CREATE FUNCTION
```

A continuación, ejecute la siguiente consulta para ejecutar la función `exec` que, a su vez, ejecuta las instrucciones y altera los permisos.

```
SELECT exec('ALTER TABLE ' || quote_ident(s.nspname) || '.' || quote_ident(s.relname)
 || ' OWNER TO gis_admin;')
  FROM (
    SELECT nspname, relname
    FROM pg_class c JOIN pg_namespace n ON (c.relnamespace = n.oid)
```

```
    WHERE nspname in ('tiger','topology') AND
    relkind IN ('r','S','v') ORDER BY relkind = 'S')
s;
```

Paso 5: pruebe las extensiones

Para evitar tener que especificar el nombre del esquema, añada el esquema `tiger` a la ruta de búsqueda usando el siguiente comando.

```
SET search_path=public,tiger;
SET
```

Pruebe el esquema `tiger` usando la siguiente instrucción SELECT.

```
SELECT address, streetname, streettypeabbrev, zip
 FROM normalize_address('1 Devonshire Place, Boston, MA 02109') AS na;
address | streetname | streettypeabbrev |  zip
---------+------------+------------------+-------
       1 | Devonshire | Pl               | 02109
(1 row)
```

Para obtener más información sobre esta extensión, consulte Tiger Geocoder en la documentación de PostGIS.

Pruebe el acceso al esquema `topology` usando la siguiente instrucción `SELECT`. Esto llama a la función `createtopology` para registrar un nuevo objeto de topología (my_new_topo) con el identificador de referencia espacial especificado (26986) y la tolerancia predeterminada (0,5). Para obtener más información, visite CreateTopology en la documentación de PostgreSQL.

```
SELECT topology.createtopology('my_new_topo',26986,0.5);
 createtopology
----------------
              1
(1 row)
```

Paso 6: Actualice la extensión de PostGIS

Cada nueva versión de PostgreSQL admite una o más versiones de la extensión de PostGIS compatibles con esa versión. La actualización del motor de PostgreSQL a una nueva versión no actualiza automáticamente la extensión de PostGIS. Antes de actualizar el motor de PostgreSQL,

normalmente se actualiza PostGIS a la versión más reciente disponible para la versión actual de PostgreSQL. Para obtener más información, consulte Versiones de extensión PostGIS.

Después de actualizar el motor de PostgreSQL, vuelva a actualizar la extensión de PostGIS a la versión compatible con la versión del motor de PostgreSQL recién actualizada. Para obtener más información sobre la actualización del motor PostgreSQL, consulte Realización de una actualización de la versión principal de RDS para PostgreSQL.

Puede comprobar si hay disponibles actualizaciones de la versión de la extensión PostGIS en su instancia de base de datos de RDS para PostgreSQL en cualquier momento. Para ello, ejecute el siguiente comando. Esta función está disponible con PostGIS 2.5.0 y versiones posteriores.

```
SELECT postGIS_extensions_upgrade();
```

Si su aplicación no es compatible con la última versión de PostGIS, puede instalar una versión anterior de PostGIS que esté disponible en su versión principal de la siguiente manera.

```
CREATE EXTENSION postgis VERSION "2.5.5";
```

Si desea actualizar a una versión específica de PostGIS desde una versión anterior, también puede utilizar el siguiente comando.

```
ALTER EXTENSION postgis UPDATE TO "2.5.5";
```

Dependiendo de la versión desde la que se actualice, es posible que tenga que volver a utilizar esta función. El resultado de la primera ejecución de la función determina si se necesita una función de actualización adicional. Por ejemplo, eso es lo que ocurre para la actualización de PostGIS 2 a PostGIS 3. Para obtener más información, consulte Actualización de PostGIS 2 a PostGIS 3.

Si actualizó esta extensión para prepararse para una actualización de la versión principal del motor de PostgreSQL, puede continuar con otras tareas preliminares. Para obtener más información, consulte Realización de una actualización de la versión principal de RDS para PostgreSQL.

Versiones de extensión PostGIS

Le recomendamos que instale las versiones de todas las extensiones, como PostGIS, como se indica en Versiones de extensión para Amazon RDS para PostgreSQL en las Notas de la versión de Amazon RDS para PostgreSQL Para obtener una lista de las versiones que están disponibles en su versión, utilice el siguiente comando.

```
SELECT * FROM pg_available_extension_versions WHERE name='postgis';
```

Puede encontrar información sobre la versión en las siguientes secciones de las Notas de la versión de Amazon RDS para PostgreSQL:

- Extensiones de PostgreSQL versión 16 admitidas en Amazon RDS
- Extensiones de PostgreSQL versión 15 admitidas en Amazon RDS
- Extensiones de PostgreSQL 14 admitidas en Amazon RDS
- Extensiones de PostgreSQL 13 admitidas en Amazon RDS
- Extensiones de PostgreSQL 12 admitidas en Amazon RDS
- Extensiones de PostgreSQL 11 admitidas en Amazon RDS
- Extensiones de PostgreSQL 10 admitidas en Amazon RDS
- Extensiones de PostgreSQL 9.6.x admitidas en Amazon RDS

Actualización de PostGIS 2 a PostGIS 3

A partir de la versión 3.0, la funcionalidad de trama de PostGIS es una extensión separada, `postgis_raster`. Esta extensión tiene su propia ruta de instalación y actualización. Esto elimina del núcleo docenas de funciones, tipos de datos y otros artefactos necesarios para el procesamiento de imágenes de trama desde la extensión `postgis` principal. Esto significa que si su caso de uso no requiere procesamiento de tramas, no es necesario que instale la extensión `postgis_raster`.

En el siguiente ejemplo de actualización, el primer comando de actualización extrae la funcionalidad de trama en la extensión `postgis_raster`. Luego, se requiere un segundo comando de actualización para actualizar `postgis_raster` a la nueva versión.

Para actualizar de PostGIS 2 a PostGIS 3

1. Identifique la versión predeterminada de PostGIS que está disponible para la versión de PostgreSQL en su Instancia de base de datos RDS para PostgreSQL. Para ello, ejecute la siguiente consulta.

```
SELECT * FROM pg_available_extensions
    WHERE default_version > installed_version;
  name   | default_version | installed_version |                                comment
---------+-----------------+-------------------
+-------------------------------------------------------------
```

```
 postgis | 3.1.4           | 2.3.7             | PostGIS geometry and geography
 spatial types and functions
(1 row)
```

2. Identifique las versiones de PostGIS instaladas en cada base de datos en la instancia de base de datos de RDS para PostgreSQL. En otras palabras, consulte la base de datos de cada usuario de la siguiente manera.

```
SELECT
    e.extname AS "Name",
    e.extversion AS "Version",
    n.nspname AS "Schema",
    c.description AS "Description"
FROM
    pg_catalog.pg_extension e
    LEFT JOIN pg_catalog.pg_namespace n ON n.oid = e.extnamespace
    LEFT JOIN pg_catalog.pg_description c ON c.objoid = e.oid
    AND c.classoid = 'pg_catalog.pg_extension'::pg_catalog.regclass
WHERE
    e.extname LIKE '%postgis%'
ORDER BY
    1;
  Name   | Version | Schema |                            Description
---------+---------+--------
+------------------------------------------------------------------------
 postgis | 2.3.7   | public | PostGIS geometry, geography, and raster spatial types
 and functions
(1 row)
```

Esta falta de correspondencia entre la versión predeterminada (PostGIS 3.1.4) y la versión instalada (PostGIS 2.3.7) significa que debe actualizar la extensión de PostGIS.

```
ALTER EXTENSION postgis UPDATE;
ALTER EXTENSION
WARNING: unpackaging raster
WARNING: PostGIS Raster functionality has been unpackaged
```

3. Ejecute la siguiente consulta para comprobar que la funcionalidad ráster ahora está en su propio paquete.

```
SELECT
    probin,
```

```
    count(*)
FROM
    pg_proc
WHERE
    probin LIKE '%postgis%'
GROUP BY
    probin;
          probin          | count
--------------------------+-------
 $libdir/rtpostgis-2.3    | 107
 $libdir/postgis-3        | 487
(2 rows)
```

El resultado muestra que aún hay una diferencia entre las versiones. Las funciones de PostGIS son de la versión 3 (postgis-3), mientras que las funciones ráster (rtpostgis) son de la versión 2 (rtpostgis-2.3). Para completar la actualización, vuelva a ejecutar el comando de actualización, como se indica a continuación.

```
postgres=> SELECT postgis_extensions_upgrade();
```

Puede ignorar los mensajes de advertencia sin problemas. Vuelva a ejecutar la siguiente consulta para comprobar que la actualización se ha completado. La actualización se completa cuando en PostGIS y en todas las extensiones relacionadas deja de aparecer una marca que indica que deben actualizarse.

```
SELECT postgis_full_version();
```

4. Utilice la siguiente consulta para ver el proceso de actualización completado y las extensiones empaquetadas por separado, y compruebe que las versiones coinciden.

```
SELECT
    e.extname AS "Name",
    e.extversion AS "Version",
    n.nspname AS "Schema",
    c.description AS "Description"
FROM
    pg_catalog.pg_extension e
    LEFT JOIN pg_catalog.pg_namespace n ON n.oid = e.extnamespace
    LEFT JOIN pg_catalog.pg_description c ON c.objoid = e.oid
        AND c.classoid = 'pg_catalog.pg_extension'::pg_catalog.regclass
WHERE
```

```
    e.extname LIKE '%postgis%'
ORDER BY
    1;
      Name      | Version | Schema |                            Description
----------------+---------+--------
+------------------------------------------------------------------------
 postgis        | 3.1.5   | public | PostGIS geometry, geography, and raster
 spatial types and functions
 postgis_raster | 3.1.5   | public | PostGIS raster types and functions
(2 rows)
```

El resultado muestra que la extensión de PostGIS 2 se ha actualizado a PostGIS 3 y que ambas, `postgis`y la extensión `postgis_raster` ya separada, son de la versión 3.1.5.

Una vez completada esta actualización, si no tiene pensado usar la funcionalidad de trama, puede eliminar la extensión de la siguiente manera.

```
DROP EXTENSION postgis_raster;
```

Uso de los contenedores de datos externos compatibles para Amazon RDS for PostgreSQL

Un FDW es un tipo específico de extensión que proporciona acceso a datos externos. Por ejemplo, la extensión `oracle_fdw` permite a su clúster de bases de datos de RDS for PostgreSQL trabajar con bases de datos Oracle. Otro ejemplo, cuando utiliza la extensión nativa de PostgreSQL `postgres_fdw`, puede acceder a los datos almacenados en instancias de bases de datos de PostgreSQL externas a su instancia de base de datos de RDS for PostgreSQL.

A continuación, puede encontrar información sobre varios contenedores de datos externos de PostgreSQL compatibles.

Temas

- Uso de la extensión log_fdw para acceder al registro de base de datos mediante SQL
- Uso de la extensión postgres_fdw para acceder a datos externos
- Uso de bases de datos MySQL con la extensión mysql_fdw
- Uso de una base de datos de Oracle con la extensión oracle_fdw
- Uso de bases de datos de SQL Server con la extensión mysql_fdw

Uso de la extensión log_fdw para acceder al registro de base de datos mediante SQL

La instancia de base de datos de RDS para PostgreSQL admite la extensión `log_fdw`, que se puede utilizar para el acceso al registro del motor de base de datos a través de una interfaz SQL. La extensión `log_fdw` proporciona dos funciones que facilitan la creación de tablas externas para los registros de la base de datos:

- `list_postgres_log_files`: muestra los archivos del directorio de registro de la base de datos y el tamaño del archivo en bytes.
- `create_foreign_table_for_log_file(table_name text, server_name text, log_file_name text)`: crea una tabla externa para el archivo especificado en la base de datos actual.

Todas las funciones creadas por `log_fdw` pertenecen a `rds_superuser`. Los miembros del rol `rds_superuser` pueden conceder acceso a estas funciones a otros usuarios de la base de datos.

De forma predeterminada, Amazon RDS genera los archivos de registro en formato `stderr` (error estándar), como se especifica en el parámetro `log_destination`. Solo hay dos opciones para este parámetro: `stderr` y `csvlog` (valores separados por comas, CSV). Si se añade la opción `csvlog` al parámetro, Amazon RDS generará tanto el registro `stderr` como el registro `csvlog`. Esto puede afectar a la capacidad de almacenamiento del clúster de base de datos, por lo que debe tener en cuenta los demás parámetros que afectan a la gestión de jlos registros. Para obtener más información, consulte Configuración del destino del registro (`stderr, csvlog`).

Uno de los beneficios de generar registros `csvlog` es que la extensión `log_fdw` permite crear tablas externas con los datos perfectamente divididos en varias columnas. Para ello, la instancia debe asociarse a un grupo de parámetros de base de datos personalizado para que usted pueda cambiar la configuración de `log_destination`. Para obtener información acerca de cómo hacerlo, consulte Uso de parámetros en su instancia de base de datos de RDS for PostgreSQL.

En el ejemplo siguiente se presupone que el parámetro `log_destination` incluye `cvslog`.

Para utilizar la extensión log_fdw

1. Instale la extensión de `log_fdw`.

```
postgres=> CREATE EXTENSION log_fdw;
CREATE EXTENSION
```

2. Cree el servidor de registros como contenedor de datos externo.

```
postgres=> CREATE SERVER log_server FOREIGN DATA WRAPPER log_fdw;
CREATE SERVER
```

3. Seleccione todos los elementos de una lista de archivos de registro.

```
postgres=> SELECT * FROM list_postgres_log_files() ORDER BY 1;
```

   A continuación, se muestra una respuesta de ejemplo.

```
         file_name           | file_size_bytes
-----------------------------+-----------------
 postgresql.log.2023-08-09-22.csv |            1111
 postgresql.log.2023-08-09-23.csv |            1172
 postgresql.log.2023-08-10-00.csv |            1744
 postgresql.log.2023-08-10-01.csv |            1102
```

```
(4 rows)
```

4. Crear una tabla con una sola columna log_entry para el archivo seleccionado.

```
postgres=> SELECT create_foreign_table_for_log_file('my_postgres_error_log',
     'log_server', 'postgresql.log.2023-08-09-22.csv');
```

La respuesta no proporciona más detalles que el hecho de que la tabla ya existe.

```
----------------------------------
(1 row)
```

5. Seleccione una muestra del archivo de registro. El siguiente código recupera la hora del registro y la descripción del mensaje de error.

```
postgres=> SELECT log_time, message FROM my_postgres_error_log ORDER BY 1;
```

A continuación, se muestra una respuesta de ejemplo.

```
            log_time             |                                 message
---------------------------------
+--------------------------------------------------------------------------------
Tue Aug 09 15:45:18.172 2023 PDT | ending log output to stderr
Tue Aug 09 15:45:18.175 2023 PDT | database system was interrupted; last known up
 at 2023-08-09 22:43:34 UTC
Tue Aug 09 15:45:18.223 2023 PDT | checkpoint record is at 0/90002E0
Tue Aug 09 15:45:18.223 2023 PDT | redo record is at 0/90002A8; shutdown FALSE
Tue Aug 09 15:45:18.223 2023 PDT | next transaction ID: 0/1879; next OID: 24578
Tue Aug 09 15:45:18.223 2023 PDT | next MultiXactId: 1; next MultiXactOffset: 0
Tue Aug 09 15:45:18.223 2023 PDT | oldest unfrozen transaction ID: 1822, in
 database 1
(7 rows)
```

Uso de la extensión postgres_fdw para acceder a datos externos

Puede acceder a los datos en una tabla en un servidor de base de datos remoto con la extensión postgres_fdw. Si establece una conexión remota desde su instancia de base de datos de PostgreSQL, el acceso también está disponible para su réplica de lectura.

Para utilizar postgres_fdw para acceder a un servidor de base de datos remoto

1. Instale la extensión postgres_fdw.

```
CREATE EXTENSION postgres_fdw;
```

2. Cree el servidor de datos externo utilizando CREATE SERVER.

```
CREATE SERVER foreign_server
FOREIGN DATA WRAPPER postgres_fdw
OPTIONS (host 'xxx.xx.xxx.xx', port '5432', dbname 'foreign_db');
```

3. Cree un mapeo de usuario para identificar la función que utilizar en el servidor remoto.

> **Important**
>
> Para redactar la contraseña para que no aparezca en los registros, configure `log_statement=none` en el nivel de sesión. Si se establece en el nivel de parámetro, no se redacta la contraseña.

```
CREATE USER MAPPING FOR local_user
SERVER foreign_server
OPTIONS (user 'foreign_user', password 'password');
```

4. Cree una tabla que se mapee a la tabla del servidor remoto.

```
CREATE FOREIGN TABLE foreign_table (
        id integer NOT NULL,
        data text)
SERVER foreign_server
OPTIONS (schema_name 'some_schema', table_name 'some_table');
```

Uso de bases de datos MySQL con la extensión mysql_fdw

Para tener acceso desde una instancia de base de datos de RDS para PostgresSQL a una base de datos compatible con MySQL, puede instalar y utilizar la extensión `mysql_fdw`. Este contenedor de datos externo le permite trabajar con RDS for MySQL, Aurora MySQL, MariaDB y otras bases de datos compatibles con MySQL. La conexión desde la instancia de base de datos de RDS

para PostgreSQL a la base de datos MySQL se cifra tanto como sea posible, depeniendo de la configuración del cliente y del servidor. No obstante, puede aplicar cifrado si lo desea. Para obtener más información, consulte Uso de cifrado en tránsito con la extensión.

La extensión `mysql_fdw` es complatible con las versiones de Amazon RDS para PostgreSQL 14.2, 13.6 y posteriores. Es compatible con selecciones, inserciones, actualizaciones y eliminaciones de una base de datos de RDS for PostgreSQL en tablas de una instancia de base de datos compatible con MySQL.

Temas

- Configuración de una base de datos de RDS para PostgreSQL para utilizar la extensión mysql_fdw
- Ejemplo: Acceso a una base de datos de RDS para MySQL desde RDS para PostgreSQL
- Uso de cifrado en tránsito con la extensión

Configuración de una base de datos de RDS para PostgreSQL para utilizar la extensión mysql_fdw

Para configurar la extensión `mysql_fdw` en la instancia de base de datos de RDS para PostgreSQL es necesario cargar la extensión en la instancia y, a continuación, crear el punto de conexión a la instancia de base de datos MySQL. Para esa tarea debe disponer de los siguientes detalles sobre la instancia de base de datos MySQL:

- Nombre de host o del punto de conexión. Con una instancia de base de datos de RDS para MySQL el punto de conexión puede encontrarse a través de la consola. Elija la pestaña Conectividad y seguridad y busque en la sección “Punto de enlace y puerto”.
- Número de puerto. El número de puerto predeterminado para MySQL es 3306.
- Nombre de la base de datos. El identificador de la base de datos.

También tiene que proporcionar acceso en el grupo de seguridad o en la lista de control de acceso (ACL) para el puerto MySQL, 3306. Tanto la instancia de base de datos de RDS para PostgreSQL como la de RDS para MySQL necesitan acceso al puerto 3306. Si el acceso no está configurado correctamente, al intentar conectarse a una tabla compatible con MySQL aparecerá un mensaje de error similar al siguiente:

```
ERROR: failed to connect to MySQL: Can't connect to MySQL server on 'hostname.aws-
region.rds.amazonaws.com:3306' (110)
```

En el procedimiento que sigue, usted (como cuenta de `rds_superuser`) crea el servidor externo. A continuación, concede acceso al servidor externo a usuarios específicos. A continuación, estos usuarios crean sus propias asignaciones a las cuentas de usuario de MySQL adecuadas para trabajar con la instancia de base de datos MySQL.

Para utilizar mysql_fdw para acceder a un servidor de base de datos MySQL

1. Conéctese a la instancia de base de datos PostgreSQL a través de una cuenta que tenga el rol de `rds_superuser`. Si al crear la instancia de base de datos de RDS para PostgreSQL aceptó los valores predeterminados, el nombre de usuario será `postgres` y se podrá conectar mediante la herramienta de línea de comandos `psql` de este modo:

   ```
   psql --host=your-DB-instance.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password
   ```

2. Instale la extensión `mysql_fdw` de la siguiente manera:

   ```
   postgres=> CREATE EXTENSION mysql_fdw;
   CREATE EXTENSION
   ```

Una vez instalada la extensión en la instancia de base de datos de RDS para PostgreSQL, configure el servidor externo que proporciona la conexión a una base de datos MySQL.

Para crear el servidor externo

Realice estas tareas en la instancia de base de datos RDS para PostgreSQL. Para seguir estos pasos se entiende que está conectado como usuario con privilegios `rds_superuser`, como `postgres`.

1. Cree un servidor externo en la instancia de base de datos RDS for PostgreSQL:

   ```
   postgres=> CREATE SERVER mysql-db FOREIGN DATA WRAPPER mysql_fdw OPTIONS (host 'db-
   name.111122223333.aws-region.rds.amazonaws.com', port '3306');
   CREATE SERVER
   ```

2. Conceda a los usuarios que corresponsa acceso al servidor externo. Deben ser usuarios que no sean administradores, es decir, usuarios que no tengan el rol `rds_superuser`.

   ```
   postgres=> GRANT USAGE ON FOREIGN SERVER mysql-db to user1;
   ```

```
GRANT
```

Los usuarios de PostgreSQL crean y administran sus propias conexiones a la base de datos MySQL a través del servidor externo.

Ejemplo: Acceso a una base de datos de RDS para MySQL desde RDS para PostgreSQL

Supongamos que tiene una tabla simple en una instancia de base de datos de PostgreSQL. Los usuarios de RDS para PostgreSQL desean consultar (`SELECT`), insertar (`INSERT`), actualizar (`UPDATE`) y eliminar (`DELETE`) elementos de la tabla. Supongamos que la exstensión `mysql_fdw` se creó en la instancia de base de datos de RDS for PostgreSQL, como se detalla en el procedimiento anterior. Después de conectarse a la instancia de base de datos de RDS for PostgreSQL como usuario con privilegios `rds_superuser`, podrá continuar con los pasos que se describen a continuación.

1. Cree un servidor externo en la instancia de base de datos de RDS para PostgreSQL:

```
test=> CREATE SERVER mysqldb FOREIGN DATA WRAPPER mysql_fdw OPTIONS (host 'your-
DB.aws-region.rds.amazonaws.com', port '3306');
CREATE SERVER
```

2. Conceda permiso de uso a un usuario que no tiene permisos `rds_superuser`, por ejemplo `user1`.

```
test=> GRANT USAGE ON FOREIGN SERVER mysqldb TO user1;
GRANT
```

3. Conéctese como*user1* y, a continuación, cree una asignación para el usuario de MySQL:

```
test=> CREATE USER MAPPING FOR user1 SERVER mysqldb OPTIONS (username 'myuser',
 password 'mypassword');
CREATE USER MAPPING
```

4. Cree una tabla externa vinculada a la tabla MySQL:

```
test=> CREATE FOREIGN TABLE mytab (a int, b text) SERVER mysqldb OPTIONS (dbname
 'test', table_name '');
CREATE FOREIGN TABLE
```

5. Ejecute una consulta simple en la tabla externa:

```
test=> SELECT * FROM mytab;
a |   b
---+-------
1 | apple
(1 row)
```

6. Puede añadir, modificar y quitar datos de la tabla MySQL. Por ejemplo:

```
test=> INSERT INTO mytab values (2, 'mango');
INSERT 0 1
```

Ejecute la consulta SELECT de nuevo para ver los resultados:

```
test=> SELECT * FROM mytab ORDER BY 1;
 a |   b
---+-------
1 | apple
2 | mango
(2 rows)
```

Uso de cifrado en tránsito con la extensión

De forma predeterminada, la conexión a MySQL desde RDS para PostgreSQL utiliza cifrado en tránsito (TLS/SSL). No obstante, la conexión vuelve a ser no cifrada cuando la configuración del cliente y del servidor difieren. Puede aplicar el cifrado para todas las conexiones salientes especificando la opción REQUIRE SSL en las cuentas de usuario de RDS for MySQL. Este mismo método también funciona para las cuentas de usuario de MariaDB y Aurora MySQL.

Para cuentas de usuario MySQL configuradas en REQUIRE SSL, el intento de conexión falla si no se puede establecer una conexión segura.

Para aplicar el cifrado de cuentas de usuario de bases de datos MySQL existentes, puede utilizar el comando ALTER USER. La sintaxis varía en función de la versión de MySQL, como se muestra en la siguiente tabla. Para obtener más información, consulte ALTER USER en el manual de referencia de MySQL.

MySQL 5.7, MySQL 8.0	MySQL 5.6
`ALTER USER 'user'@'%' REQUIRE SSL;`	`GRANT USAGE ON *.* to 'user'@'%' REQUIRE SSL;`

Para obtener más información acerca de la extensión `mysql_fdw`, consulte la documentación sobre mysql_fdw.

Uso de una base de datos de Oracle con la extensión oracle_fdw

Para acceder a una base de datos de Oracle desde su instancia de base de datos de RDS for PostgreSQL puede instalar y utilizar la extensión `oracle_fdw`. Esta extensión es un contenedor de datos externos para bases de datos Oracle. Para obtener más información sobre la extensión, consulte la documentación de oracle_fdw.

La extensión `oracle_fdw` es compatible con las versiones 12.7, 13.3 y las versiones posteriores de RDS for PostgreSQL.

Temas

- Activación de la extensión oracle_fdw
- Ejemplo: Usar un servidor externo vinculado a una Amazon RDS for Oracle Database
- Trabajo con cifrado en tránsito
- Comprensión y permisos de la vista pg_user_mappings

Activación de la extensión oracle_fdw

Para utilizar la extensión oracle_fdw, lleve a cabo el siguiente procedimiento.

Para habilitar la extensión oracle_fdw

- Ejecute el siguiente comando con una cuenta que tenga los permisos `rds_superuser`.

```
CREATE EXTENSION oracle_fdw;
```

Ejemplo: Usar un servidor externo vinculado a una Amazon RDS for Oracle Database

El siguiente ejemplo muestra el uso de un servidor externo vinculado a una base de datos de Amazon RDS for Oracle.

Crear un servidor externo vinculado a una base de datos de RDS for Oracle

1. Tenga en cuenta lo siguiente en la instancia de base de datos de RDS for Oracle:
   - punto de enlace
   - Puerto
   - Nombre de base de datos
2. Cree un servidor externo.

```
test=> CREATE SERVER oradb FOREIGN DATA WRAPPER oracle_fdw OPTIONS (dbserver
 '//endpoint:port/DB_name');
CREATE SERVER
```

3. Otorgue uso a un usuario que no tenga permisos `rds_superuser`, por ejemplo `user1`.

```
test=> GRANT USAGE ON FOREIGN SERVER oradb TO user1;
GRANT
```

4. Conéctese como `user1` y cree una asignación a un usuario de Oracle.

```
test=> CREATE USER MAPPING FOR user1 SERVER oradb OPTIONS (user 'oracleuser',
 password 'mypassword');
CREATE USER MAPPING
```

5. Cree una tabla externa vinculada a una tabla de Oracle.

```
test=> CREATE FOREIGN TABLE mytab (a int) SERVER oradb OPTIONS (table 'MYTABLE');
CREATE FOREIGN TABLE
```

6. Consulte la tabla externa.

```
test=>  SELECT * FROM mytab;
a
---
1
```

```
(1 row)
```

Si la consulta informa el siguiente error, verifique el grupo de seguridad y la lista de control de acceso (ACL) para asegurarse de que ambas instancias puedan comunicarse.

```
ERROR: connection for foreign table "mytab" cannot be established
DETAIL: ORA-12170: TNS:Connect timeout occurred
```

Trabajo con cifrado en tránsito

El cifrado de PostgreSQL a Oracle en tránsito se basa en una combinación de parámetros de configuración de cliente y servidor. Para obtener un ejemplo que utiliza Oracle 21c, consulte About the Values for Negotiating Encryption and Integrity en la documentación de Oracle. El cliente utilizado para oracle_fdw en Amazon RDS está configurado con `ACCEPTED`, lo que significa que el cifrado depende de la configuración del servidor de base de datos de Oracle y utiliza la biblioteca de seguridad de Oracle (libnnz) para cifrado.

Si su base de datos está en RDS for Oracle, consulte Oracle Native Network Encryption para configurar el cifrado.

Comprensión y permisos de la vista pg_user_mappings

El catálogo de PostgreSQL `pg_user_mapping` almacena la asignación desde un usuario RDS for PostgreSQL en el usuario de un servidor de datos externo (remoto). El acceso al catálogo está restringido, pero usted utiliza la vista `pg_user_mappings` para ver las asignaciones. A continuación, se muestra un ejemplo sobre cómo se aplican los permisos en una base de datos de Oracle de ejemplo, aunque esta información es válida también en general para cualquier contenedor de datos externo.

En el siguiente resultado, puede encontrar roles y permisos asignados a tres usuarios de ejemplo diferentes. Usuarios de `rdssu1` y `rdssu2` son miembros del rol `rds_superuser`, y el usuario `user1` no lo es. En el ejemplo se usa el metacomando `\du` de `psql` para enumerar los roles existentes.

```
test=>  \du
                                                    List of roles
    Role name    |                         Attributes                         |
                Member of
```

```
-----------------+-------------------------------------------------------------
+-----------------------------------------------------------
 rdssu1          |                                                             |
 {rds_superuser}
 rdssu2          |                                                             |
 {rds_superuser}
 user1           |                                                             | {}
```

Todos los usuarios, incluidos los usuarios con privilegios `rds_superuser`, pueden ver sus propias asignaciones de usuarios (`umoptions`) en la tabla `pg_user_mappings`. Como se muestra en el siguiente ejemplo, cuando `rdssu1` intenta obtener todas las asignaciones de usuario, se genera un a pesar de los privilegios `rds_superuser` de `rdssu1`:

```
test=> SELECT * FROM pg_user_mapping;
ERROR: permission denied for table pg_user_mapping
```

A continuación, se muestran algunos ejemplos:

```
test=> SET SESSION AUTHORIZATION rdssu1;
SET
test=> SELECT * FROM pg_user_mappings;
 umid  | srvid | srvname | umuser | usename    |            umoptions
-------+-------+---------+--------+------------+---------------------------------
 16414 | 16411 | oradb   |  16412 | user1      |
 16423 | 16411 | oradb   |  16421 | rdssu1     | {user=oracleuser,password=mypwd}
 16424 | 16411 | oradb   |  16422 | rdssu2     |
 (3 rows)

test=> SET SESSION AUTHORIZATION rdssu2;
SET
test=> SELECT * FROM pg_user_mappings;
 umid  | srvid | srvname | umuser | usename    |            umoptions
-------+-------+---------+--------+------------+---------------------------------
 16414 | 16411 | oradb   |  16412 | user1      |
 16423 | 16411 | oradb   |  16421 | rdssu1     |
 16424 | 16411 | oradb   |  16422 | rdssu2     | {user=oracleuser,password=mypwd}
 (3 rows)

test=> SET SESSION AUTHORIZATION user1;
SET
test=> SELECT * FROM pg_user_mappings;
 umid  | srvid | srvname | umuser | usename    |           umoptions
```

```
-------+-------+---------+--------+------------+--------------------------------
 16414 | 16411 | oradb   |  16412 | user1      | {user=oracleuser,password=mypwd}
 16423 | 16411 | oradb   |  16421 | rdssu1     |
 16424 | 16411 | oradb   |  16422 | rdssu2     |
 (3 rows)
```

Debido a las diferencias en la implementación de `information_schema._pg_user_mappings` y `pg_catalog.pg_user_mappings`, un `rds_superuser` que se crea manualmente requiere permisos adicionales para ver las contraseñas en `pg_catalog.pg_user_mappings`.

No requieren otros permisos para un `rds_superuser` para ver las contraseñas en `information_schema._pg_user_mappings`.

Los usuarios que no tienen el rol `rds_superuser` pueden ver contraseñas en `pg_user_mappings` solo en las condiciones que se describen a continuación:

- El usuario actual es el usuario que se está asignando y es el propietario del servidor o tiene el privilegio de `USAGE` en él.
- El usuario actual es el propietario del servidor, y la asignación es para `PUBLIC`.

Uso de bases de datos de SQL Server con la extensión mysql_fdw

Puede utilizar la extensión de PostgreSQL `tds_fdw` para acceder a bases de datos compatibles con el protocolo de flujo de datos tabular (TDS), como bases de datos Sybase y Microsoft SQL Server. Este contenedor de datos externo le permite conectarse desde suinstancia de base de datos RDS for PostgreSQL a bases de datos que utilizan el protocolo TDS, incluido Amazon RDS for Microsoft SQL Server. Para obtener más información, consulte la documentación sobre tds-fdw/tds_fdw en GitHub.

La extensión `tds_fdw` es compatible con las versiones 14.2, 13.6 y posteriores de Amazon RDS for PostgreSQL.

Configuración de la base de datos de Aurora PostgreSQL para utilizar la extensión mysql_fdw

En los procedimientos que siguen encontrará un ejemplo de configuración y uso de `tds_fdw` con una instancia de base de datos RDS for PostgreSQL. Antes de poder conectarse a una base de datos SQL Server mediante `tds_fdw`, tiene que obtener los siguientes detalles de la instancia:

- Nombre de host o del punto de conexión. Para instancias de RDS for MySQL encontrará los puntos de conexión con la consola. Elija la pestaña Conectividad y seguridad y busque en la sección “Punto de enlace y puerto”.
- Número de puerto. El puerto 1433 es el predeterminado para Microsoft SQL Server.
- Nombre de la base de datos. El identificador de la base de datos.

También deberá proporcionar acceso en el grupo de seguridad o en la lista de control de acceso (ACL) al puerto MySQL, 1433. Tanto el clúster de bases de datos de Aurora PostgreSQL como necesitan poder acceder al puerto 1433. Si el acceso no está configurado correctamente, cuando intente consultar Microsoft SQL Server aparecerá el siguiente mensaje de error:

```
ERROR: DB-Library error: DB #: 20009, DB Msg: Unable to connect:
Adaptive Server is unavailable or does not exist (mssql2019.aws-
region.rds.amazonaws.com), OS #: 0, OS Msg: Success, Level: 9
```

Para usar tds_fdw para conectarse a una base de datos de SQL Server

1. Conéctese a su instancia de base de datos PostgreSQL con una cuenta con rol `rds_superuser`:

   ```
   psql --host=your-DB-instance.aws-region.rds.amazonaws.com --port=5432 --
   username=test --password
   ```

2. Instale la extensión `tds_fdw`.

   ```
   test=> CREATE EXTENSION tds_fdw;
   CREATE EXTENSION
   ```

Después de instalar la extensión en su instancia de base de datos RDS for PostgreSQL, configure el servidor externo.

Para crear el servidor externo

Realice estas tareas en la instancia de base de datos RDS for PostgreSQL con una cuenta que con privilegios `rds_superuser`.

1. Cree un servidor externo en la instancia de base de datos RDS for PostgreSQL:

```
test=> CREATE SERVER sqlserverdb FOREIGN DATA WRAPPER tds_fdw OPTIONS
 (servername 'mssql2019.aws-region.rds.amazonaws.com', port '1433', database
 'tds_fdw_testing');
CREATE SERVER
```

Para acceder a datos no que sean ASCII en el lado de SQLServer, cree un enlace de servidor con la opción character_set en la instancia de base de datos de RDS para PostgreSQL:

```
test=> CREATE SERVER sqlserverdb FOREIGN DATA WRAPPER tds_fdw OPTIONS (servername
 'mssql2019.aws-region.rds.amazonaws.com', port '1433', database 'tds_fdw_testing',
 character_set 'UTF-8');
CREATE SERVER
```

2. Conceda permisos a un usuario que no tenga los privilegios del rol `rds_superuser`, por ejemplo `user1`:

```
test=> GRANT USAGE ON FOREIGN SERVER sqlserverdb TO user1;
```

3. Conéctese como user1 y, a continuación, cree una asignación para el usuario de SQL Server:

```
test=> CREATE USER MAPPING FOR user1 SERVER sqlserverdb OPTIONS (username
 'sqlserveruser', password 'password');
CREATE USER MAPPING
```

4. Cree una tabla externa vinculada a una tabla de SQL Server.

```
test=> CREATE FOREIGN TABLE mytab (a int) SERVER sqlserverdb OPTIONS (table
 'MYTABLE');
CREATE FOREIGN TABLE
```

5. Consulte la tabla externa:

```
test=> SELECT * FROM mytab;
 a
---
 1
(1 row)
```

Uso de cifrado en tránsito para la conexión

La conexión de RDS for PostgreSQLa SQL Server utiliza cifrado en tránsito (TLS/SSL) según la configuración de la base de datos de SQL Server. Si SQL Server no está configurado para el cifrado, el RDS para el cliente PostgreSQL que realiza la solicitud a la base de datos de SQL Server vuelve a no ir cifrado.

Puede aplicar el cifrado para la conexión a RDS para instancias de base de datos de SQL Server configurando el parámetro `rds.force_ssl`. Para saber cómo, consulte Requerir que las conexiones a la instancia de base de datos usen SSL. Para obtener más información sobre la configuración de SSL/TLS para RDS for SQL Server, consulte Uso de SSL con una instancia de base de datos de Microsoft SQL Server.

Uso de Extensiones de lenguaje de confianza para PostgreSQL

Extensiones de lenguaje de confianza para PostgreSQL es un kit de desarrollo de código abierto para crear extensiones de PostgreSQL. Le permite crear extensiones de PostgreSQL de alto rendimiento y ejecutarlas de forma segura en su instancia de base de datos de RDS para PostgreSQL. Al utilizar Extensiones de lenguaje de confianza (TLE) para PostgreSQL, puede crear extensiones de PostgreSQL que sigan el enfoque documentado para ampliar la funcionalidad de PostgreSQL. Para obtener más información, consulte el punto Packaging Related Objects into an Extension (Empaquetar objetos relacionados en una extensión) en la documentación de PostgreSQL.

Una ventaja clave de TLE es que se puede utilizar en entornos que no proporcionan acceso al sistema de archivos subyacente a la instancia de PostgreSQL. Anteriormente, la instalación de una nueva extensión requería acceso al sistema de archivos. TLE elimina esta restricción. Pues proporciona un entorno de desarrollo para crear nuevas extensiones para cualquier base de datos de PostgreSQL, incluidas las que se ejecutan en los instancias de base de datos de RDS para PostgreSQL.

TLE está diseñado para evitar el acceso a recursos no seguros para las extensiones que se crean con TLE. Su entorno de ejecución limita el impacto de cualquier defecto de extensión a una única conexión de base de datos. TLE también proporciona a los administradores de bases de datos un control preciso sobre quién puede instalar las extensiones y proporciona un modelo de permisos para ejecutarlas.

TLE es compatible con las siguientes versiones de RDS para PostgreSQL:

- Versión 17.1 y otras versiones 17 superiores
- Versión 16.1 y versiones posteriores a 16
- Versión 15.2 y versiones posteriores a 15
- Versión 14.5 y versiones posteriores a 14
- Versión 13.12 y versiones posteriores a 13

El entorno de desarrollo y el entorno de ejecución de Extensiones de lenguaje de confianza se empaquetan como la extensión `pg_tle` de PostgreSQL, versión 1.0.1. Admite la creación de extensiones en JavaScript, Perl, Tcl, PL/pgSQL y SQL. La extensión `pg_tle` se instala en la instancia de base de datos de RDS para PostgreSQL del mismo modo que se instalan otras extensiones de PostgreSQL. Una vez configurada `pg_tle`, los desarrolladores pueden usarla para crear nuevas extensiones de PostgreSQL, conocidas como extensiones TLE.

En los temas siguientes, encontrará información sobre cómo configurar Extensiones de lenguaje de confianza y cómo comenzar a crear sus propias extensiones TLE.

Temas

- Terminología
- Requisitos para usar Extensiones de lenguaje de confianza para PostgreSQL
- Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL
- Información general de Extensiones de lenguaje de confianza para PostgreSQL
- Creación de extensiones TLE para RDS para PostgreSQL
- Eliminar las extensiones TLE de una base de datos
- Desinstalación de Extensiones de lenguaje de confianza para PostgreSQL
- Uso de enlaces de PostgreSQL con sus extensiones TLE
- Uso de tipos de datos personalizados en TLE
- Referencia de funciones para Extensiones de lenguaje de confianza para PostgreSQL
- Referencia de enlaces para Extensiones de lenguaje de confianza para PostgreSQL

Terminología

Para entender mejor Extensiones de lenguaje de confianza, consulta el siguiente glosario para ver los términos utilizados en este tema.

Extensiones de lenguaje de confianza para PostgreSQL

> Extensiones de lenguaje de confianza para PostgreSQL es el nombre oficial del kit de desarrollo de código abierto que se incluye como extensión `pg_tle`. Está disponible para su uso en cualquier sistema PostgreSQL. Para obtener más información, consulte aws/pg_tle en GitHub.

Extensiones de lenguaje de confianza

> Extensiones de lenguaje de confianza es la versión abreviada de Extensiones de lenguaje de confianza para PostgreSQL. En esta documentación se utilizan el nombre abreviado y sus siglas (TLE).

lenguaje de confianza

Un lenguaje de confianza es un lenguaje de programación o de scripting que tiene atributos de seguridad específicos. Por ejemplo, los lenguajes de confianza suelen restringir el acceso al sistema de archivos y limitan el uso de las propiedades de red especificadas. El kit de desarrollo TLE está diseñado para ser compatible con lenguajes de confianza. PostgreSQL admite varios lenguajes diferentes que se utilizan para crear extensiones fiables o no fiables. Para ver un ejemplo, consulte el punto Trusted and Untrusted PL/Perl (PL/Perl fiable y no fiable) en la documentación de PostgreSQL. Al crear una extensión con Extensiones de lenguaje de confianza, la extensión utiliza mecanismos de lenguaje de confianza de forma inherente.

Extensión TLE

Una extensión TLE es una extensión de PostgreSQL que se ha creado mediante el kit de desarrollo de Extensiones de lenguaje de confianza (TLE).

Requisitos para usar Extensiones de lenguaje de confianza para PostgreSQL

Estos son los requisitos para configurar y usar el kit de desarrollo TLE.

- Versiones de RDS para PostgreSQL: las extensiones de lenguaje de confianza se admiten en RDS para PostgreSQL versiones 13.12 y versiones 13 posteriores, 14.5 y versiones 14 posteriores, y 15.2 y versiones posteriores únicamente.
  - Si necesita actualizar su instancia de RDS para PostgreSQL, consulte Actualizaciones del motor de base de datos de RDS para PostgreSQL.
  - Si aún no tiene un clúster de base de datos de Aurora que ejecute PostgreSQL, puede crear una. Para obtener más información, consulte Instancia de base de datos de RDS para PostgreSQL, consulte Creación de una instancia de base de datos de PostgreSQL y conexión a ella.
- Requiere privilegios de **`rds_superuser`**: para instalar y configurar la extensión `pg_tle`, el rol de usuario de la base de datos debe tener permisos del rol `rds_superuser`. De forma predeterminada, este rol se otorga al usuario `postgres` que crea el Instancia de base de datos RDS para PostgreSQL.
- Requiere un grupo de parámetros de base de datos personalizado: su instancia de base de datos de RDS para PostgreSQL debe configurarse con un grupo de parámetros de base de datos personalizado.

- Si su instancia de base de datos de RDS para PostgreSQL no está configurado con un grupo de parámetros de base de datos personalizado, debe crear uno y asociarlo su instancia de base de datos de RDS para PostgreSQL. Para obtener un breve resumen de los pasos, consulte Creación y aplicación de un grupo de parámetros de base de datos personalizado.
- Si su instancia de base de datos de RDS para PostgreSQL ya se ha configurado con un grupo de parámetros de base de datos personalizado, puede configurar Extensiones de lenguaje de confianza. Para obtener más información, consulte Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL.

Creación y aplicación de un grupo de parámetros de base de datos personalizado

Siga los siguientes pasos para crear un grupo de parámetros de base de datos personalizado y configure su instancia de base de datos de RDS para PostgreSQL para utilizarlo.

Consola

Para crear un grupo de parámetros de base de datos personalizado y utilizarlo con su instancia de base de datos de RDS para PostgreSQL

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Elija Parameter groups (Grupos de parámetros) en el menú de Amazon RDS.
3. Elija Create parameter group.
4. En la página Parameter group details (Detalles del grupo de parámetros), escriba la siguiente información.
   - En Parameter group family (Familia de grupo de parámetros), elija postgres14.
   - En Type (Tipo), elija DB Parameter Group (Grupo de parámetros de bases de datos).
   - En Group name (Nombre de grupo), asigne al grupo de parámetros un nombre significativo en el contexto de sus operaciones.
   - En Description (Descripción), introduzca una descripción útil para que los demás miembros de su equipo puedan encontrarla fácilmente.
5. Seleccione Crear. El grupo de parámetros de base de datos personalizado se crea en su Región de AWS. Ahora puede modificar su instancia de base de datos de RDS para PostgreSQL para usarlo. Para ello, siga los siguientes pasos.
6. Seleccione Databases (Bases de datos) en el menú de Amazon RDS.

7. Elija la instancia de base de datos de RDS para PostgreSQL que desea usar con TLE de entre las enumeradas y, a continuación, elija Modify (Modificar).
8. En la En la página Modify DB cluster settings (Modificar la configuración del clúster de base de datos), busque Database options (Opciones de la base de datos) y elija su grupo de parámetros de base de datos personalizado en el selector.
9. Elija Continue (Continuar) para guardar el cambio.
10. Elija Apply immediately (Aplicar inmediatamente) para poder seguir configurando la instancia de base de datos de RDS para PostgreSQL para utilizar TLE.

Para continuar con la configuración del sistema para Extensiones de lenguaje de confianza, consulte Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL.

Para obtener más información sobre cómo trabajar con Grupos de parámetros de base de datos, consulte Grupos de parámetros de base de datos para instancias de Amazon RDS.

AWS CLI

Puede evitar especificar el argumento `--region` al utilizar los comandos de la CLI al configurar su AWS CLI con su Región de AWS predeterminada. Para obtener más información, consulte Fundamentos de configuración en la Guía del usuario de AWS Command Line Interface.

Para crear un grupo de parámetros de base de datos personalizado y utilizarlo con su instancia de base de datos de RDS para PostgreSQL

1. Utilice el comando create-db-parameter-group de la AWS CLI para crear un grupo de parámetros de base de datos personalizado basado en postgres14 para su Región de AWS.

   Para Linux, macOS o:Unix

   ```
   aws rds create-db-parameter-group \
     --region aws-region \
     --db-parameter-group-name custom-params-for-pg-tle \
     --db-parameter-group-family postgres14 \
     --description "My custom DB parameter group for Trusted Language Extensions"
   ```

   En:Windows

   ```
   aws rds create-db-parameter-group ^
   ```

```
  --region aws-region ^
  --db-parameter-group-name custom-params-for-pg-tle ^
  --db-parameter-group-family postgres14 ^
  --description "My custom DB parameter group for Trusted Language Extensions"
```

Su grupo de parámetros de base de datos personalizado está disponible en su Región de AWS, por lo que puede modificar instancia de base de datos de RDS para PostgreSQL para utilizarla.

2. Utilice el comando modify-db-instance de la AWS CLI para aplicar su grupo de parámetros de base de datos personalizado a su instancia de base de datos de RDS para PostgreSQL. Este comando reinicia inmediatamente la instancia activa.

   Para Linux, macOS o:Unix

   ```
   aws rds modify-db-instance \
     --region aws-region \
     --db-instance-identifier your-instance-name \
     --db-parameter-group-name custom-params-for-pg-tle \
     --apply-immediately
   ```

   En:Windows

   ```
   aws rds modify-db-instance ^
     --region aws-region ^
     --db-instance-identifier your-instance-name ^
     --db-parameter-group-name custom-params-for-pg-tle ^
     --apply-immediately
   ```

Para continuar con la configuración del sistema para Extensiones de lenguaje de confianza, consulte Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL.

Para obtener más información, consulte Grupos de parámetros para Amazon RDS.

Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL

En los pasos siguientes se supone que su instancia de base de datos de RDS para PostgreSQL está asociada a un grupo de parámetros de base de datos personalizado. Puede utilizar la AWS Management Console o la AWS CLI para estos pasos.

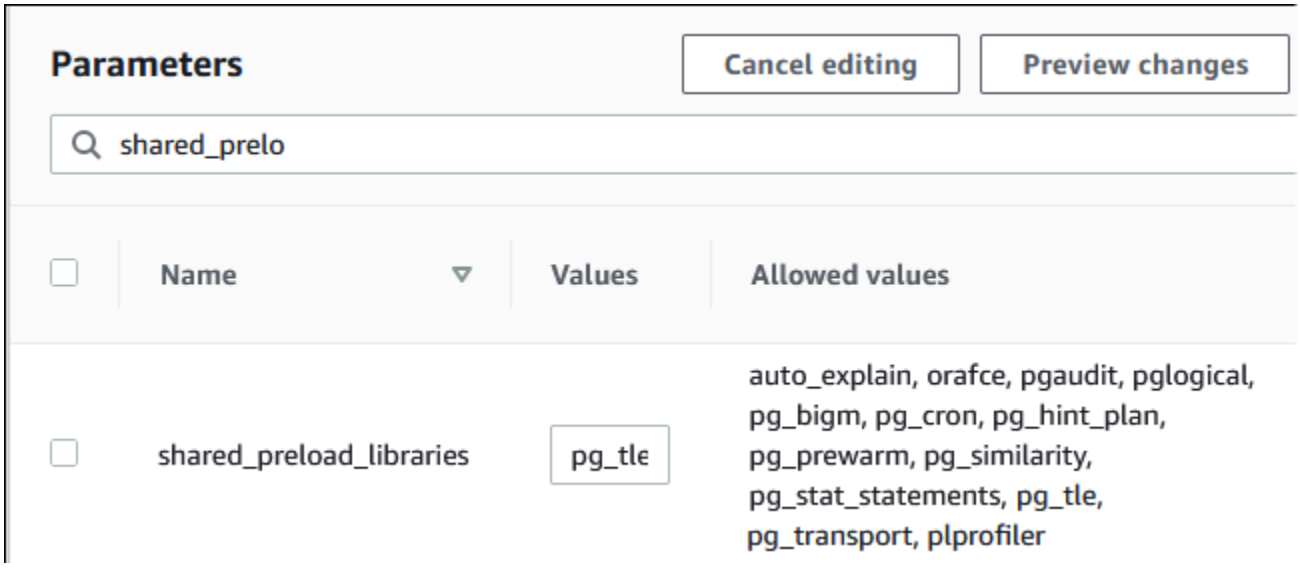
Al configurar Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL, las instala en una base de datos específica para que las usen los usuarios de la base de datos que tienen permisos en esa base de datos.

Consola

Para configurar Extensiones de lenguaje de confianza

Realice los siguientes pasos con una cuenta que sea miembro del grupo (rol) `rds_superuser`.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija la instancia de base de datos de RDS for PostgreSQL.
3. Abra la pestaña Configuration (Configuración) para su Instancia de base de datos RDS para PostgreSQL. Entre los detalles de la instancia, busque el enlace del grupo de parámetros.
4. Elija el enlace para abrir los parámetros personalizados asociados al Instancia de base de datos RDS para PostgreSQL.
5. En el campo de búsqueda Parametes (Parámetros), escriba `shared_pre` para buscar el parámetro `shared_preload_libraries`.
6. Seleccione Edit parameters (Editar parámetros) para acceder a los valores de las propiedades.
7. Añada `pg_tle` a la lista en el campo Values (Valores). Utilice una coma para separar los elementos de la lista de valores.



8. Reinicie la instancia de base de datos de RDS for PostgreSQL para que surta efecto el cambio en el parámetro `shared_preload_libraries`.

9. Cuando la instancia esté disponible, verifique si se ha inicializado `pg_tle`. Use `psql` para conectarse a la instancia de base de datos de RDS for PostgreSQL y, a continuación, ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
shared_preload_libraries
--------------------------
rdsutils,pg_tle
(1 row)
```

10. Con la extensión `pg_tle` inicializada, ahora ya puede crear la extensión.

```
CREATE EXTENSION pg_tle;
```

Para comprobar que la extensión esté instalada, use el metacomando `psql`.

```
labdb=> \dx
                          List of installed extensions
  Name   | Version |   Schema   |                Description
---------+---------+------------+-------------------------------------------
 pg_tle  | 1.0.1   | pgtle      | Trusted-Language Extensions for PostgreSQL
 plpgsql | 1.0     | pg_catalog | PL/pgSQL procedural language
```

11. Asigne el rol `pgtle_admin` al nombre de usuario principal que creó para la instancia de base de datos de RDS para PostgreSQL al configurarla. Si ha aceptado el valor predeterminado, es `postgres`.

```
labdb=> GRANT pgtle_admin TO postgres;
GRANT ROLE
```

Puede comprobar si se ha realizado la concesión con el metacomando `psql`, tal como se muestra en el siguiente ejemplo. Solo los roles `pgtle_admin` y `postgres` se muestran en el resultado. Para obtener más información, consulte Descripción del rol rds_superuser.

```
labdb=> \du
                           List of roles
    Role name    |           Attributes            |              Member of
-----------------+---------------------------------
+---------------------------------
pgtle_admin     | Cannot login                    | {}
```

```
postgres        | Create role, Create DB          +| {rds_superuser,pgtle_admin}
                | Password valid until infinity    |...
```

12. Cierre la sesión de `psql` con el metacomando `\q`.

```
\q
```

Para empezar a crear extensiones TLE, consulte Ejemplo: creación de una extensión de lenguaje de confianza mediante SQL.

AWS CLI

Puede evitar especificar el argumento `--region` al utilizar los comandos de la CLI al configurar su AWS CLI con su Región de AWS predeterminada. Para obtener más información, consulte Fundamentos de configuración en la Guía del usuario de AWS Command Line Interface.

Para configurar Extensiones de lenguaje de confianza

1. Use el comando modify-db-cluster-parameter-group de AWS CLI para añadir `pg_tle` al parámetro `shared_preload_libraries`.

```
aws rds modify-db-parameter-group \
   --db-parameter-group-name custom-param-group-name \
   --parameters
 "ParameterName=shared_preload_libraries,ParameterValue=pg_tle,ApplyMethod=pending-
reboot" \
   --region aws-region
```

2. Use el comando reboot-db-instance de AWS CLI para reiniciar la instancia de base de datos de RDS para PostgreSQL e inicialice la biblioteca de `pg_tle`.

```
aws rds reboot-db-instance \
    --db-instance-identifier your-instance \
    --region aws-region
```

3. Cuando la instancia esté disponible, puede verificar si `pg_tle` se ha inicializado. Use `psql` para conectarse a la instancia de base de datos de RDS for PostgreSQL y, a continuación, ejecute el siguiente comando.

```
SHOW shared_preload_libraries;
```

```
shared_preload_libraries
--------------------------
rdsutils,pg_tle
(1 row)
```

Con `pg_tle` inicializado, ahora ya puede crear la extensión.

```
CREATE EXTENSION pg_tle;
```

4. Asigne el rol `pgtle_admin` al nombre de usuario principal que creó para la instancia de base de datos de RDS para PostgreSQL al configurarla. Si ha aceptado el valor predeterminado, es `postgres`.

```
GRANT pgtle_admin TO postgres;
GRANT ROLE
```

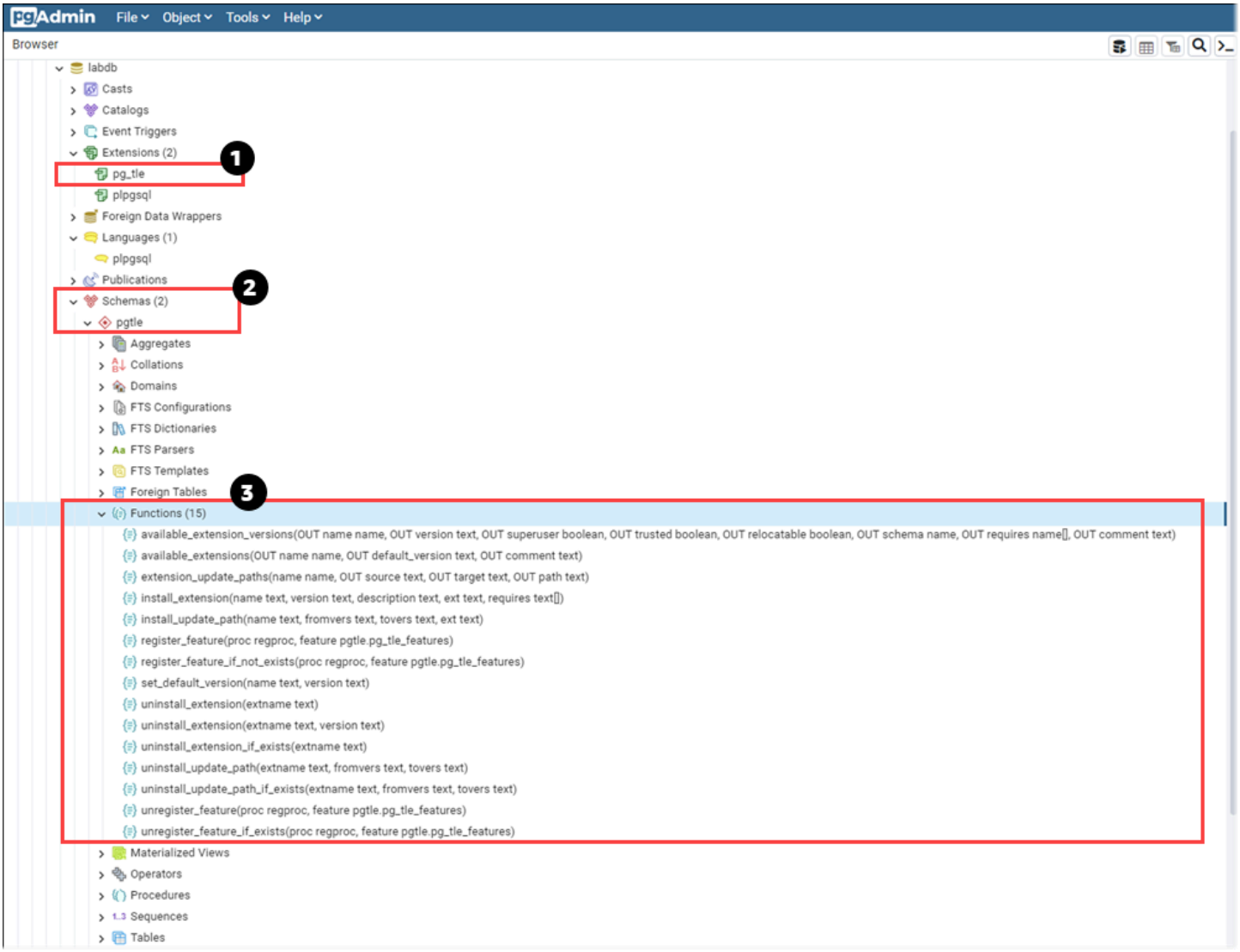
5. Cierre la sesión de `psql` de la siguiente manera.

```
labdb=> \q
```

Para empezar a crear extensiones TLE, consulte Ejemplo: creación de una extensión de lenguaje de confianza mediante SQL.

Información general de Extensiones de lenguaje de confianza para PostgreSQL

Extensiones de lenguaje de confianza para PostgreSQL es una extensión de PostgreSQL que se instala en la instancia de base de datos de RDS para PostgreSQL de la misma manera que se configuran otras extensiones de PostgreSQL. En la siguiente imagen de un ejemplo de base de datos de la herramienta de cliente pgAdmin, puede ver algunos de los componentes que componen la extensión `pg_tle`.



Puede ver los siguientes detalles.

1. El kit de desarrollo de Extensiones de lenguaje de confianza (TLE) está empaquetado como la extensión `pg_tle`. De este modo, `pg_tle` se añade a las extensiones disponibles para la base de datos en la que se instala.
2. TLE tiene su propio esquema: `pgtle`. Este esquema contiene funciones auxiliares (3) para instalar y administrar las extensiones que cree.
3. TLE proporciona más de una docena de funciones auxiliares para instalar, registrar y administrar las extensiones. Para obtener más información sobre estas funciones, consulte Referencia de funciones para Extensiones de lenguaje de confianza para PostgreSQL.

Otros componentes de la extensión `pg_tle` incluyen lo siguiente:

- El rol **`pgtle_admin`**: el rol `pgtle_admin` se crea al instalar la extensión `pg_tle`. Este rol es privilegiado y debe tratarse como tal. Le recomendamos encarecidamente que siga el principio de privilegio mínimo al conceder el rol `pgtle_admin` a los usuarios de la base de datos. En otras palabras, conceda el rol `pgtle_admin` solo a los usuarios de bases de datos que estén autorizados a crear, instalar y administrar nuevas extensiones TLE, como `postgres`.
- La tabla **`pgtle.feature_info`**: la tabla `pgtle.feature_info` es una tabla protegida que contiene información sobre los TLE, los enlaces, los procedimientos y las funciones personalizados almacenados que utilizan. Si tiene privilegios `pgtle_admin`, utilice las siguientes funciones de Extensiones de lenguaje de confianza para añadir y actualizar la información de la tabla.
  - pgtle.register_feature
  - pgtle.register_feature_if_not_exists
  - pgtle.unregister_feature
  - pgtle.unregister_feature_if_exists

Creación de extensiones TLE para RDS para PostgreSQL

Puede instalar cualquier extensión que cree con TLE en cualquier instancia de base de datos de RDS para PostgreSQL que tenga la extensión `pg_tle` instalada. La extensión `pg_tle` se limita a la base de datos PostgreSQL en la que está instalada. Las extensiones que cree con TLE están incluidas en la misma base de datos.

Utilice las distintas funciones de `pgtle` para instalar el código que conforma la extensión TLE. Todas las siguientes funciones de Extensiones de lenguaje de confianza requieren el rol `pgtle_admin`.

- pgtle.install_extension
- pgtle.install_update_path
- pgtle.register_feature
- pgtle.register_feature_if_not_exists
- pgtle.set_default_version
- pgtle.uninstall_extension(name)
- pgtle.uninstall_extension(nombre, versión)
- pgtle.uninstall_extension_if_exists
- pgtle.uninstall_update_path
- pgtle.uninstall_update_path_if_exists

- pgtle.unregister_feature
- pgtle.unregister_feature_if_exists

Ejemplo: creación de una extensión de lenguaje de confianza mediante SQL

El siguiente ejemplo muestra cómo crear una extensión TLE denominada `pg_distance` que contenga algunas funciones SQL para calcular distancias mediante diferentes fórmulas. En la lista, puede encontrar la función para calcular la distancia Manhattan y la función para calcular la distancia euclidiana. Para obtener más información sobre la diferencia entre estas fórmulas, consulte Geometría del taxista y Geometría euclidiana en la Wikipedia.

Puede utilizar este ejemplo en su instancia de base de datos de RDS para PostgreSQL si tiene la extensión `pg_tle` configurada como se detalla en Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL.

> **Note**
>
> Debe tener los privilegios del rol `pgtle_admin` para seguir este procedimiento.

Para crear la extensión TLE de ejemplo

En los pasos siguientes se utiliza un ejemplo de base de datos denominado `labdb`. Esta base de datos es propiedad del usuario `postgres` principal. El rol `postgres` también tiene los permisos del rol `pgtle_admin`.

1. Use `psql` para conectarse a la Instancia de base de datos RDS para PostgreSQL.

   ```
   psql --host=db-instance-123456789012.aws-region.rds.amazonaws.com
   --port=5432 --username=postgres --password --dbname=labdb
   ```

2. Cree una extensión TLE denominada `pg_distance` copiando el siguiente código y pegándolo en la consola de sesión de `psql`.

   ```
   SELECT pgtle.install_extension
   (
    'pg_distance',
    '0.1',
     'Distance functions for two points',
   $_pg_tle_$
   ```

```
    CREATE FUNCTION dist(x1 float8, y1 float8, x2 float8, y2 float8, norm int)
    RETURNS float8
    AS $$
      SELECT (abs(x2 - x1) ^ norm + abs(y2 - y1) ^ norm) ^ (1::float8 / norm);
    $$ LANGUAGE SQL;

    CREATE FUNCTION manhattan_dist(x1 float8, y1 float8, x2 float8, y2 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 1);
    $$ LANGUAGE SQL;

    CREATE FUNCTION euclidean_dist(x1 float8, y1 float8, x2 float8, y2 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 2);
    $$ LANGUAGE SQL;
$_pg_tle_$
);
```

Debería ver un resultado como el siguiente.

```
install_extension
---------------
 t
(1 row)
```

Los artefactos que componen la extensión `pg_distance` ahora ya están instalados en su base de datos. Estos artefactos incluyen el archivo de control y el código de la extensión, que son elementos que deben estar presentes para poder crear la extensión mediante el comando `CREATE EXTENSION`. En otras palabras, aún debe crear la extensión para que sus funciones estén disponibles para los usuarios de la base de datos.

3. Para crear la extensión, utilice el comando `CREATE EXTENSION` como lo haría con cualquier otra extensión. Al igual que con otras extensiones, el usuario de la base de datos debe tener los permisos `CREATE` en la base de datos.

```
CREATE EXTENSION pg_distance;
```

4. Para probar la extensión TLE `pg_distance`, puede utilizarla para calcular la distancia Manhattan entre cuatro puntos.

```
labdb=> SELECT manhattan_dist(1, 1, 5, 5);
8
```

Para calcular la distancia euclidiana entre el mismo conjunto de puntos, puede utilizar lo siguiente.

```
labdb=> SELECT euclidean_dist(1, 1, 5, 5);
5.656854249492381
```

La extensión `pg_distance` carga las funciones de la base de datos y las pone a disposición de cualquier usuario con permisos en la base de datos.

Modificación de su extensión TLE

Para mejorar el rendimiento de las consultas para las funciones incluidas en esta extensión TLE, añada los dos atributos de PostgreSQL siguientes a sus especificaciones.

- `IMMUTABLE`: el atributo `IMMUTABLE` garantiza que el optimizador de consultas pueda utilizar optimizaciones para mejorar los tiempos de respuesta de las consultas. Para obtener más información, consulte Function Volatility Categories (Categorías de volatilidad de función) en la documentación de PostgreSQL.
- `PARALLEL SAFE`: el atributo `PARALLEL SAFE` es otro atributo que permite a PostgreSQL ejecutar la función en modo paralelo. Para obtener más información, consulte CREATE FUNCTION en la documentación de PostgreSQL.

En el siguiente ejemplo, puede ver cómo se usa la función `pgtle.install_update_path` para agregar estos atributos a cada función a fin de crear una versión `0.2` de la extensión TLE `pg_distance`. Para obtener más información acerca de esta función, consulte pgtle.install_update_path. Debe tener el rol `pgtle_admin` para realizar esta tarea.

Para actualizar una extensión TLE existente y especificar la versión predeterminada

1. Conecte con la instancia de base de datos de RDS para PostgreSQL con `psql` u otra herramienta de cliente como pgAdmin.

```
psql --host=db-instance-123456789012.aws-region.rds.amazonaws.com
```

```
--port=5432 --username=postgres --password --dbname=labdb
```

2. Modifique una extensión TLE existente copiando el siguiente código y pegándolo en la consola de sesión de `psql`.

```
SELECT pgtle.install_update_path
(
 'pg_distance',
 '0.1',
 '0.2',
$_pg_tle_$
    CREATE OR REPLACE FUNCTION dist(x1 float8, y1 float8, x2 float8, y2 float8,
 norm int)
    RETURNS float8
    AS $$
      SELECT (abs(x2 - x1) ^ norm + abs(y2 - y1) ^ norm) ^ (1::float8 / norm);
    $$ LANGUAGE SQL IMMUTABLE PARALLEL SAFE;

    CREATE OR REPLACE FUNCTION manhattan_dist(x1 float8, y1 float8, x2 float8, y2
 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 1);
    $$ LANGUAGE SQL IMMUTABLE PARALLEL SAFE;

    CREATE OR REPLACE FUNCTION euclidean_dist(x1 float8, y1 float8, x2 float8, y2
 float8)
    RETURNS float8
    AS $$
      SELECT dist(x1, y1, x2, y2, 2);
    $$ LANGUAGE SQL IMMUTABLE PARALLEL SAFE;
$_pg_tle_$
);
```

Verá una respuesta similar a la siguiente.

```
install_update_path
--------------------
 t
(1 row)
```

Puede hacer que esta versión de la extensión sea la versión predeterminada para que los usuarios de la base de datos no tengan que especificar una versión al crear o actualizar la extensión en su base de datos.

3. Para especificar que la versión modificada (versión 0.2) de la extensión TLE es la versión predeterminada, utilice la función `pgtle.set_default_version` tal como se muestra en el siguiente ejemplo.

```
SELECT pgtle.set_default_version('pg_distance', '0.2');
```

Para obtener más información acerca de esta función, consulte pgtle.set_default_version.

4. Con el código en su lugar, puede actualizar la extensión TLE instalada de la forma habitual, mediante el comando `ALTER EXTENSION ... UPDATE`, tal como se muestra aquí:

```
ALTER EXTENSION pg_distance UPDATE;
```

Eliminar las extensiones TLE de una base de datos

Puede eliminar sus extensiones TLE mediante el comando `DROP EXTENSION` de la misma manera que lo hace con otras extensiones de PostgreSQL. Al eliminar la extensión, no se eliminan los archivos de instalación que la componen, lo que permite a los usuarios volver a crearla. Para eliminar la extensión y sus archivos de instalación, realice el siguiente proceso de dos pasos.

Para eliminar la extensión TLE y eliminar sus archivos de instalación

1. Use `psql` u otra herramienta de cliente para conectarse a la instancia de base de datos de RDS para PostgreSQL.

```
psql --host=.111122223333.aws-region.rds.amazonaws.com --port=5432 --
username=postgres --password --dbname=dbname
```

2. Elimine la extensión tal como haría con cualquier extensión de PostgreSQL.

```
DROP EXTENSION your-TLE-extension
```

Por ejemplo, si crea la extensión `pg_distance` tal como se indica en Ejemplo: creación de una extensión de lenguaje de confianza mediante SQL, puede eliminarla de la siguiente manera.

```
DROP EXTENSION pg_distance;
```

Verá un resultado que confirma que se ha eliminado la extensión, de la siguiente manera.

```
DROP EXTENSION
```

En este punto, la extensión ya no está activa en la base de datos. Sin embargo, sus archivos de instalación y su archivo de control siguen disponibles en la base de datos, por lo que los usuarios de la base de datos pueden volver a crear la extensión si lo desean.

- Si desea dejar los archivos de extensión intactos para que los usuarios de la base de datos puedan crear su extensión TLE, puede detenerse aquí.
- Si desea eliminar todos los archivos que conforman la extensión, proceda con el siguiente paso.

3. Para eliminar todos los archivos de instalación de la extensión, utilice la función `pgtle.uninstall_extension`. Esta función elimina todos los archivos de código y control de la extensión.

```
SELECT pgtle.uninstall_extension('your-tle-extension-name');
```

Por ejemplo, para eliminar todos los archivos de instalación `pg_distance`, utilice el siguiente comando.

```
SELECT pgtle.uninstall_extension('pg_distance');
 uninstall_extension
---------------------
 t
(1 row)
```

Desinstalación de Extensiones de lenguaje de confianza para PostgreSQL

Si ya no quiere crear sus propias extensiones TLE con TLE, puede eliminar la extensión `pg_tle` y eliminar todos los artefactos. Esta acción incluye eliminar cualquier extensión TLE de la base de datos y el esquema `pgtle`.

Para eliminar la extensión **pg_tle** y su esquema de una base de datos

1. Use psql u otra herramienta de cliente para conectarse a la instancia de base de datos de RDS para PostgreSQL.

   ```
   psql --host=.111122223333.aws-region.rds.amazonaws.com --port=5432 --
   username=postgres --password --dbname=dbname
   ```

2. Elimine la extensión pg_tle de la base de datos. Si la base de datos está ejecutando sus propias extensiones TLE, también debe eliminar esas extensiones. Para ello, puede utilizar la palabra clave CASCADE, tal como se muestra a continuación.

   ```
   DROP EXTENSION pg_tle CASCADE;
   ```

   Si la extensión pg_tle no sigue activa en la base de datos, no es necesario que utilice la palabra clave CASCADE.

3. Elimine el esquema pgtle. Esta acción elimina todas las funciones de administración de la base de datos.

   ```
   DROP SCHEMA pgtle CASCADE;
   ```

   El comando devuelve lo siguiente cuando se completa el proceso.

   ```
   DROP SCHEMA
   ```

   Se eliminan la extensión pg_tle, su esquema y sus funciones, así como todos los artefactos. Para crear nuevas extensiones con TLE, vuelva a realizar el proceso de configuración. Para obtener más información, consulte Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL.

Uso de enlaces de PostgreSQL con sus extensiones TLE

Un enlace es un mecanismo de devolución de llamada disponible en PostgreSQL que permite a los desarrolladores llamar a funciones personalizadas u otras rutinas durante las operaciones normales de la base de datos. El kit de desarrollo de TLE admite enlaces de PostgreSQL para que pueda integrar funciones personalizadas con el comportamiento de PostgreSQL en el tiempo de ejecución. Por ejemplo, puede utilizar un enlace para asociar el proceso de autenticación a su propio código

personalizado o para modificar el proceso de planificación y ejecución de consultas según sus necesidades específicas.

Sus extensiones TLE pueden utilizar enlaces. Si un enlace tiene un alcance global, se aplica a todas las bases de datos. Por lo tanto, si su extensión TLE usa un enlace global, debe crear su extensión TLE en todas las bases de datos a las que puedan acceder sus usuarios.

Cuando usa la extensión `pg_tle` para crear sus propias Extensiones de lenguaje de confianza, puede usar los enlaces disponibles de una API de SQL para crear las funciones de su extensión. Debe registrar cualquier enlace con `pg_tle`. Para algunos enlaces, es posible que también tenga que establecer varios parámetros de configuración. Por ejemplo, el enlace de retención `passcode` se puede configurar como activado, desactivado u obligatorio. Para obtener más información sobre los requisitos específicos de los enlaces `pg_tle` disponibles, consulte Referencia de enlaces para Extensiones de lenguaje de confianza para PostgreSQL.

Ejemplo: Crear una extensión que utilice un enlace de PostgreSQL

El ejemplo descrito en esta sección utiliza un enlace de PostgreSQL para comprobar la contraseña proporcionada durante operaciones SQL específicas e impide que los usuarios de la base de datos establezcan sus contraseñas iguales a las que figuran en la tabla `password_check.bad_passwords`. La tabla contiene las diez opciones de contraseñas más utilizadas, pero fáciles de descifrar.

Para configurar este ejemplo en su instancia de base de datos de RDS para PostgreSQL, ya tiene que tener Extensiones de lenguaje de confianza instalado. Para obtener más información, consulte Configuración de Extensiones de lenguaje de confianza en su instancia de base de datos de RDS para PostgreSQL.

Para configurar el ejemplo del enlace de verificación de contraseñas

1. Use `psql` para conectarse a la Instancia de base de datos RDS para PostgreSQL.

```
psql --host=db-instance-123456789012.aws-region.rds.amazonaws.com
--port=5432 --username=postgres --password --dbname=labdb
```

2. Copie el código de la Lista de códigos del enlace password_check y péguelo en su base de datos.

```
SELECT pgtle.install_extension (
  'my_password_check_rules',
```

```
  '1.0',
  'Do not let users use the 10 most commonly used passwords',
$_pgtle_$
  CREATE SCHEMA password_check;
  REVOKE ALL ON SCHEMA password_check FROM PUBLIC;
  GRANT USAGE ON SCHEMA password_check TO PUBLIC;

  CREATE TABLE password_check.bad_passwords (plaintext) AS
  VALUES
    ('123456'),
    ('password'),
    ('12345678'),
    ('qwerty'),
    ('123456789'),
    ('12345'),
    ('1234'),
    ('111111'),
    ('1234567'),
    ('dragon');
  CREATE UNIQUE INDEX ON password_check.bad_passwords (plaintext);

  CREATE FUNCTION password_check.passcheck_hook(username text, password text,
 password_type pgtle.password_types, valid_until timestamptz, valid_null boolean)
  RETURNS void AS $$
    DECLARE
      invalid bool := false;
    BEGIN
      IF password_type = 'PASSWORD_TYPE_MD5' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE ('md5' || md5(bp.plaintext || username)) = password
        ) INTO invalid;
        IF invalid THEN
          RAISE EXCEPTION 'Cannot use passwords from the common password
 dictionary';
        END IF;
      ELSIF password_type = 'PASSWORD_TYPE_PLAINTEXT' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE bp.plaintext = password
        ) INTO invalid;
        IF invalid THEN
```

```
          RAISE EXCEPTION 'Cannot use passwords from the common password
 dictionary';
        END IF;
      END IF;
    END
  $$ LANGUAGE plpgsql SECURITY DEFINER;

  GRANT EXECUTE ON FUNCTION password_check.passcheck_hook TO PUBLIC;

  SELECT pgtle.register_feature('password_check.passcheck_hook', 'passcheck');
$_pgtle_$
);
```

Cuando la extensión se haya cargado en la base de datos, verá un resultado como el siguiente.

```
 install_extension
-------------------
 t
(1 row)
```

3. Mientras siga conectado a la base de datos, ya podrá crear la extensión.

```
CREATE EXTENSION my_password_check_rules;
```

4. Puede confirmar que la extensión se ha creado en la base de datos mediante el siguiente metacomando `psql`.

```
\dx
                       List of installed extensions
          Name           | Version |   Schema   |
 Description
-------------------------+---------+------------
+-------------------------------------------------------------
 my_password_check_rules | 1.0     | public     | Prevent use of any of the top-ten
 most common bad passwords
 pg_tle                  | 1.0.1   | pgtle      | Trusted-Language Extensions for
 PostgreSQL
 plpgsql                 | 1.0     | pg_catalog | PL/pgSQL procedural language
(3 rows)
```

5. Abra otra sesión de terminal para trabajar con la AWS CLI. Debe modificar su grupo de parámetros de base de datos personalizado para activar el enlace de verificación de

contraseñas. Para ello, utilice el comando modify-db-parameter-group de la CLI tal como se muestra en el siguiente ejemplo.

```
aws rds modify-db-parameter-group \
    --region aws-region \
    --db-parameter-group-name your-custom-parameter-group \
    --parameters
 "ParameterName=pgtle.enable_password_check,ParameterValue=on,ApplyMethod=immediate"
```

Cuando el parámetro se haya activado correctamente, verá un resultado como el siguiente.

```
(
    "DBParameterGroupName": "docs-lab-parameters-for-tle"
}
```

Puede que el cambio en la configuración del grupo de parámetros tarde unos minutos en aplicarse. Sin embargo, este parámetro es dinámico, por lo que no es necesario reiniciar la instancia de base de datos de RDS para PostgreSQL para que la configuración surta efecto.

6. Abra la sesión `psql` y consulte la base de datos para comprobar que el enlace password_check esté activado.

```
labdb=> SHOW pgtle.enable_password_check;
pgtle.enable_password_check
----------------------------
on
(1 row)
```

El enlace password-check ahora está activo. Puede probarlo creando un rol nuevo y utilizando una de las contraseñas incorrectas, tal como se muestra en el siguiente ejemplo.

```
CREATE ROLE test_role PASSWORD 'password';
ERROR:  Cannot use passwords from the common password dictionary
CONTEXT:  PL/pgSQL function
 password_check.passcheck_hook(text,text,pgtle.password_types,timestamp with time
 zone,boolean) line 21 at RAISE
SQL statement "SELECT password_check.passcheck_hook(
    $1::pg_catalog.text,
    $2::pg_catalog.text,
    $3::pgtle.password_types,
```

```
    $4::pg_catalog.timestamptz,
    $5::pg_catalog.bool)"
```

El resultado se ha modificado para que se pueda leer.

El siguiente ejemplo muestra que el comportamiento `\password` del metacomando interactivo `pgsql` también se ve afectado por el enlace password_check.

```
postgres=> SET password_encryption TO 'md5';
SET
postgres=> \password
Enter new password for user "postgres":*****
Enter it again:*****
ERROR:  Cannot use passwords from the common password dictionary
CONTEXT:  PL/pgSQL function
 password_check.passcheck_hook(text,text,pgtle.password_types,timestamp with time
 zone,boolean) line 12 at RAISE
SQL statement "SELECT password_check.passcheck_hook($1::pg_catalog.text,
 $2::pg_catalog.text, $3::pgtle.password_types, $4::pg_catalog.timestamptz,
 $5::pg_catalog.bool)"
```

Puede eliminar esta extensión TLE y desinstalar sus archivos de código fuente si lo desea. Para obtener más información, consulte Eliminar las extensiones TLE de una base de datos.

Lista de códigos del enlace password_check

El código de ejemplo que se muestra aquí define la especificación de la extensión TLE `my_password_check_rules`. Al copiar este código y pegarlo en la base de datos, el código de la extensión `my_password_check_rules` se carga en la base de datos y el enlace `password_check` queda registrado para que lo utilice la extensión.

```
SELECT pgtle.install_extension (
  'my_password_check_rules',
  '1.0',
  'Do not let users use the 10 most commonly used passwords',
$_pgtle_$
  CREATE SCHEMA password_check;
  REVOKE ALL ON SCHEMA password_check FROM PUBLIC;
  GRANT USAGE ON SCHEMA password_check TO PUBLIC;

  CREATE TABLE password_check.bad_passwords (plaintext) AS
  VALUES
```

```
    ('123456'),
    ('password'),
    ('12345678'),
    ('qwerty'),
    ('123456789'),
    ('12345'),
    ('1234'),
    ('111111'),
    ('1234567'),
    ('dragon');
  CREATE UNIQUE INDEX ON password_check.bad_passwords (plaintext);

  CREATE FUNCTION password_check.passcheck_hook(username text, password text,
 password_type pgtle.password_types, valid_until timestamptz, valid_null boolean)
  RETURNS void AS $$
    DECLARE
      invalid bool := false;
    BEGIN
      IF password_type = 'PASSWORD_TYPE_MD5' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE ('md5' || md5(bp.plaintext || username)) = password
        ) INTO invalid;
        IF invalid THEN
          RAISE EXCEPTION 'Cannot use passwords from the common password dictionary';
        END IF;
      ELSIF password_type = 'PASSWORD_TYPE_PLAINTEXT' THEN
        SELECT EXISTS(
          SELECT 1
          FROM password_check.bad_passwords bp
          WHERE bp.plaintext = password
        ) INTO invalid;
        IF invalid THEN
          RAISE EXCEPTION 'Cannot use passwords from the common password dictionary';
        END IF;
      END IF;
    END
  $$ LANGUAGE plpgsql SECURITY DEFINER;

  GRANT EXECUTE ON FUNCTION password_check.passcheck_hook TO PUBLIC;

  SELECT pgtle.register_feature('password_check.passcheck_hook', 'passcheck');
$_pgtle_$
```

```
);
```

Uso de tipos de datos personalizados en TLE

PostgreSQL admite comandos para registrar nuevos tipos base (también conocidos como tipos escalares) para gestionar con eficiencia estructuras de datos complejas en su base de datos. Un tipo base le permite personalizar la forma en que se almacenan los datos internamente y cómo convertirlos a una representación textual externa y desde ella. Estos tipos de datos personalizados son útiles a la hora de ampliar PostgreSQL para que admita dominios funcionales en los que un tipo integrado, como un número o un texto, no puede proporcionar una semántica de búsqueda suficiente.

RDS para PostgreSQL le permite crear tipos de datos personalizados en su extensión de lenguaje de confianza y definir funciones que admitan operaciones de SQL e indexación para estos nuevos tipos de datos. Los tipos de datos personalizados están disponibles para las siguientes versiones:

- RDS para PostgreSQL, versión 15.4 y versiones 15 posteriores
- RDS para PostgreSQL, versión 14.9 y versiones 14 posteriores
- RDS para PostgreSQL, versión 13.12 y versiones 13 posteriores

Para obtener más información, consulte Trusted Language Base types.

Referencia de funciones para Extensiones de lenguaje de confianza para PostgreSQL

Consulte la siguiente documentación de referencia sobre las funciones disponibles en Extensiones de lengua de confianza para PostgreSQL. Utilice estas funciones para instalar, registrar, actualizar y administrar sus extensiones TLE, es decir, las extensiones de PostgreSQL que desarrolla con el kit de desarrollo de Extensiones de lenguaje de confianza.

Funciones

- pgtle.available_extensions
- pgtle.available_extension_versions
- pgtle.extension_update_paths
- pgtle.install_extension
- pgtle.install_update_path

- pgtle.register_feature
- pgtle.register_feature_if_not_exists
- pgtle.set_default_version
- pgtle.uninstall_extension(name)
- pgtle.uninstall_extension(nombre, versión)
- pgtle.uninstall_extension_if_exists
- pgtle.uninstall_update_path
- pgtle.uninstall_update_path_if_exists
- pgtle.unregister_feature
- pgtle.unregister_feature_if_exists

pgtle.available_extensions

La función `pgtle.available_extensions` es una función de devolución de conjuntos. Devuelve todas las extensiones TLE disponibles en la base de datos. Cada fila devuelta contiene información sobre una sola extensión TLE.

Prototipo de función

```
pgtle.available_extensions()
```

Rol

Ninguna.

Argumentos

Ninguna.

Salida

- `name`: nombre de la extensión TLE.
- `default_version`: versión de la extensión TLE que se utilizará cuando se llame a `CREATE EXTENSION` sin especificar una versión.
- `description`: descripción más detallada acerca de la extensión TLE.

Ejemplo de uso

```
SELECT * FROM pgtle.available_extensions();
```

pgtle.available_extension_versions

La función `available_extension_versions` es una función de devolución de conjuntos. Esta función devuelve una lista de todas las extensiones de TLE disponibles y sus versiones. Cada fila contiene información sobre una versión específica de la extensión TLE dada, incluso si requiere un rol específico.

Prototipo de función

```
pgtle.available_extension_versions()
```

Rol

Ninguna.

Argumentos

Ninguna.

Salida

- `name`: nombre de la extensión TLE.
- `version`: versión de la extensión TLE.
- `superuser`: este valor es siempre `false` para sus extensiones TLE. Los permisos necesarios para crear la extensión TLE o actualizarla son los mismos que para crear otros objetos en la base de datos dada.
- `trusted`: este valor es siempre `false` para una extensión TLE.
- `relocatable`: este valor es siempre `false` para una extensión TLE.
- `schema`: especifica el nombre del esquema en el que está instalada la extensión TLE.
- `requires`: matriz que contiene los nombres de otras extensiones que necesita esta extensión TLE.
- `description`: descripción detallada de la extensión TLE.

Para obtener más información acerca de los valores de salida, vea Packaging Related Objects into an Extension > Extension Files (Empaquetar objetos relacionados en una extensión > Archivos de extensión) en la documentación de PostgreSQL.

Ejemplo de uso

```
SELECT * FROM pgtle.available_extension_versions();
```

pgtle.extension_update_paths

La función `extension_update_paths` es una función de devolución de conjuntos. Devuelve una lista de todas las rutas de actualización posibles para una extensión TLE. Cada fila incluye las actualizaciones a un nivel superior o inferior disponibles para esa extensión TLE.

Prototipo de función

```
pgtle.extension_update_paths(name)
```

Rol

Ninguna.

Argumentos

`name`: nombre de la extensión TLE desde la que se obtienen las rutas de actualización.

Salida

- `source`: versión de origen de una actualización.
- `target`: versión de destino de una actualización.
- `path`: ruta de actualización utilizada para actualizar una extensión TLE de una versión `source` a otra `target`, por ejemplo, `0.1--0.2`.

Ejemplo de uso

```
SELECT * FROM pgtle.extension_update_paths('your-TLE');
```

pgtle.install_extension

La función `install_extension` le permite instalar los artefactos que componen la extensión TLE en la base de datos, después de lo cual se puede crear mediante el comando `CREATE EXTENSION`.

Prototipo de función

```
pgtle.install_extension(name text, version text, description text, ext text, requires
 text[] DEFAULT NULL::text[])
```

Rol

Ninguna.

Argumentos

- `name`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.
- `version`: versión de la extensión TLE.
- `description`: descripción detallada acerca de la extensión TLE. Esta descripción se muestra en el campo `comment` de `pgtle.available_extensions()`.
- `ext`: contenido de la extensión TLE. Este valor contiene objetos como funciones.
- `requires`: parámetro opcional que especifica las dependencias de esta extensión TLE. La extensión `pg_tle` se añade automáticamente como una dependencia.

Muchos de estos argumentos son los mismos que se incluyen en un archivo de control de extensiones para instalar una extensión de PostgreSQL en el sistema de archivos de una instancia de PostgreSQL. Para obtener más información acerca de las extensiones de PostgreSQL, vea Extension Files (Archivos de extensión) en Packaging Related Objects into an Extension (Empaquetar objetos relacionados en una extensión) en la documentación de PostgreSQL.

Salida

Esta función devuelve `OK` en caso de éxito y `NULL` en caso de error.

- `OK`: la extensión TLE se ha instalado correctamente en la base de datos.
- `NULL`: la extensión TLE no se ha instalado correctamente en la base de datos.

Ejemplo de uso

```
SELECT pgtle.install_extension(
 'pg_tle_test',
 '0.1',
 'My first pg_tle extension',
$_pgtle_$
  CREATE FUNCTION my_test()
  RETURNS INT
  AS $$
    SELECT 42;
  $$ LANGUAGE SQL IMMUTABLE;
$_pgtle_$
);
```

pgtle.install_update_path

La función `install_update_path` proporciona una ruta de actualización entre dos versiones diferentes de una extensión TLE. Esta función permite a los usuarios de la extensión TLE actualizar su versión mediante la sintaxis `ALTER EXTENSION ... UPDATE`.

Prototipo de función

```
pgtle.install_update_path(name text, fromvers text, tovers text, ext text)
```

Rol

`pgtle_admin`

Argumentos

- `name`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.
- `fromvers`: versión de origen de la extensión TLE utilizada para la actualización.
- `tovers`: versión de destino de la extensión TLE utilizada para la actualización.
- `ext`: contenido de la actualización. Este valor contiene objetos como funciones.

Salida

Ninguna.

Ejemplo de uso

```
SELECT pgtle.install_update_path('pg_tle_test', '0.1', '0.2',
  $_pgtle_$
    CREATE OR REPLACE FUNCTION my_test()
    RETURNS INT
    AS $$
      SELECT 21;
    $$ LANGUAGE SQL IMMUTABLE;
  $_pgtle_$
);
```

pgtle.register_feature

La función `register_feature` añade la característica interna de PostgreSQL especificada a la tabla `pgtle.feature_info`. Los enlaces de PostgreSQL son un ejemplo de una característica interna de PostgreSQL. El kit de desarrollo de Extensiones de lenguaje de confianza admite el uso de enlaces de PostgreSQL. Actualmente, esta función admite la siguiente característica.

- `passcheck`: registra el enlace de comprobación de contraseñas con su procedimiento o función que personaliza el comportamiento de comprobación de contraseñas de PostgreSQL.

Prototipo de función

```
pgtle.register_feature(proc regproc, feature pg_tle_feature)
```

Rol

`pgtle_admin`

Argumentos

- `proc`: nombre de un procedimiento o función almacenados que se utilizarán en la característica.
- `feature`: nombre de una característica `pg_tle` (como `passcheck`) para registrarla con la función.

Salida

Ninguna.

Ejemplo de uso

```
SELECT pgtle.register_feature('pw_hook', 'passcheck');
```

pgtle.register_feature_if_not_exists

La función `pgtle.register_feature_if_not_exists` añade la función de PostgreSQL especificada a la tabla `pgtle.feature_info` e identifica la extensión TLE u otro procedimiento o función que utilice la característica. Para obtener más información sobre los enlaces y las extensiones de lenguaje de confianza, consulte Uso de enlaces de PostgreSQL con sus extensiones TLE.

Prototipo de función

```
pgtle.register_feature_if_not_exists(proc regproc, feature pg_tle_feature)
```

Rol

`pgtle_admin`

Argumentos

- `proc`: nombre de una función procedimiento almacenado que contiene la lógica (código) que se utilizará como una característica de la extensión TLE. Por ejemplo, el código `pw_hook`.
- `feature`: nombre de una la característica de PostgreSQL para registrarla para la función TLE. Actualmente, la única característica disponible es el enlace `passcheck`. Para obtener más información, consulte Enlace de comprobación de contraseñas (passcheck).

Salida

Devuelve `true` después de registrar la característica para la extensión especificada. Devuelve `false` si la característica ya está registrada.

Ejemplo de uso

```
SELECT pgtle.register_feature_if_not_exists('pw_hook', 'passcheck');
```

pgtle.set_default_version

La función `set_default_version` le permite especificar un `default_version` para su extensión TLE. Puede utilizar esta función para definir una ruta de actualización y designar la versión como la predeterminada para la extensión TLE. Cuando los usuarios de la base de datos especifican la extensión TLE en los comandos `CREATE EXTENSION` y `ALTER EXTENSION ... UPDATE`, esa versión de la extensión TLE se crea en la base de datos para ese usuario.

Esta función devuelve `true` en caso de realizarse correctamente. Si la extensión TLE especificada en el argumento `name` no existe, la función devuelve un error. Del mismo modo, si el `version` de la extensión TLE no existe, devuelve un error.

Prototipo de función

```
pgtle.set_default_version(name text, version text)
```

Rol

`pgtle_admin`

Argumentos

- `name`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.
- `version`: versión de la extensión TLE para establecer la predeterminada.

Salida

- `true`: cuando la configuración de la versión predeterminada se realiza correctamente, la función devuelve `true`.
- `ERROR`: devuelve un mensaje de error si no existe una extensión TLE con el nombre o la versión especificados.

Ejemplo de uso

```
SELECT * FROM pgtle.set_default_version('my-extension', '1.1');
```

pgtle.uninstall_extension(name)

La función `uninstall_extension` elimina todas las versiones de una extensión TLE de una base de datos. Esta función evita futuras llamadas de `CREATE EXTENSION` para evitar instalar la extensión TLE. Si la extensión TLE no existe en la base de datos, se genera un error.

La función `uninstall_extension` no elimina una extensión TLE que esté activa actualmente en la base de datos. Para eliminar una extensión TLE que está activa actualmente, debes llamar explícitamente a `DROP EXTENSION` para eliminarla.

Prototipo de función

```
pgtle.uninstall_extension(extname text)
```

Rol

`pgtle_admin`

Argumentos

- `extname`: nombre de la extensión TLE que se va a desinstalar. Este nombre es el mismo que se usó con `CREATE EXTENSION` para cargar la extensión TLE para usarla en una base de datos determinada.

Salida

Ninguna.

Ejemplo de uso

```
SELECT * FROM pgtle.uninstall_extension('pg_tle_test');
```

pgtle.uninstall_extension(nombre, versión)

La función `uninstall_extension(name, version)` elimina la versión especificada de la extensión TLE de la base de datos. Esta función impide a `CREATE EXTENSION` y `ALTER EXTENSION` instalar o actualizar una extensión TLE a la versión especificada. Esta función también elimina todas las rutas de actualización posibles de la extensión TLE especificada. Esta función no desinstala la extensión TLE si actualmente está activa en la base de datos. Debe llamar

explícitamente a `DROP EXTENSION` para eliminar la extensión TLE. Para desinstalar todas las versiones de una extensión TLE, consulte pgtle.uninstall_extension(name).

Prototipo de función

```
pgtle.uninstall_extension(extname text, version text)
```

Rol

`pgtle_admin`

Argumentos

- `extname`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.
- `version`: versión de la extensión TLE que se va a desinstalar de la base de datos.

Salida

Ninguna.

Ejemplo de uso

```
SELECT * FROM pgtle.uninstall_extension('pg_tle_test', '0.2');
```

pgtle.uninstall_extension_if_exists

La función `uninstall_extension_if_exists` elimina todas las versiones de una extensión TLE de una base de datos determinada. Si la extensión TLE no existe, la función la devuelve en silencio (no se genera ningún mensaje de error). Si la extensión especificada está activa actualmente en una base de datos, esta función no la elimina. Debe llamar explícitamente a `DROP EXTENSION` para eliminar la extensión TLE antes de utilizar esta función para desinstalar sus artefactos.

Prototipo de función

```
pgtle.uninstall_extension_if_exists(extname text)
```

Rol

`pgtle_admin`

Argumentos

- `extname`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.

Salida

La función `uninstall_extension_if_exists` de vuelve `true` después de desinstalar la extensión especificada. Si la extensión especificada no existe, la función devuelve `false`.

- `true`: devuelve `true` después de desinstalar la extensión TLE.
- `false`: devuelve `false` cuando la extensión TLE no existe en la base de datos.

Ejemplo de uso

```
SELECT * FROM pgtle.uninstall_extension_if_exists('pg_tle_test');
```

pgtle.uninstall_update_path

La función `uninstall_update_path` elimina la ruta de actualización específica de una extensión TLE. Esto impide que `ALTER EXTENSION ... UPDATE TO` se utilice como ruta de actualización.

Si una de las versiones de esta ruta de actualización utiliza actualmente la extensión TLE, permanecerá en la base de datos.

Si la ruta de actualización especificada no existe, esta función genera un error.

Prototipo de función

```
pgtle.uninstall_update_path(extname text, fromvers text, tovers text)
```

Rol

`pgtle_admin`

Argumentos

- `extname`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.

- `fromvers`: versión de origen de la extensión TLE utilizada en la ruta de actualización.
- `tovers`: versión de destino de la extensión TLE utilizada en la ruta de actualización.

Salida

Ninguna.

Ejemplo de uso

```
SELECT * FROM pgtle.uninstall_update_path('pg_tle_test', '0.1', '0.2');
```

pgtle.uninstall_update_path_if_exists

La función `uninstall_update_path_if_exists` es similar a `uninstall_update_path` en el sentido de que elimina la ruta de actualización especificada de una extensión TLE. Sin embargo, si la ruta de actualización no existe, esta función no generará ningún mensaje de error. En su lugar, la función devuelve `false`.

Prototipo de función

```
pgtle.uninstall_update_path_if_exists(extname text, fromvers text, tovers text)
```

Rol

`pgtle_admin`

Argumentos

- `extname`: nombre de la extensión TLE. Este valor se utiliza cuando se llama a `CREATE EXTENSION`.
- `fromvers`: versión de origen de la extensión TLE utilizada en la ruta de actualización.
- `tovers`: versión de destino de la extensión TLE utilizada en la ruta de actualización.

Salida

- `true`: la función ha actualizado correctamente la ruta de la extensión TLE.
- `false`: la función no ha podido actualizar la ruta de la extensión TLE.

Ejemplo de uso

```
SELECT * FROM pgtle.uninstall_update_path_if_exists('pg_tle_test', '0.1', '0.2');
```

pgtle.unregister_feature

La función `unregister_feature` proporciona una forma de eliminar las funciones que se han registrado para usar características `pg_tle`, como los enlaces. Para obtener información sobre el registro de una característica, consulte pgtle.register_feature.

Prototipo de función

```
pgtle.unregister_feature(proc regproc, feature pg_tle_features)
```

Rol

`pgtle_admin`

Argumentos

- `proc`: nombre de una función almacenada para registrarse en una característica de `pg_tle`.
- `feature`: nombre de la característica `pg_tle` para registrarla con la función. Por ejemplo, `passcheck` es una característica que se puede registrar para que la utilicen las extensiones de lenguaje de confianza que desarrolle. Para obtener más información, consulte Enlace de comprobación de contraseñas (passcheck).

Salida

Ninguna.

Ejemplo de uso

```
SELECT * FROM pgtle.unregister_feature('pw_hook', 'passcheck');
```

pgtle.unregister_feature_if_exists

La función `unregister_feature` proporciona una forma de eliminar las funciones que se registraron para usar funciones `pg_tle`, como los enlaces. Para obtener más información, consulte Uso de enlaces de PostgreSQL con sus extensiones TLE. Devuelve `true` después de anular satisfactoriamente el registro de la función. Devuelve `false` si la función no se ha registrado.

Para obtener información sobre el registro de funciones `pg_tle` para sus extensiones TLE, consulte pgtle.register_feature.

Prototipo de función

```
pgtle.unregister_feature_if_exists('proc regproc', 'feature pg_tle_features')
```

Rol

`pgtle_admin`

Argumentos

- `proc`: nombre de la función almacenada que se registró para incluir una función `pg_tle`.
- `feature`: nombre de la función `pg_tle` que se registró con la extensión de lenguaje de confianza.

Salida

Devuelve `true` o `false`, de la siguiente manera.

- `true`: la función ha cancelado satisfactoriamente el registro de la función de la extensión.
- `false`: la función no ha podido anular el registro de la función de la extensión TLE.

Ejemplo de uso

```
SELECT * FROM pgtle.unregister_feature_if_exists('pw_hook', 'passcheck');
```

Referencia de enlaces para Extensiones de lenguaje de confianza para PostgreSQL

Extensiones de lenguaje de confianza para PostgreSQL admite los enlaces de PostgreSQL. Un enlace es un mecanismo interno de devolución de llamada disponible para los desarrolladores para ampliar la funcionalidad principal de PostgreSQL. Mediante el uso de enlaces, los desarrolladores pueden implementar sus propias funciones o procedimientos para utilizarlos durante diversas operaciones de bases de datos, modificando así el comportamiento de PostgreSQL de alguna manera. Por ejemplo, puede utilizar un enlace `passcheck` para personalizar la forma en que

PostgreSQL gestiona las contraseñas proporcionadas al crear o cambiar las contraseñas de los usuarios (roles).

Consulte la siguiente documentación para obtener información sobre el enlace de passcheck disponible para sus extensiones TLE. Para obtener más información sobre los enlaces disponibles, incluido el enlace de autenticación del cliente, consulte los enlaces de Extensiones de lenguaje de confianza.

Enlace de comprobación de contraseñas (passcheck)

El enlace `passcheck` se utiliza para personalizar el comportamiento de PostgreSQL durante el proceso de comprobación de contraseñas para los siguientes comandos SQL y el metacomando `psql`.

- `CREATE ROLE` *`username`* `...PASSWORD`: para obtener más información, consulte CREATE ROLE en la documentación de PostgreSQL.
- `ALTER ROLE` *`username`*`...PASSWORD`: para obtener más información, consulte ALTER ROLE en la documentación de PostgreSQL.
- `\password` *`username`*: este metacomando `psql` interactivo cambia de forma segura la contraseña del usuario especificado mediante un hash de la contraseña antes de utilizar la sintaxis `ALTER ROLE ... PASSWORD` de forma transparente. El metacomando es un contenedor seguro para el comando `ALTER ROLE ... PASSWORD`, por lo que el enlace se aplica al comportamiento del metacomando `psql`.

Para ver un ejemplo, consulta Lista de códigos del enlace password_check.

Contenido

- Prototipo de función
- Argumentos
- Configuración
- Notas de uso

Prototipo de función

```
passcheck_hook(username text, password text, password_type pgtle.password_types,
 valid_until timestamptz, valid_null boolean)
```

Argumentos

La función de enlace `passcheck` acepta los argumentos siguientes:

- `username`: el nombre (como texto) del rol (nombre de usuario) que establece una contraseña.
- `password`: la contraseña en texto sin formato o con hash. La contraseña introducida debe coincidir con el tipo especificado en `password_type`.
- `password_type`: especifique el formato `pgtle.password_type` de la contraseña. Este formato puede ser uno de los siguientes:
  - `PASSWORD_TYPE_PLAINTEXT`: una contraseña sin formato.
  - `PASSWORD_TYPE_MD5`: una contraseña que se ha cifrado con hash mediante el algoritmo MD5 (resumen de mensaje 5).
  - `PASSWORD_TYPE_SCRAM_SHA_256`: una contraseña que se ha cifrado con hash mediante el algoritmo SCRAM-SHA-256.
- `valid_until`: especifica el momento en que la contraseña deja de ser válida. Este argumento es opcional. Si utiliza este argumento, especifique la hora como valor `timestamptz`.
- `valid_null`: si este valor booleano está establecido en `true`, la opción `valid_until` se establece en `NULL`.

Configuración

La función `pgtle.enable_password_check` controla si el enlace de passcheck está activo. El enlace de passcheck tiene tres ajustes posibles.

- `off`: desactiva el enlace de comprobación de contraseñas `passcheck`. Este es el valor predeterminado.
- on: activa el enlace de comprobación de contraseñas `passcode` para cotejarlas con la tabla.
- `require`: requiere que se defina un enlace de comprobación de contraseñas.

Notas de uso

Para activar o desactivar el enlace `passcheck`, debe modificar el grupo de parámetros de base de datos personalizado de su instancia de base de datos de RDS para PostgreSQL.

Para Linux, macOS o Unix:

```
aws rds modify-db-parameter-group \
```

```
    --region aws-region \
    --db-parameter-group-name your-custom-parameter-group \
    --parameters
 "ParameterName=pgtle.enable_password_check,ParameterValue=on,ApplyMethod=immediate"
```

Para Windows:

```
aws rds modify-db-parameter-group ^
    --region aws-region ^
    --db-parameter-group-name your-custom-parameter-group ^
    --parameters
 "ParameterName=pgtle.enable_password_check,ParameterValue=on,ApplyMethod=immediate"
```

Ejemplos de código de Amazon RDS con SDK de AWS

Los siguientes ejemplos de código muestran cómo utilizar Amazon RDS con un kit de desarrollo de software (SDK) de AWS.

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica llamando a varias funciones dentro del mismo servicio.

Los ejemplos con varios servicios son aplicaciones de muestra que funcionan con varios Servicios de AWS.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Introducción

Introducción a Amazon RDS

En los siguientes ejemplos de código se muestra cómo empezar a utilizar Amazon RDS.

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.RDS;
using Amazon.RDS.Model;

namespace RDSActions;
```

```
public static class HelloRds
{
    static async Task Main(string[] args)
    {
        var rdsClient = new AmazonRDSClient();

        Console.WriteLine($"Hello Amazon RDS! Following are some of your DB
 instances:");
        Console.WriteLine();

        // You can use await and any of the async methods to get a response.
        // Let's get the first twenty DB instances.
        var response = await rdsClient.DescribeDBInstancesAsync(
            new DescribeDBInstancesRequest()
            {
                MaxRecords = 20 // Must be between 20 and 100.
            });

        foreach (var instance in response.DBInstances)
        {
            Console.WriteLine($"\tDB name: {instance.DBName}");
            Console.WriteLine($"\tArn: {instance.DBInstanceArn}");
            Console.WriteLine($"\tIdentifier: {instance.DBInstanceIdentifier}");
            Console.WriteLine();
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Código del archivo de CMake CMakeLists.txt.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS rds)

# Set this project's name.
project("hello_rds")

# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
 libraries for the AWS SDK.
    string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
 "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
    list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
     # Copy relevant AWS SDK for C++ libraries into the current binary directory
 for running and debugging.

     # set(BIN_SUB_DIR "/Debug") # If you are building from the command line, you
 may need to uncomment this
                                 # and set the proper subdirectory to the
 executables' location.

     AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
 ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
        hello_rds.cpp)
```

```
target_link_libraries(${PROJECT_NAME}
        ${AWSSDK_LINK_LIBRARIES})
```

Código del archivo de origen hello_rds.cpp.

```
#include <aws/core/Aws.h>
#include <aws/rds/RDSClient.h>
#include <aws/rds/model/DescribeDBInstancesRequest.h>
#include <iostream>

/*
 *  A "Hello Rds" starter application which initializes an Amazon Relational
 Database Service (Amazon RDS) client and
 *  describes the Amazon RDS instances.
 *
 *  main function
 *
 *  Usage: 'hello_rds'
 *
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    // Optionally change the log level for debugging.
//   options.loggingOptions.logLevel = Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    int result = 0;
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::RDS::RDSClient rdsClient(clientConfig);
        Aws::String marker;
        std::vector<Aws::String> instanceDBIDs;

        do {
            Aws::RDS::Model::DescribeDBInstancesRequest request;

            if (!marker.empty()) {
                request.SetMarker(marker);
            }
```

```
            Aws::RDS::Model::DescribeDBInstancesOutcome outcome =
                    rdsClient.DescribeDBInstances(request);

            if (outcome.IsSuccess()) {
                for (auto &instance: outcome.GetResult().GetDBInstances()) {
                    instanceDBIDs.push_back(instance.GetDBInstanceIdentifier());
                }
                marker = outcome.GetResult().GetMarker();
            } else {
                result = 1;
                std::cerr << "Error with RDS::DescribeDBInstances. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                break;
            }
        } while (!marker.empty());

        std::cout << instanceDBIDs.size() << " RDS instances found." <<
 std::endl;
        for (auto &instanceDBID: instanceDBIDs) {
            std::cout << "   Instance: " << instanceDBID << std::endl;
        }
    }

    Aws::ShutdownAPI(options); // Should only be called once.
    return result;
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para C++.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/rds"
)

// main uses the AWS SDK for Go V2 to create an Amazon Relational Database
 Service (Amazon RDS)
// client and list up to 20 DB instances in your account.
// This example uses the default settings specified in your shared credentials
// and config files.
func main() {
 sdkConfig, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  fmt.Println("Couldn't load default configuration. Have you set up your AWS
 account?")
  fmt.Println(err)
  return
 }
 rdsClient := rds.NewFromConfig(sdkConfig)
 const maxInstances = 20
 fmt.Printf("Let's list up to %v DB instances.\n", maxInstances)
 output, err := rdsClient.DescribeDBInstances(context.TODO(),
  &rds.DescribeDBInstancesInput{MaxRecords: aws.Int32(maxInstances)})
 if err != nil {
  fmt.Printf("Couldn't list DB instances: %v\n", err)
  return
 }
 if len(output.DBInstances) == 0 {
  fmt.Println("No DB instances found.")
 } else {
  for _, instance := range output.DBInstances {
   fmt.Printf("DB instance %v has database %v.\n",
 *instance.DBInstanceIdentifier,
    *instance.DBName)
  }
 }
```

```
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.DescribeDbInstancesResponse;
import software.amazon.awssdk.services.rds.model.DBInstance;
import software.amazon.awssdk.services.rds.model.RdsException;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class DescribeDBInstances {

    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();
```

```
        describeInstances(rdsClient);
        rdsClient.close();
    }

    public static void describeInstances(RdsClient rdsClient) {
        try {
            DescribeDbInstancesResponse response =
 rdsClient.describeDBInstances();
            List<DBInstance> instanceList = response.dbInstances();
            for (DBInstance instance : instanceList) {
                System.out.println("Instance ARN is: " +
 instance.dbInstanceArn());
                System.out.println("The Engine is " + instance.engine());
                System.out.println("Connection endpoint is" +
 instance.endpoint().address());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
"""
Purpose
```

```
Shows how to use the AWS SDK for Python (Boto3) with the Amazon Relational
 Database Service
(Amazon RDS) to list the databases in your account.
"""

import boto3
from botocore.exceptions import ClientError

# Create an RDS client
rds_client = boto3.client("rds")

# Create a paginator for the describe_db_instances operation
paginator = rds_client.get_paginator("describe_db_instances")

try:
    # Use the paginator to get a list of DB instances
    response_iterator = paginator.paginate(
        PaginationConfig={
            "MaxItems": 123,
            "PageSize": 50,  # Adjust PageSize as needed
            "StartingToken": None,
        }
    )

    # Iterate through the pages of the response
    instances_found = False
    for page in response_iterator:
        if "DBInstances" in page and page["DBInstances"]:
            instances_found = True
            print("Your RDS instances are:")
            for db in page["DBInstances"]:
                print(db["DBInstanceIdentifier"])

    if not instances_found:
        print("No RDS instances found!")

except ClientError as e:
    print(f"Couldn't list RDS instances. Here's why: {e.response['Error']
['Message']}")
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require 'aws-sdk-rds'
require 'logger'

# RDSManager is a class responsible for managing RDS operations
# such as listing all RDS DB instances in the current AWS account.
class RDSManager
  def initialize(client)
    @client = client
    @logger = Logger.new($stdout)
  end

  # Lists and prints all RDS DB instances in the current AWS account.
  def list_db_instances
    @logger.info('Listing RDS DB instances')

    paginator = @client.describe_db_instances
    instances = []

    paginator.each_page do |page|
      instances.concat(page.db_instances)
    end

    if instances.empty?
      @logger.info('No instances found.')
    else
      @logger.info("Found #{instances.count} instance(s):")
      instances.each do |instance|
```

```
        @logger.info(" * #{instance.db_instance_identifier}
 (#{instance.db_instance_status})")
      end
    end
  end
end

if $PROGRAM_NAME == __FILE__
  rds_client = Aws::RDS::Client.new(region: 'us-west-2')
  manager = RDSManager.new(rds_client)
  manager.list_db_instances
end
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Ruby.

Ejemplos de código

- Acciones de Amazon RDS con SDK de AWS
  - Uso de CreateDBInstance con un AWS SDK o la CLI
  - Uso de CreateDBParameterGroup con un AWS SDK o la CLI
  - Uso de CreateDBSnapshot con un AWS SDK o la CLI
  - Uso de DeleteDBInstance con un AWS SDK o la CLI
  - Uso de DeleteDBParameterGroup con un AWS SDK o la CLI
  - Uso de DescribeAccountAttributes con un AWS SDK o la CLI
  - Uso de DescribeDBEngineVersions con un AWS SDK o la CLI
  - Uso de DescribeDBInstances con un AWS SDK o la CLI
  - Uso de DescribeDBParameterGroups con un AWS SDK o la CLI
  - Uso de DescribeDBParameters con un AWS SDK o la CLI
  - Uso de DescribeDBSnapshots con un AWS SDK o la CLI
  - Uso de DescribeOrderableDBInstanceOptions con un AWS SDK o la CLI
  - Uso de GenerateRDSAuthToken con un AWS SDK o la CLI
  - Uso de ModifyDBInstance con un AWS SDK o la CLI
  - Uso de ModifyDBParameterGroup con un AWS SDK o la CLI

  - Uso de RebootDBInstance con un AWS SDK o la CLI
- Escenarios de Amazon RDS con SDK de AWS
  - Comience a utilizar las instancias de base de datos de Amazon RDS con un SDK de AWS
- Ejemplos sin servidor para Amazon RDS en los que se utilizan SDK de AWS
  - Conexión a una base de datos de Amazon RDS en una función de Lambda
- Ejemplos en diversos servicios de Amazon RDS con SDK de AWS
  - Crear un rastreador de elementos de trabajo de Aurora Serverless

Acciones de Amazon RDS con SDK de AWS

Los siguientes ejemplos de código muestran cómo llevar a cabo acciones individuales de Amazon RDS con los SDK de AWS. Estos fragmentos llaman a la API de RDS y son fragmentos de código de programas más grandes que deben ejecutarse en contexto. En cada ejemplo se incluye un enlace a GitHub, con instrucciones de configuración y ejecución del código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para obtener una lista completa, consulte la Referencia de la API de Amazon Relational Database Service (Amazon RDS).

Ejemplos

- Uso de CreateDBInstance con un AWS SDK o la CLI
- Uso de CreateDBParameterGroup con un AWS SDK o la CLI
- Uso de CreateDBSnapshot con un AWS SDK o la CLI
- Uso de DeleteDBInstance con un AWS SDK o la CLI
- Uso de DeleteDBParameterGroup con un AWS SDK o la CLI
- Uso de DescribeAccountAttributes con un AWS SDK o la CLI
- Uso de DescribeDBEngineVersions con un AWS SDK o la CLI
- Uso de DescribeDBInstances con un AWS SDK o la CLI
- Uso de DescribeDBParameterGroups con un AWS SDK o la CLI
- Uso de DescribeDBParameters con un AWS SDK o la CLI
- Uso de DescribeDBSnapshots con un AWS SDK o la CLI
- Uso de DescribeOrderableDBInstanceOptions con un AWS SDK o la CLI
- Uso de GenerateRDSAuthToken con un AWS SDK o la CLI

- Uso de ModifyDBInstance con un AWS SDK o la CLI
- Uso de ModifyDBParameterGroup con un AWS SDK o la CLI
- Uso de RebootDBInstance con un AWS SDK o la CLI

Uso de **`CreateDBInstance`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `CreateDBInstance`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   /// <summary>
   /// Create an RDS DB instance with a particular set of properties. Use the
action DescribeDBInstancesAsync
   /// to determine when the DB instance is ready to use.
   /// </summary>
   /// <param name="dbName">Name for the DB instance.</param>
   /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
   /// <param name="parameterGroupName">DB parameter group to associate with the
instance.</param>
   /// <param name="dbEngine">The engine for the DB instance.</param>
   /// <param name="dbEngineVersion">Version for the DB instance.</param>
   /// <param name="instanceClass">Class for the DB instance.</param>
   /// <param name="allocatedStorage">The amount of storage in gibibytes (GiB)
to allocate to the DB instance.</param>
   /// <param name="adminName">Admin user name.</param>
   /// <param name="adminPassword">Admin user password.</param>
```

```
    /// <returns>DB instance object.</returns>
    public async Task<DBInstance> CreateDBInstance(string dbName, string
dbInstanceIdentifier,
        string parameterGroupName, string dbEngine, string dbEngineVersion,
        string instanceClass, int allocatedStorage, string adminName, string
adminPassword)
    {
        var response = await _amazonRDS.CreateDBInstanceAsync(
            new CreateDBInstanceRequest()
            {
                DBName = dbName,
                DBInstanceIdentifier = dbInstanceIdentifier,
                DBParameterGroupName = parameterGroupName,
                Engine = dbEngine,
                EngineVersion = dbEngineVersion,
                DBInstanceClass = instanceClass,
                AllocatedStorage = allocatedStorage,
                MasterUsername = adminName,
                MasterUserPassword = adminPassword
            });

        return response.DBInstance;
    }
```

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
```

```
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::CreateDBInstanceRequest request;
        request.SetDBName(DB_NAME);
        request.SetDBInstanceIdentifier(DB_INSTANCE_IDENTIFIER);
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        request.SetEngine(engineVersion.GetEngine());
        request.SetEngineVersion(engineVersion.GetEngineVersion());
        request.SetDBInstanceClass(dbInstanceClass);
        request.SetStorageType(DB_STORAGE_TYPE);
        request.SetAllocatedStorage(DB_ALLOCATED_STORAGE);
        request.SetMasterUsername(administratorName);
        request.SetMasterUserPassword(administratorPassword);

        Aws::RDS::Model::CreateDBInstanceOutcome outcome =
                client.CreateDBInstance(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB instance creation has started."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::CreateDBInstance. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            cleanUpResources(PARAMETER_GROUP_NAME, "", client);
            return false;
        }
```

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Creación de una instancia de base de datos

En el siguiente ejemplo `create-db-instance`, se utilizan las opciones necesarias para lanzar una nueva instancia de base de datos.

```
aws rds create-db-instance \
    --db-instance-identifier test-mysql-instance \
    --db-instance-class db.t3.micro \
    --engine mysql \
    --master-username admin \
    --master-user-password secret99 \
    --allocated-storage 20
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "test-mysql-instance",
        "DBInstanceClass": "db.t3.micro",
        "Engine": "mysql",
        "DBInstanceStatus": "creating",
        "MasterUsername": "admin",
        "AllocatedStorage": 20,
        "PreferredBackupWindow": "12:55-13:25",
        "BackupRetentionPeriod": 1,
        "DBSecurityGroups": [],
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "sg-12345abc",
                "Status": "active"
            }
        ],
        "DBParameterGroups": [
            {
                "DBParameterGroupName": "default.mysql5.7",
                "ParameterApplyStatus": "in-sync"
            }
        ],
        "DBSubnetGroup": {
            "DBSubnetGroupName": "default",
            "DBSubnetGroupDescription": "default",
            "VpcId": "vpc-2ff2ff2f",
            "SubnetGroupStatus": "Complete",
            "Subnets": [
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2c"
```

```
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2d"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2a"
                    },
                    "SubnetStatus": "Active"
                },
                {
                    "SubnetIdentifier": "subnet-########",
                    "SubnetAvailabilityZone": {
                        "Name": "us-west-2b"
                    },
                    "SubnetStatus": "Active"
                }
            ]
        },
        "PreferredMaintenanceWindow": "sun:08:07-sun:08:37",
        "PendingModifiedValues": {
            "MasterUserPassword": "****"
        },
        "MultiAZ": false,
        "EngineVersion": "5.7.22",
        "AutoMinorVersionUpgrade": true,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "general-public-license",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "default:mysql-5-7",
                "Status": "in-sync"
            }
        ],
        "PubliclyAccessible": true,
        "StorageType": "gp2",
        "DbInstancePort": 0,
```

```
        "StorageEncrypted": false,
        "DbiResourceId": "db-5555EXAMPLE44444444EXAMPLE",
        "CACertificateIdentifier": "rds-ca-2019",
        "DomainMemberships": [],
        "CopyTagsToSnapshot": false,
        "MonitoringInterval": 0,
        "DBInstanceArn": "arn:aws:rds:us-west-2:123456789012:db:test-mysql-
instance",
        "IAMDatabaseAuthenticationEnabled": false,
        "PerformanceInsightsEnabled": false,
        "DeletionProtection": false,
        "AssociatedRoles": []
    }
}
```

Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// CreateInstance creates a DB instance.
func (instances *DbInstances) CreateInstance(instanceName string, dbName string,
 dbEngine string, dbEngineVersion string, parameterGroupName string,
 dbInstanceClass string,
```

```
 storageType string, allocatedStorage int32, adminName string, adminPassword
 string) (
 *types.DBInstance, error) {
 output, err := instances.RdsClient.CreateDBInstance(context.TODO(),
 &rds.CreateDBInstanceInput{
  DBInstanceIdentifier: aws.String(instanceName),
  DBName:               aws.String(dbName),
  DBParameterGroupName: aws.String(parameterGroupName),
  Engine:               aws.String(dbEngine),
  EngineVersion:        aws.String(dbEngineVersion),
  DBInstanceClass:      aws.String(dbInstanceClass),
  StorageType:          aws.String(storageType),
  AllocatedStorage:     aws.Int32(allocatedStorage),
  MasterUsername:       aws.String(adminName),
  MasterUserPassword:   aws.String(adminPassword),
 })
 if err != nil {
  log.Printf("Couldn't create instance %v: %v\n", instanceName, err)
  return nil, err
 } else {
  return output.DBInstance, nil
 }
}
```

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import com.google.gson.Gson;
```

```
import
 software.amazon.awssdk.auth.credentials.EnvironmentVariableCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.DescribeDbInstancesRequest;
import software.amazon.awssdk.services.rds.model.CreateDbInstanceRequest;
import software.amazon.awssdk.services.rds.model.CreateDbInstanceResponse;
import software.amazon.awssdk.services.rds.model.RdsException;
import software.amazon.awssdk.services.rds.model.DescribeDbInstancesResponse;
import software.amazon.awssdk.services.rds.model.DBInstance;
import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
import
 software.amazon.awssdk.services.secretsmanager.model.GetSecretValueRequest;
import
 software.amazon.awssdk.services.secretsmanager.model.GetSecretValueResponse;

import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example requires an AWS Secrets Manager secret that contains the
 * database credentials. If you do not create a
 * secret, this example will not work. For more details, see:
 *
 * https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_how-
services-use-secrets_RS.html
 *
 *
 */

public class CreateDBInstance {
    public static long sleepTime = 20;

    public static void main(String[] args) {
        final String usage = """

                Usage:
```

```
                    <dbInstanceIdentifier> <dbName> <secretName>

                Where:
                    dbInstanceIdentifier - The database instance identifier.\s
                    dbName - The database name.\s
                    secretName - The name of the AWS Secrets Manager secret that
contains the database credentials."
                """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String dbInstanceIdentifier = args[0];
        String dbName = args[1];
        String secretName = args[2];
        Gson gson = new Gson();
        User user = gson.fromJson(String.valueOf(getSecretValues(secretName)),
User.class);
        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        createDatabaseInstance(rdsClient, dbInstanceIdentifier, dbName,
user.getUsername(), user.getPassword());
        waitForInstanceReady(rdsClient, dbInstanceIdentifier);
        rdsClient.close();
    }

    private static SecretsManagerClient getSecretClient() {
        Region region = Region.US_WEST_2;
        return SecretsManagerClient.builder()
                .region(region)

.credentialsProvider(EnvironmentVariableCredentialsProvider.create())
                .build();
    }

    private static String getSecretValues(String secretName) {
        SecretsManagerClient secretClient = getSecretClient();
        GetSecretValueRequest valueRequest = GetSecretValueRequest.builder()
                .secretId(secretName)
```

```
                .build();

        GetSecretValueResponse valueResponse =
secretClient.getSecretValue(valueRequest);
        return valueResponse.secretString();
    }

    public static void createDatabaseInstance(RdsClient rdsClient,
            String dbInstanceIdentifier,
            String dbName,
            String userName,
            String userPassword) {

        try {
            CreateDbInstanceRequest instanceRequest =
CreateDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .allocatedStorage(100)
                    .dbName(dbName)
                    .engine("mysql")
                    .dbInstanceClass("db.m4.large")
                    .engineVersion("8.0")
                    .storageType("standard")
                    .masterUsername(userName)
                    .masterUserPassword(userPassword)
                    .build();

            CreateDbInstanceResponse response =
rdsClient.createDBInstance(instanceRequest);
            System.out.print("The status is " +
response.dbInstance().dbInstanceStatus());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Waits until the database instance is available.
    public static void waitForInstanceReady(RdsClient rdsClient, String
dbInstanceIdentifier) {
        boolean instanceReady = false;
        String instanceReadyStr;
        System.out.println("Waiting for instance to become available.");
```

```
        try {
            DescribeDbInstancesRequest instanceRequest =
DescribeDbInstancesRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .build();

            // Loop until the cluster is ready.
            while (!instanceReady) {
                DescribeDbInstancesResponse response =
rdsClient.describeDBInstances(instanceRequest);
                List<DBInstance> instanceList = response.dbInstances();
                for (DBInstance instance : instanceList) {
                    instanceReadyStr = instance.dbInstanceStatus();
                    if (instanceReadyStr.contains("available"))
                        instanceReady = true;
                    else {
                        System.out.print(".");
                        Thread.sleep(sleepTime * 1000);
                    }
                }
            }
            System.out.println("Database instance is available!");

        } catch (RdsException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de la API de AWS SDK for Java 2.x.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun createDatabaseInstance(
    dbInstanceIdentifierVal: String?,
    dbNamedbVal: String?,
    masterUsernameVal: String?,
    masterUserPasswordVal: String?,
) {
    val instanceRequest =
        CreateDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            allocatedStorage = 100
            dbName = dbNamedbVal
            engine = "mysql"
            dbInstanceClass = "db.m4.large"
            engineVersion = "8.0"
            storageType = "standard"
            masterUsername = masterUsernameVal
            masterUserPassword = masterUserPasswordVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbInstance(instanceRequest)
        print("The status is ${response.dbInstance?.dbInstanceStatus}")
    }
}

// Waits until the database instance is available.
suspend fun waitForInstanceReady(dbInstanceIdentifierVal: String?) {
    val sleepTime: Long = 20
    var instanceReady = false
    var instanceReadyStr: String
    println("Waiting for instance to become available.")

    val instanceRequest =
        DescribeDbInstancesRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        while (!instanceReady) {
            val response = rdsClient.describeDbInstances(instanceRequest)
            val instanceList = response.dbInstances
            if (instanceList != null) {
                for (instance in instanceList) {
```

```
                    instanceReadyStr = instance.dbInstanceStatus.toString()
                    if (instanceReadyStr.contains("available")) {
                        instanceReady = true
                    } else {
                        println("...$instanceReadyStr")
                        delay(sleepTime * 1000)
                    }
                }
            }
        }
        println("Database instance is available!")
    }
}
```

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de la API de AWS SDK para Kotlin.

PHP

SDK para PHP

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require __DIR__ . '/vendor/autoload.php';

use Aws\Exception\AwsException;



$rdsClient = new Aws\Rds\RdsClient([
    'region' => 'us-east-2'
]);

$dbIdentifier = '<<{{db-identifier}}>>';
```

```
$dbClass = 'db.t2.micro';
$storage = 5;
$engine = 'MySQL';
$username = 'MyUser';
$password = 'MyPassword';

try {
    $result = $rdsClient->createDBInstance([
        'DBInstanceIdentifier' => $dbIdentifier,
        'DBInstanceClass' => $dbClass,
        'AllocatedStorage' => $storage,
        'Engine' => $engine,
        'MasterUsername' => $username,
        'MasterUserPassword' => $password,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    echo $e->getMessage();
    echo "\n";
}
```

- Para obtener información sobre la API, consulte CreateDBInstance en la Referencia de la API de AWS SDK para PHP.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
```

```
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_db_instance(
        self,
        db_name,
        instance_id,
        parameter_group_name,
        db_engine,
        db_engine_version,
        instance_class,
        storage_type,
        allocated_storage,
        admin_name,
        admin_password,
    ):
        """
        Creates a DB instance.

        :param db_name: The name of the database that is created in the DB
instance.
        :param instance_id: The ID to give the newly created DB instance.
        :param parameter_group_name: A parameter group to associate with the DB
instance.
        :param db_engine: The database engine of a database to create in the DB
instance.
        :param db_engine_version: The engine version for the created database.
        :param instance_class: The DB instance class for the newly created DB
instance.
        :param storage_type: The storage type of the DB instance.
        :param allocated_storage: The amount of storage allocated on the DB
instance, in GiBs.
        :param admin_name: The name of the admin user for the created database.
        :param admin_password: The admin password for the created database.
```

```
        :return: Data about the newly created DB instance.
        """
        try:
            response = self.rds_client.create_db_instance(
                DBName=db_name,
                DBInstanceIdentifier=instance_id,
                DBParameterGroupName=parameter_group_name,
                Engine=db_engine,
                EngineVersion=db_engine_version,
                DBInstanceClass=instance_class,
                StorageType=storage_type,
                AllocatedStorage=allocated_storage,
                MasterUsername=admin_name,
                MasterUserPassword=admin_password,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't create DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

- Para obtener detalles sobre la API, consulte CreateDBInstance en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`CreateDBParameterGroup`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `CreateDBParameterGroup`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   /// <summary>
   /// Create a new DB parameter group. Use the action
DescribeDBParameterGroupsAsync
   /// to determine when the DB parameter group is ready to use.
   /// </summary>
   /// <param name="name">Name of the DB parameter group.</param>
   /// <param name="family">Family of the DB parameter group.</param>
   /// <param name="description">Description of the DB parameter group.</param>
   /// <returns>The new DB parameter group.</returns>
   public async Task<DBParameterGroup> CreateDBParameterGroup(
       string name, string family, string description)
   {
       var response = await _amazonRDS.CreateDBParameterGroupAsync(
           new CreateDBParameterGroupRequest()
           {
               DBParameterGroupName = name,
               DBParameterGroupFamily = family,
               Description = description
           });
       return response.DBParameterGroup;
   }
```

- Para obtener información sobre la API, consulte CreateDBParameterGroup en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::CreateDBParameterGroupRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        request.SetDBParameterGroupFamily(dbParameterGroupFamily);
        request.SetDescription("Example parameter group.");

        Aws::RDS::Model::CreateDBParameterGroupOutcome outcome =
                client.CreateDBParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully created."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::CreateDBParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
```

- Para obtener información sobre la API, consulte CreateDBParameterGroup en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Creación de un grupo de parámetros de base de datos

En el siguiente ejemplo `create-db-parameter-group`, se crea un grupo de parámetros de base de datos.

```
aws rds create-db-parameter-group \
    --db-parameter-group-name mydbparametergroup \
    --db-parameter-group-family MySQL5.6 \
    --description "My new parameter group"
```

Salida:

```
{
    "DBParameterGroup": {
        "DBParameterGroupName": "mydbparametergroup",
        "DBParameterGroupFamily": "mysql5.6",
        "Description": "My new parameter group",
        "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:mydbparametergroup"
    }
}
```

Para obtener más información, consulte Creación de un grupo de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CreateDBParameterGroup en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// CreateParameterGroup creates a DB parameter group that is based on the
 specified
// parameter group family.
func (instances *DbInstances) CreateParameterGroup(
 parameterGroupName string, parameterGroupFamily string, description string) (
 *types.DBParameterGroup, error) {

 output, err := instances.RdsClient.CreateDBParameterGroup(context.TODO(),
  &rds.CreateDBParameterGroupInput{
   DBParameterGroupName:   aws.String(parameterGroupName),
   DBParameterGroupFamily: aws.String(parameterGroupFamily),
   Description:            aws.String(description),
  })
 if err != nil {
  log.Printf("Couldn't create parameter group %v: %v\n", parameterGroupName, err)
  return nil, err
 } else {
  return output.DBParameterGroup, err
 }
}
```

- Para obtener información sobre la API, consulte CreateDBParameterGroup en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void createDBParameterGroup(RdsClient rdsClient, String
dbGroupName, String dbParameterGroupFamily) {
       try {
           CreateDbParameterGroupRequest groupRequest =
CreateDbParameterGroupRequest.builder()
                   .dbParameterGroupName(dbGroupName)
                   .dbParameterGroupFamily(dbParameterGroupFamily)
                   .description("Created by using the AWS SDK for Java")
                   .build();

           CreateDbParameterGroupResponse response =
rdsClient.createDBParameterGroup(groupRequest);
           System.out.println("The group name is " +
response.dbParameterGroup().dbParameterGroupName());

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obtener información sobre la API, consulte CreateDBParameterGroup en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
```

```
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_parameter_group(
        self, parameter_group_name, parameter_group_family, description
    ):
        """
        Creates a DB parameter group that is based on the specified parameter
group
        family.

        :param parameter_group_name: The name of the newly created parameter
group.
        :param parameter_group_family: The family that is used as the basis of
the new
                                       parameter group.
        :param description: A description given to the parameter group.
        :return: Data about the newly created parameter group.
        """
        try:
            response = self.rds_client.create_db_parameter_group(
                DBParameterGroupName=parameter_group_name,
                DBParameterGroupFamily=parameter_group_family,
                Description=description,
            )
        except ClientError as err:
            logger.error(
                "Couldn't create parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Para obtener detalles sobre la API, consulte CreateDBParameterGroup en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de `CreateDBSnapshot` con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `CreateDBSnapshot`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Create a snapshot of a DB instance.
    /// </summary>
    /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
    /// <param name="snapshotIdentifier">Identifier for the snapshot.</param>
    /// <returns>DB snapshot object.</returns>
    public async Task<DBSnapshot> CreateDBSnapshot(string dbInstanceIdentifier,
string snapshotIdentifier)
    {
```

```
        var response = await _amazonRDS.CreateDBSnapshotAsync(
            new CreateDBSnapshotRequest()
            {
                DBSnapshotIdentifier = snapshotIdentifier,
                DBInstanceIdentifier = dbInstanceIdentifier
            });

        return response.DBSnapshot;
    }
```

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::CreateDBSnapshotRequest request;
            request.SetDBInstanceIdentifier(DB_INSTANCE_IDENTIFIER);
            request.SetDBSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::CreateDBSnapshotOutcome outcome =
                    client.CreateDBSnapshot(request);

            if (outcome.IsSuccess()) {
                std::cout << "Snapshot creation has started."
                          << std::endl;
```

```
            }
            else {
                std::cerr << "Error with RDS::CreateDBSnapshot. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
 client);
                return false;
            }
```

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Creación de una instantánea de base de datos

En el siguiente ejemplo `create-db-snapshot`, se crea una instantánea de base de datos.

```
aws rds create-db-snapshot \
    --db-instance-identifier database-mysql \
    --db-snapshot-identifier mydbsnapshot
```

Salida:

```
{
    "DBSnapshot": {
        "DBSnapshotIdentifier": "mydbsnapshot",
        "DBInstanceIdentifier": "database-mysql",
        "Engine": "mysql",
        "AllocatedStorage": 100,
        "Status": "creating",
        "Port": 3306,
        "AvailabilityZone": "us-east-1b",
        "VpcId": "vpc-6594f31c",
        "InstanceCreateTime": "2019-04-30T15:45:53.663Z",
        "MasterUsername": "admin",
        "EngineVersion": "5.6.40",
        "LicenseModel": "general-public-license",
```

```
        "SnapshotType": "manual",
        "Iops": 1000,
        "OptionGroupName": "default:mysql-5-6",
        "PercentProgress": 0,
        "StorageType": "io1",
        "Encrypted": true,
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/
AKIAIOSFODNN7EXAMPLE",
        "DBSnapshotArn": "arn:aws:rds:us-
east-1:123456789012:snapshot:mydbsnapshot",
        "IAMDatabaseAuthenticationEnabled": false,
        "ProcessorFeatures": [],
        "DbiResourceId": "db-AKIAIOSFODNN7EXAMPLE"
    }
}
```

Para obtener más información, consulte Creación de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// CreateSnapshot creates a snapshot of a DB instance.
func (instances *DbInstances) CreateSnapshot(instanceName string, snapshotName
 string) (
```

```
 *types.DBSnapshot, error) {
 output, err := instances.RdsClient.CreateDBSnapshot(context.TODO(),
 &rds.CreateDBSnapshotInput{
  DBInstanceIdentifier: aws.String(instanceName),
  DBSnapshotIdentifier: aws.String(snapshotName),
 })
 if err != nil {
  log.Printf("Couldn't create snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return output.DBSnapshot, nil
 }
}
```

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   // Create an Amazon RDS snapshot.
   public static void createSnapshot(RdsClient rdsClient, String
dbInstanceIdentifier, String dbSnapshotIdentifier) {
       try {
           CreateDbSnapshotRequest snapshotRequest =
CreateDbSnapshotRequest.builder()
                   .dbInstanceIdentifier(dbInstanceIdentifier)
                   .dbSnapshotIdentifier(dbSnapshotIdentifier)
                   .build();

           CreateDbSnapshotResponse response =
rdsClient.createDBSnapshot(snapshotRequest);
```

```
            System.out.println("The Snapshot id is " +
 response.dbSnapshot().dbiResourceId());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK for Java 2.x.

PHP

SDK para PHP

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require __DIR__ . '/vendor/autoload.php';

use Aws\Exception\AwsException;



$rdsClient = new Aws\Rds\RdsClient([
    'region' => 'us-east-2'
]);

$dbIdentifier = '<<{{db-identifier}}>>';
$snapshotName = '<<{{backup_2018_12_25}}>>';

try {
    $result = $rdsClient->createDBSnapshot([
        'DBInstanceIdentifier' => $dbIdentifier,
        'DBSnapshotIdentifier' => $snapshotName,
```

```
    ]);
    var_dump($result);
} catch (AwsException $e) {
    echo $e->getMessage();
    echo "\n";
}
```

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK para PHP.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def create_snapshot(self, snapshot_id, instance_id):
```

```
        """
        Creates a snapshot of a DB instance.

        :param snapshot_id: The ID to give the created snapshot.
        :param instance_id: The ID of the DB instance to snapshot.
        :return: Data about the newly created snapshot.
        """
        try:
            response = self.rds_client.create_db_snapshot(
                DBSnapshotIdentifier=snapshot_id,
DBInstanceIdentifier=instance_id
            )
            snapshot = response["DBSnapshot"]
        except ClientError as err:
            logger.error(
                "Couldn't create snapshot of %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot
```

- Para obtener información sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK para Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-rds"  # v2: require 'aws-sdk'
```

```
# Create a snapshot for an Amazon Relational Database Service (Amazon RDS)
# DB instance.
#
# @param rds_resource [Aws::RDS::Resource] The resource containing SDK logic.
# @param db_instance_name [String] The name of the Amazon RDS DB instance.
# @return [Aws::RDS::DBSnapshot, nil] The snapshot created, or nil if error.
def create_snapshot(rds_resource, db_instance_name)
  id = "snapshot-#{rand(10**6)}"
  db_instance = rds_resource.db_instance(db_instance_name)
  db_instance.create_snapshot({
                                db_snapshot_identifier: id
                              })
rescue Aws::Errors::ServiceError => e
  puts "Couldn't create DB instance snapshot #{id}:\n #{e.message}"
end
```

- Para obtener detalles sobre la API, consulte CreateDBSnapshot en la Referencia de la API de AWS SDK para Ruby.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DeleteDBInstance`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DeleteDBInstance`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/// <summary>
/// Delete a particular DB instance.
/// </summary>
/// <param name="dbInstanceIdentifier">DB instance identifier.</param>
/// <returns>DB instance object.</returns>
public async Task<DBInstance> DeleteDBInstance(string dbInstanceIdentifier)
{
    var response = await _amazonRDS.DeleteDBInstanceAsync(
        new DeleteDBInstanceRequest()
        {
            DBInstanceIdentifier = dbInstanceIdentifier,
            SkipFinalSnapshot = true,
            DeleteAutomatedBackups = true
        });

    return response.DBInstance;
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::DeleteDBInstanceRequest request;
            request.SetDBInstanceIdentifier(dbInstanceIdentifier);
            request.SetSkipFinalSnapshot(true);
            request.SetDeleteAutomatedBackups(true);

            Aws::RDS::Model::DeleteDBInstanceOutcome outcome =
                    client.DeleteDBInstance(request);

            if (outcome.IsSuccess()) {
                std::cout << "DB instance deletion has started."
                          << std::endl;
            }
            else {
                std::cerr << "Error with RDS::DeleteDBInstance. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = false;
            }
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Eliminación de una instancia de base de datos

En el siguiente ejemplo `delete-db-instance`, se elimina la instancia de base de datos especificada tras crear una instantánea de base de datos final denominada `test-instance-final-snap`.

```
aws rds delete-db-instance \
    --db-instance-identifier test-instance \
    --final-db-snapshot-identifier test-instance-final-snap
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "test-instance",
        "DBInstanceStatus": "deleting",
        ...some output truncated...
    }
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
```

```
}



// DeleteInstance deletes a DB instance.
func (instances *DbInstances) DeleteInstance(instanceName string) error {
 _, err := instances.RdsClient.DeleteDBInstance(context.TODO(),
 &rds.DeleteDBInstanceInput{
  DBInstanceIdentifier:   aws.String(instanceName),
  SkipFinalSnapshot:      true,
  DeleteAutomatedBackups: aws.Bool(true),
 })
 if err != nil {
  log.Printf("Couldn't delete instance %v: %v\n", instanceName, err)
  return err
 } else {
  return nil
 }
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.DeleteDbInstanceRequest;
import software.amazon.awssdk.services.rds.model.DeleteDbInstanceResponse;
import software.amazon.awssdk.services.rds.model.RdsException;
```

```
/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class DeleteDBInstance {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <dbInstanceIdentifier>\s

                Where:
                    dbInstanceIdentifier - The database instance identifier\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String dbInstanceIdentifier = args[0];
        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        deleteDatabaseInstance(rdsClient, dbInstanceIdentifier);
        rdsClient.close();
    }

    public static void deleteDatabaseInstance(RdsClient rdsClient, String
 dbInstanceIdentifier) {
        try {
            DeleteDbInstanceRequest deleteDbInstanceRequest =
 DeleteDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .deleteAutomatedBackups(true)
                    .skipFinalSnapshot(true)
                    .build();
```

```
            DeleteDbInstanceResponse response =
 rdsClient.deleteDBInstance(deleteDbInstanceRequest);
            System.out.print("The status of the database is " +
 response.dbInstance().dbInstanceStatus());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de la API de AWS SDK for Java 2.x.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun deleteDatabaseInstance(dbInstanceIdentifierVal: String?) {
    val deleteDbInstanceRequest =
        DeleteDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            deleteAutomatedBackups = true
            skipFinalSnapshot = true
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.deleteDbInstance(deleteDbInstanceRequest)
        print("The status of the database is
 ${response.dbInstance?.dbInstanceStatus}")
    }
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de la API de AWS SDK para Kotlin.

PHP

SDK para PHP

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require __DIR__ . '/vendor/autoload.php';

use Aws\Exception\AwsException;


//Create an RDSClient
$rdsClient = new Aws\Rds\RdsClient([
    'region' => 'us-east-1'
]);

$dbIdentifier = '<<{{db-identifier}}>>';

try {
    $result = $rdsClient->deleteDBInstance([
        'DBInstanceIdentifier' => $dbIdentifier,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    echo $e->getMessage();
    echo "\n";
}
```

- Para obtener información sobre la API, consulte DeleteDBInstance en la Referencia de la API de AWS SDK para PHP.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def delete_db_instance(self, instance_id):
        """
        Deletes a DB instance.

        :param instance_id: The ID of the DB instance to delete.
        :return: Data about the deleted DB instance.
        """
        try:
            response = self.rds_client.delete_db_instance(
                DBInstanceIdentifier=instance_id,
```

```
                SkipFinalSnapshot=True,
                DeleteAutomatedBackups=True,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't delete DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

- Para obtener detalles sobre la API, consulte DeleteDBInstance en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DeleteDBParameterGroup`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DeleteDBParameterGroup`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Delete a DB parameter group. The group cannot be a default DB parameter
group
    /// or be associated with any DB instances.
    /// </summary>
    /// <param name="name">Name of the DB parameter group.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteDBParameterGroup(string name)
    {
        var response = await _amazonRDS.DeleteDBParameterGroupAsync(
            new DeleteDBParameterGroupRequest()
            {
                DBParameterGroupName = name,
            });
        return response.HttpStatusCode == HttpStatusCode.OK;
    }
```

- Para obtener información sobre la API, consulte DeleteDBParameterGroup en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    Aws::Client::ClientConfiguration clientConfig;
    // Optional: Set to the AWS Region (overrides config file).
    // clientConfig.region = "us-east-1";

Aws::RDS::RDSClient client(clientConfig);

    Aws::RDS::Model::DeleteDBParameterGroupRequest request;
    request.SetDBParameterGroupName(parameterGroupName);

    Aws::RDS::Model::DeleteDBParameterGroupOutcome outcome =
            client.DeleteDBParameterGroup(request);

    if (outcome.IsSuccess()) {
        std::cout << "The DB parameter group was successfully deleted."
                  << std::endl;
    }
    else {
        std::cerr << "Error with RDS::DeleteDBParameterGroup. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
        result = false;
    }
```

- Para obtener información sobre la API, consulte DeleteDBParameterGroup en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Eliminación de un grupo de parámetros de base de datos

En el siguiente ejemplo command, se elimina un grupo de parámetros de base de datos.

```
aws rds delete-db-parameter-group \
    --db-parameter-group-name mydbparametergroup
```

Este comando no genera ninguna salida.

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DeleteDBParameterGroup en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// DeleteParameterGroup deletes the named DB parameter group.
func (instances *DbInstances) DeleteParameterGroup(parameterGroupName string)
 error {
 _, err := instances.RdsClient.DeleteDBParameterGroup(context.TODO(),
  &rds.DeleteDBParameterGroupInput{
   DBParameterGroupName: aws.String(parameterGroupName),
```

```
  })
 if err != nil {
  log.Printf("Couldn't delete parameter group %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}
```

- Para obtener información sobre la API, consulte DeleteDBParameterGroup en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   // Delete the parameter group after database has been deleted.
   // An exception is thrown if you attempt to delete the para group while
database
   // exists.
   public static void deleteParaGroup(RdsClient rdsClient, String dbGroupName,
String dbARN)
           throws InterruptedException {
       try {
           boolean isDataDel = false;
           boolean didFind;
           String instanceARN;

           // Make sure that the database has been deleted.
           while (!isDataDel) {
               DescribeDbInstancesResponse response =
rdsClient.describeDBInstances();
               List<DBInstance> instanceList = response.dbInstances();
```

```
                int listSize = instanceList.size();
                didFind = false;
                int index = 1;
                for (DBInstance instance : instanceList) {
                    instanceARN = instance.dbInstanceArn();
                    if (instanceARN.compareTo(dbARN) == 0) {
                        System.out.println(dbARN + " still exists");
                        didFind = true;
                    }
                    if ((index == listSize) && (!didFind)) {
                        // Went through the entire list and did not find the
database ARN.
                        isDataDel = true;
                    }
                    Thread.sleep(sleepTime * 1000);
                    index++;
                }
            }

            // Delete the para group.
            DeleteDbParameterGroupRequest parameterGroupRequest =
DeleteDbParameterGroupRequest.builder()
                    .dbParameterGroupName(dbGroupName)
                    .build();

            rdsClient.deleteDBParameterGroup(parameterGroupRequest);
            System.out.println(dbGroupName + " was deleted.");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte DeleteDBParameterGroup en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def delete_parameter_group(self, parameter_group_name):
        """
        Deletes a DB parameter group.

        :param parameter_group_name: The name of the parameter group to delete.
        :return: Data about the parameter group.
        """
        try:
            self.rds_client.delete_db_parameter_group(
                DBParameterGroupName=parameter_group_name
            )
        except ClientError as err:
            logger.error(
                "Couldn't delete parameter group %s. Here's why: %s: %s",
```

```
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- Para obtener detalles sobre la API, consulte DeleteDBParameterGroup en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeAccountAttributes`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeAccountAttributes`.

CLI

AWS CLI

Descripción de atributos de cuenta

En el siguiente ejemplo `describe-account-attributes`, se recuperan los atributos de la cuenta actual de AWS.

```
aws rds describe-account-attributes
```

Salida:

```
{
    "AccountQuotas": [
        {
            "Max": 40,
            "Used": 4,
            "AccountQuotaName": "DBInstances"
        },
        {
            "Max": 40,
            "Used": 0,
```

```
            "AccountQuotaName": "ReservedDBInstances"
        },
        {
            "Max": 100000,
            "Used": 40,
            "AccountQuotaName": "AllocatedStorage"
        },
        {
            "Max": 25,
            "Used": 0,
            "AccountQuotaName": "DBSecurityGroups"
        },
        {
            "Max": 20,
            "Used": 0,
            "AccountQuotaName": "AuthorizationsPerDBSecurityGroup"
        },
        {
            "Max": 50,
            "Used": 1,
            "AccountQuotaName": "DBParameterGroups"
        },
        {
            "Max": 100,
            "Used": 3,
            "AccountQuotaName": "ManualSnapshots"
        },
        {
            "Max": 20,
            "Used": 0,
            "AccountQuotaName": "EventSubscriptions"
        },
        {
            "Max": 50,
            "Used": 1,
            "AccountQuotaName": "DBSubnetGroups"
        },
        {
            "Max": 20,
            "Used": 1,
            "AccountQuotaName": "OptionGroups"
        },
        {
            "Max": 20,
```

```
            "Used": 6,
            "AccountQuotaName": "SubnetsPerDBSubnetGroup"
        },
        {
            "Max": 5,
            "Used": 0,
            "AccountQuotaName": "ReadReplicasPerMaster"
        },
        {
            "Max": 40,
            "Used": 1,
            "AccountQuotaName": "DBClusters"
        },
        {
            "Max": 50,
            "Used": 0,
            "AccountQuotaName": "DBClusterParameterGroups"
        },
        {
            "Max": 5,
            "Used": 0,
            "AccountQuotaName": "DBClusterRoles"
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeAccountAttributes en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
```

```
import software.amazon.awssdk.services.rds.model.AccountQuota;
import software.amazon.awssdk.services.rds.model.RdsException;
import
 software.amazon.awssdk.services.rds.model.DescribeAccountAttributesResponse;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class DescribeAccountAttributes {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        getAccountAttributes(rdsClient);
        rdsClient.close();
    }

    public static void getAccountAttributes(RdsClient rdsClient) {
        try {
            DescribeAccountAttributesResponse response =
 rdsClient.describeAccountAttributes();
            List<AccountQuota> quotasList = response.accountQuotas();
            for (AccountQuota quotas : quotasList) {
                System.out.println("Name is: " + quotas.accountQuotaName());
                System.out.println("Max value is " + quotas.max());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeAccountAttributes en la Referencia de la API de AWS SDK for Java 2.x.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun getAccountAttributes() {
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response =
 rdsClient.describeAccountAttributes(DescribeAccountAttributesRequest {})
        response.accountQuotas?.forEach { quotas ->
            val response = response.accountQuotas
            println("Name is: ${quotas.accountQuotaName}")
            println("Max value is ${quotas.max}")
        }
    }
}
```

- Para obtener información acerca de la API, consulte DescribeAccountAttributes en la Referencia de la API del SDK de AWS para Kotlin.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeDBEngineVersions`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDBEngineVersions`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Get a list of DB engine versions for a particular DB engine.
    /// </summary>
    /// <param name="engine">Name of the engine.</param>
    /// <param name="dbParameterGroupFamily">Optional parameter group family
name.</param>
    /// <returns>List of DBEngineVersions.</returns>
    public async Task<List<DBEngineVersion>> DescribeDBEngineVersions(string
engine,
        string dbParameterGroupFamily = null)
    {
        var response = await _amazonRDS.DescribeDBEngineVersionsAsync(
            new DescribeDBEngineVersionsRequest()
            {
                Engine = engine,
                DBParameterGroupFamily = dbParameterGroupFamily
            });
        return response.DBEngineVersions;
    }
```

- Para obtener información sobre la API, consulte DescribeDBEngineVersions en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets available DB engine versions for an engine name and
//! an optional parameter group family.
/*!
 \sa getDBEngineVersions()
 \param engineName: A DB engine name.
 \param parameterGroupFamily: A parameter group family name, ignored if empty.
 \param engineVersionsResult: Vector of 'DBEngineVersion' objects returned by the
 routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::getDBEngineVersions(const Aws::String &engineName,
                                      const Aws::String &parameterGroupFamily,

 Aws::Vector<Aws::RDS::Model::DBEngineVersion> &engineVersionsResult,
                                      const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBEngineVersionsRequest request;
    request.SetEngine(engineName);
    if (!parameterGroupFamily.empty()) {
        request.SetDBParameterGroupFamily(parameterGroupFamily);
    }

    engineVersionsResult.clear();
    Aws::String marker; // Used for pagination.
```

```
    do {
        if (!marker.empty()) {
            request.SetMarker(marker);
        }


        Aws::RDS::Model::DescribeDBEngineVersionsOutcome outcome =
                client.DescribeDBEngineVersions(request);

        if (outcome.IsSuccess()) {
            auto &engineVersions = outcome.GetResult().GetDBEngineVersions();
            engineVersionsResult.insert(engineVersionsResult.end(),
 engineVersions.begin(),
                                        engineVersions.end());
            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with RDS::DescribeDBEngineVersionsRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }

    } while (!marker.empty());


    return true;
}
```

- Para obtener información sobre la API, consulte DescribeDBEngineVersions en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Descripción de las versiones del motor de base de datos para el motor de base de datos MySQL

El siguiente ejemplo `describe-db-engine-versions` se muestran detalles sobre cada una de las versiones del motor de base de datos especificado.

```
aws rds describe-db-engine-versions \
    --engine mysql
```

Salida:

```
{
    "DBEngineVersions": [
        {
            "Engine": "mysql",
            "EngineVersion": "5.5.46",
            "DBParameterGroupFamily": "mysql5.5",
            "DBEngineDescription": "MySQL Community Edition",
            "DBEngineVersionDescription": "MySQL 5.5.46",
            "ValidUpgradeTarget": [
                {
                    "Engine": "mysql",
                    "EngineVersion": "5.5.53",
                    "Description": "MySQL 5.5.53",
                    "AutoUpgrade": false,
                    "IsMajorVersionUpgrade": false
                },
                {
                    "Engine": "mysql",
                    "EngineVersion": "5.5.54",
                    "Description": "MySQL 5.5.54",
                    "AutoUpgrade": false,
                    "IsMajorVersionUpgrade": false
                },
                {
                    "Engine": "mysql",
                    "EngineVersion": "5.5.57",
                    "Description": "MySQL 5.5.57",
                    "AutoUpgrade": false,
                    "IsMajorVersionUpgrade": false
                },
                ...some output truncated...
            ]
        }
```

Para obtener más información acerca de Amazon RDS, consulte ¿Qué es Amazon Relational Database Service (Amazon RDS)? en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBEngineVersions en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// GetEngineVersions gets database engine versions that are available for the
 specified engine
// and parameter group family.
func (instances *DbInstances) GetEngineVersions(engine string,
 parameterGroupFamily string) (
 []types.DBEngineVersion, error) {
 output, err := instances.RdsClient.DescribeDBEngineVersions(context.TODO(),
  &rds.DescribeDBEngineVersionsInput{
   Engine:                 aws.String(engine),
   DBParameterGroupFamily: aws.String(parameterGroupFamily),
  })
 if err != nil {
  log.Printf("Couldn't get engine versions for %v: %v\n", engine, err)
  return nil, err
 } else {
  return output.DBEngineVersions, nil
 }
}
```

- Para obtener información sobre la API, consulte DescribeDBEngineVersions en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void describeDBEngines(RdsClient rdsClient) {
       try {
           DescribeDbEngineVersionsRequest engineVersionsRequest =
DescribeDbEngineVersionsRequest.builder()
                   .defaultOnly(true)
                   .engine("mysql")
                   .maxRecords(20)
                   .build();

           DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(engineVersionsRequest);
           List<DBEngineVersion> engines = response.dbEngineVersions();

           // Get all DBEngineVersion objects.
           for (DBEngineVersion engineOb : engines) {
               System.out.println("The name of the DB parameter group family for
the database engine is "
                       + engineOb.dbParameterGroupFamily());
               System.out.println("The name of the database engine " +
engineOb.engine());
               System.out.println("The version number of the database engine " +
engineOb.engineVersion());
           }

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
```

```
    }
```

- Para obtener información sobre la API, consulte DescribeDBEngineVersions en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_engine_versions(self, engine, parameter_group_family=None):
        """
        Gets database engine versions that are available for the specified engine
        and parameter group family.

        :param engine: The database engine to look up.
```

```
        :param parameter_group_family: When specified, restricts the returned
list of
                                       engine versions to those that are
compatible with
                                       this parameter group family.
        :return: The list of database engine versions.
        """
        try:
            kwargs = {"Engine": engine}
            if parameter_group_family is not None:
                kwargs["DBParameterGroupFamily"] = parameter_group_family
            response = self.rds_client.describe_db_engine_versions(**kwargs)
            versions = response["DBEngineVersions"]
        except ClientError as err:
            logger.error(
                "Couldn't get engine versions for %s. Here's why: %s: %s",
                engine,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return versions
```

- Para obtener detalles sobre la API, consulte DescribeDBEngineVersions en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeDBInstances`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDBInstances`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Returns a list of DB instances.
    /// </summary>
    /// <param name="dbInstanceIdentifier">Optional name of a specific DB
instance.</param>
    /// <returns>List of DB instances.</returns>
    public async Task<List<DBInstance>> DescribeDBInstances(string
dbInstanceIdentifier = null)
    {
        var results = new List<DBInstance>();
        var instancesPaginator = _amazonRDS.Paginators.DescribeDBInstances(
            new DescribeDBInstancesRequest
            {
                DBInstanceIdentifier = dbInstanceIdentifier
            });
        // Get the entire list using the paginator.
        await foreach (var instances in instancesPaginator.DBInstances)
        {
            results.Add(instances);
        }
        return results;
    }
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets a DB instance description.
/*!
 \sa describeDBInstance()
 \param dbInstanceIdentifier: A DB instance identifier.
 \param instanceResult: The 'DBInstance' object containing the description.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::describeDBInstance(const Aws::String &dbInstanceIdentifier,
                                     Aws::RDS::Model::DBInstance &instanceResult,
                                     const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBInstancesRequest request;
    request.SetDBInstanceIdentifier(dbInstanceIdentifier);

    Aws::RDS::Model::DescribeDBInstancesOutcome outcome =
            client.DescribeDBInstances(request);

    bool result = true;
    if (outcome.IsSuccess()) {
        instanceResult = outcome.GetResult().GetDBInstances()[0];
    }
    else if (outcome.GetError().GetErrorType() !=
             Aws::RDS::RDSErrors::D_B_INSTANCE_NOT_FOUND_FAULT) {
        result = false;
        std::cerr << "Error with RDS::DescribeDBInstances. "
```

```
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
        // This example does not log an error if the DB instance does not exist.
        // Instead, instanceResult is set to empty.
    else {
        instanceResult = Aws::RDS::Model::DBInstance();
    }

    return result;
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Descripción de una instancia de base de datos

En siguiente ejemplo `describe-db-instances`, se recuperan los detalles sobre la instancia de base de datos especificada.

```
aws rds describe-db-instances \
    --db-instance-identifier mydbinstancecf
```

Salida:

```
{
    "DBInstances": [
        {
            "DBInstanceIdentifier": "mydbinstancecf",
            "DBInstanceClass": "db.t3.small",
            "Engine": "mysql",
            "DBInstanceStatus": "available",
            "MasterUsername": "masterawsuser",
            "Endpoint": {
                "Address": "mydbinstancecf.abcexample.us-
east-1.rds.amazonaws.com",
                "Port": 3306,
```

```
                "HostedZoneId": "Z2R2ITUGPM61AM"
            },
            ...some output truncated...
        }
    ]
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// GetInstance gets data about a DB instance.
func (instances *DbInstances) GetInstance(instanceName string) (
 *types.DBInstance, error) {
 output, err := instances.RdsClient.DescribeDBInstances(context.TODO(),
  &rds.DescribeDBInstancesInput{
   DBInstanceIdentifier: aws.String(instanceName),
  })
 if err != nil {
  var notFoundError *types.DBInstanceNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("DB instance %v does not exist.\n", instanceName)
   err = nil
  } else {
   log.Printf("Couldn't get instance %v: %v\n", instanceName, err)
```

```
  }
  return nil, err
 } else {
  return &output.DBInstances[0], nil
 }
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.DescribeDbInstancesResponse;
import software.amazon.awssdk.services.rds.model.DBInstance;
import software.amazon.awssdk.services.rds.model.RdsException;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class DescribeDBInstances {

    public static void main(String[] args) {
```

```
        Region region = Region.US_EAST_1;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        describeInstances(rdsClient);
        rdsClient.close();
    }

    public static void describeInstances(RdsClient rdsClient) {
        try {
            DescribeDbInstancesResponse response =
 rdsClient.describeDBInstances();
            List<DBInstance> instanceList = response.dbInstances();
            for (DBInstance instance : instanceList) {
                System.out.println("Instance ARN is: " +
 instance.dbInstanceArn());
                System.out.println("The Engine is " + instance.engine());
                System.out.println("Connection endpoint is" +
 instance.endpoint().address());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK for Java 2.x.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun describeInstances() {
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbInstances(DescribeDbInstancesRequest
 {})
        response.dbInstances?.forEach { instance ->
            println("Instance Identifier is ${instance.dbInstanceIdentifier}")
            println("The Engine is ${instance.engine}")
            println("Connection endpoint is ${instance.endpoint?.address}")
        }
    }
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Kotlin.

PHP

SDK para PHP

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require __DIR__ . '/vendor/autoload.php';

use Aws\Exception\AwsException;


//Create an RDSClient
$rdsClient = new Aws\Rds\RdsClient([
    'region' => 'us-east-2'
]);

try {
    $result = $rdsClient->describeDBInstances();
    foreach ($result['DBInstances'] as $instance) {
        print('<p>DB Identifier: ' . $instance['DBInstanceIdentifier']);
```

```
        print('<br />Endpoint: ' . $instance['Endpoint']["Address"]
            . ':' . $instance['Endpoint']["Port"]);
        print('<br />Current Status: ' . $instance["DBInstanceStatus"]);
        print('</p>');
    }
    print(" Raw Result ");
    var_dump($result);
} catch (AwsException $e) {
    echo $e->getMessage();
    echo "\n";
}
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para PHP.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
```

```
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_db_instance(self, instance_id):
        """
        Gets data about a DB instance.

        :param instance_id: The ID of the DB instance to retrieve.
        :return: The retrieved DB instance.
        """
        try:
            response = self.rds_client.describe_db_instances(
                DBInstanceIdentifier=instance_id
            )
            db_inst = response["DBInstances"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBInstanceNotFound":
                logger.info("Instance %s does not exist.", instance_id)
            else:
                logger.error(
                    "Couldn't get DB instance %s. Here's why: %s: %s",
                    instance_id,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return db_inst
```

- Para obtener información sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-rds"  # v2: require 'aws-sdk'

# List all Amazon Relational Database Service (Amazon RDS) DB instances.
#
# @param rds_resource [Aws::RDS::Resource] An SDK for Ruby Amazon RDS resource.
# @return [Array, nil] List of all DB instances, or nil if error.
def list_instances(rds_resource)
  db_instances = []
  rds_resource.db_instances.each do |i|
    db_instances.append({
                          "name": i.id,
                          "status": i.db_instance_status
                        })
  end
  db_instances
rescue Aws::Errors::ServiceError => e
  puts "Couldn't list instances:\n#{e.message}"
end
```

- Para obtener detalles sobre la API, consulte DescribeDBInstances en la Referencia de la API de AWS SDK para Ruby.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeDBParameterGroups`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDBParameterGroups`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Get descriptions of DB parameter groups.
    /// </summary>
    /// <param name="name">Optional name of the DB parameter group to describe.</
param>
    /// <returns>The list of DB parameter group descriptions.</returns>
    public async Task<List<DBParameterGroup>> DescribeDBParameterGroups(string
 name = null)
    {
        var response = await _amazonRDS.DescribeDBParameterGroupsAsync(
            new DescribeDBParameterGroupsRequest()
            {
                DBParameterGroupName = name
            });
        return response.DBParameterGroups;
    }
```

- Para obtener información sobre la API, consulte DescribeDBParameterGroups en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::DescribeDBParameterGroupsRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);

        Aws::RDS::Model::DescribeDBParameterGroupsOutcome outcome =
                client.DescribeDBParameterGroups(request);

        if (outcome.IsSuccess()) {
            std::cout << "DB parameter group named '" <<
                      PARAMETER_GROUP_NAME << "' already exists." << std::endl;
            dbParameterGroupFamily = outcome.GetResult().GetDBParameterGroups()
[0].GetDBParameterGroupFamily();
        }

        else {
            std::cerr << "Error with RDS::DescribeDBParameterGroups. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
```

- Para obtener información sobre la API, consulte DescribeDBParameterGroups en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Descripción del grupo de parámetros de base de datos

En el siguiente ejemplo `describe-db-parameter-groups`, se recuperan los detalles sobre los grupos de parámetros de base de datos.

```
aws rds describe-db-parameter-groups
```

Salida:

```
{
    "DBParameterGroups": [
        {
            "DBParameterGroupName": "default.aurora-mysql5.7",
            "DBParameterGroupFamily": "aurora-mysql5.7",
            "Description": "Default parameter group for aurora-mysql5.7",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.aurora-mysql5.7"
        },
        {
            "DBParameterGroupName": "default.aurora-postgresql9.6",
            "DBParameterGroupFamily": "aurora-postgresql9.6",
            "Description": "Default parameter group for aurora-postgresql9.6",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.aurora-postgresql9.6"
        },
        {
            "DBParameterGroupName": "default.aurora5.6",
            "DBParameterGroupFamily": "aurora5.6",
            "Description": "Default parameter group for aurora5.6",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.aurora5.6"
        },
        {
            "DBParameterGroupName": "default.mariadb10.1",
            "DBParameterGroupFamily": "mariadb10.1",
            "Description": "Default parameter group for mariadb10.1",
            "DBParameterGroupArn": "arn:aws:rds:us-
east-1:123456789012:pg:default.mariadb10.1"
        },
```

```
        ...some output truncated...
    ]
}
```

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBParameterGroups en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// GetParameterGroup gets a DB parameter group by name.
func (instances *DbInstances) GetParameterGroup(parameterGroupName string) (
 *types.DBParameterGroup, error) {
 output, err := instances.RdsClient.DescribeDBParameterGroups(
  context.TODO(), &rds.DescribeDBParameterGroupsInput{
   DBParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  var notFoundError *types.DBParameterGroupNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("Parameter group %v does not exist.\n", parameterGroupName)
   err = nil
  } else {
   log.Printf("Error getting parameter group %v: %v\n", parameterGroupName, err)
  }
```

```
  return nil, err
 } else {
  return &output.DBParameterGroups[0], err
 }
}
```

- Para obtener información sobre la API, consulte DescribeDBParameterGroups en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   public static void describeDbParameterGroups(RdsClient rdsClient, String
dbGroupName) {
       try {
           DescribeDbParameterGroupsRequest groupsRequest =
DescribeDbParameterGroupsRequest.builder()
                   .dbParameterGroupName(dbGroupName)
                   .maxRecords(20)
                   .build();

           DescribeDbParameterGroupsResponse response =
rdsClient.describeDBParameterGroups(groupsRequest);
           List<DBParameterGroup> groups = response.dbParameterGroups();
           for (DBParameterGroup group : groups) {
               System.out.println("The group name is " +
group.dbParameterGroupName());
               System.out.println("The group description is " +
group.description());
           }

       } catch (RdsException e) {
```

```
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte DescribeDBParameterGroups en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_parameter_group(self, parameter_group_name):
        """
        Gets a DB parameter group.
```

```
        :param parameter_group_name: The name of the parameter group to retrieve.
        :return: The parameter group.
        """
        try:
            response = self.rds_client.describe_db_parameter_groups(
                DBParameterGroupName=parameter_group_name
            )
            parameter_group = response["DBParameterGroups"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBParameterGroupNotFound":
                logger.info("Parameter group %s does not exist.",
parameter_group_name)
            else:
                logger.error(
                    "Couldn't get parameter group %s. Here's why: %s: %s",
                    parameter_group_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return parameter_group
```

- Para obtener información sobre las API, consulte DescribeDBParameterGroups en la Referencia de la API de AWS para Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-rds"  # v2: require 'aws-sdk'

# List all Amazon Relational Database Service (Amazon RDS) parameter groups.
```

```
#
# @param rds_resource [Aws::RDS::Resource] An SDK for Ruby Amazon RDS resource.
# @return [Array, nil] List of all parameter groups, or nil if error.
def list_parameter_groups(rds_resource)
  parameter_groups = []
  rds_resource.db_parameter_groups.each do |p|
    parameter_groups.append({
                              "name": p.db_parameter_group_name,
                              "description": p.description
                            })
  end
  parameter_groups
rescue Aws::Errors::ServiceError => e
  puts "Couldn't list parameter groups:\n #{e.message}"
end
```

- Para obtener información acerca de la API, consulte DescribeDBParameterGroups en la Referencia de la API de AWS SDK para Ruby.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeDBParameters`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDBParameters`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Get a list of DB parameters from a specific parameter group.
    /// </summary>
    /// <param name="dbParameterGroupName">Name of a specific DB parameter
group.</param>
    /// <param name="source">Optional source for selecting parameters.</param>
    /// <returns>List of parameter values.</returns>
    public async Task<List<Parameter>> DescribeDBParameters(string
dbParameterGroupName, string source = null)
    {
        var results = new List<Parameter>();
        var paginateParameters = _amazonRDS.Paginators.DescribeDBParameters(
            new DescribeDBParametersRequest()
            {
                DBParameterGroupName = dbParameterGroupName,
                Source = source
            });
        // Get the entire list using the paginator.
        await foreach (var parameters in paginateParameters.Parameters)
        {
            results.Add(parameters);
        }
        return results;
    }
```

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets DB parameters using the 'DescribeDBParameters' api.
/*!
 \sa getDBParameters()
 \param parameterGroupName: The name of the parameter group.
 \param namePrefix: Prefix string to filter results by parameter name.
 \param source: A source such as 'user', ignored if empty.
 \param parametersResult: Vector of 'Parameter' objects returned by the routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::getDBParameters(const Aws::String &parameterGroupName,
                                  const Aws::String &namePrefix,
                                  const Aws::String &source,
                                  Aws::Vector<Aws::RDS::Model::Parameter>
 &parametersResult,
                                  const Aws::RDS::RDSClient &client) {
    Aws::String marker;
    do {
        Aws::RDS::Model::DescribeDBParametersRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }
        if (!source.empty()) {
            request.SetSource(source);
```

```
        }

        Aws::RDS::Model::DescribeDBParametersOutcome outcome =
                client.DescribeDBParameters(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::Parameter> &parameters =
                    outcome.GetResult().GetParameters();
            for (const Aws::RDS::Model::Parameter &parameter: parameters) {
                if (!namePrefix.empty()) {
                    if (parameter.GetParameterName().find(namePrefix) == 0) {
                        parametersResult.push_back(parameter);
                    }
                }
                else {
                    parametersResult.push_back(parameter);
                }
            }

            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with RDS::DescribeDBParameters. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    return true;
}
```

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Descripción de los parámetros de un grupo de parámetros de base de datos

En el siguiente ejemplo `describe-db-parameters`, se recuperan los detalles del grupo de parámetros de base de datos especificado.

```
aws rds describe-db-parameters \
    --db-parameter-group-name mydbpg
```

Salida:

```
{
    "Parameters": [
        {
            "ParameterName": "allow-suspicious-udfs",
            "Description": "Controls whether user-defined functions that have
 only an xxx symbol for the main function can be loaded",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot"
        },
        {
            "ParameterName": "auto_generate_certs",
            "Description": "Controls whether the server autogenerates SSL key and
 certificate files in the data directory, if they do not already exist.",
            "Source": "engine-default",
            "ApplyType": "static",
            "DataType": "boolean",
            "AllowedValues": "0,1",
            "IsModifiable": false,
            "ApplyMethod": "pending-reboot"
        },
        ...some output truncated...
    ]
}
```

Para obtener más información, consulte Trabajo con los grupos de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// GetParameters gets the parameters that are contained in a DB parameter group.
func (instances *DbInstances) GetParameters(parameterGroupName string, source
 string) (
 []types.Parameter, error) {

 var output *rds.DescribeDBParametersOutput
 var params []types.Parameter
 var err error
 parameterPaginator := rds.NewDescribeDBParametersPaginator(instances.RdsClient,
  &rds.DescribeDBParametersInput{
   DBParameterGroupName: aws.String(parameterGroupName),
   Source:               aws.String(source),
  })
 for parameterPaginator.HasMorePages() {
  output, err = parameterPaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get parameters for %v: %v\n", parameterGroupName, err)
   break
  } else {
   params = append(params, output.Parameters...)
  }
 }
 return params, err
}
```

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   // Retrieve parameters in the group.
   public static void describeDbParameters(RdsClient rdsClient, String
dbGroupName, int flag) {
       try {
           DescribeDbParametersRequest dbParameterGroupsRequest;
           if (flag == 0) {
               dbParameterGroupsRequest = DescribeDbParametersRequest.builder()
                       .dbParameterGroupName(dbGroupName)
                       .build();
           } else {
               dbParameterGroupsRequest = DescribeDbParametersRequest.builder()
                       .dbParameterGroupName(dbGroupName)
                       .source("user")
                       .build();
           }

           DescribeDbParametersResponse response =
rdsClient.describeDBParameters(dbParameterGroupsRequest);
           List<Parameter> dbParameters = response.parameters();
           String paraName;
           for (Parameter para : dbParameters) {
               // Only print out information about either auto_increment_offset
or
               // auto_increment_increment.
               paraName = para.parameterName();
               if ((paraName.compareTo("auto_increment_offset") == 0)
```

```
                        || (paraName.compareTo("auto_increment_increment ") ==
0)) {
                    System.out.println("*** The parameter name is  " + paraName);
                    System.out.println("*** The parameter value is  " +
para.parameterValue());
                    System.out.println("*** The parameter data type is " +
para.dataType());
                    System.out.println("*** The parameter description is " +
para.description());
                    System.out.println("*** The parameter allowed values  is " +
para.allowedValues());
                }
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
```

```
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_parameters(self, parameter_group_name, name_prefix="", source=None):
        """
        Gets the parameters that are contained in a DB parameter group.

        :param parameter_group_name: The name of the parameter group to query.
        :param name_prefix: When specified, the retrieved list of parameters is
filtered
                            to contain only parameters that start with this
prefix.
        :param source: When specified, only parameters from this source are
retrieved.
                       For example, a source of 'user' retrieves only parameters
that
                       were set by a user.
        :return: The list of requested parameters.
        """
        try:
            kwargs = {"DBParameterGroupName": parameter_group_name}
            if source is not None:
                kwargs["Source"] = source
            parameters = []
            paginator = self.rds_client.get_paginator("describe_db_parameters")
            for page in paginator.paginate(**kwargs):
                parameters += [
                    p
                    for p in page["Parameters"]
                    if p["ParameterName"].startswith(name_prefix)
                ]
        except ClientError as err:
            logger.error(
                "Couldn't get parameters for %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
```

```
                err.response["Error"]["Message"],
            )
            raise
        else:
            return parameters
```

- Para obtener información sobre la API, consulte DescribeDBParameters en la Referencia de la API de AWS SDK para Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-rds"  # v2: require 'aws-sdk'

# List all Amazon Relational Database Service (Amazon RDS) parameter groups.
#
# @param rds_resource [Aws::RDS::Resource] An SDK for Ruby Amazon RDS resource.
# @return [Array, nil] List of all parameter groups, or nil if error.
def list_parameter_groups(rds_resource)
  parameter_groups = []
  rds_resource.db_parameter_groups.each do |p|
    parameter_groups.append({
                              "name": p.db_parameter_group_name,
                              "description": p.description
                            })
  end
  parameter_groups
rescue Aws::Errors::ServiceError => e
  puts "Couldn't list parameter groups:\n #{e.message}"
end
```

- Para obtener información acerca de la API, consulte DescribeDBParameters en la Referencia de la API de AWS SDK para Ruby.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeDBSnapshots`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeDBSnapshots`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   /// <summary>
   /// Return a list of DB snapshots for a particular DB instance.
   /// </summary>
   /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
   /// <returns>List of DB snapshots.</returns>
   public async Task<List<DBSnapshot>> DescribeDBSnapshots(string
dbInstanceIdentifier)
   {
       var results = new List<DBSnapshot>();
       var snapshotsPaginator = _amazonRDS.Paginators.DescribeDBSnapshots(
           new DescribeDBSnapshotsRequest()
           {
```

```
                DBInstanceIdentifier = dbInstanceIdentifier
            });

        // Get the entire list using the paginator.
        await foreach (var snapshots in snapshotsPaginator.DBSnapshots)
        {
            results.Add(snapshots);
        }
        return results;
    }
```

- Para obtener información sobre la API, consulte DescribeDBSnapshots en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

            Aws::RDS::Model::DescribeDBSnapshotsRequest request;
            request.SetDBSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::DescribeDBSnapshotsOutcome outcome =
                    client.DescribeDBSnapshots(request);

            if (outcome.IsSuccess()) {
                snapshot = outcome.GetResult().GetDBSnapshots()[0];
            }
```

```
            else {
                std::cerr << "Error with RDS::DescribeDBSnapshots. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
 client);
                return false;
            }
```

- Para obtener información sobre la API, consulte DescribeDBSnapshots en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Ejemplo 1: Descripción de una instantánea de base de datos para una instancia de base de datos

En el siguiente ejemplo `describe-db-snapshots`, se recuperan los detalles de una instantánea de base de datos de una instancia de base de datos.

```
aws rds describe-db-snapshots \
    --db-snapshot-identifier mydbsnapshot
```

Salida:

```
{
    "DBSnapshots": [
        {
            "DBSnapshotIdentifier": "mydbsnapshot",
            "DBInstanceIdentifier": "mysqldb",
            "SnapshotCreateTime": "2018-02-08T22:28:08.598Z",
            "Engine": "mysql",
            "AllocatedStorage": 20,
            "Status": "available",
            "Port": 3306,
            "AvailabilityZone": "us-east-1f",
            "VpcId": "vpc-6594f31c",
            "InstanceCreateTime": "2018-02-08T22:24:55.973Z",
```

```
            "MasterUsername": "mysqladmin",
            "EngineVersion": "5.6.37",
            "LicenseModel": "general-public-license",
            "SnapshotType": "manual",
            "OptionGroupName": "default:mysql-5-6",
            "PercentProgress": 100,
            "StorageType": "gp2",
            "Encrypted": false,
            "DBSnapshotArn": "arn:aws:rds:us-
east-1:123456789012:snapshot:mydbsnapshot",
            "IAMDatabaseAuthenticationEnabled": false,
            "ProcessorFeatures": [],
            "DbiResourceId": "db-AKIAIOSFODNN7EXAMPLE"
        }
    ]
}
```

Para obtener más información, consulte Creación de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

Ejemplo 2: Búsqueda del número de instantáneas manuales realizadas

En el siguiente ejemplo de `describe-db-snapshots` se utiliza el operador `length` como opción `--query` para devolver el número de instantáneas manuales que se han realizado en una región concreta de AWS.

```
aws rds describe-db-snapshots \
    --snapshot-type manual \
    --query "length(*[].{DBSnapshots:SnapshotType})" \
    --region eu-central-1
```

Salida:

```
35
```

Para obtener más información, consulte Creación de una instantánea de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte DescribeDBSnapshots en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// GetSnapshot gets a DB instance snapshot.
func (instances *DbInstances) GetSnapshot(snapshotName string)
 (*types.DBSnapshot, error) {
 output, err := instances.RdsClient.DescribeDBSnapshots(context.TODO(),
  &rds.DescribeDBSnapshotsInput{
   DBSnapshotIdentifier: aws.String(snapshotName),
  })
 if err != nil {
  log.Printf("Couldn't get snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return &output.DBSnapshots[0], nil
 }
}
```

- Para obtener información sobre la API, consulte DescribeDBSnapshots en la Referencia de la API de AWS SDK para Go.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_snapshot(self, snapshot_id):
        """
        Gets a DB instance snapshot.

        :param snapshot_id: The ID of the snapshot to retrieve.
        :return: The retrieved snapshot.
        """
        try:
            response = self.rds_client.describe_db_snapshots(
                DBSnapshotIdentifier=snapshot_id
            )
            snapshot = response["DBSnapshots"][0]
        except ClientError as err:
            logger.error(
```

```
                "Couldn't get snapshot %s. Here's why: %s: %s",
                snapshot_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot
```

- Para obtener información sobre la API, consulte DescribeDBSnapshots en la Referencia de la API de AWS SDK para Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-rds" # v2: require 'aws-sdk'

# List all Amazon Relational Database Service (Amazon RDS) DB instance
# snapshots.
#
# @param rds_resource [Aws::RDS::Resource] An SDK for Ruby Amazon RDS resource.
# @return instance_snapshots [Array, nil] All instance snapshots, or nil if
 error.
def list_instance_snapshots(rds_resource)
  instance_snapshots = []
  rds_resource.db_snapshots.each do |s|
    instance_snapshots.append({
                                "id": s.snapshot_id,
                                "status": s.status
                              })
  end
  instance_snapshots
```

```
rescue Aws::Errors::ServiceError => e
  puts "Couldn't list instance snapshots:\n #{e.message}"
end
```

- Para obtener detalles sobre la API, consulte DescribeDBSnapshots en la Referencia de la API de AWS SDK para Ruby.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`DescribeOrderableDBInstanceOptions`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `DescribeOrderableDBInstanceOptions`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/// <summary>
/// Get a list of orderable DB instance options for a specific
/// engine and engine version.
/// </summary>
```

```
    /// <param name="engine">Name of the engine.</param>
    /// <param name="engineVersion">Version of the engine.</param>
    /// <returns>List of OrderableDBInstanceOptions.</returns>
    public async Task<List<OrderableDBInstanceOption>>
DescribeOrderableDBInstanceOptions(string engine, string engineVersion)
    {
        // Use a paginator to get a list of DB instance options.
        var results = new List<OrderableDBInstanceOption>();
        var paginateInstanceOptions =
_amazonRDS.Paginators.DescribeOrderableDBInstanceOptions(
            new DescribeOrderableDBInstanceOptionsRequest()
            {
                Engine = engine,
                EngineVersion = engineVersion,
            });
        // Get the entire list using the paginator.
        await foreach (var instanceOptions in
paginateInstanceOptions.OrderableDBInstanceOptions)
        {
            results.Add(instanceOptions);
        }
        return results;
    }
```

- Para obtener información sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
```

```
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);


//! Routine which gets available 'micro' DB instance classes, displays the list
//! to the user, and returns the user selection.
/*!
 \sa chooseMicroDBInstanceClass()
 \param engineName: The DB engine name.
 \param engineVersion: The DB engine version.
 \param dbInstanceClass: String for DB instance class chosen by the user.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::chooseMicroDBInstanceClass(const Aws::String &engine,
                                             const Aws::String &engineVersion,
                                             Aws::String &dbInstanceClass,
                                             const Aws::RDS::RDSClient &client) {
    std::vector<Aws::String> instanceClasses;
    Aws::String marker;
    do {
        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsRequest request;
        request.SetEngine(engine);
        request.SetEngineVersion(engineVersion);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsOutcome outcome =
                client.DescribeOrderableDBInstanceOptions(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::OrderableDBInstanceOption>
 &options =
                    outcome.GetResult().GetOrderableDBInstanceOptions();
            for (const Aws::RDS::Model::OrderableDBInstanceOption &option:
 options) {
                const Aws::String &instanceClass = option.GetDBInstanceClass();
                if (instanceClass.find("micro") != std::string::npos) {
                    if (std::find(instanceClasses.begin(), instanceClasses.end(),
                                  instanceClass) ==
                        instanceClasses.end()) {
                        instanceClasses.push_back(instanceClass);
```

```
                    }
                }
            }
            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with RDS::DescribeOrderableDBInstanceOptions. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    std::cout << "The available micro DB instance classes for your database
 engine are:"
              << std::endl;
    for (int i = 0; i < instanceClasses.size(); ++i) {
        std::cout << "   " << i + 1 << ": " << instanceClasses[i] << std::endl;
    }

    int choice = askQuestionForIntRange(
            "Which micro DB instance class do you want to use? ",
            1, static_cast<int>(instanceClasses.size()));
    dbInstanceClass = instanceClasses[choice - 1];
    return true;
}
```

- Para obtener información sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Descripción de las opciones de instancias de base de datos ordenables

En el siguiente ejemplo `describe-orderable-db-instance-options`, se recuperan detalles sobre las opciones ordenables de una instancia de base de datos que ejecuta el motor de base de datos MySQL.

```
aws rds describe-orderable-db-instance-options \
```

```
    --engine mysql
```

Salida:

```
{
    "OrderableDBInstanceOptions": [
        {
            "MinStorageSize": 5,
            "ReadReplicaCapable": true,
            "MaxStorageSize": 6144,
            "AvailabilityZones": [
                {
                    "Name": "us-east-1a"
                },
                {
                    "Name": "us-east-1b"
                },
                {
                    "Name": "us-east-1c"
                },
                {
                    "Name": "us-east-1d"
                }
            ],
            "SupportsIops": false,
            "AvailableProcessorFeatures": [],
            "MultiAZCapable": true,
            "DBInstanceClass": "db.m1.large",
            "Vpc": true,
            "StorageType": "gp2",
            "LicenseModel": "general-public-license",
            "EngineVersion": "5.5.46",
            "SupportsStorageEncryption": false,
            "SupportsEnhancedMonitoring": true,
            "Engine": "mysql",
            "SupportsIAMDatabaseAuthentication": false,
            "SupportsPerformanceInsights": false
        }
    ]
    ...some output truncated...
}
```

- Para obtener información sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// GetOrderableInstances uses a paginator to get DB instance options that can be
 used to create DB instances that are
// compatible with a set of specifications.
func (instances *DbInstances) GetOrderableInstances(engine string, engineVersion
 string) (
 []types.OrderableDBInstanceOption, error) {

 var output *rds.DescribeOrderableDBInstanceOptionsOutput
 var instanceOptions []types.OrderableDBInstanceOption
 var err error
 orderablePaginator :=
 rds.NewDescribeOrderableDBInstanceOptionsPaginator(instances.RdsClient,
  &rds.DescribeOrderableDBInstanceOptionsInput{
   Engine:        aws.String(engine),
   EngineVersion: aws.String(engineVersion),
  })
 for orderablePaginator.HasMorePages() {
  output, err = orderablePaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get orderable DB instance options: %v\n", err)
   break
```

```
  } else {
   instanceOptions = append(instanceOptions,
 output.OrderableDBInstanceOptions...)
  }
 }
 return instanceOptions, err
}
```

- Para obtener información sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   // Get a list of allowed engine versions.
   public static void getAllowedEngines(RdsClient rdsClient, String
dbParameterGroupFamily) {
       try {
           DescribeDbEngineVersionsRequest versionsRequest =
DescribeDbEngineVersionsRequest.builder()
                   .dbParameterGroupFamily(dbParameterGroupFamily)
                   .engine("mysql")
                   .build();

           DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(versionsRequest);
           List<DBEngineVersion> dbEngines = response.dbEngineVersions();
           for (DBEngineVersion dbEngine : dbEngines) {
               System.out.println("The engine version is " +
dbEngine.engineVersion());
               System.out.println("The engine description is " +
dbEngine.dbEngineDescription());
```

```
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- Para obtener información sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_orderable_instances(self, db_engine, db_engine_version):
```

```
        """
        Gets DB instance options that can be used to create DB instances that are
        compatible with a set of specifications.

        :param db_engine: The database engine that must be supported by the DB
instance.
        :param db_engine_version: The engine version that must be supported by
the DB instance.
        :return: The list of DB instance options that can be used to create a
compatible DB instance.
        """
        try:
            inst_opts = []
            paginator = self.rds_client.get_paginator(
                "describe_orderable_db_instance_options"
            )
            for page in paginator.paginate(
                Engine=db_engine, EngineVersion=db_engine_version
            ):
                inst_opts += page["OrderableDBInstanceOptions"]
        except ClientError as err:
            logger.error(
                "Couldn't get orderable DB instances. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return inst_opts
```

- Para obtener detalles sobre la API, consulte DescribeOrderableDBInstanceOptions en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`GenerateRDSAuthToken`** con un AWS SDK o la CLI

En el siguiente ejemplo de código, se muestra cómo usar `GenerateRDSAuthToken`.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Utilice la clase RdsUtilities para generar un token de autenticación.

```
public class GenerateRDSAuthToken {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <dbInstanceIdentifier> <masterUsername>

                Where:
                    dbInstanceIdentifier - The database instance identifier.\s
                    masterUsername - The master user name.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String dbInstanceIdentifier = args[0];
        String masterUsername = args[1];
        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        String token = getAuthToken(rdsClient, dbInstanceIdentifier,
 masterUsername);
        System.out.println("The token response is " + token);
    }

    public static String getAuthToken(RdsClient rdsClient, String
 dbInstanceIdentifier, String masterUsername) {
```

```
        RdsUtilities utilities = rdsClient.utilities();
        try {
            GenerateAuthenticationTokenRequest tokenRequest =
 GenerateAuthenticationTokenRequest.builder()
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .username(masterUsername)
                    .port(3306)
                    .hostname(dbInstanceIdentifier)
                    .build();

            return utilities.generateAuthenticationToken(tokenRequest);

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- Para obtener información acerca de la API, consulte GenerateRDSAuthToken en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`ModifyDBInstance`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `ModifyDBInstance`.

CLI

AWS CLI

Ejemplo 1: para modificar una instancia de base de datos

En el siguiente ejemplo de `modify-db-instance` se asocia un grupo de opciones y un grupo de parámetros a una instancia de base de datos de Microsoft SQL Server compatible.

El parámetro `--apply-immediately` hace que los grupos de opciones y parámetros se asocien de inmediato, en lugar de esperar hasta el siguiente período de mantenimiento.

```
aws rds modify-db-instance \
    --db-instance-identifier database-2 \
    --option-group-name test-se-2017 \
    --db-parameter-group-name test-sqlserver-se-2017 \
    --apply-immediately
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "database-2",
        "DBInstanceClass": "db.r4.large",
        "Engine": "sqlserver-se",
        "DBInstanceStatus": "available",

        ...output omitted...

        "DBParameterGroups": [
            {
                "DBParameterGroupName": "test-sqlserver-se-2017",
                "ParameterApplyStatus": "applying"
            }
        ],
        "AvailabilityZone": "us-west-2d",

        ...output omitted...

        "MultiAZ": true,
        "EngineVersion": "14.00.3281.6.v1",
        "AutoMinorVersionUpgrade": false,
        "ReadReplicaDBInstanceIdentifiers": [],
        "LicenseModel": "license-included",
        "OptionGroupMemberships": [
            {
                "OptionGroupName": "test-se-2017",
                "Status": "pending-apply"
            }
        ],
        "CharacterSetName": "SQL_Latin1_General_CP1_CI_AS",
        "SecondaryAvailabilityZone": "us-west-2c",
```

```
        "PubliclyAccessible": true,
        "StorageType": "gp2",

        ...output omitted...

        "DeletionProtection": false,
        "AssociatedRoles": [],
        "MaxAllocatedStorage": 1000
    }
}
```

Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS.

Ejemplo 2: para asociar un grupo de seguridad VPC con una instancia de base de datos

El siguiente ejemplo de `modify-db-instance` asocia un grupo de seguridad de VPC específico y elimina los grupos de seguridad de base de datos de una instancia de base de datos:

```
aws rds modify-db-instance \
    --db-instance-identifier dbName \
    --vpc-security-group-ids sg-ID
```

Salida:

```
{
"DBInstance": {
    "DBInstanceIdentifier": "dbName",
    "DBInstanceClass": "db.t3.micro",
    "Engine": "mysql",
    "DBInstanceStatus": "available",
    "MasterUsername": "admin",
    "Endpoint": {
        "Address": "dbName.abcdefghijk.us-west-2.rds.amazonaws.com",
        "Port": 3306,
        "HostedZoneId": "ABCDEFGHIJK1234"
    },
    "AllocatedStorage": 20,
    "InstanceCreateTime": "2024-02-15T00:37:58.793000+00:00",
    "PreferredBackupWindow": "11:57-12:27",
    "BackupRetentionPeriod": 7,
    "DBSecurityGroups": [],
```

```
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-ID",
            "Status": "active"
        }
    ],
    ... output omitted ...
    "MultiAZ": false,
    "EngineVersion": "8.0.35",
    "AutoMinorVersionUpgrade": true,
    "ReadReplicaDBInstanceIdentifiers": [],
    "LicenseModel": "general-public-license",

    ... output ommited ...
    }
}
```

Para obtener más información, consulte Control de acceso con grupos de seguridad en la Guía de usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDBInstance en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.ModifyDbInstanceRequest;
import software.amazon.awssdk.services.rds.model.ModifyDbInstanceResponse;
import software.amazon.awssdk.services.rds.model.RdsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
```

```
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class ModifyDBInstance {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <dbInstanceIdentifier> <dbSnapshotIdentifier>\s
                Where:
                    dbInstanceIdentifier - The database instance identifier.\s
                    masterUserPassword - The updated password that corresponds to
 the master user name.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String dbInstanceIdentifier = args[0];
        String masterUserPassword = args[1];
        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        updateIntance(rdsClient, dbInstanceIdentifier, masterUserPassword);
        rdsClient.close();
    }

    public static void updateIntance(RdsClient rdsClient, String
 dbInstanceIdentifier, String masterUserPassword) {
        try {
            // For a demo - modify the DB instance by modifying the master
 password.
            ModifyDbInstanceRequest modifyDbInstanceRequest =
 ModifyDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .publiclyAccessible(true)
                    .masterUserPassword(masterUserPassword)
```

```
                    .build();

            ModifyDbInstanceResponse instanceResponse =
 rdsClient.modifyDBInstance(modifyDbInstanceRequest);
            System.out.print("The ARN of the modified database is: " +
 instanceResponse.dbInstance().dbInstanceArn());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener información sobre la API, consulte ModifyDBInstance en la Referencia de la API de AWS SDK for Java 2.x.

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
suspend fun updateIntance(
    dbInstanceIdentifierVal: String?,
    masterUserPasswordVal: String?,
) {
    val request =
        ModifyDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            publiclyAccessible = true
            masterUserPassword = masterUserPasswordVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val instanceResponse = rdsClient.modifyDbInstance(request)
```

```
        println("The ARN of the modified database is
 ${instanceResponse.dbInstance?.dbInstanceArn}")
    }
}
```

- Para obtener información acerca de la API, consulte ModifyDBInstance en la Referencia de la API del SDK de AWS para Kotlin.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **`ModifyDBParameterGroup`** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `ModifyDBParameterGroup`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Comience a utilizar instancias de base de datos

.NET

SDK para .NET

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    /// <summary>
    /// Update a DB parameter group. Use the action
DescribeDBParameterGroupsAsync
    /// to determine when the DB parameter group is ready to use.
    /// </summary>
    /// <param name="name">Name of the DB parameter group.</param>
```

```
    /// <param name="parameters">List of parameters. Maximum of 20 per request.</
param>
    /// <returns>The updated DB parameter group name.</returns>
    public async Task<string> ModifyDBParameterGroup(
        string name, List<Parameter> parameters)
    {
        var response = await _amazonRDS.ModifyDBParameterGroupAsync(
            new ModifyDBParameterGroupRequest()
            {
                DBParameterGroupName = name,
                Parameters = parameters,
            });
        return response.DBParameterGroupName;
    }
```

- Para obtener información sobre la API, consulte ModifyDBParameterGroup en la Referencia de la API de AWS SDK para .NET.

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::RDS::RDSClient client(clientConfig);

        Aws::RDS::Model::ModifyDBParameterGroupRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        request.SetParameters(updateParameters);

        Aws::RDS::Model::ModifyDBParameterGroupOutcome outcome =
```

```
                client.ModifyDBParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully modified."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::ModifyDBParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Para obtener información sobre la API, consulte ModifyDBParameterGroup en la Referencia de la API de AWS SDK para C++.

CLI

AWS CLI

Modificación de un grupo de parámetros de base de datos

En el siguiente ejemplo `modify-db-parameter-group`, se cambia el valor del parámetro `clr enabled` en un grupo de parámetros de base de datos. El parámetro `--apply-immediately` hace que el grupo de parámetros de la base de datos se modifique de inmediato, en lugar de esperar hasta el siguiente período de mantenimiento.

```
aws rds modify-db-parameter-group \
    --db-parameter-group-name test-sqlserver-se-2017 \
    --parameters "ParameterName='clr
 enabled',ParameterValue=1,ApplyMethod=immediate"
```

Salida:

```
{
    "DBParameterGroupName": "test-sqlserver-se-2017"
}
```

Para obtener más información, consulte Modificación de parámetros de un grupo de parámetros de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte ModifyDBParameterGroup en la Referencia de comandos de la AWS CLI.

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
type DbInstances struct {
 RdsClient *rds.Client
}



// UpdateParameters updates parameters in a named DB parameter group.
func (instances *DbInstances) UpdateParameters(parameterGroupName string, params
 []types.Parameter) error {
 _, err := instances.RdsClient.ModifyDBParameterGroup(context.TODO(),
  &rds.ModifyDBParameterGroupInput{
   DBParameterGroupName: aws.String(parameterGroupName),
   Parameters:           params,
  })
 if err != nil {
  log.Printf("Couldn't update parameters in %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}
```

- Para obtener información sobre la API, consulte ModifyDBParameterGroup en la Referencia de la API de AWS SDK para Go.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
   // Modify auto_increment_offset and auto_increment_increment parameters.
   public static void modifyDBParas(RdsClient rdsClient, String dbGroupName) {
       try {
           Parameter parameter1 = Parameter.builder()
                   .parameterName("auto_increment_offset")
                   .applyMethod("immediate")
                   .parameterValue("5")
                   .build();

           List<Parameter> paraList = new ArrayList<>();
           paraList.add(parameter1);
           ModifyDbParameterGroupRequest groupRequest =
ModifyDbParameterGroupRequest.builder()
                   .dbParameterGroupName(dbGroupName)
                   .parameters(paraList)
                   .build();

           ModifyDbParameterGroupResponse response =
rdsClient.modifyDBParameterGroup(groupRequest);
           System.out.println("The parameter group " +
response.dbParameterGroupName() + " was successfully modified");

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- Para obtener información sobre la API, consulte ModifyDBParameterGroup en la Referencia de la API de AWS SDK for Java 2.x.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def update_parameters(self, parameter_group_name, update_parameters):
        """
        Updates parameters in a custom DB parameter group.

        :param parameter_group_name: The name of the parameter group to update.
        :param update_parameters: The parameters to update in the group.
        :return: Data about the modified parameter group.
        """
        try:
            response = self.rds_client.modify_db_parameter_group(
                DBParameterGroupName=parameter_group_name,
 Parameters=update_parameters
            )
        except ClientError as err:
```

```
            logger.error(
                "Couldn't update parameters in %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Para obtener información acerca de la API, consulte ModifyDBParameterGroup en la Referencia de la API del SDK de AWS para Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de **RebootDBInstance** con un AWS SDK o la CLI

Los siguientes ejemplos de código muestran cómo utilizar `RebootDBInstance`.

CLI

AWS CLI

Reinicio de una instancia de base de datos

En el siguiente ejemplo `reboot-db-instance`, se inicia un reinicio de la instancia de base de datos especificada.

```
aws rds reboot-db-instance \
    --db-instance-identifier test-mysql-instance
```

Salida:

```
{
    "DBInstance": {
        "DBInstanceIdentifier": "test-mysql-instance",
        "DBInstanceClass": "db.t3.micro",
        "Engine": "mysql",
```

```
        "DBInstanceStatus": "rebooting",
        "MasterUsername": "admin",
        "Endpoint": {
            "Address": "test-mysql-instance.############.us-
west-2.rds.amazonaws.com",
            "Port": 3306,
            "HostedZoneId": "Z1PVIF0EXAMPLE"
        },

    ... output omitted...

    }
}
```

Para obtener más información, consulte Reinicio de una instancia de base de datos en la Guía del usuario de Amazon RDS.

- Para obtener información sobre la API, consulte RebootDBInstance en la Referencia de comandos de la AWS CLI.

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.RebootDbInstanceRequest;
import software.amazon.awssdk.services.rds.model.RebootDbInstanceResponse;
import software.amazon.awssdk.services.rds.model.RdsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
```

```
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class RebootDBInstance {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <dbInstanceIdentifier>\s

                Where:
                    dbInstanceIdentifier - The database instance identifier\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String dbInstanceIdentifier = args[0];
        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();

        rebootInstance(rdsClient, dbInstanceIdentifier);
        rdsClient.close();
    }

    public static void rebootInstance(RdsClient rdsClient, String
 dbInstanceIdentifier) {
        try {
            RebootDbInstanceRequest rebootDbInstanceRequest =
 RebootDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .build();

            RebootDbInstanceResponse instanceResponse =
 rdsClient.rebootDBInstance(rebootDbInstanceRequest);
            System.out.print("The database " +
 instanceResponse.dbInstance().dbInstanceArn() + " was rebooted");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
```

```
            System.exit(1);
        }
    }
}
```

- Para obtener información acerca de la API, consulte RebootDBInstance en la Referencia de la API de AWS SDK for Java 2.x.

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Escenarios de Amazon RDS con SDK de AWS

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes en Amazon RDS con SDK de AWS. Estos escenarios muestran cómo llevar a cabo tareas específicas llamando a varias funciones dentro de Amazon RDS. En cada escenario se incluye un enlace a GitHub, con instrucciones de configuración y ejecución del código.

Ejemplos

- Comience a utilizar las instancias de base de datos de Amazon RDS con un SDK de AWS

Comience a utilizar las instancias de base de datos de Amazon RDS con un SDK de AWS

En el siguiente ejemplo de código, se muestra cómo:

- Cree un grupo de parámetros de base de datos personalizado y defina los valores de los parámetros.
- Cree una instancia de base de datos que esté configurada para utilizar el grupo de parámetros. La instancia de base de datos también contiene una base de datos.
- Cree una instantánea de la instancia.
- Elimine la instancia y el grupo de parámetros.

.NET

SDK para .NET

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecutar un escenario interactivo en un símbolo del sistema.

```
/// <summary>
/// Scenario for RDS DB instance example.
/// </summary>
public class RDSInstanceScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.

    This .NET example performs the following tasks:
    1.  Returns a list of the available DB engine families using the
 DescribeDBEngineVersionsAsync method.
    2.  Selects an engine family and creates a custom DB parameter group using
 the CreateDBParameterGroupAsync method.
    3.  Gets the parameter groups using the DescribeDBParameterGroupsAsync
 method.
    4.  Gets parameters in the group using the DescribeDBParameters method.
    5.  Parses and displays parameters in the group.
    6.  Modifies both the auto_increment_offset and auto_increment_increment
 parameters
        using the ModifyDBParameterGroupAsync method.
    7.  Gets and displays the updated parameters using the DescribeDBParameters
 method with a source of "user".
    8.  Gets a list of allowed engine versions using the
 DescribeDBEngineVersionsAsync method.
    9.  Displays and selects from a list of micro instance classes available for
 the selected engine and version.
    10. Creates an RDS DB instance that contains a MySql database and uses the
 parameter group
        using the CreateDBInstanceAsync method.
```

```
   11. Waits for DB instance to be ready using the DescribeDBInstancesAsync
method.
   12. Prints out the connection endpoint string for the new DB instance.
   13. Creates a snapshot of the DB instance using the CreateDBSnapshotAsync
method.
   14. Waits for DB snapshot to be ready using the DescribeDBSnapshots method.
   15. Deletes the DB instance using the DeleteDBInstanceAsync method.
   16. Waits for DB instance to be deleted using the DescribeDbInstances method.
   17. Deletes the parameter group using the DeleteDBParameterGroupAsync.
   */

   private static readonly string sepBar = new('-', 80);
   private static RDSWrapper rdsWrapper = null!;
   private static ILogger logger = null!;
   private static readonly string engine = "mysql";
   static async Task Main(string[] args)
   {
       // Set up dependency injection for the Amazon RDS service.
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                   .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
           .ConfigureServices((_, services) =>
               services.AddAWSService<IAmazonRDS>()
                   .AddTransient<RDSWrapper>()
           )
           .Build();

       logger = LoggerFactory.Create(builder =>
       {
           builder.AddConsole();
       }).CreateLogger<RDSInstanceScenario>();

       rdsWrapper = host.Services.GetRequiredService<RDSWrapper>();

       Console.WriteLine(sepBar);
       Console.WriteLine(
           "Welcome to the Amazon Relational Database Service (Amazon RDS) DB
instance scenario example.");
       Console.WriteLine(sepBar);
```

```
        try
        {
            var parameterGroupFamily = await ChooseParameterGroupFamily();

            var parameterGroup = await
CreateDbParameterGroup(parameterGroupFamily);

            var parameters = await
DescribeParametersInGroup(parameterGroup.DBParameterGroupName,
                new List<string> { "auto_increment_offset",
"auto_increment_increment" });

            await ModifyParameters(parameterGroup.DBParameterGroupName,
parameters);

            await
DescribeUserSourceParameters(parameterGroup.DBParameterGroupName);

            var engineVersionChoice = await
ChooseDbEngineVersion(parameterGroupFamily);

            var instanceChoice = await ChooseDbInstanceClass(engine,
engineVersionChoice.EngineVersion);

            var newInstanceIdentifier = "Example-Instance-" + DateTime.Now.Ticks;

            var newInstance = await CreateRdsNewInstance(parameterGroup, engine,
engineVersionChoice.EngineVersion,
                instanceChoice.DBInstanceClass, newInstanceIdentifier);
            if (newInstance != null)
            {
                DisplayConnectionString(newInstance);

                await CreateSnapshot(newInstance);

                await DeleteRdsInstance(newInstance);
            }

            await DeleteParameterGroup(parameterGroup);

            Console.WriteLine("Scenario complete.");
            Console.WriteLine(sepBar);
        }
        catch (Exception ex)
```

```
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// Choose the RDS DB parameter group family from a list of available
options.
    /// </summary>
    /// <returns>The selected parameter group family.</returns>
    public static async Task<string> ChooseParameterGroupFamily()
    {
        Console.WriteLine(sepBar);
        // 1. Get a list of available engines.
        var engines = await rdsWrapper.DescribeDBEngineVersions(engine);

        Console.WriteLine("1. The following is a list of available DB parameter
group families:");
        int i = 1;
        var parameterGroupFamilies = engines.GroupBy(e =>
e.DBParameterGroupFamily).ToList();
        foreach (var parameterGroupFamily in parameterGroupFamilies)
        {
            // List the available parameter group families.
            Console.WriteLine(
                $"\t{i}. Family: {parameterGroupFamily.Key}");
            i++;
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > parameterGroupFamilies.Count)
        {
            Console.WriteLine("Select an available DB parameter group family by
entering a number from the list above:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        var parameterGroupFamilyChoice = parameterGroupFamilies[choiceNumber -
1];
        Console.WriteLine(sepBar);
        return parameterGroupFamilyChoice.Key;
    }

    /// <summary>
```

```
   /// Create and get information on a DB parameter group.
   /// </summary>
   /// <param name="dbParameterGroupFamily">The DBParameterGroupFamily for the
new DB parameter group.</param>
   /// <returns>The new DBParameterGroup.</returns>
   public static async Task<DBParameterGroup> CreateDbParameterGroup(string
dbParameterGroupFamily)
   {
       Console.WriteLine(sepBar);
       Console.WriteLine($"2. Create new DB parameter group with family
{dbParameterGroupFamily}:");

       var parameterGroup = await rdsWrapper.CreateDBParameterGroup(
           "ExampleParameterGroup-" + DateTime.Now.Ticks,
           dbParameterGroupFamily, "New example parameter group");

       var groupInfo =
           await rdsWrapper.DescribeDBParameterGroups(parameterGroup
               .DBParameterGroupName);

       Console.WriteLine(
           $"3. New DB parameter group: \n\t{groupInfo[0].Description}, \n\tARN
{groupInfo[0].DBParameterGroupArn}");
       Console.WriteLine(sepBar);
       return parameterGroup;
   }

   /// <summary>
   /// Get and describe parameters from a DBParameterGroup.
   /// </summary>
   /// <param name="parameterGroupName">Name of the DBParameterGroup.</param>
   /// <param name="parameterNames">Optional specific names of parameters to
describe.</param>
   /// <returns>The list of requested parameters.</returns>
   public static async Task<List<Parameter>> DescribeParametersInGroup(string
parameterGroupName, List<string>? parameterNames = null)
   {
       Console.WriteLine(sepBar);
       Console.WriteLine("4. Get some parameters from the group.");
       Console.WriteLine(sepBar);

       var parameters =
           await rdsWrapper.DescribeDBParameters(parameterGroupName);
```

```
        var matchingParameters =
            parameters.Where(p => parameterNames == null ||
parameterNames.Contains(p.ParameterName)).ToList();

        Console.WriteLine("5. Parameter information:");
        matchingParameters.ForEach(p =>
            Console.WriteLine(
                $"\n\tParameter: {p.ParameterName}." +
                $"\n\tDescription: {p.Description}." +
                $"\n\tAllowed Values: {p.AllowedValues}." +
                $"\n\tValue: {p.ParameterValue}."));

        Console.WriteLine(sepBar);

        return matchingParameters;
    }

    /// <summary>
    /// Modify a parameter from a DBParameterGroup.
    /// </summary>
    /// <param name="parameterGroupName">Name of the DBParameterGroup.</param>
    /// <param name="parameters">The parameters to modify.</param>
    /// <returns>Async task.</returns>
    public static async Task ModifyParameters(string parameterGroupName,
List<Parameter> parameters)
    {
        Console.WriteLine(sepBar);
        Console.WriteLine("6. Modify some parameters in the group.");

        foreach (var p in parameters)
        {
            if (p.IsModifiable && p.DataType == "integer")
            {
                int newValue = 0;
                while (newValue == 0)
                {
                    Console.WriteLine(
                        $"Enter a new value for {p.ParameterName} from the
allowed values {p.AllowedValues} ");

                    var choice = Console.ReadLine();
                    Int32.TryParse(choice, out newValue);
                }
```

```
                p.ParameterValue = newValue.ToString();
            }
        }

        await rdsWrapper.ModifyDBParameterGroup(parameterGroupName, parameters);

        Console.WriteLine(sepBar);
    }

    /// <summary>
    /// Describe the user source parameters in the group.
    /// </summary>
    /// <param name="parameterGroupName">Name of the DBParameterGroup.</param>
    /// <returns>Async task.</returns>
    public static async Task DescribeUserSourceParameters(string
parameterGroupName)
    {
        Console.WriteLine(sepBar);
        Console.WriteLine("7. Describe user source parameters in the group.");

        var parameters =
            await rdsWrapper.DescribeDBParameters(parameterGroupName, "user");


        parameters.ForEach(p =>
            Console.WriteLine(
                $"\n\tParameter: {p.ParameterName}." +
                $"\n\tDescription: {p.Description}." +
                $"\n\tAllowed Values: {p.AllowedValues}." +
                $"\n\tValue: {p.ParameterValue}."));

        Console.WriteLine(sepBar);
    }


    /// <summary>
    /// Choose a DB engine version.
    /// </summary>
    /// <param name="dbParameterGroupFamily">DB parameter group family for engine
choice.</param>
    /// <returns>The selected engine version.</returns>
    public static async Task<DBEngineVersion> ChooseDbEngineVersion(string
dbParameterGroupFamily)
    {
```

```
        Console.WriteLine(sepBar);
        // Get a list of allowed engines.
        var allowedEngines =
            await rdsWrapper.DescribeDBEngineVersions(engine,
 dbParameterGroupFamily);

        Console.WriteLine($"Available DB engine versions for parameter group
 family {dbParameterGroupFamily}:");
        int i = 1;
        foreach (var version in allowedEngines)
        {
            Console.WriteLine(
                $"\t{i}. Engine: {version.Engine} Version
 {version.EngineVersion}.");
            i++;
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > allowedEngines.Count)
        {
            Console.WriteLine("8. Select an available DB engine version by
 entering a number from the list above:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        var engineChoice = allowedEngines[choiceNumber - 1];
        Console.WriteLine(sepBar);
        return engineChoice;
    }

    /// <summary>
    /// Choose a DB instance class for a particular engine and engine version.
    /// </summary>
    /// <param name="engine">DB engine for DB instance choice.</param>
    /// <param name="engineVersion">DB engine version for DB instance choice.</
param>
    /// <returns>The selected orderable DB instance option.</returns>
    public static async Task<OrderableDBInstanceOption>
 ChooseDbInstanceClass(string engine, string engineVersion)
    {
        Console.WriteLine(sepBar);
        // Get a list of allowed DB instance classes.
        var allowedInstances =
```

```
            await rdsWrapper.DescribeOrderableDBInstanceOptions(engine,
 engineVersion);

        Console.WriteLine($"8. Available micro DB instance classes for engine
 {engine} and version {engineVersion}:");
        int i = 1;

        // Filter to micro instances for this example.
        allowedInstances = allowedInstances
            .Where(i => i.DBInstanceClass.Contains("micro")).ToList();

        foreach (var instance in allowedInstances)
        {
            Console.WriteLine(
                $"\t{i}. Instance class: {instance.DBInstanceClass} (storage type
 {instance.StorageType})");
            i++;
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > allowedInstances.Count)
        {
            Console.WriteLine("9. Select an available DB instance class by
 entering a number from the list above:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        var instanceChoice = allowedInstances[choiceNumber - 1];
        Console.WriteLine(sepBar);
        return instanceChoice;
    }

    /// <summary>
    /// Create a new RDS DB instance.
    /// </summary>
    /// <param name="parameterGroup">Parameter group to use for the DB
 instance.</param>
    /// <param name="engineName">Engine to use for the DB instance.</param>
    /// <param name="engineVersion">Engine version to use for the DB instance.</
param>
    /// <param name="instanceClass">Instance class to use for the DB instance.</
param>
```

```
   /// <param name="instanceIdentifier">Instance identifier to use for the DB
instance.</param>
   /// <returns>The new DB instance.</returns>
   public static async Task<DBInstance?> CreateRdsNewInstance(DBParameterGroup
parameterGroup,
       string engineName, string engineVersion, string instanceClass, string
instanceIdentifier)
   {
       Console.WriteLine(sepBar);
       Console.WriteLine($"10. Create a new DB instance with identifier
{instanceIdentifier}.");
       bool isInstanceReady = false;
       DBInstance newInstance;
       var instances = await rdsWrapper.DescribeDBInstances();
       isInstanceReady = instances.FirstOrDefault(i =>
           i.DBInstanceIdentifier == instanceIdentifier)?.DBInstanceStatus ==
"available";

       if (isInstanceReady)
       {
           Console.WriteLine("Instance already created.");
           newInstance = instances.First(i => i.DBInstanceIdentifier ==
instanceIdentifier);
       }
       else
       {
           Console.WriteLine("Please enter an admin user name:");
           var username = Console.ReadLine();

           Console.WriteLine("Please enter an admin password:");
           var password = Console.ReadLine();

           newInstance = await rdsWrapper.CreateDBInstance(
               "ExampleInstance",
               instanceIdentifier,
               parameterGroup.DBParameterGroupName,
               engineName,
               engineVersion,
               instanceClass,
               20,
               username,
               password
           );
```

```
            // 11. Wait for the DB instance to be ready.

            Console.WriteLine("11. Waiting for DB instance to be ready...");
            while (!isInstanceReady)
            {
                instances = await
 rdsWrapper.DescribeDBInstances(instanceIdentifier);
                isInstanceReady = instances.FirstOrDefault()?.DBInstanceStatus ==
 "available";
                newInstance = instances.First();
                Thread.Sleep(30000);
            }
        }

        Console.WriteLine(sepBar);
        return newInstance;
    }

    /// <summary>
    /// Display a connection string for an RDS DB instance.
    /// </summary>
    /// <param name="instance">The DB instance to use to get a connection
 string.</param>
    public static void DisplayConnectionString(DBInstance instance)
    {
        Console.WriteLine(sepBar);
        // Display the connection string.
        Console.WriteLine("12. New DB instance connection string: ");
        Console.WriteLine(
            $"\n{engine} -h {instance.Endpoint.Address} -P
 {instance.Endpoint.Port} "
            + $"-u {instance.MasterUsername} -p [YOUR PASSWORD]\n");

        Console.WriteLine(sepBar);
    }

    /// <summary>
    /// Create a snapshot from an RDS DB instance.
    /// </summary>
    /// <param name="instance">DB instance to use when creating a snapshot.</
param>
    /// <returns>The snapshot object.</returns>
    public static async Task<DBSnapshot> CreateSnapshot(DBInstance instance)
    {
```

```
        Console.WriteLine(sepBar);
        // Create a snapshot.
        Console.WriteLine($"13. Creating snapshot from DB instance
{instance.DBInstanceIdentifier}.");
        var snapshot = await
rdsWrapper.CreateDBSnapshot(instance.DBInstanceIdentifier, "ExampleSnapshot-" +
DateTime.Now.Ticks);

        // Wait for the snapshot to be available
        bool isSnapshotReady = false;

        Console.WriteLine($"14. Waiting for snapshot to be ready...");
        while (!isSnapshotReady)
        {
            var snapshots = await
rdsWrapper.DescribeDBSnapshots(instance.DBInstanceIdentifier);
            isSnapshotReady = snapshots.FirstOrDefault()?.Status == "available";
            snapshot = snapshots.First();
            Thread.Sleep(30000);
        }

        Console.WriteLine(
            $"Snapshot {snapshot.DBSnapshotIdentifier} status is
{snapshot.Status}.");
        Console.WriteLine(sepBar);
        return snapshot;
    }

    /// <summary>
    /// Delete an RDS DB instance.
    /// </summary>
    /// <param name="instance">The DB instance to delete.</param>
    /// <returns>Async task.</returns>
    public static async Task DeleteRdsInstance(DBInstance newInstance)
    {
        Console.WriteLine(sepBar);
        // Delete the DB instance.
        Console.WriteLine($"15. Delete the DB instance
{newInstance.DBInstanceIdentifier}.");
        await rdsWrapper.DeleteDBInstance(newInstance.DBInstanceIdentifier);

        // Wait for the DB instance to delete.
        Console.WriteLine($"16. Waiting for the DB instance to delete...");
        bool isInstanceDeleted = false;
```

```
        while (!isInstanceDeleted)
        {
            var instance = await rdsWrapper.DescribeDBInstances();
            isInstanceDeleted = instance.All(i => i.DBInstanceIdentifier !=
 newInstance.DBInstanceIdentifier);
            Thread.Sleep(30000);
        }

        Console.WriteLine("DB instance deleted.");
        Console.WriteLine(sepBar);
    }

    /// <summary>
    /// Delete a DB parameter group.
    /// </summary>
    /// <param name="parameterGroup">The parameter group to delete.</param>
    /// <returns>Async task.</returns>
    public static async Task DeleteParameterGroup(DBParameterGroup
 parameterGroup)
    {
        Console.WriteLine(sepBar);
        // Delete the parameter group.
        Console.WriteLine($"17. Delete the DB parameter group
 {parameterGroup.DBParameterGroupName}.");
        await
 rdsWrapper.DeleteDBParameterGroup(parameterGroup.DBParameterGroupName);

        Console.WriteLine(sepBar);
    }
```

Métodos envolventes utilizados por el escenario para las acciones de la instancia de base de datos.

```
/// <summary>
/// Wrapper methods to use Amazon Relational Database Service (Amazon RDS) with
 DB instance operations.
/// </summary>
public partial class RDSWrapper
{
    private readonly IAmazonRDS _amazonRDS;
```

```
    public RDSWrapper(IAmazonRDS amazonRDS)
    {
        _amazonRDS = amazonRDS;
    }


    /// <summary>
    /// Get a list of DB engine versions for a particular DB engine.
    /// </summary>
    /// <param name="engine">Name of the engine.</param>
    /// <param name="dbParameterGroupFamily">Optional parameter group family
name.</param>
    /// <returns>List of DBEngineVersions.</returns>
    public async Task<List<DBEngineVersion>> DescribeDBEngineVersions(string
engine,
        string dbParameterGroupFamily = null)
    {
        var response = await _amazonRDS.DescribeDBEngineVersionsAsync(
            new DescribeDBEngineVersionsRequest()
            {
                Engine = engine,
                DBParameterGroupFamily = dbParameterGroupFamily
            });
        return response.DBEngineVersions;
    }



    /// <summary>
    /// Get a list of orderable DB instance options for a specific
    /// engine and engine version.
    /// </summary>
    /// <param name="engine">Name of the engine.</param>
    /// <param name="engineVersion">Version of the engine.</param>
    /// <returns>List of OrderableDBInstanceOptions.</returns>
    public async Task<List<OrderableDBInstanceOption>>
DescribeOrderableDBInstanceOptions(string engine, string engineVersion)
    {
        // Use a paginator to get a list of DB instance options.
        var results = new List<OrderableDBInstanceOption>();
        var paginateInstanceOptions =
_amazonRDS.Paginators.DescribeOrderableDBInstanceOptions(
            new DescribeOrderableDBInstanceOptionsRequest()
            {
```

```
                Engine = engine,
                EngineVersion = engineVersion,
            });
        // Get the entire list using the paginator.
        await foreach (var instanceOptions in
paginateInstanceOptions.OrderableDBInstanceOptions)
        {
            results.Add(instanceOptions);
        }
        return results;
    }



    /// <summary>
    /// Returns a list of DB instances.
    /// </summary>
    /// <param name="dbInstanceIdentifier">Optional name of a specific DB
instance.</param>
    /// <returns>List of DB instances.</returns>
    public async Task<List<DBInstance>> DescribeDBInstances(string
dbInstanceIdentifier = null)
    {
        var results = new List<DBInstance>();
        var instancesPaginator = _amazonRDS.Paginators.DescribeDBInstances(
            new DescribeDBInstancesRequest
            {
                DBInstanceIdentifier = dbInstanceIdentifier
            });
        // Get the entire list using the paginator.
        await foreach (var instances in instancesPaginator.DBInstances)
        {
            results.Add(instances);
        }
        return results;
    }



    /// <summary>
    /// Create an RDS DB instance with a particular set of properties. Use the
action DescribeDBInstancesAsync
    /// to determine when the DB instance is ready to use.
    /// </summary>
```

```
   /// <param name="dbName">Name for the DB instance.</param>
   /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
   /// <param name="parameterGroupName">DB parameter group to associate with the
instance.</param>
   /// <param name="dbEngine">The engine for the DB instance.</param>
   /// <param name="dbEngineVersion">Version for the DB instance.</param>
   /// <param name="instanceClass">Class for the DB instance.</param>
   /// <param name="allocatedStorage">The amount of storage in gibibytes (GiB)
to allocate to the DB instance.</param>
   /// <param name="adminName">Admin user name.</param>
   /// <param name="adminPassword">Admin user password.</param>
   /// <returns>DB instance object.</returns>
   public async Task<DBInstance> CreateDBInstance(string dbName, string
dbInstanceIdentifier,
       string parameterGroupName, string dbEngine, string dbEngineVersion,
       string instanceClass, int allocatedStorage, string adminName, string
adminPassword)
   {
       var response = await _amazonRDS.CreateDBInstanceAsync(
           new CreateDBInstanceRequest()
           {
               DBName = dbName,
               DBInstanceIdentifier = dbInstanceIdentifier,
               DBParameterGroupName = parameterGroupName,
               Engine = dbEngine,
               EngineVersion = dbEngineVersion,
               DBInstanceClass = instanceClass,
               AllocatedStorage = allocatedStorage,
               MasterUsername = adminName,
               MasterUserPassword = adminPassword
           });

       return response.DBInstance;
   }



   /// <summary>
   /// Delete a particular DB instance.
   /// </summary>
   /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
   /// <returns>DB instance object.</returns>
   public async Task<DBInstance> DeleteDBInstance(string dbInstanceIdentifier)
   {
```

```
        var response = await _amazonRDS.DeleteDBInstanceAsync(
            new DeleteDBInstanceRequest()
            {
                DBInstanceIdentifier = dbInstanceIdentifier,
                SkipFinalSnapshot = true,
                DeleteAutomatedBackups = true
            });

        return response.DBInstance;
    }
```

Métodos envolventes utilizados por el escenario para los grupos de parámetros de base de datos.

```
/// <summary>
/// Wrapper methods to use Amazon Relational Database Service (Amazon RDS) with
 parameter groups.
/// </summary>
public partial class RDSWrapper
{

    /// <summary>
    /// Get descriptions of DB parameter groups.
    /// </summary>
    /// <param name="name">Optional name of the DB parameter group to describe.</
param>
    /// <returns>The list of DB parameter group descriptions.</returns>
    public async Task<List<DBParameterGroup>> DescribeDBParameterGroups(string
 name = null)
    {
        var response = await _amazonRDS.DescribeDBParameterGroupsAsync(
            new DescribeDBParameterGroupsRequest()
            {
                DBParameterGroupName = name
            });
        return response.DBParameterGroups;
    }
```

```
    /// <summary>
    /// Create a new DB parameter group. Use the action
 DescribeDBParameterGroupsAsync
    /// to determine when the DB parameter group is ready to use.
    /// </summary>
    /// <param name="name">Name of the DB parameter group.</param>
    /// <param name="family">Family of the DB parameter group.</param>
    /// <param name="description">Description of the DB parameter group.</param>
    /// <returns>The new DB parameter group.</returns>
    public async Task<DBParameterGroup> CreateDBParameterGroup(
        string name, string family, string description)
    {
        var response = await _amazonRDS.CreateDBParameterGroupAsync(
            new CreateDBParameterGroupRequest()
            {
                DBParameterGroupName = name,
                DBParameterGroupFamily = family,
                Description = description
            });
        return response.DBParameterGroup;
    }



    /// <summary>
    /// Update a DB parameter group. Use the action
 DescribeDBParameterGroupsAsync
    /// to determine when the DB parameter group is ready to use.
    /// </summary>
    /// <param name="name">Name of the DB parameter group.</param>
    /// <param name="parameters">List of parameters. Maximum of 20 per request.</
param>
    /// <returns>The updated DB parameter group name.</returns>
    public async Task<string> ModifyDBParameterGroup(
        string name, List<Parameter> parameters)
    {
        var response = await _amazonRDS.ModifyDBParameterGroupAsync(
            new ModifyDBParameterGroupRequest()
            {
                DBParameterGroupName = name,
                Parameters = parameters,
            });
        return response.DBParameterGroupName;
    }
```

```
   /// <summary>
   /// Delete a DB parameter group. The group cannot be a default DB parameter
group
   /// or be associated with any DB instances.
   /// </summary>
   /// <param name="name">Name of the DB parameter group.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> DeleteDBParameterGroup(string name)
   {
       var response = await _amazonRDS.DeleteDBParameterGroupAsync(
           new DeleteDBParameterGroupRequest()
           {
               DBParameterGroupName = name,
           });
       return response.HttpStatusCode == HttpStatusCode.OK;
   }



   /// <summary>
   /// Get a list of DB parameters from a specific parameter group.
   /// </summary>
   /// <param name="dbParameterGroupName">Name of a specific DB parameter
group.</param>
   /// <param name="source">Optional source for selecting parameters.</param>
   /// <returns>List of parameter values.</returns>
   public async Task<List<Parameter>> DescribeDBParameters(string
dbParameterGroupName, string source = null)
   {
       var results = new List<Parameter>();
       var paginateParameters = _amazonRDS.Paginators.DescribeDBParameters(
           new DescribeDBParametersRequest()
           {
               DBParameterGroupName = dbParameterGroupName,
               Source = source
           });
       // Get the entire list using the paginator.
       await foreach (var parameters in paginateParameters.Parameters)
       {
           results.Add(parameters);
       }
```

```
        return results;
    }
```

Métodos envolventes utilizados por el escenario para las acciones de la instantánea de base de datos.

```
/// <summary>
/// Wrapper methods to use Amazon Relational Database Service (Amazon RDS) with
 snapshots.
/// </summary>
public partial class RDSWrapper
{

    /// <summary>
    /// Create a snapshot of a DB instance.
    /// </summary>
    /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
    /// <param name="snapshotIdentifier">Identifier for the snapshot.</param>
    /// <returns>DB snapshot object.</returns>
    public async Task<DBSnapshot> CreateDBSnapshot(string dbInstanceIdentifier,
 string snapshotIdentifier)
    {
        var response = await _amazonRDS.CreateDBSnapshotAsync(
            new CreateDBSnapshotRequest()
            {
                DBSnapshotIdentifier = snapshotIdentifier,
                DBInstanceIdentifier = dbInstanceIdentifier
            });

        return response.DBSnapshot;
    }



    /// <summary>
    /// Return a list of DB snapshots for a particular DB instance.
    /// </summary>
    /// <param name="dbInstanceIdentifier">DB instance identifier.</param>
    /// <returns>List of DB snapshots.</returns>
```

```
   public async Task<List<DBSnapshot>> DescribeDBSnapshots(string
dbInstanceIdentifier)
   {
       var results = new List<DBSnapshot>();
       var snapshotsPaginator = _amazonRDS.Paginators.DescribeDBSnapshots(
           new DescribeDBSnapshotsRequest()
           {
               DBInstanceIdentifier = dbInstanceIdentifier
           });

       // Get the entire list using the paginator.
       await foreach (var snapshots in snapshotsPaginator.DBSnapshots)
       {
           results.Add(snapshots);
       }
       return results;
   }
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK para .NET.
  - CreateDBInstance
  - CreateDBParameterGroup
  - CreateDBSnapshot
  - DeleteDBInstance
  - DeleteDBParameterGroup
  - DescribeDBEngineVersions
  - DescribeDBInstances
  - DescribeDBParameterGroups
  - DescribeDBParameters
  - DescribeDBSnapshots
  - DescribeOrderableDBInstanceOptions
  - ModifyDBParameterGroup

C++

SDK para C++

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

//! Routine which creates an Amazon RDS instance and demonstrates several
 operations
//! on that instance.
/*!
 \sa gettingStartedWithDBInstances()
 \param clientConfiguration: AWS client configuration.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::gettingStartedWithDBInstances(
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::RDS::RDSClient client(clientConfig);

    printAsterisksLine();
    std::cout << "Welcome to the Amazon Relational Database Service (Amazon RDS)"
              << std::endl;
    std::cout << "get started with DB instances demo." << std::endl;
    printAsterisksLine();

    std::cout << "Checking for an existing DB parameter group named '" <<
              PARAMETER_GROUP_NAME << "'." << std::endl;
    Aws::String dbParameterGroupFamily("Undefined");
    bool parameterGroupFound = true;
    {
        // 1. Check if the DB parameter group already exists.
        Aws::RDS::Model::DescribeDBParameterGroupsRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);

        Aws::RDS::Model::DescribeDBParameterGroupsOutcome outcome =
```

```
                client.DescribeDBParameterGroups(request);

        if (outcome.IsSuccess()) {
            std::cout << "DB parameter group named '" <<
                      PARAMETER_GROUP_NAME << "' already exists." << std::endl;
            dbParameterGroupFamily = outcome.GetResult().GetDBParameterGroups()
[0].GetDBParameterGroupFamily();
        }
        else if (outcome.GetError().GetErrorType() ==
                 Aws::RDS::RDSErrors::D_B_PARAMETER_GROUP_NOT_FOUND_FAULT) {
            std::cout << "DB parameter group named '" <<
                      PARAMETER_GROUP_NAME << "' does not exist." << std::endl;
            parameterGroupFound = false;
        }
        else {
            std::cerr << "Error with RDS::DescribeDBParameterGroups. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    }

    if (!parameterGroupFound) {
        Aws::Vector<Aws::RDS::Model::DBEngineVersion> engineVersions;

        // 2. Get available engine versions for the specified engine.
        if (!getDBEngineVersions(DB_ENGINE, NO_PARAMETER_GROUP_FAMILY,
                                 engineVersions, client)) {
            return false;
        }

        std::cout << "Getting available database engine versions for " <<
 DB_ENGINE
                  << "."
                  << std::endl;
        std::vector<Aws::String> families;
        for (const Aws::RDS::Model::DBEngineVersion &version: engineVersions) {
            Aws::String family = version.GetDBParameterGroupFamily();
            if (std::find(families.begin(), families.end(), family) ==
                families.end()) {
                families.push_back(family);
                std::cout << "  " << families.size() << ": " << family <<
 std::endl;
            }
```

```
        }

        int choice = askQuestionForIntRange("Which family do you want to use? ",
1,
                                            static_cast<int>(families.size()));
        dbParameterGroupFamily = families[choice - 1];
    }
    if (!parameterGroupFound) {
        // 3.  Create a DB parameter group.
        Aws::RDS::Model::CreateDBParameterGroupRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        request.SetDBParameterGroupFamily(dbParameterGroupFamily);
        request.SetDescription("Example parameter group.");

        Aws::RDS::Model::CreateDBParameterGroupOutcome outcome =
                client.CreateDBParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully created."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::CreateDBParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    }

    printAsterisksLine();
    std::cout << "Let's set some parameter values in your parameter group."
              << std::endl;

    Aws::String marker;
    Aws::Vector<Aws::RDS::Model::Parameter> autoIncrementParameters;
    // 4.  Get the parameters in the DB parameter group.
    if (!getDBParameters(PARAMETER_GROUP_NAME, AUTO_INCREMENT_PREFIX, NO_SOURCE,
                         autoIncrementParameters,
                         client)) {
        cleanUpResources(PARAMETER_GROUP_NAME, "", client);
        return false;
    }

    Aws::Vector<Aws::RDS::Model::Parameter> updateParameters;
```

```
    for (Aws::RDS::Model::Parameter &autoIncParameter: autoIncrementParameters) {
        if (autoIncParameter.GetIsModifiable() &&
            (autoIncParameter.GetDataType() == "integer")) {
            std::cout << "The " << autoIncParameter.GetParameterName()
                      << " is described as: " <<
                      autoIncParameter.GetDescription() << "." << std::endl;
            if (autoIncParameter.ParameterValueHasBeenSet()) {
                std::cout << "The current value is "
                          << autoIncParameter.GetParameterValue()
                          << "." << std::endl;
            }
            std::vector<int> splitValues = splitToInts(
                    autoIncParameter.GetAllowedValues(), '-');
            if (splitValues.size() == 2) {
                int newValue = askQuestionForIntRange(
                        Aws::String("Enter a new value in the range ") +
                        autoIncParameter.GetAllowedValues() + ": ",
                        splitValues[0], splitValues[1]);
                autoIncParameter.SetParameterValue(std::to_string(newValue));
                updateParameters.push_back(autoIncParameter);

            }
            else {
                std::cerr << "Error parsing " <<
autoIncParameter.GetAllowedValues()
                          << std::endl;
            }
        }
    }

    {
        // 5.  Modify the auto increment parameters in the group.
        Aws::RDS::Model::ModifyDBParameterGroupRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        request.SetParameters(updateParameters);

        Aws::RDS::Model::ModifyDBParameterGroupOutcome outcome =
                client.ModifyDBParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully modified."
                      << std::endl;
        }
```

```
        else {
            std::cerr << "Error with RDS::ModifyDBParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
    }

    std::cout
            << "You can get a list of parameters you've set by specifying a
source of 'user'."
            << std::endl;

    Aws::Vector<Aws::RDS::Model::Parameter> userParameters;
    // 6.  Display the modified parameters in the group.
    if (!getDBParameters(PARAMETER_GROUP_NAME, NO_NAME_PREFIX, "user",
userParameters,
                         client)) {
        cleanUpResources(PARAMETER_GROUP_NAME, "", client);
        return false;
    }

    for (const auto &userParameter: userParameters) {
        std::cout << "  " << userParameter.GetParameterName() << ", " <<
                  userParameter.GetDescription() << ", parameter value - "
                  << userParameter.GetParameterValue() << std::endl;
    }

    printAsterisksLine();
    std::cout << "Checking for an existing DB instance." << std::endl;

    Aws::RDS::Model::DBInstance dbInstance;
    // 7.  Check if the DB instance already exists.
    if (!describeDBInstance(DB_INSTANCE_IDENTIFIER, dbInstance, client)) {
        cleanUpResources(PARAMETER_GROUP_NAME, "", client);
        return false;
    }

    if (dbInstance.DbInstancePortHasBeenSet()) {
        std::cout << "The DB instance already exists." << std::endl;
    }
    else {
        std::cout << "Let's create a DB instance." << std::endl;
        const Aws::String administratorName = askQuestion(
                "Enter an administrator username for the database: ");
```

```
        const Aws::String administratorPassword = askQuestion(
                "Enter a password for the administrator (at least 8 characters):
");
        Aws::Vector<Aws::RDS::Model::DBEngineVersion> engineVersions;

        // 8.  Get a list of available engine versions.
        if (!getDBEngineVersions(DB_ENGINE, dbParameterGroupFamily,
engineVersions,
                                 client)) {
            cleanUpResources(PARAMETER_GROUP_NAME, "", client);
            return false;
        }

        std::cout << "The available engines for your parameter group are:" <<
std::endl;

        int index = 1;
        for (const Aws::RDS::Model::DBEngineVersion &engineVersion:
engineVersions) {
            std::cout << "  " << index << ": " <<
engineVersion.GetEngineVersion()
                      << std::endl;
            ++index;
        }
        int choice = askQuestionForIntRange("Which engine do you want to use? ",
1,

static_cast<int>(engineVersions.size()));
        const Aws::RDS::Model::DBEngineVersion engineVersion =
engineVersions[choice -
                                                                              1];

        Aws::String dbInstanceClass;
        // 9.  Get a list of micro instance classes.
        if (!chooseMicroDBInstanceClass(engineVersion.GetEngine(),
                                        engineVersion.GetEngineVersion(),
                                        dbInstanceClass,
                                        client)) {
            cleanUpResources(PARAMETER_GROUP_NAME, "", client);
            return false;
        }

        std::cout << "Creating a DB instance named '" << DB_INSTANCE_IDENTIFIER
                  << "' and database '" << DB_NAME << "'.\n"
```

```
                << "The DB instance is configured to use your custom parameter
group '"
                << PARAMETER_GROUP_NAME << "',\n"
                << "selected engine version " <<
engineVersion.GetEngineVersion()
                << ",\n"
                << "selected DB instance class '" << dbInstanceClass << "',"
                << " and " << DB_ALLOCATED_STORAGE << " GiB of " <<
DB_STORAGE_TYPE
                << " storage.\nThis typically takes several minutes." <<
std::endl;

       Aws::RDS::Model::CreateDBInstanceRequest request;
       request.SetDBName(DB_NAME);
       request.SetDBInstanceIdentifier(DB_INSTANCE_IDENTIFIER);
       request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
       request.SetEngine(engineVersion.GetEngine());
       request.SetEngineVersion(engineVersion.GetEngineVersion());
       request.SetDBInstanceClass(dbInstanceClass);
       request.SetStorageType(DB_STORAGE_TYPE);
       request.SetAllocatedStorage(DB_ALLOCATED_STORAGE);
       request.SetMasterUsername(administratorName);
       request.SetMasterUserPassword(administratorPassword);

       Aws::RDS::Model::CreateDBInstanceOutcome outcome =
               client.CreateDBInstance(request);

       if (outcome.IsSuccess()) {
           std::cout << "The DB instance creation has started."
                     << std::endl;
       }
       else {
           std::cerr << "Error with RDS::CreateDBInstance. "
                     << outcome.GetError().GetMessage()
                     << std::endl;
           cleanUpResources(PARAMETER_GROUP_NAME, "", client);
           return false;
       }
   }

   std::cout << "Waiting for the DB instance to become available." << std::endl;

   int counter = 0;
   // 11. Wait for the DB instance to become available.
```

```
   do {
       std::this_thread::sleep_for(std::chrono::seconds(1));
       ++counter;
       if (counter > 900) {
           std::cerr << "Wait for instance to become available timed out ofter "
                     << counter
                     << " seconds." << std::endl;
           cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
client);
           return false;
       }

       dbInstance = Aws::RDS::Model::DBInstance();
       if (!describeDBInstance(DB_INSTANCE_IDENTIFIER, dbInstance, client)) {
           cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
client);
           return false;
       }

       if ((counter % 20) == 0) {
           std::cout << "Current DB instance status is '"
                     << dbInstance.GetDBInstanceStatus()
                     << "' after " << counter << " seconds." << std::endl;
       }
   } while (dbInstance.GetDBInstanceStatus() != "available");

   if (dbInstance.GetDBInstanceStatus() == "available") {
       std::cout << "The DB instance has been created." << std::endl;
   }

   printAsterisksLine();

   // 12. Display the connection string that can be used to connect a 'mysql'
shell to the database.
   displayConnection(dbInstance);

   printAsterisksLine();

   if (askYesNoQuestion(
           "Do you want to create a snapshot of your DB instance (y/n)? ")) {
       Aws::String snapshotID(DB_INSTANCE_IDENTIFIER + "-" +
                              Aws::String(Aws::Utils::UUID::RandomUUID()));
       {
```

```
            std::cout << "Creating a snapshot named " << snapshotID << "." <<
std::endl;
            std::cout << "This typically takes a few minutes." << std::endl;

            // 13. Create a snapshot of the DB instance.
            Aws::RDS::Model::CreateDBSnapshotRequest request;
            request.SetDBInstanceIdentifier(DB_INSTANCE_IDENTIFIER);
            request.SetDBSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::CreateDBSnapshotOutcome outcome =
                    client.CreateDBSnapshot(request);

            if (outcome.IsSuccess()) {
                std::cout << "Snapshot creation has started."
                          << std::endl;
            }
            else {
                std::cerr << "Error with RDS::CreateDBSnapshot. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
client);
                return false;
            }
        }

        std::cout << "Waiting for snapshot to become available." << std::endl;

        Aws::RDS::Model::DBSnapshot snapshot;
        counter = 0;
        do {
            std::this_thread::sleep_for(std::chrono::seconds(1));
            ++counter;
            if (counter > 600) {
                std::cerr << "Wait for snapshot to be available timed out ofter "
                          << counter
                          << " seconds." << std::endl;
                cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
client);
                return false;
            }

            // 14. Wait for the snapshot to become available.
            Aws::RDS::Model::DescribeDBSnapshotsRequest request;
```

```
            request.SetDBSnapshotIdentifier(snapshotID);

            Aws::RDS::Model::DescribeDBSnapshotsOutcome outcome =
                    client.DescribeDBSnapshots(request);

            if (outcome.IsSuccess()) {
                snapshot = outcome.GetResult().GetDBSnapshots()[0];
            }
            else {
                std::cerr << "Error with RDS::DescribeDBSnapshots. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
 client);
                return false;
            }

            if ((counter % 20) == 0) {
                std::cout << "Current snapshot status is '"
                          << snapshot.GetStatus()
                          << "' after " << counter << " seconds." << std::endl;
            }
        } while (snapshot.GetStatus() != "available");

        if (snapshot.GetStatus() != "available") {
            std::cout << "A snapshot has been created." << std::endl;
        }
    }

    printAsterisksLine();

    bool result = true;
    if (askYesNoQuestion(
            "Do you want to delete the DB instance and parameter group (y/n)? "))
 {
        result = cleanUpResources(PARAMETER_GROUP_NAME, DB_INSTANCE_IDENTIFIER,
 client);
    }

    return result;
}


//! Routine which gets DB parameters using the 'DescribeDBParameters' api.
```

```
/*!
 \sa getDBParameters()
 \param parameterGroupName: The name of the parameter group.
 \param namePrefix: Prefix string to filter results by parameter name.
 \param source: A source such as 'user', ignored if empty.
 \param parametersResult: Vector of 'Parameter' objects returned by the routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::getDBParameters(const Aws::String &parameterGroupName,
                                  const Aws::String &namePrefix,
                                  const Aws::String &source,
                                  Aws::Vector<Aws::RDS::Model::Parameter>
 &parametersResult,
                                  const Aws::RDS::RDSClient &client) {
    Aws::String marker;
    do {
        Aws::RDS::Model::DescribeDBParametersRequest request;
        request.SetDBParameterGroupName(PARAMETER_GROUP_NAME);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }
        if (!source.empty()) {
            request.SetSource(source);
        }

        Aws::RDS::Model::DescribeDBParametersOutcome outcome =
                client.DescribeDBParameters(request);

        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::Parameter> &parameters =
                    outcome.GetResult().GetParameters();
            for (const Aws::RDS::Model::Parameter &parameter: parameters) {
                if (!namePrefix.empty()) {
                    if (parameter.GetParameterName().find(namePrefix) == 0) {
                        parametersResult.push_back(parameter);
                    }
                }
                else {
                    parametersResult.push_back(parameter);
                }
            }

            marker = outcome.GetResult().GetMarker();
```

```
        }
        else {
            std::cerr << "Error with RDS::DescribeDBParameters. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    return true;
}


//! Routine which gets available DB engine versions for an engine name and
//! an optional parameter group family.
/*!
 \sa getDBEngineVersions()
 \param engineName: A DB engine name.
 \param parameterGroupFamily: A parameter group family name, ignored if empty.
 \param engineVersionsResult: Vector of 'DBEngineVersion' objects returned by the
 routine.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::getDBEngineVersions(const Aws::String &engineName,
                                      const Aws::String &parameterGroupFamily,

 Aws::Vector<Aws::RDS::Model::DBEngineVersion> &engineVersionsResult,
                                      const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBEngineVersionsRequest request;
    request.SetEngine(engineName);
    if (!parameterGroupFamily.empty()) {
        request.SetDBParameterGroupFamily(parameterGroupFamily);
    }

    engineVersionsResult.clear();
    Aws::String marker; // Used for pagination.

    do {
        if (!marker.empty()) {
            request.SetMarker(marker);
        }
```

```
        Aws::RDS::Model::DescribeDBEngineVersionsOutcome outcome =
                client.DescribeDBEngineVersions(request);

        if (outcome.IsSuccess()) {
            auto &engineVersions = outcome.GetResult().GetDBEngineVersions();
            engineVersionsResult.insert(engineVersionsResult.end(),
 engineVersions.begin(),
                                        engineVersions.end());
            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with RDS::DescribeDBEngineVersionsRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }

    } while (!marker.empty());


    return true;
}


//! Routine which gets a DB instance description.
/*!
 \sa describeDBInstance()
 \param dbInstanceIdentifier: A DB instance identifier.
 \param instanceResult: The 'DBInstance' object containing the description.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::describeDBInstance(const Aws::String &dbInstanceIdentifier,
                                     Aws::RDS::Model::DBInstance &instanceResult,
                                     const Aws::RDS::RDSClient &client) {
    Aws::RDS::Model::DescribeDBInstancesRequest request;
    request.SetDBInstanceIdentifier(dbInstanceIdentifier);

    Aws::RDS::Model::DescribeDBInstancesOutcome outcome =
            client.DescribeDBInstances(request);

    bool result = true;
    if (outcome.IsSuccess()) {
        instanceResult = outcome.GetResult().GetDBInstances()[0];
```

```
    }
    else if (outcome.GetError().GetErrorType() !=
             Aws::RDS::RDSErrors::D_B_INSTANCE_NOT_FOUND_FAULT) {
        result = false;
        std::cerr << "Error with RDS::DescribeDBInstances. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
        // This example does not log an error if the DB instance does not exist.
        // Instead, instanceResult is set to empty.
    else {
        instanceResult = Aws::RDS::Model::DBInstance();
    }

    return result;
}


//! Routine which gets available 'micro' DB instance classes, displays the list
//! to the user, and returns the user selection.
/*!
 \sa chooseMicroDBInstanceClass()
 \param engineName: The DB engine name.
 \param engineVersion: The DB engine version.
 \param dbInstanceClass: String for DB instance class chosen by the user.
 \param client: 'RDSClient' instance.
 \return bool: Successful completion.
 */
bool AwsDoc::RDS::chooseMicroDBInstanceClass(const Aws::String &engine,
                                             const Aws::String &engineVersion,
                                             Aws::String &dbInstanceClass,
                                             const Aws::RDS::RDSClient &client) {
    std::vector<Aws::String> instanceClasses;
    Aws::String marker;
    do {
        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsRequest request;
        request.SetEngine(engine);
        request.SetEngineVersion(engineVersion);
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::RDS::Model::DescribeOrderableDBInstanceOptionsOutcome outcome =
                client.DescribeOrderableDBInstanceOptions(request);
```

```
        if (outcome.IsSuccess()) {
            const Aws::Vector<Aws::RDS::Model::OrderableDBInstanceOption>
 &options =
                    outcome.GetResult().GetOrderableDBInstanceOptions();
            for (const Aws::RDS::Model::OrderableDBInstanceOption &option:
 options) {
                const Aws::String &instanceClass = option.GetDBInstanceClass();
                if (instanceClass.find("micro") != std::string::npos) {
                    if (std::find(instanceClasses.begin(), instanceClasses.end(),
                                  instanceClass) ==
                        instanceClasses.end()) {
                        instanceClasses.push_back(instanceClass);
                    }
                }
            }
            marker = outcome.GetResult().GetMarker();
        }
        else {
            std::cerr << "Error with RDS::DescribeOrderableDBInstanceOptions. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!marker.empty());

    std::cout << "The available micro DB instance classes for your database
 engine are:"
              << std::endl;
    for (int i = 0; i < instanceClasses.size(); ++i) {
        std::cout << "   " << i + 1 << ": " << instanceClasses[i] << std::endl;
    }

    int choice = askQuestionForIntRange(
            "Which micro DB instance class do you want to use? ",
            1, static_cast<int>(instanceClasses.size()));
    dbInstanceClass = instanceClasses[choice - 1];
    return true;
}

//! Routine which deletes resources created by the scenario.
/*!
\sa cleanUpResources()
\param parameterGroupName: A parameter group name, this may be empty.
```

```
\param dbInstanceIdentifier: A DB instance identifier, this may be empty.
\param client: 'RDSClient' instance.
\return bool: Successful completion.
*/
bool AwsDoc::RDS::cleanUpResources(const Aws::String &parameterGroupName,
                                   const Aws::String &dbInstanceIdentifier,
                                   const Aws::RDS::RDSClient &client) {
    bool result = true;
    if (!dbInstanceIdentifier.empty()) {
        {
            // 15. Delete the DB instance.
            Aws::RDS::Model::DeleteDBInstanceRequest request;
            request.SetDBInstanceIdentifier(dbInstanceIdentifier);
            request.SetSkipFinalSnapshot(true);
            request.SetDeleteAutomatedBackups(true);

            Aws::RDS::Model::DeleteDBInstanceOutcome outcome =
                    client.DeleteDBInstance(request);

            if (outcome.IsSuccess()) {
                std::cout << "DB instance deletion has started."
                          << std::endl;
            }
            else {
                std::cerr << "Error with RDS::DeleteDBInstance. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = false;
            }
        }

        std::cout
                << "Waiting for DB instance to delete before deleting the
 parameter group."
                << std::endl;
        std::cout << "This may take a while." << std::endl;

        int counter = 0;
        Aws::RDS::Model::DBInstance dbInstance;
        do {
            std::this_thread::sleep_for(std::chrono::seconds(1));
            ++counter;
            if (counter > 800) {
```

```
                std::cerr << "Wait for instance to delete timed out ofter " <<
 counter
                          << " seconds." << std::endl;
                return false;
            }

            dbInstance = Aws::RDS::Model::DBInstance();
            // 16. Wait for the DB instance to be deleted.
            if (!describeDBInstance(dbInstanceIdentifier, dbInstance, client)) {
                return false;
            }

            if (dbInstance.DBInstanceIdentifierHasBeenSet() && (counter % 20) ==
 0) {
                std::cout << "Current DB instance status is '"
                          << dbInstance.GetDBInstanceStatus()
                          << "' after " << counter << " seconds." << std::endl;
            }
        } while (dbInstance.DBInstanceIdentifierHasBeenSet());
    }

    if (!parameterGroupName.empty()) {
        // 17. Delete the parameter group.
        Aws::RDS::Model::DeleteDBParameterGroupRequest request;
        request.SetDBParameterGroupName(parameterGroupName);

        Aws::RDS::Model::DeleteDBParameterGroupOutcome outcome =
                client.DeleteDBParameterGroup(request);

        if (outcome.IsSuccess()) {
            std::cout << "The DB parameter group was successfully deleted."
                      << std::endl;
        }
        else {
            std::cerr << "Error with RDS::DeleteDBParameterGroup. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            result = false;
        }
    }

    return result;
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK para C++.
  - CreateDBInstance
  - CreateDBParameterGroup
  - CreateDBSnapshot
  - DeleteDBInstance
  - DeleteDBParameterGroup
  - DescribeDBEngineVersions
  - DescribeDBInstances
  - DescribeDBParameterGroups
  - DescribeDBParameters
  - DescribeDBSnapshots
  - DescribeOrderableDBInstanceOptions
  - ModifyDBParameterGroup

Go

SDK para Go V2

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecutar un escenario interactivo en un símbolo del sistema.

```
// GetStartedInstances is an interactive example that shows you how to use the
 AWS SDK for Go
// with Amazon Relation Database Service (Amazon RDS) to do the following:
//
//  1. Create a custom DB parameter group and set parameter values.
```

```
//  2. Create a DB instance that is configured to use the parameter group. The DB
 instance
//     also contains a database.
//  3. Take a snapshot of the DB instance.
//  4. Delete the DB instance and parameter group.
type GetStartedInstances struct {
 sdkConfig  aws.Config
 instances  actions.DbInstances
 questioner demotools.IQuestioner
 helper     IScenarioHelper
 isTestRun  bool
}

// NewGetStartedInstances constructs a GetStartedInstances instance from a
 configuration.
// It uses the specified config to get an Amazon RDS
// client and create wrappers for the actions used in the scenario.
func NewGetStartedInstances(sdkConfig aws.Config, questioner
 demotools.IQuestioner,
 helper IScenarioHelper) GetStartedInstances {
 rdsClient := rds.NewFromConfig(sdkConfig)
 return GetStartedInstances{
  sdkConfig:  sdkConfig,
  instances:  actions.DbInstances{RdsClient: rdsClient},
  questioner: questioner,
  helper:     helper,
 }
}

// Run runs the interactive scenario.
func (scenario GetStartedInstances) Run(dbEngine string, parameterGroupName
 string,
 instanceName string, dbName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Println("Welcome to the Amazon Relational Database Service (Amazon RDS) DB
 Instance demo.")
 log.Println(strings.Repeat("-", 88))
```

```
 parameterGroup := scenario.CreateParameterGroup(dbEngine, parameterGroupName)
 scenario.SetUserParameters(parameterGroupName)
 instance := scenario.CreateInstance(instanceName, dbEngine, dbName,
 parameterGroup)
 scenario.DisplayConnection(instance)
 scenario.CreateSnapshot(instance)
 scenario.Cleanup(instance, parameterGroup)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}

// CreateParameterGroup shows how to get available engine versions for a
 specified
// database engine and create a DB parameter group that is compatible with a
// selected engine family.
func (scenario GetStartedInstances) CreateParameterGroup(dbEngine string,
 parameterGroupName string) *types.DBParameterGroup {

 log.Printf("Checking for an existing DB parameter group named %v.\n",
  parameterGroupName)
 parameterGroup, err := scenario.instances.GetParameterGroup(parameterGroupName)
 if err != nil {
  panic(err)
 }
 if parameterGroup == nil {
  log.Printf("Getting available database engine versions for %v.\n", dbEngine)
  engineVersions, err := scenario.instances.GetEngineVersions(dbEngine, "")
  if err != nil {
   panic(err)
  }

  familySet := map[string]struct{}{}
  for _, family := range engineVersions {
   familySet[*family.DBParameterGroupFamily] = struct{}{}
  }
  var families []string
  for family := range familySet {
   families = append(families, family)
  }
  sort.Strings(families)
  familyIndex := scenario.questioner.AskChoice("Which family do you want to use?
\n", families)
```

```
  log.Println("Creating a DB parameter group.")
  _, err = scenario.instances.CreateParameterGroup(
   parameterGroupName, families[familyIndex], "Example parameter group.")
  if err != nil {
   panic(err)
  }
  parameterGroup, err = scenario.instances.GetParameterGroup(parameterGroupName)
  if err != nil {
   panic(err)
  }
 }
 log.Printf("Parameter group %v:\n", *parameterGroup.DBParameterGroupFamily)
 log.Printf("\tName: %v\n", *parameterGroup.DBParameterGroupName)
 log.Printf("\tARN: %v\n", *parameterGroup.DBParameterGroupArn)
 log.Printf("\tFamily: %v\n", *parameterGroup.DBParameterGroupFamily)
 log.Printf("\tDescription: %v\n", *parameterGroup.Description)
 log.Println(strings.Repeat("-", 88))
 return parameterGroup
}

// SetUserParameters shows how to get the parameters contained in a custom
 parameter
// group and update some of the parameter values in the group.
func (scenario GetStartedInstances) SetUserParameters(parameterGroupName string)
 {
 log.Println("Let's set some parameter values in your parameter group.")
 dbParameters, err := scenario.instances.GetParameters(parameterGroupName, "")
 if err != nil {
  panic(err)
 }
 var updateParams []types.Parameter
 for _, dbParam := range dbParameters {
  if strings.HasPrefix(*dbParam.ParameterName, "auto_increment") &&
   dbParam.IsModifiable && *dbParam.DataType == "integer" {
   log.Printf("The %v parameter is described as:\n\t%v",
    *dbParam.ParameterName, *dbParam.Description)
   rangeSplit := strings.Split(*dbParam.AllowedValues, "-")
   lower, _ := strconv.Atoi(rangeSplit[0])
   upper, _ := strconv.Atoi(rangeSplit[1])
   newValue := scenario.questioner.AskInt(
    fmt.Sprintf("Enter a value between %v and %v:", lower, upper),
    demotools.InIntRange{Lower: lower, Upper: upper})
   dbParam.ParameterValue = aws.String(strconv.Itoa(newValue))
   updateParams = append(updateParams, dbParam)
```

```
  }
 }
 err = scenario.instances.UpdateParameters(parameterGroupName, updateParams)
 if err != nil {
  panic(err)
 }
 log.Println("To get a list of parameters that you set previously, specify a
 source of 'user'.")
 userParameters, err := scenario.instances.GetParameters(parameterGroupName,
 "user")
 if err != nil {
  panic(err)
 }
 log.Println("Here are the parameters you set:")
 for _, param := range userParameters {
  log.Printf("\t%v: %v\n", *param.ParameterName, *param.ParameterValue)
 }
 log.Println(strings.Repeat("-", 88))
}

// CreateInstance shows how to create a DB instance that contains a database of a
// specified type. The database is also configured to use a custom DB parameter
 group.
func (scenario GetStartedInstances) CreateInstance(instanceName string, dbEngine
 string,
 dbName string, parameterGroup *types.DBParameterGroup) *types.DBInstance {

 log.Println("Checking for an existing DB instance.")
 instance, err := scenario.instances.GetInstance(instanceName)
 if err != nil {
  panic(err)
 }
 if instance == nil {
  adminUsername := scenario.questioner.Ask(
   "Enter an administrator username for the database: ", demotools.NotEmpty{})
  adminPassword := scenario.questioner.AskPassword(
   "Enter a password for the administrator (at least 8 characters): ", 7)
  engineVersions, err := scenario.instances.GetEngineVersions(dbEngine,
   *parameterGroup.DBParameterGroupFamily)
  if err != nil {
   panic(err)
  }
  var engineChoices []string
  for _, engine := range engineVersions {
```

```
  engineChoices = append(engineChoices, *engine.EngineVersion)
 }
 engineIndex := scenario.questioner.AskChoice(
  "The available engines for your parameter group are:\n", engineChoices)
 engineSelection := engineVersions[engineIndex]
 instOpts, err :=
scenario.instances.GetOrderableInstances(*engineSelection.Engine,
  *engineSelection.EngineVersion)
 if err != nil {
  panic(err)
 }
 optSet := map[string]struct{}{}
 for _, opt := range instOpts {
  if strings.Contains(*opt.DBInstanceClass, "micro") {
   optSet[*opt.DBInstanceClass] = struct{}{}
  }
 }
 var optChoices []string
 for opt := range optSet {
  optChoices = append(optChoices, opt)
 }
 sort.Strings(optChoices)
 optIndex := scenario.questioner.AskChoice(
  "The available micro DB instance classes for your database engine are:\n",
optChoices)
 storageType := "standard"
 allocatedStorage := int32(5)
 log.Printf("Creating a DB instance named %v and database %v.\n"+
  "The DB instance is configured to use your custom parameter group %v,\n"+
  "selected engine %v,\n"+
  "selected DB instance class %v,"+
  "and %v GiB of %v storage.\n"+
  "This typically takes several minutes.",
  instanceName, dbName, *parameterGroup.DBParameterGroupName,
*engineSelection.EngineVersion,
  optChoices[optIndex], allocatedStorage, storageType)
 instance, err = scenario.instances.CreateInstance(
  instanceName, dbName, *engineSelection.Engine, *engineSelection.EngineVersion,
  *parameterGroup.DBParameterGroupName, optChoices[optIndex], storageType,
  allocatedStorage, adminUsername, adminPassword)
 if err != nil {
  panic(err)
 }
 for *instance.DBInstanceStatus != "available" {
```

```
   scenario.helper.Pause(30)
   instance, err = scenario.instances.GetInstance(instanceName)
   if err != nil {
    panic(err)
   }
  }
  log.Println("Instance created and available.")
 }
 log.Println("Instance data:")
 log.Printf("\tDBInstanceIdentifier: %v\n", *instance.DBInstanceIdentifier)
 log.Printf("\tARN: %v\n", *instance.DBInstanceArn)
 log.Printf("\tStatus: %v\n", *instance.DBInstanceStatus)
 log.Printf("\tEngine: %v\n", *instance.Engine)
 log.Printf("\tEngine version: %v\n", *instance.EngineVersion)
 log.Println(strings.Repeat("-", 88))
 return instance
}

// DisplayConnection displays connection information about a DB instance and tips
// on how to connect to it.
func (scenario GetStartedInstances) DisplayConnection(instance *types.DBInstance)
 {
 log.Println(
  "You can now connect to your database by using your favorite MySQL client.\n" +
   "One way to connect is by using the 'mysql' shell on an Amazon EC2 instance\n"
 +
   "that is running in the same VPC as your DB instance. Pass the endpoint,\n" +
   "port, and administrator username to 'mysql'. Then, enter your password\n" +
   "when prompted:")
 log.Printf("\n\tmysql -h %v -P %v -u %v -p\n",
  *instance.Endpoint.Address, instance.Endpoint.Port, *instance.MasterUsername)
 log.Println("For more information, see the User Guide for RDS:\n" +
  "\thttps://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
CHAP_GettingStarted.CreatingConnecting.MySQL.html#CHAP_GettingStarted.Connecting.MySQL")
 log.Println(strings.Repeat("-", 88))
}

// CreateSnapshot shows how to create a DB instance snapshot and wait until it's
 available.
func (scenario GetStartedInstances) CreateSnapshot(instance *types.DBInstance) {
 if scenario.questioner.AskBool(
  "Do you want to create a snapshot of your DB instance (y/n)? ", "y") {
  snapshotId := fmt.Sprintf("%v-%v", *instance.DBInstanceIdentifier,
 scenario.helper.UniqueId())
```

```
  log.Printf("Creating a snapshot named %v. This typically takes a few minutes.
\n", snapshotId)
  snapshot, err :=
 scenario.instances.CreateSnapshot(*instance.DBInstanceIdentifier, snapshotId)
  if err != nil {
   panic(err)
  }
  for *snapshot.Status != "available" {
   scenario.helper.Pause(30)
   snapshot, err = scenario.instances.GetSnapshot(snapshotId)
   if err != nil {
    panic(err)
   }
  }
  log.Println("Snapshot data:")
  log.Printf("\tDBSnapshotIdentifier: %v\n", *snapshot.DBSnapshotIdentifier)
  log.Printf("\tARN: %v\n", *snapshot.DBSnapshotArn)
  log.Printf("\tStatus: %v\n", *snapshot.Status)
  log.Printf("\tEngine: %v\n", *snapshot.Engine)
  log.Printf("\tEngine version: %v\n", *snapshot.EngineVersion)
  log.Printf("\tDBInstanceIdentifier: %v\n", *snapshot.DBInstanceIdentifier)
  log.Printf("\tSnapshotCreateTime: %v\n", *snapshot.SnapshotCreateTime)
  log.Println(strings.Repeat("-", 88))
 }
}

// Cleanup shows how to clean up a DB instance and DB parameter group.
// Before the DB parameter group can be deleted, all associated DB instances must
 first be deleted.
func (scenario GetStartedInstances) Cleanup(
 instance *types.DBInstance, parameterGroup *types.DBParameterGroup) {

 if scenario.questioner.AskBool(
  "\nDo you want to delete the database instance and parameter group (y/n)? ",
 "y") {
  log.Printf("Deleting database instance %v.\n", *instance.DBInstanceIdentifier)
  err := scenario.instances.DeleteInstance(*instance.DBInstanceIdentifier)
  if err != nil {
   panic(err)
  }
  log.Println(
   "Waiting for the DB instance to delete. This typically takes several
 minutes.")
  for instance != nil {
```

```
   scenario.helper.Pause(30)
   instance, err = scenario.instances.GetInstance(*instance.DBInstanceIdentifier)
   if err != nil {
    panic(err)
   }
  }
  log.Printf("Deleting parameter group %v.",
 *parameterGroup.DBParameterGroupName)
  err =
 scenario.instances.DeleteParameterGroup(*parameterGroup.DBParameterGroupName)
  if err != nil {
   panic(err)
  }
 }
}
```

Defina las funciones a las que llama el escenario para administrar las acciones de Amazon RDS.

```
type DbInstances struct {
 RdsClient *rds.Client
}


// GetParameterGroup gets a DB parameter group by name.
func (instances *DbInstances) GetParameterGroup(parameterGroupName string) (
 *types.DBParameterGroup, error) {
 output, err := instances.RdsClient.DescribeDBParameterGroups(
  context.TODO(), &rds.DescribeDBParameterGroupsInput{
   DBParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  var notFoundError *types.DBParameterGroupNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("Parameter group %v does not exist.\n", parameterGroupName)
   err = nil
  } else {
   log.Printf("Error getting parameter group %v: %v\n", parameterGroupName, err)
  }
  return nil, err
```

```
 } else {
  return &output.DBParameterGroups[0], err
 }
}



// CreateParameterGroup creates a DB parameter group that is based on the
 specified
// parameter group family.
func (instances *DbInstances) CreateParameterGroup(
 parameterGroupName string, parameterGroupFamily string, description string) (
 *types.DBParameterGroup, error) {

 output, err := instances.RdsClient.CreateDBParameterGroup(context.TODO(),
  &rds.CreateDBParameterGroupInput{
   DBParameterGroupName:   aws.String(parameterGroupName),
   DBParameterGroupFamily: aws.String(parameterGroupFamily),
   Description:            aws.String(description),
  })
 if err != nil {
  log.Printf("Couldn't create parameter group %v: %v\n", parameterGroupName, err)
  return nil, err
 } else {
  return output.DBParameterGroup, err
 }
}



// DeleteParameterGroup deletes the named DB parameter group.
func (instances *DbInstances) DeleteParameterGroup(parameterGroupName string)
 error {
 _, err := instances.RdsClient.DeleteDBParameterGroup(context.TODO(),
  &rds.DeleteDBParameterGroupInput{
   DBParameterGroupName: aws.String(parameterGroupName),
  })
 if err != nil {
  log.Printf("Couldn't delete parameter group %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
}
```

```
// GetParameters gets the parameters that are contained in a DB parameter group.
func (instances *DbInstances) GetParameters(parameterGroupName string, source
 string) (
 []types.Parameter, error) {

 var output *rds.DescribeDBParametersOutput
 var params []types.Parameter
 var err error
 parameterPaginator := rds.NewDescribeDBParametersPaginator(instances.RdsClient,
  &rds.DescribeDBParametersInput{
   DBParameterGroupName: aws.String(parameterGroupName),
   Source:               aws.String(source),
  })
 for parameterPaginator.HasMorePages() {
  output, err = parameterPaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get parameters for %v: %v\n", parameterGroupName, err)
   break
  } else {
   params = append(params, output.Parameters...)
  }
 }
 return params, err
}



// UpdateParameters updates parameters in a named DB parameter group.
func (instances *DbInstances) UpdateParameters(parameterGroupName string, params
 []types.Parameter) error {
 _, err := instances.RdsClient.ModifyDBParameterGroup(context.TODO(),
  &rds.ModifyDBParameterGroupInput{
   DBParameterGroupName: aws.String(parameterGroupName),
   Parameters:           params,
  })
 if err != nil {
  log.Printf("Couldn't update parameters in %v: %v\n", parameterGroupName, err)
  return err
 } else {
  return nil
 }
```

```
}



// CreateSnapshot creates a snapshot of a DB instance.
func (instances *DbInstances) CreateSnapshot(instanceName string, snapshotName
 string) (
 *types.DBSnapshot, error) {
 output, err := instances.RdsClient.CreateDBSnapshot(context.TODO(),
 &rds.CreateDBSnapshotInput{
  DBInstanceIdentifier: aws.String(instanceName),
  DBSnapshotIdentifier: aws.String(snapshotName),
 })
 if err != nil {
  log.Printf("Couldn't create snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return output.DBSnapshot, nil
 }
}



// GetSnapshot gets a DB instance snapshot.
func (instances *DbInstances) GetSnapshot(snapshotName string)
 (*types.DBSnapshot, error) {
 output, err := instances.RdsClient.DescribeDBSnapshots(context.TODO(),
  &rds.DescribeDBSnapshotsInput{
   DBSnapshotIdentifier: aws.String(snapshotName),
  })
 if err != nil {
  log.Printf("Couldn't get snapshot %v: %v\n", snapshotName, err)
  return nil, err
 } else {
  return &output.DBSnapshots[0], nil
 }
}



// CreateInstance creates a DB instance.
func (instances *DbInstances) CreateInstance(instanceName string, dbName string,
 dbEngine string, dbEngineVersion string, parameterGroupName string,
 dbInstanceClass string,
```

```
 storageType string, allocatedStorage int32, adminName string, adminPassword
 string) (
 *types.DBInstance, error) {
 output, err := instances.RdsClient.CreateDBInstance(context.TODO(),
 &rds.CreateDBInstanceInput{
  DBInstanceIdentifier: aws.String(instanceName),
  DBName:               aws.String(dbName),
  DBParameterGroupName: aws.String(parameterGroupName),
  Engine:               aws.String(dbEngine),
  EngineVersion:        aws.String(dbEngineVersion),
  DBInstanceClass:      aws.String(dbInstanceClass),
  StorageType:          aws.String(storageType),
  AllocatedStorage:     aws.Int32(allocatedStorage),
  MasterUsername:       aws.String(adminName),
  MasterUserPassword:   aws.String(adminPassword),
 })
 if err != nil {
  log.Printf("Couldn't create instance %v: %v\n", instanceName, err)
  return nil, err
 } else {
  return output.DBInstance, nil
 }
}



// GetInstance gets data about a DB instance.
func (instances *DbInstances) GetInstance(instanceName string) (
 *types.DBInstance, error) {
 output, err := instances.RdsClient.DescribeDBInstances(context.TODO(),
  &rds.DescribeDBInstancesInput{
   DBInstanceIdentifier: aws.String(instanceName),
  })
 if err != nil {
  var notFoundError *types.DBInstanceNotFoundFault
  if errors.As(err, &notFoundError) {
   log.Printf("DB instance %v does not exist.\n", instanceName)
   err = nil
  } else {
   log.Printf("Couldn't get instance %v: %v\n", instanceName, err)
  }
  return nil, err
 } else {
  return &output.DBInstances[0], nil
```

```
 }
}



// DeleteInstance deletes a DB instance.
func (instances *DbInstances) DeleteInstance(instanceName string) error {
 _, err := instances.RdsClient.DeleteDBInstance(context.TODO(),
 &rds.DeleteDBInstanceInput{
  DBInstanceIdentifier:   aws.String(instanceName),
  SkipFinalSnapshot:      true,
  DeleteAutomatedBackups: aws.Bool(true),
 })
 if err != nil {
  log.Printf("Couldn't delete instance %v: %v\n", instanceName, err)
  return err
 } else {
  return nil
 }
}



// GetEngineVersions gets database engine versions that are available for the
 specified engine
// and parameter group family.
func (instances *DbInstances) GetEngineVersions(engine string,
 parameterGroupFamily string) (
 []types.DBEngineVersion, error) {
 output, err := instances.RdsClient.DescribeDBEngineVersions(context.TODO(),
  &rds.DescribeDBEngineVersionsInput{
   Engine:                 aws.String(engine),
   DBParameterGroupFamily: aws.String(parameterGroupFamily),
  })
 if err != nil {
  log.Printf("Couldn't get engine versions for %v: %v\n", engine, err)
  return nil, err
 } else {
  return output.DBEngineVersions, nil
 }
}
```

```
// GetOrderableInstances uses a paginator to get DB instance options that can be
 used to create DB instances that are
// compatible with a set of specifications.
func (instances *DbInstances) GetOrderableInstances(engine string, engineVersion
 string) (
 []types.OrderableDBInstanceOption, error) {

 var output *rds.DescribeOrderableDBInstanceOptionsOutput
 var instanceOptions []types.OrderableDBInstanceOption
 var err error
 orderablePaginator :=
 rds.NewDescribeOrderableDBInstanceOptionsPaginator(instances.RdsClient,
  &rds.DescribeOrderableDBInstanceOptionsInput{
   Engine:        aws.String(engine),
   EngineVersion: aws.String(engineVersion),
  })
 for orderablePaginator.HasMorePages() {
  output, err = orderablePaginator.NextPage(context.TODO())
  if err != nil {
   log.Printf("Couldn't get orderable DB instance options: %v\n", err)
   break
  } else {
   instanceOptions = append(instanceOptions,
 output.OrderableDBInstanceOptions...)
  }
 }
 return instanceOptions, err
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK para Go.
  - CreateDBInstance
  - CreateDBParameterGroup
  - CreateDBSnapshot
  - DeleteDBInstance
  - DeleteDBParameterGroup
  - DescribeDBEngineVersions
  - DescribeDBInstances

- DescribeDBParameterGroups
- DescribeDBParameters
- DescribeDBSnapshots
- DescribeOrderableDBInstanceOptions
- ModifyDBParameterGroup

Java

SDK para Java 2.x

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecute varias operaciones.

```
import com.google.gson.Gson;
import
 software.amazon.awssdk.auth.credentials.EnvironmentVariableCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rds.RdsClient;
import software.amazon.awssdk.services.rds.model.CreateDbInstanceRequest;
import software.amazon.awssdk.services.rds.model.CreateDbInstanceResponse;
import software.amazon.awssdk.services.rds.model.CreateDbParameterGroupResponse;
import software.amazon.awssdk.services.rds.model.CreateDbSnapshotRequest;
import software.amazon.awssdk.services.rds.model.CreateDbSnapshotResponse;
import software.amazon.awssdk.services.rds.model.DBEngineVersion;
import software.amazon.awssdk.services.rds.model.DBInstance;
import software.amazon.awssdk.services.rds.model.DBParameterGroup;
import software.amazon.awssdk.services.rds.model.DBSnapshot;
import software.amazon.awssdk.services.rds.model.DeleteDbInstanceRequest;
import software.amazon.awssdk.services.rds.model.DeleteDbInstanceResponse;
import software.amazon.awssdk.services.rds.model.DescribeDbEngineVersionsRequest;
import
 software.amazon.awssdk.services.rds.model.DescribeDbEngineVersionsResponse;
import software.amazon.awssdk.services.rds.model.DescribeDbInstancesRequest;
import software.amazon.awssdk.services.rds.model.DescribeDbInstancesResponse;
```

```
import
 software.amazon.awssdk.services.rds.model.DescribeDbParameterGroupsResponse;
import software.amazon.awssdk.services.rds.model.DescribeDbParametersResponse;
import software.amazon.awssdk.services.rds.model.DescribeDbSnapshotsRequest;
import software.amazon.awssdk.services.rds.model.DescribeDbSnapshotsResponse;
import
 software.amazon.awssdk.services.rds.model.DescribeOrderableDbInstanceOptionsResponse;
import software.amazon.awssdk.services.rds.model.ModifyDbParameterGroupResponse;
import software.amazon.awssdk.services.rds.model.OrderableDBInstanceOption;
import software.amazon.awssdk.services.rds.model.Parameter;
import software.amazon.awssdk.services.rds.model.RdsException;
import software.amazon.awssdk.services.rds.model.CreateDbParameterGroupRequest;
import
 software.amazon.awssdk.services.rds.model.DescribeDbParameterGroupsRequest;
import software.amazon.awssdk.services.rds.model.DescribeDbParametersRequest;
import software.amazon.awssdk.services.rds.model.ModifyDbParameterGroupRequest;
import
 software.amazon.awssdk.services.rds.model.DescribeOrderableDbInstanceOptionsRequest;
import software.amazon.awssdk.services.rds.model.DeleteDbParameterGroupRequest;
import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
import
 software.amazon.awssdk.services.secretsmanager.model.GetSecretValueRequest;
import
 software.amazon.awssdk.services.secretsmanager.model.GetSecretValueResponse;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * This example requires an AWS Secrets Manager secret that contains the
 * database credentials. If you do not create a
 * secret, this example will not work. For details, see:
 *
 * https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_how-
services-use-secrets_RS.html
 *
 * This Java example performs these tasks:
```

```
 *
 * 1. Returns a list of the available DB engines.
 * 2. Selects an engine family and create a custom DB parameter group.
 * 3. Gets the parameter groups.
 * 4. Gets parameters in the group.
 * 5. Modifies the auto_increment_offset parameter.
 * 6. Gets and displays the updated parameters.
 * 7. Gets a list of allowed engine versions.
 * 8. Gets a list of micro instance classes available for the selected engine.
 * 9. Creates an RDS database instance that contains a MySql database and uses
 * the parameter group.
 * 10. Waits for the DB instance to be ready and prints out the connection
 * endpoint value.
 * 11. Creates a snapshot of the DB instance.
 * 12. Waits for an RDS DB snapshot to be ready.
 * 13. Deletes the RDS DB instance.
 * 14. Deletes the parameter group.
 */
public class RDSScenario {
    public static long sleepTime = 20;
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) throws InterruptedException {
        final String usage = """

                Usage:
                    <dbGroupName> <dbParameterGroupFamily> <dbInstanceIdentifier>
 <dbName> <dbSnapshotIdentifier> <secretName>

                Where:
                    dbGroupName - The database group name.\s
                    dbParameterGroupFamily - The database parameter group name
 (for example, mysql8.0).
                    dbInstanceIdentifier - The database instance identifier\s
                    dbName - The database name.\s
                    dbSnapshotIdentifier - The snapshot identifier.\s
                    secretName - The name of the AWS Secrets Manager secret that
 contains the database credentials"
                """;

        if (args.length != 6) {
            System.out.println(usage);
            System.exit(1);
```

```
        }

        String dbGroupName = args[0];
        String dbParameterGroupFamily = args[1];
        String dbInstanceIdentifier = args[2];
        String dbName = args[3];
        String dbSnapshotIdentifier = args[4];
        String secretName = args[5];

        Gson gson = new Gson();
        User user = gson.fromJson(String.valueOf(getSecretValues(secretName)),
User.class);
        String masterUsername = user.getUsername();
        String masterUserPassword = user.getPassword();

        Region region = Region.US_WEST_2;
        RdsClient rdsClient = RdsClient.builder()
                .region(region)
                .build();
        System.out.println(DASHES);
        System.out.println("Welcome to the Amazon RDS example scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Return a list of the available DB engines");
        describeDBEngines(rdsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Create a custom parameter group");
        createDBParameterGroup(rdsClient, dbGroupName, dbParameterGroupFamily);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Get the parameter group");
        describeDbParameterGroups(rdsClient, dbGroupName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get the parameters in the group");
        describeDbParameters(rdsClient, dbGroupName, 0);
        System.out.println(DASHES);

        System.out.println(DASHES);
```

```
        System.out.println("5. Modify the auto_increment_offset parameter");
        modifyDBParas(rdsClient, dbGroupName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Display the updated value");
        describeDbParameters(rdsClient, dbGroupName, -1);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Get a list of allowed engine versions");
        getAllowedEngines(rdsClient, dbParameterGroupFamily);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Get a list of micro instance classes available for
the selected engine");
        getMicroInstances(rdsClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println(
                "9. Create an RDS database instance that contains a MySql
database and uses the parameter group");
        String dbARN = createDatabaseInstance(rdsClient, dbGroupName,
dbInstanceIdentifier, dbName, masterUsername,
                masterUserPassword);
        System.out.println("The ARN of the new database is " + dbARN);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Wait for DB instance to be ready");
        waitForInstanceReady(rdsClient, dbInstanceIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("11. Create a snapshot of the DB instance");
        createSnapshot(rdsClient, dbInstanceIdentifier, dbSnapshotIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("12. Wait for DB snapshot to be ready");
        waitForSnapshotReady(rdsClient, dbInstanceIdentifier,
dbSnapshotIdentifier);
```

```
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("13. Delete the DB instance");
        deleteDatabaseInstance(rdsClient, dbInstanceIdentifier);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("14. Delete the parameter group");
        deleteParaGroup(rdsClient, dbGroupName, dbARN);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("The Scenario has successfully completed.");
        System.out.println(DASHES);

        rdsClient.close();
    }

    private static SecretsManagerClient getSecretClient() {
        Region region = Region.US_WEST_2;
        return SecretsManagerClient.builder()
                .region(region)

.credentialsProvider(EnvironmentVariableCredentialsProvider.create())
                .build();
    }

    public static String getSecretValues(String secretName) {
        SecretsManagerClient secretClient = getSecretClient();
        GetSecretValueRequest valueRequest = GetSecretValueRequest.builder()
                .secretId(secretName)
                .build();

        GetSecretValueResponse valueResponse =
secretClient.getSecretValue(valueRequest);
        return valueResponse.secretString();
    }

    // Delete the parameter group after database has been deleted.
    // An exception is thrown if you attempt to delete the para group while
database
    // exists.
```

```
   public static void deleteParaGroup(RdsClient rdsClient, String dbGroupName,
String dbARN)
           throws InterruptedException {
       try {
           boolean isDataDel = false;
           boolean didFind;
           String instanceARN;

           // Make sure that the database has been deleted.
           while (!isDataDel) {
               DescribeDbInstancesResponse response =
rdsClient.describeDBInstances();
               List<DBInstance> instanceList = response.dbInstances();
               int listSize = instanceList.size();
               didFind = false;
               int index = 1;
               for (DBInstance instance : instanceList) {
                   instanceARN = instance.dbInstanceArn();
                   if (instanceARN.compareTo(dbARN) == 0) {
                       System.out.println(dbARN + " still exists");
                       didFind = true;
                   }
                   if ((index == listSize) && (!didFind)) {
                       // Went through the entire list and did not find the
database ARN.
                       isDataDel = true;
                   }
                   Thread.sleep(sleepTime * 1000);
                   index++;
               }
           }

           // Delete the para group.
           DeleteDbParameterGroupRequest parameterGroupRequest =
DeleteDbParameterGroupRequest.builder()
                   .dbParameterGroupName(dbGroupName)
                   .build();

           rdsClient.deleteDBParameterGroup(parameterGroupRequest);
           System.out.println(dbGroupName + " was deleted.");

       } catch (RdsException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
```

```
        }
    }

    // Delete the DB instance.
    public static void deleteDatabaseInstance(RdsClient rdsClient, String
dbInstanceIdentifier) {
        try {
            DeleteDbInstanceRequest deleteDbInstanceRequest =
DeleteDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .deleteAutomatedBackups(true)
                    .skipFinalSnapshot(true)
                    .build();

            DeleteDbInstanceResponse response =
rdsClient.deleteDBInstance(deleteDbInstanceRequest);
            System.out.print("The status of the database is " +
response.dbInstance().dbInstanceStatus());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Waits until the snapshot instance is available.
    public static void waitForSnapshotReady(RdsClient rdsClient, String
dbInstanceIdentifier,
            String dbSnapshotIdentifier) {
        try {
            boolean snapshotReady = false;
            String snapshotReadyStr;
            System.out.println("Waiting for the snapshot to become available.");

            DescribeDbSnapshotsRequest snapshotsRequest =
DescribeDbSnapshotsRequest.builder()
                    .dbSnapshotIdentifier(dbSnapshotIdentifier)
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .build();

            while (!snapshotReady) {
                DescribeDbSnapshotsResponse response =
rdsClient.describeDBSnapshots(snapshotsRequest);
                List<DBSnapshot> snapshotList = response.dbSnapshots();
```

```
                for (DBSnapshot snapshot : snapshotList) {
                    snapshotReadyStr = snapshot.status();
                    if (snapshotReadyStr.contains("available")) {
                        snapshotReady = true;
                    } else {
                        System.out.print(".");
                        Thread.sleep(sleepTime * 1000);
                    }
                }
            }

            System.out.println("The Snapshot is available!");
        } catch (RdsException | InterruptedException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Create an Amazon RDS snapshot.
    public static void createSnapshot(RdsClient rdsClient, String
dbInstanceIdentifier, String dbSnapshotIdentifier) {
        try {
            CreateDbSnapshotRequest snapshotRequest =
CreateDbSnapshotRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .dbSnapshotIdentifier(dbSnapshotIdentifier)
                    .build();

            CreateDbSnapshotResponse response =
rdsClient.createDBSnapshot(snapshotRequest);
            System.out.println("The Snapshot id is " +
response.dbSnapshot().dbiResourceId());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Waits until the database instance is available.
    public static void waitForInstanceReady(RdsClient rdsClient, String
dbInstanceIdentifier) {
        boolean instanceReady = false;
        String instanceReadyStr;
```

```
        System.out.println("Waiting for instance to become available.");
        try {
            DescribeDbInstancesRequest instanceRequest =
DescribeDbInstancesRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
                    .build();

            String endpoint = "";
            while (!instanceReady) {
                DescribeDbInstancesResponse response =
rdsClient.describeDBInstances(instanceRequest);
                List<DBInstance> instanceList = response.dbInstances();
                for (DBInstance instance : instanceList) {
                    instanceReadyStr = instance.dbInstanceStatus();
                    if (instanceReadyStr.contains("available")) {
                        endpoint = instance.endpoint().address();
                        instanceReady = true;
                    } else {
                        System.out.print(".");
                        Thread.sleep(sleepTime * 1000);
                    }
                }
            }
            System.out.println("Database instance is available! The connection
endpoint is " + endpoint);

        } catch (RdsException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    // Create a database instance and return the ARN of the database.
    public static String createDatabaseInstance(RdsClient rdsClient,
            String dbGroupName,
            String dbInstanceIdentifier,
            String dbName,
            String masterUsername,
            String masterUserPassword) {

        try {
            CreateDbInstanceRequest instanceRequest =
CreateDbInstanceRequest.builder()
                    .dbInstanceIdentifier(dbInstanceIdentifier)
```

```
                    .allocatedStorage(100)
                    .dbName(dbName)
                    .dbParameterGroupName(dbGroupName)
                    .engine("mysql")
                    .dbInstanceClass("db.m4.large")
                    .engineVersion("8.0")
                    .storageType("standard")
                    .masterUsername(masterUsername)
                    .masterUserPassword(masterUserPassword)
                    .build();

            CreateDbInstanceResponse response =
rdsClient.createDBInstance(instanceRequest);
            System.out.print("The status is " +
response.dbInstance().dbInstanceStatus());
            return response.dbInstance().dbInstanceArn();

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }

        return "";
    }

    // Get a list of micro instances.
    public static void getMicroInstances(RdsClient rdsClient) {
        try {
            DescribeOrderableDbInstanceOptionsRequest dbInstanceOptionsRequest =
DescribeOrderableDbInstanceOptionsRequest
                    .builder()
                    .engine("mysql")
                    .build();

            DescribeOrderableDbInstanceOptionsResponse response = rdsClient

.describeOrderableDBInstanceOptions(dbInstanceOptionsRequest);
            List<OrderableDBInstanceOption> orderableDBInstances =
response.orderableDBInstanceOptions();
            for (OrderableDBInstanceOption dbInstanceOption :
orderableDBInstances) {
                System.out.println("The engine version is " +
dbInstanceOption.engineVersion());
```

```
                System.out.println("The engine description is " +
dbInstanceOption.engine());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Get a list of allowed engine versions.
    public static void getAllowedEngines(RdsClient rdsClient, String
dbParameterGroupFamily) {
        try {
            DescribeDbEngineVersionsRequest versionsRequest =
DescribeDbEngineVersionsRequest.builder()
                    .dbParameterGroupFamily(dbParameterGroupFamily)
                    .engine("mysql")
                    .build();

            DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(versionsRequest);
            List<DBEngineVersion> dbEngines = response.dbEngineVersions();
            for (DBEngineVersion dbEngine : dbEngines) {
                System.out.println("The engine version is " +
dbEngine.engineVersion());
                System.out.println("The engine description is " +
dbEngine.dbEngineDescription());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Modify auto_increment_offset and auto_increment_increment parameters.
    public static void modifyDBParas(RdsClient rdsClient, String dbGroupName) {
        try {
            Parameter parameter1 = Parameter.builder()
                    .parameterName("auto_increment_offset")
                    .applyMethod("immediate")
                    .parameterValue("5")
                    .build();
```

```
            List<Parameter> paraList = new ArrayList<>();
            paraList.add(parameter1);
            ModifyDbParameterGroupRequest groupRequest =
ModifyDbParameterGroupRequest.builder()
                    .dbParameterGroupName(dbGroupName)
                    .parameters(paraList)
                    .build();

            ModifyDbParameterGroupResponse response =
rdsClient.modifyDBParameterGroup(groupRequest);
            System.out.println("The parameter group " +
response.dbParameterGroupName() + " was successfully modified");

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    // Retrieve parameters in the group.
    public static void describeDbParameters(RdsClient rdsClient, String
dbGroupName, int flag) {
        try {
            DescribeDbParametersRequest dbParameterGroupsRequest;
            if (flag == 0) {
                dbParameterGroupsRequest = DescribeDbParametersRequest.builder()
                        .dbParameterGroupName(dbGroupName)
                        .build();
            } else {
                dbParameterGroupsRequest = DescribeDbParametersRequest.builder()
                        .dbParameterGroupName(dbGroupName)
                        .source("user")
                        .build();
            }

            DescribeDbParametersResponse response =
rdsClient.describeDBParameters(dbParameterGroupsRequest);
            List<Parameter> dbParameters = response.parameters();
            String paraName;
            for (Parameter para : dbParameters) {
                // Only print out information about either auto_increment_offset
or
                // auto_increment_increment.
```

```
                paraName = para.parameterName();
                if ((paraName.compareTo("auto_increment_offset") == 0)
                        || (paraName.compareTo("auto_increment_increment ") ==
0)) {
                    System.out.println("*** The parameter name is  " + paraName);
                    System.out.println("*** The parameter value is  " +
para.parameterValue());
                    System.out.println("*** The parameter data type is " +
para.dataType());
                    System.out.println("*** The parameter description is " +
para.description());
                    System.out.println("*** The parameter allowed values  is " +
para.allowedValues());
                }
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeDbParameterGroups(RdsClient rdsClient, String
dbGroupName) {
        try {
            DescribeDbParameterGroupsRequest groupsRequest =
DescribeDbParameterGroupsRequest.builder()
                    .dbParameterGroupName(dbGroupName)
                    .maxRecords(20)
                    .build();

            DescribeDbParameterGroupsResponse response =
rdsClient.describeDBParameterGroups(groupsRequest);
            List<DBParameterGroup> groups = response.dbParameterGroups();
            for (DBParameterGroup group : groups) {
                System.out.println("The group name is " +
group.dbParameterGroupName());
                System.out.println("The group description is " +
group.description());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
```

```
        }
    }

    public static void createDBParameterGroup(RdsClient rdsClient, String
dbGroupName, String dbParameterGroupFamily) {
        try {
            CreateDbParameterGroupRequest groupRequest =
CreateDbParameterGroupRequest.builder()
                    .dbParameterGroupName(dbGroupName)
                    .dbParameterGroupFamily(dbParameterGroupFamily)
                    .description("Created by using the AWS SDK for Java")
                    .build();

            CreateDbParameterGroupResponse response =
rdsClient.createDBParameterGroup(groupRequest);
            System.out.println("The group name is " +
response.dbParameterGroup().dbParameterGroupName());

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeDBEngines(RdsClient rdsClient) {
        try {
            DescribeDbEngineVersionsRequest engineVersionsRequest =
DescribeDbEngineVersionsRequest.builder()
                    .defaultOnly(true)
                    .engine("mysql")
                    .maxRecords(20)
                    .build();

            DescribeDbEngineVersionsResponse response =
rdsClient.describeDBEngineVersions(engineVersionsRequest);
            List<DBEngineVersion> engines = response.dbEngineVersions();

            // Get all DBEngineVersion objects.
            for (DBEngineVersion engineOb : engines) {
                System.out.println("The name of the DB parameter group family for
the database engine is "
                        + engineOb.dbParameterGroupFamily());
                System.out.println("The name of the database engine " +
engineOb.engine());
```

```
                System.out.println("The version number of the database engine " +
 engineOb.engineVersion());
            }

        } catch (RdsException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK for Java 2.x.
  - CreateDBInstance
  - CreateDBParameterGroup
  - CreateDBSnapshot
  - DeleteDBInstance
  - DeleteDBParameterGroup
  - DescribeDBEngineVersions
  - DescribeDBInstances
  - DescribeDBParameterGroups
  - DescribeDBParameters
  - DescribeDBSnapshots
  - DescribeOrderableDBInstanceOptions
  - ModifyDBParameterGroup

Kotlin

SDK para Kotlin

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
/**
Before running this code example, set up your development environment, including
 your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

This example requires an AWS Secrets Manager secret that contains the database
 credentials. If you do not create a
secret, this example will not work. For more details, see:

https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_how-
services-use-secrets_RS.html

This example performs the following tasks:

1. Returns a list of the available DB engines by invoking the
 DescribeDbEngineVersions method.
2. Selects an engine family and create a custom DB parameter group by invoking
 the createDBParameterGroup method.
3. Gets the parameter groups by invoking the DescribeDbParameterGroups method.
4. Gets parameters in the group by invoking the DescribeDbParameters method.
5. Modifies both the auto_increment_offset and auto_increment_increment
 parameters by invoking the modifyDbParameterGroup method.
6. Gets and displays the updated parameters.
7. Gets a list of allowed engine versions by invoking the
 describeDbEngineVersions method.
8. Gets a list of micro instance classes available for the selected engine.
9. Creates an Amazon Relational Database Service (Amazon RDS) database instance
 that contains a MySQL database and uses the parameter group.
10. Waits for DB instance to be ready and prints out the connection endpoint
 value.
11. Creates a snapshot of the DB instance.
12. Waits for the DB snapshot to be ready.
13. Deletes the DB instance.
14. Deletes the parameter group.
 */

var sleepTime: Long = 20

suspend fun main(args: Array<String>) {
```

```
   val usage = """
       Usage:
           <dbGroupName> <dbParameterGroupFamily> <dbInstanceIdentifier>
<dbName> <dbSnapshotIdentifier><secretName>

       Where:
           dbGroupName - The database group name.
           dbParameterGroupFamily - The database parameter group name.
           dbInstanceIdentifier - The database instance identifier.
           dbName -  The database name.
           dbSnapshotIdentifier - The snapshot identifier.
           secretName - The name of the AWS Secrets Manager secret that contains
the database credentials.
   """

   if (args.size != 6) {
       println(usage)
       exitProcess(1)
   }

   val dbGroupName = args[0]
   val dbParameterGroupFamily = args[1]
   val dbInstanceIdentifier = args[2]
   val dbName = args[3]
   val dbSnapshotIdentifier = args[4]
   val secretName = args[5]

   val gson = Gson()
   val user = gson.fromJson(getSecretValues(secretName).toString(),
User::class.java)
   val username = user.username
   val userPassword = user.password

   println("1. Return a list of the available DB engines")
   describeDBEngines()

   println("2. Create a custom parameter group")
   createDBParameterGroup(dbGroupName, dbParameterGroupFamily)

   println("3. Get the parameter groups")
   describeDbParameterGroups(dbGroupName)

   println("4. Get the parameters in the group")
   describeDbParameters(dbGroupName, 0)
```

```
    println("5. Modify the auto_increment_offset parameter")
    modifyDBParas(dbGroupName)

    println("6. Display the updated value")
    describeDbParameters(dbGroupName, -1)

    println("7. Get a list of allowed engine versions")
    getAllowedEngines(dbParameterGroupFamily)

    println("8. Get a list of micro instance classes available for the selected
 engine")
    getMicroInstances()

    println("9. Create an RDS database instance that contains a MySql database
 and uses the parameter group")
    val dbARN = createDatabaseInstance(dbGroupName, dbInstanceIdentifier, dbName,
 username, userPassword)
    println("The ARN of the new database is $dbARN")

    println("10. Wait for DB instance to be ready")
    waitForDbInstanceReady(dbInstanceIdentifier)

    println("11. Create a snapshot of the DB instance")
    createDbSnapshot(dbInstanceIdentifier, dbSnapshotIdentifier)

    println("12. Wait for DB snapshot to be ready")
    waitForSnapshotReady(dbInstanceIdentifier, dbSnapshotIdentifier)

    println("13. Delete the DB instance")
    deleteDbInstance(dbInstanceIdentifier)

    println("14. Delete the parameter group")
    if (dbARN != null) {
        deleteParaGroup(dbGroupName, dbARN)
    }

    println("The Scenario has successfully completed.")
}

suspend fun deleteParaGroup(
    dbGroupName: String,
    dbARN: String,
) {
```

```
    var isDataDel = false
    var didFind: Boolean
    var instanceARN: String

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        // Make sure that the database has been deleted.
        while (!isDataDel) {
            val response = rdsClient.describeDbInstances()
            val instanceList = response.dbInstances
            val listSize = instanceList?.size
            isDataDel = false // Reset this value.
            didFind = false // Reset this value.
            var index = 1
            if (instanceList != null) {
                for (instance in instanceList) {
                    instanceARN = instance.dbInstanceArn.toString()
                    if (instanceARN.compareTo(dbARN) == 0) {
                        println("$dbARN still exists")
                        didFind = true
                    }
                    if (index == listSize && !didFind) {
                        // Went through the entire list and did not find the
 database name.
                        isDataDel = true
                    }
                    index++
                }
            }
        }

        // Delete the para group.
        val parameterGroupRequest =
            DeleteDbParameterGroupRequest {
                dbParameterGroupName = dbGroupName
            }
        rdsClient.deleteDbParameterGroup(parameterGroupRequest)
        println("$dbGroupName was deleted.")
    }
}

suspend fun deleteDbInstance(dbInstanceIdentifierVal: String) {
    val deleteDbInstanceRequest =
        DeleteDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
```

```
            deleteAutomatedBackups = true
            skipFinalSnapshot = true
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.deleteDbInstance(deleteDbInstanceRequest)
        print("The status of the database is
 ${response.dbInstance?.dbInstanceStatus}")
    }
}

// Waits until the snapshot instance is available.
suspend fun waitForSnapshotReady(
    dbInstanceIdentifierVal: String?,
    dbSnapshotIdentifierVal: String?,
) {
    var snapshotReady = false
    var snapshotReadyStr: String
    println("Waiting for the snapshot to become available.")

    val snapshotsRequest =
        DescribeDbSnapshotsRequest {
            dbSnapshotIdentifier = dbSnapshotIdentifierVal
            dbInstanceIdentifier = dbInstanceIdentifierVal
        }

    while (!snapshotReady) {
        RdsClient { region = "us-west-2" }.use { rdsClient ->
            val response = rdsClient.describeDbSnapshots(snapshotsRequest)
            val snapshotList: List<DbSnapshot>? = response.dbSnapshots
            if (snapshotList != null) {
                for (snapshot in snapshotList) {
                    snapshotReadyStr = snapshot.status.toString()
                    if (snapshotReadyStr.contains("available")) {
                        snapshotReady = true
                    } else {
                        print(".")
                        delay(sleepTime * 1000)
                    }
                }
            }
        }
    }
    println("The Snapshot is available!")
```

```
}

// Create an Amazon RDS snapshot.
suspend fun createDbSnapshot(
    dbInstanceIdentifierVal: String?,
    dbSnapshotIdentifierVal: String?,
) {
    val snapshotRequest =
        CreateDbSnapshotRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            dbSnapshotIdentifier = dbSnapshotIdentifierVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbSnapshot(snapshotRequest)
        print("The Snapshot id is ${response.dbSnapshot?.dbiResourceId}")
    }
}

// Waits until the database instance is available.
suspend fun waitForDbInstanceReady(dbInstanceIdentifierVal: String?) {
    var instanceReady = false
    var instanceReadyStr: String
    println("Waiting for instance to become available.")

    val instanceRequest =
        DescribeDbInstancesRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
        }
    var endpoint = ""
    while (!instanceReady) {
        RdsClient { region = "us-west-2" }.use { rdsClient ->
            val response = rdsClient.describeDbInstances(instanceRequest)
            val instanceList = response.dbInstances
            if (instanceList != null) {
                for (instance in instanceList) {
                    instanceReadyStr = instance.dbInstanceStatus.toString()
                    if (instanceReadyStr.contains("available")) {
                        endpoint = instance.endpoint?.address.toString()
                        instanceReady = true
                    } else {
                        print(".")
                        delay(sleepTime * 1000)
                    }
```

```
                }
            }
        }
    }
    println("Database instance is available! The connection endpoint is
 $endpoint")
}

// Create a database instance and return the ARN of the database.
suspend fun createDatabaseInstance(
    dbGroupNameVal: String?,
    dbInstanceIdentifierVal: String?,
    dbNameVal: String?,
    masterUsernameVal: String?,
    masterUserPasswordVal: String?,
): String? {
    val instanceRequest =
        CreateDbInstanceRequest {
            dbInstanceIdentifier = dbInstanceIdentifierVal
            allocatedStorage = 100
            dbName = dbNameVal
            dbParameterGroupName = dbGroupNameVal
            engine = "mysql"
            dbInstanceClass = "db.m4.large"
            engineVersion = "8.0"
            storageType = "standard"
            masterUsername = masterUsernameVal
            masterUserPassword = masterUserPasswordVal
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbInstance(instanceRequest)
        print("The status is ${response.dbInstance?.dbInstanceStatus}")
        return response.dbInstance?.dbInstanceArn
    }
}

// Get a list of micro instances.
suspend fun getMicroInstances() {
    val dbInstanceOptionsRequest =
        DescribeOrderableDbInstanceOptionsRequest {
            engine = "mysql"
        }
    RdsClient { region = "us-west-2" }.use { rdsClient ->
```

```
        val response =
 rdsClient.describeOrderableDbInstanceOptions(dbInstanceOptionsRequest)
        val orderableDBInstances = response.orderableDbInstanceOptions
        if (orderableDBInstances != null) {
            for (dbInstanceOption in orderableDBInstances) {
                println("The engine version is
 ${dbInstanceOption.engineVersion}")
                println("The engine description is ${dbInstanceOption.engine}")
            }
        }
    }
}

// Get a list of allowed engine versions.
suspend fun getAllowedEngines(dbParameterGroupFamilyVal: String?) {
    val versionsRequest =
        DescribeDbEngineVersionsRequest {
            dbParameterGroupFamily = dbParameterGroupFamilyVal
            engine = "mysql"
        }
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbEngineVersions(versionsRequest)
        val dbEngines: List<DbEngineVersion>? = response.dbEngineVersions
        if (dbEngines != null) {
            for (dbEngine in dbEngines) {
                println("The engine version is ${dbEngine.engineVersion}")
                println("The engine description is
 ${dbEngine.dbEngineDescription}")
            }
        }
    }
}

// Modify the auto_increment_offset parameter.
suspend fun modifyDBParas(dbGroupName: String) {
    val parameter1 =
        Parameter {
            parameterName = "auto_increment_offset"
            applyMethod = ApplyMethod.Immediate
            parameterValue = "5"
        }

    val paraList: ArrayList<Parameter> = ArrayList()
    paraList.add(parameter1)
```

```
    val groupRequest =
        ModifyDbParameterGroupRequest {
            dbParameterGroupName = dbGroupName
            parameters = paraList
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.modifyDbParameterGroup(groupRequest)
        println("The parameter group ${response.dbParameterGroupName} was
 successfully modified")
    }
}

// Retrieve parameters in the group.
suspend fun describeDbParameters(
    dbGroupName: String?,
    flag: Int,
) {
    val dbParameterGroupsRequest: DescribeDbParametersRequest
    dbParameterGroupsRequest =
        if (flag == 0) {
            DescribeDbParametersRequest {
                dbParameterGroupName = dbGroupName
            }
        } else {
            DescribeDbParametersRequest {
                dbParameterGroupName = dbGroupName
                source = "user"
            }
        }
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbParameters(dbParameterGroupsRequest)
        val dbParameters: List<Parameter>? = response.parameters
        var paraName: String
        if (dbParameters != null) {
            for (para in dbParameters) {
                // Only print out information about either auto_increment_offset
 or auto_increment_increment.
                paraName = para.parameterName.toString()
                if (paraName.compareTo("auto_increment_offset") == 0 ||
 paraName.compareTo("auto_increment_increment ") == 0) {
                    println("*** The parameter name is  $paraName")
                    System.out.println("*** The parameter value is
 ${para.parameterValue}")
```

```
                    System.out.println("*** The parameter data type is
 ${para.dataType}")
                    System.out.println("*** The parameter description is
 ${para.description}")
                    System.out.println("*** The parameter allowed values  is
 ${para.allowedValues}")
                }
            }
        }
    }
}

suspend fun describeDbParameterGroups(dbGroupName: String?) {
    val groupsRequest =
        DescribeDbParameterGroupsRequest {
            dbParameterGroupName = dbGroupName
            maxRecords = 20
        }
    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbParameterGroups(groupsRequest)
        val groups = response.dbParameterGroups
        if (groups != null) {
            for (group in groups) {
                println("The group name is ${group.dbParameterGroupName}")
                println("The group description is ${group.description}")
            }
        }
    }
}

// Create a parameter group.
suspend fun createDBParameterGroup(
    dbGroupName: String?,
    dbParameterGroupFamilyVal: String?,
) {
    val groupRequest =
        CreateDbParameterGroupRequest {
            dbParameterGroupName = dbGroupName
            dbParameterGroupFamily = dbParameterGroupFamilyVal
            description = "Created by using the AWS SDK for Kotlin"
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.createDbParameterGroup(groupRequest)
```

```
        println("The group name is
 ${response.dbParameterGroup?.dbParameterGroupName}")
    }
}

// Returns a list of the available DB engines.
suspend fun describeDBEngines() {
    val engineVersionsRequest =
        DescribeDbEngineVersionsRequest {
            defaultOnly = true
            engine = "mysql"
            maxRecords = 20
        }

    RdsClient { region = "us-west-2" }.use { rdsClient ->
        val response = rdsClient.describeDbEngineVersions(engineVersionsRequest)
        val engines: List<DbEngineVersion>? = response.dbEngineVersions

        // Get all DbEngineVersion objects.
        if (engines != null) {
            for (engineOb in engines) {
                println("The name of the DB parameter group family for the
 database engine is ${engineOb.dbParameterGroupFamily}.")
                println("The name of the database engine ${engineOb.engine}.")
                println("The version number of the database engine
 ${engineOb.engineVersion}")
            }
        }
    }
}

suspend fun getSecretValues(secretName: String?): String? {
    val valueRequest =
        GetSecretValueRequest {
            secretId = secretName
        }

    SecretsManagerClient { region = "us-west-2" }.use { secretsClient ->
        val valueResponse = secretsClient.getSecretValue(valueRequest)
        return valueResponse.secretString
    }
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Kotlin.
  - CreateDBInstance
  - CreateDBParameterGroup
  - CreateDBSnapshot
  - DeleteDBInstance
  - DeleteDBParameterGroup
  - DescribeDBEngineVersions
  - DescribeDBInstances
  - DescribeDBParameterGroups
  - DescribeDBParameters
  - DescribeDBSnapshots
  - DescribeOrderableDBInstanceOptions
  - ModifyDBParameterGroup

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecutar un escenario interactivo en un símbolo del sistema.

```
class RdsInstanceScenario:
    """Runs a scenario that shows how to get started using Amazon RDS DB
 instances."""

    def __init__(self, instance_wrapper):
        """
        :param instance_wrapper: An object that wraps Amazon RDS DB instance
 actions.
        """
```

```
        self.instance_wrapper = instance_wrapper

    def create_parameter_group(self, parameter_group_name, db_engine):
        """
        Shows how to get available engine versions for a specified database
engine and
        create a DB parameter group that is compatible with a selected engine
family.

        :param parameter_group_name: The name given to the newly created
parameter group.
        :param db_engine: The database engine to use as a basis.
        :return: The newly created parameter group.
        """
        print(
            f"Checking for an existing DB instance parameter group named
{parameter_group_name}."
        )
        parameter_group = self.instance_wrapper.get_parameter_group(
            parameter_group_name
        )
        if parameter_group is None:
            print(f"Getting available database engine versions for {db_engine}.")
            engine_versions =
self.instance_wrapper.get_engine_versions(db_engine)
            families = list({ver["DBParameterGroupFamily"] for ver in
engine_versions})
            family_index = q.choose("Which family do you want to use? ",
families)
            print(f"Creating a parameter group.")
            self.instance_wrapper.create_parameter_group(
                parameter_group_name, families[family_index], "Example parameter
group."
            )
            parameter_group = self.instance_wrapper.get_parameter_group(
                parameter_group_name
            )
        print(f"Parameter group {parameter_group['DBParameterGroupName']}:")
        pp(parameter_group)
        print("-" * 88)
        return parameter_group

    def update_parameters(self, parameter_group_name):
        """
```

```
        Shows how to get the parameters contained in a custom parameter group and
        update some of the parameter values in the group.

        :param parameter_group_name: The name of the parameter group to query and
modify.
        """
        print("Let's set some parameter values in your parameter group.")
        auto_inc_parameters = self.instance_wrapper.get_parameters(
            parameter_group_name, name_prefix="auto_increment"
        )
        update_params = []
        for auto_inc in auto_inc_parameters:
            if auto_inc["IsModifiable"] and auto_inc["DataType"] == "integer":
                print(f"The {auto_inc['ParameterName']} parameter is described
as:")
                print(f"\t{auto_inc['Description']}")
                param_range = auto_inc["AllowedValues"].split("-")
                auto_inc["ParameterValue"] = str(
                    q.ask(
                        f"Enter a value between {param_range[0]} and
{param_range[1]}: ",
                        q.is_int,
                        q.in_range(int(param_range[0]), int(param_range[1])),
                    )
                )
                update_params.append(auto_inc)
        self.instance_wrapper.update_parameters(parameter_group_name,
update_params)
        print(
            "You can get a list of parameters you've set by specifying a source
of 'user'."
        )
        user_parameters = self.instance_wrapper.get_parameters(
            parameter_group_name, source="user"
        )
        pp(user_parameters)
        print("-" * 88)

    def create_instance(self, instance_name, db_name, db_engine,
parameter_group):
        """
        Shows how to create a DB instance that contains a database of a specified
        type and is configured to use a custom DB parameter group.
```

```
        :param instance_name: The name given to the newly created DB instance.
        :param db_name: The name given to the created database.
        :param db_engine: The engine of the created database.
        :param parameter_group: The parameter group that is associated with the
DB instance.
        :return: The newly created DB instance.
        """
        print("Checking for an existing DB instance.")
        db_inst = self.instance_wrapper.get_db_instance(instance_name)
        if db_inst is None:
            print("Let's create a DB instance.")
            admin_username = q.ask(
                "Enter an administrator user name for the database: ",
q.non_empty
            )
            admin_password = q.ask(
                "Enter a password for the administrator (at least 8 characters):
",
                q.non_empty,
            )
            engine_versions = self.instance_wrapper.get_engine_versions(
                db_engine, parameter_group["DBParameterGroupFamily"]
            )
            engine_choices = [ver["EngineVersion"] for ver in engine_versions]
            print("The available engines for your parameter group are:")
            engine_index = q.choose("Which engine do you want to use? ",
engine_choices)
            engine_selection = engine_versions[engine_index]
            print(
                "The available micro DB instance classes for your database engine
are:"
            )
            inst_opts = self.instance_wrapper.get_orderable_instances(
                engine_selection["Engine"], engine_selection["EngineVersion"]
            )
            inst_choices = list(
                {
                    opt["DBInstanceClass"]
                    for opt in inst_opts
                    if "micro" in opt["DBInstanceClass"]
                }
            )
            inst_index = q.choose(
```

```
                "Which micro DB instance class do you want to use? ",
inst_choices
            )
            group_name = parameter_group["DBParameterGroupName"]
            storage_type = "standard"
            allocated_storage = 5
            print(
                f"Creating a DB instance named {instance_name} and database
{db_name}.\n"
                f"The DB instance is configured to use your custom parameter
group {group_name},\n"
                f"selected engine {engine_selection['EngineVersion']},\n"
                f"selected DB instance class {inst_choices[inst_index]},"
                f"and {allocated_storage} GiB of {storage_type} storage.\n"
                f"This typically takes several minutes."
            )
            db_inst = self.instance_wrapper.create_db_instance(
                db_name,
                instance_name,
                group_name,
                engine_selection["Engine"],
                engine_selection["EngineVersion"],
                inst_choices[inst_index],
                storage_type,
                allocated_storage,
                admin_username,
                admin_password,
            )
            while db_inst.get("DBInstanceStatus") != "available":
                wait(10)
                db_inst = self.instance_wrapper.get_db_instance(instance_name)
        print("Instance data:")
        pp(db_inst)
        print("-" * 88)
        return db_inst

    @staticmethod
    def display_connection(db_inst):
        """
        Displays connection information about a DB instance and tips on how to
        connect to it.

        :param db_inst: The DB instance to display.
        """
```

```
        print(
            "You can now connect to your database using your favorite MySql
 client.\n"
            "One way to connect is by using the 'mysql' shell on an Amazon EC2
 instance\n"
            "that is running in the same VPC as your DB instance. Pass the
 endpoint,\n"
            "port, and administrator user name to 'mysql' and enter your password
\n"
            "when prompted:\n"
        )
        print(
            f"\n\tmysql -h {db_inst['Endpoint']['Address']} -P
 {db_inst['Endpoint']['Port']} "
            f"-u {db_inst['MasterUsername']} -p\n"
        )
        print(
            "For more information, see the User Guide for Amazon RDS:\n"
            "\thttps://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/
CHAP_GettingStarted.CreatingConnecting.MySQL.html#CHAP_GettingStarted.Connecting.MySQL"
        )
        print("-" * 88)

    def create_snapshot(self, instance_name):
        """
        Shows how to create a DB instance snapshot and wait until it's available.

        :param instance_name: The name of a DB instance to snapshot.
        """
        if q.ask(
            "Do you want to create a snapshot of your DB instance (y/n)? ",
 q.is_yesno
        ):
            snapshot_id = f"{instance_name}-{uuid.uuid4()}"
            print(
                f"Creating a snapshot named {snapshot_id}. This typically takes a
 few minutes."
            )
            snapshot = self.instance_wrapper.create_snapshot(snapshot_id,
 instance_name)
            while snapshot.get("Status") != "available":
                wait(10)
                snapshot = self.instance_wrapper.get_snapshot(snapshot_id)
            pp(snapshot)
```

```
            print("-" * 88)

    def cleanup(self, db_inst, parameter_group_name):
        """
        Shows how to clean up a DB instance and parameter group.
        Before the parameter group can be deleted, all associated DB instances
must first
        be deleted.

        :param db_inst: The DB instance to delete.
        :param parameter_group_name: The DB parameter group to delete.
        """
        if q.ask(
            "\nDo you want to delete the DB instance and parameter group (y/n)?
",
            q.is_yesno,
        ):
            print(f"Deleting DB instance {db_inst['DBInstanceIdentifier']}.")

self.instance_wrapper.delete_db_instance(db_inst["DBInstanceIdentifier"])
            print(
                "Waiting for the DB instance to delete. This typically takes
several minutes."
            )
            while db_inst is not None:
                wait(10)
                db_inst = self.instance_wrapper.get_db_instance(
                    db_inst["DBInstanceIdentifier"]
                )
            print(f"Deleting parameter group {parameter_group_name}.")
            self.instance_wrapper.delete_parameter_group(parameter_group_name)

    def run_scenario(self, db_engine, parameter_group_name, instance_name,
db_name):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
%(message)s")

        print("-" * 88)
        print(
            "Welcome to the Amazon Relational Database Service (Amazon RDS)\n"
            "get started with DB instances demo."
        )
        print("-" * 88)
```

```
        parameter_group = self.create_parameter_group(parameter_group_name,
 db_engine)
        self.update_parameters(parameter_group_name)
        db_inst = self.create_instance(
            instance_name, db_name, db_engine, parameter_group
        )
        self.display_connection(db_inst)
        self.create_snapshot(instance_name)
        self.cleanup(db_inst, parameter_group_name)

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = RdsInstanceScenario(InstanceWrapper.from_client())
        scenario.run_scenario(
            "mysql",
            "doc-example-parameter-group",
            "doc-example-instance",
            "docexampledb",
        )
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

Defina las funciones a las que llama el escenario para administrar las acciones de Amazon RDS.

```
class InstanceWrapper:
    """Encapsulates Amazon RDS DB instance actions."""

    def __init__(self, rds_client):
        """
        :param rds_client: A Boto3 Amazon RDS client.
        """
        self.rds_client = rds_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
```

```
        """
        rds_client = boto3.client("rds")
        return cls(rds_client)


    def get_parameter_group(self, parameter_group_name):
        """
        Gets a DB parameter group.

        :param parameter_group_name: The name of the parameter group to retrieve.
        :return: The parameter group.
        """
        try:
            response = self.rds_client.describe_db_parameter_groups(
                DBParameterGroupName=parameter_group_name
            )
            parameter_group = response["DBParameterGroups"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBParameterGroupNotFound":
                logger.info("Parameter group %s does not exist.",
parameter_group_name)
            else:
                logger.error(
                    "Couldn't get parameter group %s. Here's why: %s: %s",
                    parameter_group_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return parameter_group


    def create_parameter_group(
        self, parameter_group_name, parameter_group_family, description
    ):
        """
        Creates a DB parameter group that is based on the specified parameter
group
        family.

        :param parameter_group_name: The name of the newly created parameter
group.
```

```
        :param parameter_group_family: The family that is used as the basis of
the new
                                       parameter group.
        :param description: A description given to the parameter group.
        :return: Data about the newly created parameter group.
        """
        try:
            response = self.rds_client.create_db_parameter_group(
                DBParameterGroupName=parameter_group_name,
                DBParameterGroupFamily=parameter_group_family,
                Description=description,
            )
        except ClientError as err:
            logger.error(
                "Couldn't create parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def delete_parameter_group(self, parameter_group_name):
        """
        Deletes a DB parameter group.

        :param parameter_group_name: The name of the parameter group to delete.
        :return: Data about the parameter group.
        """
        try:
            self.rds_client.delete_db_parameter_group(
                DBParameterGroupName=parameter_group_name
            )
        except ClientError as err:
            logger.error(
                "Couldn't delete parameter group %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

```
    def get_parameters(self, parameter_group_name, name_prefix="", source=None):
        """
        Gets the parameters that are contained in a DB parameter group.

        :param parameter_group_name: The name of the parameter group to query.
        :param name_prefix: When specified, the retrieved list of parameters is
filtered
                            to contain only parameters that start with this
prefix.
        :param source: When specified, only parameters from this source are
retrieved.
                       For example, a source of 'user' retrieves only parameters
that
                       were set by a user.
        :return: The list of requested parameters.
        """
        try:
            kwargs = {"DBParameterGroupName": parameter_group_name}
            if source is not None:
                kwargs["Source"] = source
            parameters = []
            paginator = self.rds_client.get_paginator("describe_db_parameters")
            for page in paginator.paginate(**kwargs):
                parameters += [
                    p
                    for p in page["Parameters"]
                    if p["ParameterName"].startswith(name_prefix)
                ]
        except ClientError as err:
            logger.error(
                "Couldn't get parameters for %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return parameters


    def update_parameters(self, parameter_group_name, update_parameters):
        """
        Updates parameters in a custom DB parameter group.
```

```
        :param parameter_group_name: The name of the parameter group to update.
        :param update_parameters: The parameters to update in the group.
        :return: Data about the modified parameter group.
        """
        try:
            response = self.rds_client.modify_db_parameter_group(
                DBParameterGroupName=parameter_group_name,
Parameters=update_parameters
            )
        except ClientError as err:
            logger.error(
                "Couldn't update parameters in %s. Here's why: %s: %s",
                parameter_group_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def create_snapshot(self, snapshot_id, instance_id):
        """
        Creates a snapshot of a DB instance.

        :param snapshot_id: The ID to give the created snapshot.
        :param instance_id: The ID of the DB instance to snapshot.
        :return: Data about the newly created snapshot.
        """
        try:
            response = self.rds_client.create_db_snapshot(
                DBSnapshotIdentifier=snapshot_id,
DBInstanceIdentifier=instance_id
            )
            snapshot = response["DBSnapshot"]
        except ClientError as err:
            logger.error(
                "Couldn't create snapshot of %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

```
        else:
            return snapshot


    def get_snapshot(self, snapshot_id):
        """
        Gets a DB instance snapshot.

        :param snapshot_id: The ID of the snapshot to retrieve.
        :return: The retrieved snapshot.
        """
        try:
            response = self.rds_client.describe_db_snapshots(
                DBSnapshotIdentifier=snapshot_id
            )
            snapshot = response["DBSnapshots"][0]
        except ClientError as err:
            logger.error(
                "Couldn't get snapshot %s. Here's why: %s: %s",
                snapshot_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return snapshot


    def get_engine_versions(self, engine, parameter_group_family=None):
        """
        Gets database engine versions that are available for the specified engine
        and parameter group family.

        :param engine: The database engine to look up.
        :param parameter_group_family: When specified, restricts the returned
list of
                                       engine versions to those that are
compatible with
                                       this parameter group family.
        :return: The list of database engine versions.
        """
        try:
            kwargs = {"Engine": engine}
            if parameter_group_family is not None:
```

```
                kwargs["DBParameterGroupFamily"] = parameter_group_family
            response = self.rds_client.describe_db_engine_versions(**kwargs)
            versions = response["DBEngineVersions"]
        except ClientError as err:
            logger.error(
                "Couldn't get engine versions for %s. Here's why: %s: %s",
                engine,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return versions


    def get_orderable_instances(self, db_engine, db_engine_version):
        """
        Gets DB instance options that can be used to create DB instances that are
        compatible with a set of specifications.

        :param db_engine: The database engine that must be supported by the DB
instance.
        :param db_engine_version: The engine version that must be supported by
the DB instance.
        :return: The list of DB instance options that can be used to create a
compatible DB instance.
        """
        try:
            inst_opts = []
            paginator = self.rds_client.get_paginator(
                "describe_orderable_db_instance_options"
            )
            for page in paginator.paginate(
                Engine=db_engine, EngineVersion=db_engine_version
            ):
                inst_opts += page["OrderableDBInstanceOptions"]
        except ClientError as err:
            logger.error(
                "Couldn't get orderable DB instances. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
```

```
            return inst_opts


    def get_db_instance(self, instance_id):
        """
        Gets data about a DB instance.

        :param instance_id: The ID of the DB instance to retrieve.
        :return: The retrieved DB instance.
        """
        try:
            response = self.rds_client.describe_db_instances(
                DBInstanceIdentifier=instance_id
            )
            db_inst = response["DBInstances"][0]
        except ClientError as err:
            if err.response["Error"]["Code"] == "DBInstanceNotFound":
                logger.info("Instance %s does not exist.", instance_id)
            else:
                logger.error(
                    "Couldn't get DB instance %s. Here's why: %s: %s",
                    instance_id,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return db_inst


    def create_db_instance(
        self,
        db_name,
        instance_id,
        parameter_group_name,
        db_engine,
        db_engine_version,
        instance_class,
        storage_type,
        allocated_storage,
        admin_name,
        admin_password,
    ):
        """
```

```
        Creates a DB instance.

        :param db_name: The name of the database that is created in the DB
instance.
        :param instance_id: The ID to give the newly created DB instance.
        :param parameter_group_name: A parameter group to associate with the DB
instance.
        :param db_engine: The database engine of a database to create in the DB
instance.
        :param db_engine_version: The engine version for the created database.
        :param instance_class: The DB instance class for the newly created DB
instance.
        :param storage_type: The storage type of the DB instance.
        :param allocated_storage: The amount of storage allocated on the DB
instance, in GiBs.
        :param admin_name: The name of the admin user for the created database.
        :param admin_password: The admin password for the created database.
        :return: Data about the newly created DB instance.
        """
        try:
            response = self.rds_client.create_db_instance(
                DBName=db_name,
                DBInstanceIdentifier=instance_id,
                DBParameterGroupName=parameter_group_name,
                Engine=db_engine,
                EngineVersion=db_engine_version,
                DBInstanceClass=instance_class,
                StorageType=storage_type,
                AllocatedStorage=allocated_storage,
                MasterUsername=admin_name,
                MasterUserPassword=admin_password,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't create DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

```
    def delete_db_instance(self, instance_id):
        """
        Deletes a DB instance.

        :param instance_id: The ID of the DB instance to delete.
        :return: Data about the deleted DB instance.
        """
        try:
            response = self.rds_client.delete_db_instance(
                DBInstanceIdentifier=instance_id,
                SkipFinalSnapshot=True,
                DeleteAutomatedBackups=True,
            )
            db_inst = response["DBInstance"]
        except ClientError as err:
            logger.error(
                "Couldn't delete DB instance %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return db_inst
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - CreateDBInstance
  - CreateDBParameterGroup
  - CreateDBSnapshot
  - DeleteDBInstance
  - DeleteDBParameterGroup
  - DescribeDBEngineVersions
  - DescribeDBInstances
  - DescribeDBParameterGroups

- DescribeDBParameters
- DescribeDBSnapshots
- DescribeOrderableDBInstanceOptions
- ModifyDBParameterGroup

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos sin servidor para Amazon RDS en los que se utilizan SDK de AWS

Los siguientes ejemplos de código muestran cómo utilizar Amazon RDS con los SDK de AWS.

Ejemplos

- Conexión a una base de datos de Amazon RDS en una función de Lambda

Conexión a una base de datos de Amazon RDS en una función de Lambda

En el siguiente ejemplo de código, se muestra cómo implementar una función de Lambda que se conecta a una base de datos de RDS. La función realiza una solicitud sencilla a la base de datos y devuelve el resultado.

Go

SDK para Go V2

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
/*
Golang v2 code here.
*/

package main

import (
 "context"
 "database/sql"
 "encoding/json"
 "fmt"
 "os"

 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
 _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
 Name string `json:"name"`
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {

 var dbName string = os.Getenv("DatabaseName")
 var dbUser string = os.Getenv("DatabaseUser")
 var dbHost string = os.Getenv("DBHost") // Add hostname without https
 var dbPort int = os.Getenv("Port")      // Add port number
 var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
 var region string = os.Getenv("AWS_REGION")

 cfg, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  panic("configuration error: " + err.Error())
 }

 authenticationToken, err := auth.BuildAuthToken(
  context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
 if err != nil {
  panic("failed to create authentication token: " + err.Error())
 }

 dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
```

```
  dbUser, authenticationToken, dbEndpoint, dbName,
 )

 db, err := sql.Open("mysql", dsn)
 if err != nil {
  panic(err)
 }

 defer db.Close()

 var sum int
 err = db.QueryRow("SELECT ?+? AS sum", 3, 2).Scan(&sum)
 if err != nil {
  panic(err)
 }
 s := fmt.Sprint(sum)
 message := fmt.Sprintf("The selected sum is: %s", s)

 messageBytes, err := json.Marshal(message)
 if err != nil {
  return nil, err
 }

 messageString := string(messageBytes)
 return map[string]interface{}{
  "statusCode": 200,
  "headers":    map[string]string{"Content-Type": "application/json"},
  "body":       messageString,
 }, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK para Java 2.x

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.rdsdata.RdsDataClient;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementRequest;
import software.amazon.awssdk.services.rdsdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.rdsdata.model.Field;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;

public class RdsLambdaHandler implements
 RequestHandler<APIGatewayProxyRequestEvent, APIGatewayProxyResponseEvent> {

    @Override
    public APIGatewayProxyResponseEvent handleRequest(APIGatewayProxyRequestEvent
 event, Context context) {
        APIGatewayProxyResponseEvent response = new
 APIGatewayProxyResponseEvent();

        try {
            // Obtain auth token
            String token = createAuthToken();

            // Define connection configuration
```

```
            String connectionString = String.format("jdbc:mysql://%s:%s/%s?
useSSL=true&requireSSL=true",
                    System.getenv("ProxyHostName"),
                    System.getenv("Port"),
                    System.getenv("DBName"));

            // Establish a connection to the database
            try (Connection connection =
 DriverManager.getConnection(connectionString, System.getenv("DBUserName"),
 token);
                 PreparedStatement statement =
 connection.prepareStatement("SELECT ? + ? AS sum")) {

                statement.setInt(1, 3);
                statement.setInt(2, 2);

                try (ResultSet resultSet = statement.executeQuery()) {
                    if (resultSet.next()) {
                        int sum = resultSet.getInt("sum");
                        response.setStatusCode(200);
                        response.setBody("The selected sum is: " + sum);
                    }
                }
            }

        } catch (Exception e) {
            response.setStatusCode(500);
            response.setBody("Error: " + e.getMessage());
        }

        return response;
    }

    private String createAuthToken() {
        // Create RDS Data Service client
        RdsDataClient rdsDataClient = RdsDataClient.builder()
                .region(Region.of(System.getenv("AWS_REGION")))
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        // Define authentication request
        ExecuteStatementRequest request = ExecuteStatementRequest.builder()
                .resourceArn(System.getenv("ProxyHostName"))
                .secretArn(System.getenv("DBUserName"))
```

```
                .database(System.getenv("DBName"))
                .sql("SELECT 'RDS IAM Authentication'")
                .build();

        // Execute request and obtain authentication token
        ExecuteStatementResponse response =
 rdsDataClient.executeStatement(request);
        Field tokenField = response.records().get(0).get(0);

        return tokenField.stringValue();
    }
}
```

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
Node.js code here.
*/
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {

    hostname: process.env.ProxyHostName,
```

```
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;

}

export const handler = async (event) => {
  // Execute database flow
  const result = await dbOps();
  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify("The selected sum is: " + result[0].sum)
  }
};
```

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

// RDS settings
// Using '!' (non-null assertion operator) to tell the TypeScript compiler that
 the DB settings are not null or undefined,
const proxy_host_name = process.env.PROXY_HOST_NAME!
const port = parseInt(process.env.PORT!)
const db_name = process.env.DB_NAME!
const db_user_name = process.env.DB_USER_NAME!
const aws_region = process.env.AWS_REGION!


async function createAuthToken(): Promise<string> {

    // Create RDS Signer object
    const signer = new Signer({
        hostname: proxy_host_name,
        port: port,
        region: aws_region,
        username: db_user_name
    });

    // Request authorization token from RDS, specifying the username
    const token = await signer.getAuthToken();
    return token;
}

async function dbOps(): Promise<mysql.QueryResult | undefined> {
    try {
        // Obtain auth token
        const token = await createAuthToken();
        const conn = await mysql.createConnection({
            host: proxy_host_name,
            user: db_user_name,
```

```
            password: token,
            database: db_name,
            ssl: 'Amazon RDS' // Ensure you have the CA bundle for SSL connection
        });
        const [rows, fields] = await conn.execute('SELECT ? + ? AS sum', [3, 2]);
        console.log('result:', rows);
        return rows;
    }
    catch (err) {
        console.log(err);
    }
}

export const lambdaHandler = async (event: any): Promise<{ statusCode: number;
 body: string }> => {
    // Execute database flow
    const result = await dbOps();

    // Return error is result is undefined
    if (result == undefined)
        return {
            statusCode: 500,
            body: JSON.stringify(`Error with connection to DB host`)
        }

    // Return result
    return {
        statusCode: 200,
        body: JSON.stringify(`The selected sum is: ${result[0].sum}`)
    };
};
```

PHP

SDK para PHP

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante PHP.

```
<?php
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;
use Aws\Rds\AuthTokenGenerator;
use Aws\Credentials\CredentialProvider;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }


    private function getAuthToken(): string {
        // Define connection authentication parameters
        $dbConnection = [
            'hostname' => getenv('DB_HOSTNAME'),
            'port' => getenv('DB_PORT'),
            'username' => getenv('DB_USERNAME'),
            'region' => getenv('AWS_REGION'),
        ];

        // Create RDS AuthTokenGenerator object
        $generator = new
 AuthTokenGenerator(CredentialProvider::defaultProvider());

        // Request authorization token from RDS, specifying the username
        return $generator->createToken(
            $dbConnection['hostname'] . ':' . $dbConnection['port'],
            $dbConnection['region'],
            $dbConnection['username']
        );
```

```
    }

    private function getQueryResults() {
        // Obtain auth token
        $token = $this->getAuthToken();

        // Define connection configuration
        $connectionConfig = [
            'host' => getenv('DB_HOSTNAME'),
            'user' => getenv('DB_USERNAME'),
            'password' => $token,
            'database' => getenv('DB_NAME'),
        ];

        // Create the connection to the DB
        $conn = new PDO(

"mysql:host={$connectionConfig['host']};dbname={$connectionConfig['database']}",
            $connectionConfig['user'],
            $connectionConfig['password'],
            [
                PDO::MYSQL_ATTR_SSL_CA => '/path/to/rds-ca-2019-root.pem',
                PDO::MYSQL_ATTR_SSL_VERIFY_SERVER_CERT => true,
            ]
        );

        // Obtain the result of the query
        $stmt = $conn->prepare('SELECT ?+? AS sum');
        $stmt->execute([3, 2]);

        return $stmt->fetch(PDO::FETCH_ASSOC);
    }

    /**
     * @param mixed $event
     * @param Context $context
     * @return array
     */
    public function handle(mixed $event, Context $context): array
    {
        $this->logger->info("Processing query");

        // Execute database flow
        $result = $this->getQueryResults();
```

```
        return [
            'sum' => $result['sum']
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante Python.

```
import json
import os
import boto3
import pymysql

# RDS settings
proxy_host_name = os.environ['PROXY_HOST_NAME']
port = int(os.environ['PORT'])
db_name = os.environ['DB_NAME']
db_user_name = os.environ['DB_USER_NAME']
aws_region = os.environ['AWS_REGION']


# Fetch RDS Auth Token
def get_auth_token():
    client = boto3.client('rds')
    token = client.generate_db_auth_token(
        DBHostname=proxy_host_name,
        Port=port
        DBUsername=db_user_name
```

```
        Region=aws_region
    )
    return token

def lambda_handler(event, context):
    token = get_auth_token()
    try:
        connection = pymysql.connect(
            host=proxy_host_name,
            user=db_user_name,
            password=token,
            db=db_name,
            port=port,
            ssl={'ca': 'Amazon RDS'}  # Ensure you have the CA bundle for SSL
 connection
        )

        with connection.cursor() as cursor:
            cursor.execute('SELECT %s + %s AS sum', (3, 2))
            result = cursor.fetchone()

        return result

    except Exception as e:
        return (f"Error: {str(e)}")  # Return an error message if an exception
 occurs
```

Ruby

SDK para Ruby

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
```

```
# Ruby code here.

require 'aws-sdk-rds'
require 'json'
require 'mysql2'

def lambda_handler(event:, context:)
  endpoint = ENV['DBEndpoint'] # Add the endpoint without https"
  port = ENV['Port']           # 3306
  user = ENV['DBUser']
  region = ENV['DBRegion']     # 'us-east-1'
  db_name = ENV['DBName']

  credentials = Aws::Credentials.new(
    ENV['AWS_ACCESS_KEY_ID'],
    ENV['AWS_SECRET_ACCESS_KEY'],
    ENV['AWS_SESSION_TOKEN']
  )
  rds_client = Aws::RDS::AuthTokenGenerator.new(
    region: region,
    credentials: credentials
  )

  token = rds_client.auth_token(
    endpoint: endpoint+ ':' + port,
    user_name: user,
    region: region
  )

  begin
    conn = Mysql2::Client.new(
      host: endpoint,
      username: user,
      password: token,
      port: port,
      database: db_name,
      sslca: '/var/task/global-bundle.pem',
      sslverify: true,
      enable_cleartext_plugin: true
    )
    a = 3
    b = 2
    result = conn.query("SELECT #{a} + #{b} AS sum").first['sum']
    puts result
```

```
    conn.close
    {
      statusCode: 200,
      body: result.to_json
    }
  rescue => e
    puts "Database connection failed due to #{e}"
  end
end
```

Rust

SDK para Rust

> **Note**
>
> Hay más información en GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el repositorio de ejemplos sin servidor.

Conexión a una base de datos de Amazon RDS en una función de Lambda mediante Rust.

```
use aws_config::BehaviorVersion;
use aws_credential_types::provider::ProvideCredentials;
use aws_sigv4::{
    http_request::{sign, SignableBody, SignableRequest, SigningSettings},
    sign::v4,
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use serde_json::{json, Value};
use sqlx::postgres::PgConnectOptions;
use std::env;
use std::time::{Duration, SystemTime};

const RDS_CERTS: &[u8] = include_bytes!("global-bundle.pem");

async fn generate_rds_iam_token(
    db_hostname: &str,
    port: u16,
    db_username: &str,
) -> Result<String, Error> {
    let config = aws_config::load_defaults(BehaviorVersion::v2024_03_28()).await;
```

```
    let credentials = config
        .credentials_provider()
        .expect("no credentials provider found")
        .provide_credentials()
        .await
        .expect("unable to load credentials");
    let identity = credentials.into();
    let region = config.region().unwrap().to_string();

    let mut signing_settings = SigningSettings::default();
    signing_settings.expires_in = Some(Duration::from_secs(900));
    signing_settings.signature_location =
aws_sigv4::http_request::SignatureLocation::QueryParams;

    let signing_params = v4::SigningParams::builder()
        .identity(&identity)
        .region(&region)
        .name("rds-db")
        .time(SystemTime::now())
        .settings(signing_settings)
        .build()?;

    let url = format!(
        "https://{db_hostname}:{port}/?Action=connect&DBUser={db_user}",
        db_hostname = db_hostname,
        port = port,
        db_user = db_username
    );

    let signable_request =
        SignableRequest::new("GET", &url, std::iter::empty(),
SignableBody::Bytes(&[]))
            .expect("signable request");

    let (signing_instructions, _signature) =
        sign(signable_request, &signing_params.into())?.into_parts();

    let mut url = url::Url::parse(&url).unwrap();
    for (name, value) in signing_instructions.params() {
        url.query_pairs_mut().append_pair(name, &value);
    }

    let response = url.to_string().split_off("https://".len());
```

```
    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(handler)).await
}

async fn handler(_event: LambdaEvent<Value>) -> Result<Value, Error> {
    let db_host = env::var("DB_HOSTNAME").expect("DB_HOSTNAME must be set");
    let db_port = env::var("DB_PORT")
        .expect("DB_PORT must be set")
        .parse::<u16>()
        .expect("PORT must be a valid number");
    let db_name = env::var("DB_NAME").expect("DB_NAME must be set");
    let db_user_name = env::var("DB_USERNAME").expect("DB_USERNAME must be set");

    let token = generate_rds_iam_token(&db_host, db_port, &db_user_name).await?;

    let opts = PgConnectOptions::new()
        .host(&db_host)
        .port(db_port)
        .username(&db_user_name)
        .password(&token)
        .database(&db_name)
        .ssl_root_cert_from_pem(RDS_CERTS.to_vec())
        .ssl_mode(sqlx::postgres::PgSslMode::Require);

    let pool = sqlx::postgres::PgPoolOptions::new()
        .connect_with(opts)
        .await?;

    let result: i32 = sqlx::query_scalar("SELECT $1 + $2")
        .bind(3)
        .bind(2)
        .fetch_one(&pool)
        .await?;

    println!("Result: {:?}", result);

    Ok(json!({
        "statusCode": 200,
        "content-type": "text/plain",
```

```
        "body": format!("The selected sum is: {result}")
    }))
}
```

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos en diversos servicios de Amazon RDS con SDK de AWS

Las siguientes aplicaciones de ejemplo utilizan SDK de AWS para combinar Amazon RDS con otros Servicios de AWS. Cada ejemplo incluye un enlace a GitHub, con instrucciones de configuración y ejecución de la aplicación.

Ejemplos

- Crear un rastreador de elementos de trabajo de Aurora Serverless

Crear un rastreador de elementos de trabajo de Aurora Serverless

Los siguientes ejemplos de código muestran cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo de una base de datos de Amazon Aurora sin servidor y use Amazon Simple Email Service (Amazon SES) para enviar informes.

.NET

SDK para .NET

Muestra cómo utilizar AWS SDK para .NET para crear una aplicación web que haga un seguimiento de los elementos de trabajo de una base de datos de Amazon Aurora y envíe informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). Este ejemplo usa un frontend creado con React.js para interactuar con un backend .NET RESTful.

- Integre una aplicación web de React con los servicios de AWS.
- Muestre, agregue, actualice y elimine elementos en una tabla de Aurora.
- Envíe un informe por correo electrónico de elementos de trabajo filtrados con Amazon SES.
- Implemente y administre recursos de ejemplo con el script de AWS CloudFormation incluido.

Para ver el código fuente completo y las instrucciones de configuración y ejecución, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

C++

SDK para C++

Muestra cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon Aurora sin servidor e informe al respecto.

Para obtener el código fuente completo e instrucciones sobre cómo configurar una API de REST de C++ que consulta datos de Amazon Aurora sin servidor y para su uso por parte de una aplicación React, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

Java

SDK para Java 2.x

Muestra cómo crear una aplicación web que haga un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon RDS e informe al respecto.

Para obtener el código fuente completo e instrucciones sobre cómo configurar una API de REST de Spring que consulta datos de Amazon Aurora Serverless y para su uso por parte de una aplicación React, consulte el ejemplo completo en GitHub.

Para obtener el código fuente completo e instrucciones sobre cómo configurar y ejecutar el ejemplo que utiliza la API de JDBC, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

JavaScript

SDK para JavaScript (v3)

Muestra cómo utilizar AWS SDK for JavaScript (v3) para crear una aplicación web que realice un seguimiento de los elementos de trabajo de una base de datos de Amazon Aurora y envíe informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). Este ejemplo usa un frontend creado con React.js para interactuar con un backend de Node.js de Express.

- Integre una aplicación web de React.js con Servicios de AWS.
- Cree una lista, agregue y actualice elementos en una tabla de Aurora.
- Envíe un informe por correo electrónico de elementos de trabajo filtrados con Amazon SES.
- Implemente y administre recursos de ejemplo con el script de AWS CloudFormation incluido.

Para ver el código fuente completo y las instrucciones de configuración y ejecución, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

Kotlin

SDK para Kotlin

Muestra cómo crear una aplicación web que haga un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon RDS e informe al respecto.

Para obtener el código fuente completo e instrucciones sobre cómo configurar una API de REST de Spring que consulta datos de Amazon Aurora Serverless y para su uso por parte de una aplicación React, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

PHP

SDK para PHP

Muestra cómo utilizar AWS SDK para PHP para crear una aplicación web que haga un seguimiento de los elementos de trabajo de una base de datos de Amazon RDS y envíe informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). Este ejemplo usa un front-end creado con React.js para interactuar con un backend PHP RESTful.

- Integre una aplicación web de React.js con los servicios de AWS.
- Enumere, agregue, actualice y elimine elementos de una tabla de Amazon RDS.
- Envíe un informe por correo electrónico de elementos de trabajo filtrados con Amazon SES.
- Implemente y administre recursos de ejemplo con el script de AWS CloudFormation incluido.

Para ver el código fuente completo y las instrucciones de configuración y ejecución, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS

- Servicio de datos de Amazon RDS
- Amazon SES

Python

SDK para Python (Boto3)

Muestra cómo utilizar AWS SDK para Python (Boto3) para crear un servicio REST que haga un seguimiento de los elementos de trabajo de una base de datos de Amazon Aurora sin servidor y envíe informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). En este ejemplo se utiliza el marco web de Flask para gestionar el enrutamiento HTTP y se integra con una página web de React para presentar una aplicación web completamente funcional.

- Cree un servicio REST de Flask que se integre con Servicios de AWS.
- Lea, escriba y actualice los elementos de trabajo almacenados en una base de datos de Aurora Serverless.
- Cree un secreto de AWS Secrets Manager que contenga las credenciales de la base de datos y utilícelo para autenticar las llamadas a la base de datos.
- Utilice Amazon SES para enviar informes de elementos de trabajo por correo electrónico.

Para ver el código fuente completo y las instrucciones de configuración y ejecución, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte Cómo utilizar este servicio con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Seguridad en Amazon RDS

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos que están diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y el usuario. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puedes utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener información acerca de los programas de conformidad que se aplican a Amazon RDS , consulte los servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWSque utiliza. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon RDS . En los siguientes temas, se le mostrará cómo configurar Amazon RDS para satisfacer los objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que ayuden a supervisar y proteger los recursos de Amazon RDS .

Puede administrar el acceso a los recursos y las bases de datos de Amazon RDS en una instancia de base de datos. El método que se utiliza para controlar el acceso depende del tipo de tarea que el usuario necesite realizar con Amazon RDS :

- Ejecute la instancia de base de datos en una nube privada virtual (VPC) en función del servicio de Amazon VPC para el posible control de acceso de red más grande. Para obtener más información acerca de la creación de una instancia de base de datos en una VPC, consulte VPC de Amazon y Amazon RDS.
- Utilice políticas de AWS Identity and Access Management (IAM) para asignar permisos que determinen quién puede administrar los recursos de Amazon RDS . Por ejemplo, puede utilizar IAM para determinar quién tiene permiso para crear, describir, modificar y eliminar instancias de bases de datos, etiquetar recursos o modificar grupos de seguridad.

- Utilice grupos de seguridad para controlar las direcciones IP o instancias de Amazon EC2 que pueden conectarse a las bases de datos de una instancia de bases de datos. Cuando se crea una instancia de bases de datos por primera vez, su firewall impide cualquier acceso a las bases de datos, salvo si se cumplen las reglas especificadas por un grupo de seguridad asociado.
- Utilice la capa de conexión segura (SSL) o la seguridad de la capa de transporte (TLS) con las instancias de base de datos que ejecuten los motores de base de datos Db2, MySQL, MariaDB, PostgreSQL, Oracle o Microsoft SQL Server. Para obtener más información acerca del uso de SSL/TLS con una instancia de base de datos, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos .
- Utilice el cifrado de Amazon RDS para proteger las instancias de base de datos y las instantáneas en reposo. El cifrado de Amazon RDS utiliza el algoritmo de cifrado AES-256 estándar del sector para cifrar los datos en el servidor que aloja la instancia de bases de datos. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.
- Utilice el cifrado de red y el cifrado de datos transparente con las instancias de bases de datos de Oracle; para obtener más información, consulte Oracle Native Network Encryption y Cifrado de datos transparente de Oracle
- Utilice las características de seguridad del motor de base de datos para controlar quién puede iniciar sesión en las bases de datos en una instancia de bases de datos. Estas características funcionas de igual forma que si la base de datos estuviera en su red local.

> **Note**
>
> Solo tiene que configurar la seguridad para sus casos de uso. No tiene que configurar el acceso de seguridad para procesos que Amazon RDS administra. Estos incluyen la creación de copias de seguridad, la replicación de datos entre una instancia de base de datos primaria y una réplica de lectura, y otros procesos.

Para obtener más información acerca de la administración del acceso a los recursos de Amazon RDS y las bases de datos de una instancia de bases de datos, consulte los siguientes temas.

Temas

- Autenticación de bases de datos con Amazon RDS
- Administración de contraseñas con Amazon RDS y AWS Secrets Manager
- Protección de datos en Amazon RDS

- Administración de la identidad y el acceso en Amazon RDS
- Registro y monitoreo en Amazon RDS
- Validación de la conformidad en Amazon RDS
- Resiliencia en Amazon RDS
- Seguridad de la infraestructura en Amazon RDS
- La API de Amazon RDS y los puntos de enlace de la VPC de tipo interfaz (AWS PrivateLink)
- Prácticas recomendadas de seguridad para Amazon RDS
- Control de acceso con grupos de seguridad
- Privilegios de la cuenta de usuario maestro
- Uso de roles vinculados a servicios de Amazon RDS
- VPC de Amazon y Amazon RDS

Autenticación de bases de datos con Amazon RDS

Amazon RDS admite varias formas de autenticar usuarios de bases de datos.

La autenticación con contraseña, de Kerberos y de base de datos de IAM utilizan diferentes métodos de autenticación en la base de datos. Por lo tanto, un usuario específico puede iniciar sesión en una base de datos mediante un solo método de autenticación.

Para PostgreSQL, utilice solo una de las siguientes configuraciones de rol para un usuario de una base de datos específica:

- Para utilizar la autenticación de base de datos de IAM, asigne el rol `rds_iam` al usuario.
- Para utilizar la autenticación de Kerberos, asigne el rol `rds_ad` al usuario.
- Para utilizar la autenticación con contraseña, no asigne ninguno de los roles `rds_iam` o `rds_ad` al usuario.

No asigne el rol `rds_iam` ni el rol `rds_ad` a un usuario de una base de datos de PostgreSQL, de forma directa o indirecta, mediante el acceso de concesión anidada. Si el rol `rds_iam` se agrega al usuario maestro, la autenticación de IAM tiene prioridad sobre la autenticación con contraseña, por lo que el usuario maestro tiene que iniciar sesión como usuario de IAM.

> **Important**
>
> Le recomendamos encarecidamente que no utilice el usuario maestro directamente en sus aplicaciones. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar un usuario de base de datos creado con los privilegios mínimos necesarios para su aplicación.

Temas

- Autenticación de contraseña
- Autenticación de bases de datos de IAM
- Autenticación Kerberos

Autenticación de contraseña

Con la autenticación de contraseña, la base de datos realiza toda la administración de cuentas de usuario. Puede crear usuarios con instrucciones SQL como `CREATE USER`, con la cláusula adecuada que requiere el motor de base de datos para especificar contraseñas. Por ejemplo, en MySQL la instrucción es `CREATE USER` *`nombre`* `IDENTIFIED BY` *`contraseña`*, mientras que, en PostgreSQL, la instrucción es `CREATE USER` *`nombre`* `WITH PASSWORD` *`contraseña`*.

Con la autenticación por contraseña, la base de datos controla y autentica las cuentas de usuario. Si un motor de base de datos tiene características sólidas de administración de contraseñas, puede mejorar la seguridad. La autenticación de bases de datos puede ser más fácil de administrar mediante la autenticación de contraseña cuando tiene comunidades de usuarios pequeñas. Debido a que en este caso se generan contraseñas de texto sin formato, la integración con AWS Secrets Manager puede mejorar la seguridad.

Para obtener información sobre el uso de Secrets Manager con Amazon RDS , consulte Creación de un secreto básico y Rotación de secretos para bases de datos de Amazon RDS admitidas en la Guía del usuario de AWS Secrets Manager. Si quiere obtener información para recuperar los secretos mediante programación en las aplicaciones personalizadas, consulte Recuperar el valor secreto en la guía del usuario de AWS Secrets Manager.

Autenticación de bases de datos de IAM

Puede autenticar en la instancia de bases de datos mediante la autenticación de base de datos de AWS Identity and Access Management (IAM). Con este método de autenticación, no es necesario

usar una contraseña al conectarse a una instancia de bases de datos. En su lugar, puede usar un token de autenticación.

Para obtener más información acerca de la autenticación de bases de datos de IAM, incluida información sobre la disponibilidad de motores de base de datos específicos, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

Autenticación Kerberos

Amazon RDS admite la autenticación externa de usuarios de bases de datos que usan Kerberos y Microsoft Active Directory. Kerberos es un protocolo de autenticación de red que usa tickets y criptografía de clave simétrica para eliminar la necesidad de transmitir contraseñas a través de la red. Kerberos ha sido creado en Active Directory y está diseñado para autenticar usuarios para recursos de redes, como bases de datos.

La compatibilidad de Amazon RDS con Kerberos y Active Directory ofrece beneficios de inicio de sesión único y autenticación centralizada de usuarios de bases de datos. Puede mantener sus credenciales de usuario en Active Directory. Active Directory ofrece un lugar centralizado para almacenar y administrar credenciales para varias instancias de bases de datos.

Para usar las credenciales del Active Directory autoadministrado, debe configurar una relación de confianza con AWS Directory Service para el Microsoft Active Directory al que se haya unido la instancia de base de datos .

RDS para PostgreSQL y RDS para MySQL admiten relaciones de confianza unidireccionales y bidireccionales entre bosques con autenticación selectiva o en todo el bosque.

En algunos casos, puede configurar la autenticación Kerberos a través de una relación de confianza externa. Esto requiere que el directorio de Active Directory autoadministrado tenga una configuración adicional. Esto incluye, entre otras cosas, Kerberos Forest Search Order.

Las instancias de base de datos de Microsoft SQL Server y PostgreSQL admiten relaciones de confianza entre bosques unidireccionales y bidireccionales. Las instancias de base de datos de Oracle admiten relaciones de confianza externas y entre bosques unidireccionales y bidireccionales. Para obtener más información, consulte Cuándo crear una relación de confianza en la Guía de administración de AWS Directory Service.

Para obtener información sobre la autenticación de Kerberos con un motor específico, consulte lo siguiente:

- Uso de AWS Managed Active Directory con RDS para SQL Server
- Uso de la autenticación de Kerberos para Amazon RDS para MySQL
- Configuración de la autenticación Kerberos con Amazon RDS for Oracle
- Uso de la autenticación Kerberos con Amazon RDS para PostgreSQL
- Uso de la autenticación de Kerberos para Amazon RDS para Db2 .

> **Note**
>
> Actualmente, la autenticación Kerberos no es compatible con las instancias de base de datos MariaDB.

Administración de contraseñas con Amazon RDS y AWS Secrets Manager

Amazon RDS se integra con Secrets Manager para administrar las contraseñas de usuario maestras de sus instancias de base de datos y clústeres de bases de datos Multi-AZ.

Temas

- Limitaciones de la integración de Secrets Manager con Amazon RDS
- Descripción general de la administración de contraseñas de usuarios maestros con AWS Secrets Manager
- Ventajas de administrar las contraseñas de usuarios maestros con Secrets Manager
- Permisos necesarios para la integración de Secrets Manager
- Cumplimiento de la administración de la contraseña del usuario maestro por parte de RDS en AWS Secrets Manager
- Administración de la contraseña de usuario maestro de una instancia de base de datos con Secrets Manager
- Administración de la contraseña de usuario principal para una base de datos de inquilinos de RDS para Oracle con Secrets Manager
- Administración de la contraseña de usuario maestra para un clúster de base de datos Multi-AZ con Secrets Manager
- Rotación del secreto de contraseña de usuario maestro para una instancia de base de datos
- Rotación del secreto de contraseña de usuario maestra para un clúster de base de datos Multi-AZ
- Visualización de los detalles de un secreto para una instancia de base de datos
- Visualización de los detalles de un secreto para un clúster de base de datos Multi-AZ
- Visualización de los detalles de un secreto para una base de datos de inquilinos
- Disponibilidad en regiones y versiones

Limitaciones de la integración de Secrets Manager con Amazon RDS

Las siguientes funciones no admiten la administración de contraseñas de usuario maestro con Secrets Manager:

- Crear una réplica de lectura cuando la base de datos o el clúster de base de datos de origen administran las credenciales con Secrets Manager. Esto se aplica a todos los motores de bases de datos, excepto RDS para SQL Server.
- Implementaciones azules/verdes de Amazon RDS
- Amazon RDS Custom
- Cambio de Oracle Data Guard

Descripción general de la administración de contraseñas de usuarios maestros con AWS Secrets Manager

Con AWS Secrets Manager, puede reemplazar las credenciales con codificación rígida (incluidas las contraseñas de bases de datos), con una llamada a la API de Secrets Manager para recuperar el secreto mediante programación. Para obtener más información acerca de Secrets Manager, consulte la Guía del usuario de AWS Secrets Manager.

Cuando guarda secretos de base de datos en Secrets Manager, su Cuenta de AWS incurre en cargos. Para obtener más información acerca de los precios, consulte Precios de AWS Secrets Manager.

Puede especificar que RDS administre la contraseña de usuarios maestros en Secrets Manager para una instancia de base de datos de Amazon RDS o un clúster de base de datos Multi-AZ al realizar una de las siguientes operaciones:

- Crear una instancia de base de datos
- Creación de un clúster de base de datos Multi-AZ
- Creación de una base de datos de inquilinos en una CDB de RDS para Oracle
- Modificar una instancia de base de datos
- Modificación de un clúster de base de datos Multi-AZ
- Modificación de una base de datos de inquilinos (solo RDS para Oracle)
- Restauración de una instancia de base de datos desde Amazon S3
- Restauración de una instancia de base de datos a partir de una instantánea o en un punto en el tiempo (solo RDS para Oracle)

Al especificar que RDS administre la contraseña del usuario maestro en Secrets Manager, RDS genera la contraseña y la almacena en Secrets Manager. Puede interactuar directamente con el

secreto para recuperar las credenciales del usuario maestro. También puede especificar una clave gestionada por el cliente para cifrar el secreto o utilizar la clave de KMS que proporciona Secrets Manager.

RDS administra la configuración del secreto y, de forma predeterminada, lo rota cada siete días. Puede modificar algunos de los ajustes, como el programa de rotación. Si elimina una instancia de base de datos que administra un secreto en Secrets Manager, también se eliminarán el secreto y los metadatos asociados.

Para conectarse a una instancia de base de datos o a un clúster de base de datos Multi-AZ con las credenciales en un secreto, puede recuperar el secreto en Secrets Manager. Para obtener más información, consulte Recuperar secretos de AWS Secrets Manager y Conexión a una base de datos SQL con credenciales en un secreto de AWS Secrets Manager en la Guía del usuario de AWS Secrets Manager.

Ventajas de administrar las contraseñas de usuarios maestros con Secrets Manager

La administración de las contraseñas de usuarios maestros de RDS con Secrets Manager ofrece las siguientes ventajas:

- RDS genera automáticamente las credenciales de la base de datos.
- RDS almacena y administra automáticamente las credenciales de la base de datos en AWS Secrets Manager.
- RDS rota las credenciales de la base de datos con regularidad, sin necesidad de realizar cambios en la aplicación.
- Secrets Manager protege las credenciales de la base de datos del acceso humano y de la visualización en texto plano.
- Secrets Manager permite recuperar las credenciales de la base de datos en secretos para las conexiones a bases de datos.
- Secrets Manager permite un control detallado del acceso a las credenciales de la base de datos en secretos mediante IAM.
- Si lo desea, puede separar el cifrado de bases de datos del cifrado de credenciales con diferentes claves de KMS.
- Puede eliminar la administración manual y la rotación de las credenciales de la base de datos.

- Puede monitorear fácilmente las credenciales de la base de datos con AWS CloudTrail y Amazon CloudWatch.

Para obtener más información acerca de los beneficios de Secrets Manager, consulte la Guía del usuario de AWS Secrets Manager.

Permisos necesarios para la integración de Secrets Manager

Los usuarios deben tener los permisos necesarios para realizar las operaciones relacionadas con la integración de Secrets Manager. Puede crear políticas de IAM que concedan permisos para realizar operaciones de la API concretas en los recursos especificados que necesiten. A continuación, puede asociar esas políticas a los roles o conjuntos de permisos de IAM que necesiten esos permisos. Para obtener más información, consulte Administración de la identidad y el acceso en Amazon RDS.

Para las operaciones de creación, modificación o restauración, el usuario que especifique que Amazon RDS administra la contraseña de usuario maestro en Secrets Manager debe tener permisos para realizar las siguientes operaciones:

- `kms:DescribeKey`
- `secretsmanager:CreateSecret`
- `secretsmanager:TagResource`

El permiso `kms:DescribeKey` es necesario para acceder a la clave administrada por el cliente para `MasterUserSecretKmsKeyId` y para describir `aws/secretsmanager`.

Para las operaciones de creación, modificación o restauración, el usuario que especifique la contraseña de usuario maestro en Secrets Manager debe tener permisos para realizar las siguientes operaciones:

- `kms:Decrypt`
- `kms:GenerateDataKey`
- `kms:CreateGrant`

Para las operaciones de modificación, el usuario que rote la contraseña de usuario maestro en Secrets Manager debe tener permisos para realizar la siguiente operación:

- `secretsmanager:RotateSecret`

Cumplimiento de la administración de la contraseña del usuario maestro por parte de RDS en AWS Secrets Manager

Puede utilizar las claves de condición de IAM para hacer que RDS administre la contraseña del usuario maestro en AWS Secrets Manager. La siguiente política no permite a los usuarios crear ni restaurar instancias de base de datos o clústeres de bases de datos o crear o modificar bases de datos de inquilinos a menos que RDS administre la contraseña del usuario principal en Secrets Manager.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["rds:CreateDBInstance", "rds:CreateDBCluster",
 "rds:RestoreDBInstanceFromS3", "rds:RestoreDBClusterFromS3",
                       "rds:RestoreDBInstanceFromDBSnapshot",
 "rds:RestoreDBInstanceToPointInTime", "rds:CreateTenantDatabase",
                       "rds:ModifyTenantDatabase"],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "rds:ManageMasterUserPassword": false
                }
            }
        }
    ]
}
```

> **Note**
>
> Esta política aplica la administración de contraseñas en AWS Secrets Manager cuando se crea. Sin embargo, sigue pudiendo deshabilitar la integración de Secrets Manager y establecer manualmente una contraseña maestra si modifica la instancia.
> Para evitarlo, incluya `rds:ModifyDBInstance`, `rds:ModifyDBCluster` en el bloque de acciones de la política. Tenga en cuenta que esto impide que el usuario aplique más

modificaciones a las instancias existentes que no tengan habilitada la integración de Secrets Manager.

Para obtener más información sobre el uso de las claves de condición en las políticas de IAM, consulte Claves de condición de políticas para Amazon RDS y Políticas de ejemplo: uso de claves de condición.

Administración de la contraseña de usuario maestro de una instancia de base de datos con Secrets Manager

Puede configurar la administración de RDS de la contraseña del usuario maestro en Secrets Manager realizando las siguientes acciones:

- Creación de una instancia de base de datos de Amazon RDS
- Modificación de una instancia de base de datos de Amazon RDS
- Restauración de una copia de seguridad en una instancia de base de datos MySQL.
- Restauración a una instancia de base de datos (solo RDS para Oracle)
- Restauración de una instancia de base de datos a un momento especificado para Amazon RDS (solo RDS para Oracle)

Puede realizar las operaciones anteriores con la consola de RDS, la AWS CLI o la API de RDS.

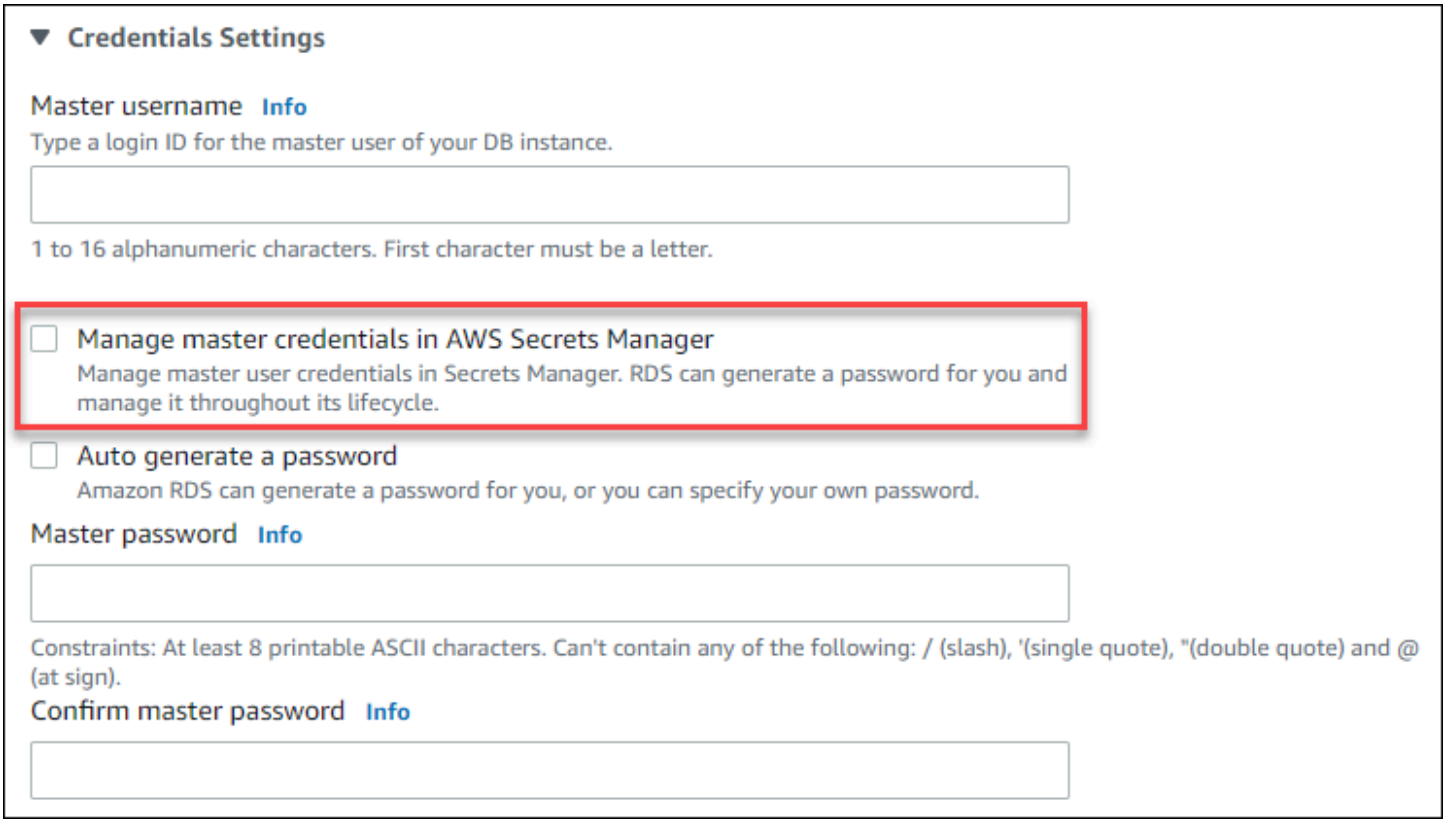
Consola

Siga las instrucciones para crear o modificar una instancia de base de datos con la consola de RDS:

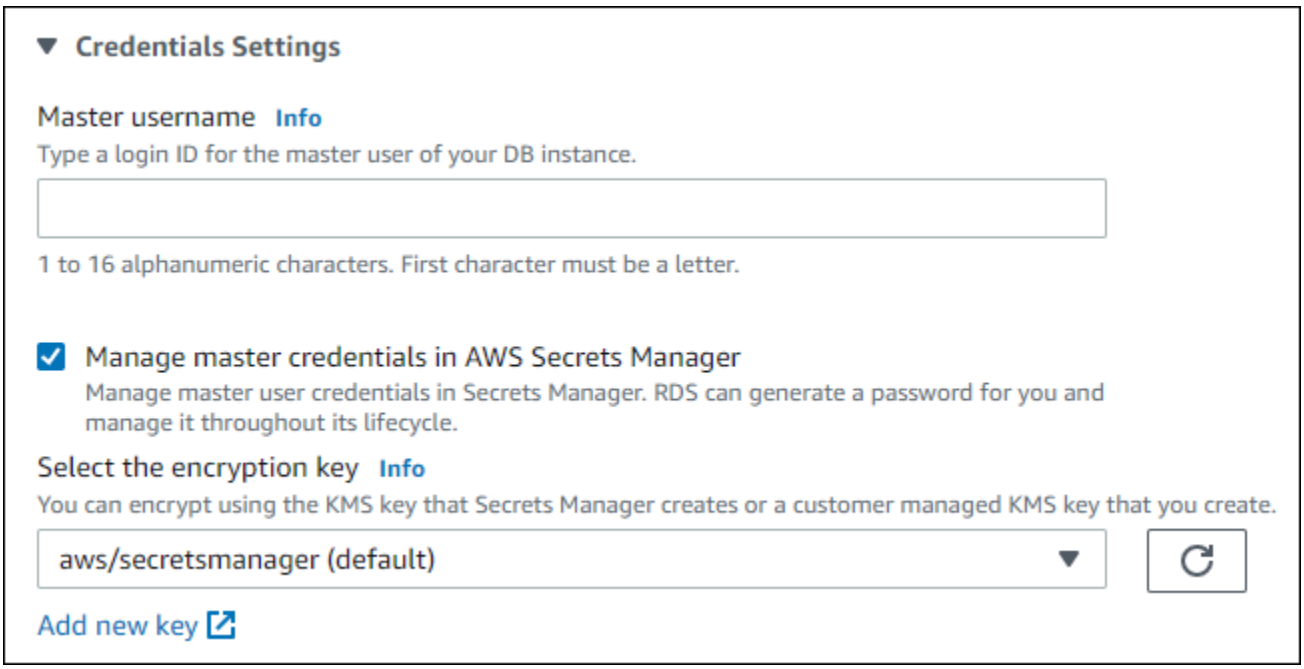
- Creación de una instancia de base de datos
- Modificación de una instancia de base de datos de Amazon RDS
- Importación de datos desde Amazon S3 a una nueva instancia de base de datos de MySQL

Al utilizar la consola de RDS para realizar una de estas operaciones, puede especificar que RDS administre la contraseña del usuario maestro en Secrets Manager. Cuando crea o restaura una instancia de base de datos, seleccione Administrar las credenciales principales en AWS Secrets Manager en la Configuración de credenciales. Cuando modifique una instancia de base de datos, seleccione Administrar las credenciales principales en AWS Secrets Manager en Configuración.

La siguiente imagen es un ejemplo de la configuración Manage master credentials in AWS Secrets Manager (Administrar las credenciales maestras en AWS Secrets Manager) que se utiliza al crear o restaurar una instancia de base de datos.



Al seleccionar esta opción, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.



Puede optar por cifrar el secreto con una clave de KMS que proporcione Secrets Manager o con la clave gestionada por el cliente que cree usted. Una vez que RDS administre las credenciales de base de datos para una instancia de base de datos, no se puede cambiar la clave de KMS utilizada para cifrar el secreto.

Puede elegir otros ajustes para cumplir con sus requisitos. Para obtener más información sobre la configuración disponible al crear una instancia de bases de datos, consulte Configuración de instancias de base de datos. Para obtener más información sobre la configuración disponible al modificar una instancia de bases de datos, consulte Configuración de instancias de base de datos.

AWS CLI

Para administrar la contraseña del usuario maestro con RDS en Secrets Manager, especifique la opción `--manage-master-user-password` en uno de los siguientes comandos AWS CLI:

- create-db-instance
- modify-db-instance
- restore-db-instance-from-s3
- restore-db-instance-from-db-snapshot (solo RDS para Oracle)
- restore-db-instance-to-point-in-time (solo RDS para Oracle)

Al seleccionar la opción `--manage-master-user-password` en estos comandos, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.

Para cifrar el secreto, también puede especificar una clave gestionada por el cliente o utilizar la clave de KMS que proporciona Secrets Manager. Use la opción `--master-user-secret-kms-key-id` para especificar una clave administrada por el cliente. El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para especificar una clave en una Cuenta de AWS diferente, debe utilizar la clave de ARN o el alias de ARN. Una vez que RDS administre las credenciales de base de datos para una instancia de base de datos, no se puede cambiar la clave de KMS que se utiliza para cifrar el secreto.

Puede elegir otros ajustes para cumplir con sus requisitos. Para obtener más información sobre la configuración disponible al crear cada instancia de bases de datos, consulte Configuración de instancias de base de datos. Para obtener más información sobre la configuración disponible al modificar cada instancia de bases de datos, consulte Configuración de instancias de base de datos.

En el siguiente ejemplo se crea una instancia de base de datos y se especifica que RDS administra la contraseña del usuario principal en Secrets Manager. El secreto se cifra mediante la clave de KMS que proporciona Secrets Manager.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --engine mysql \
    --engine-version 8.0.39 \
    --db-instance-class db.r5b.large \
    --allocated-storage 200 \
    --master-username testUser \
    --manage-master-user-password
```

Para Windows:

```
aws rds create-db-instance ^
    --db-instance-identifier mydbinstance ^
    --engine mysql ^
    --engine-version 8.0.39 ^
    --db-instance-class db.r5b.large ^
    --allocated-storage 200 ^
```

```
    --master-username testUser ^
    --manage-master-user-password
```

API de RDS

Para especificar que RDS administre la contraseña del usuario maestro en Secrets Manager, defina el parámetro `ManageMasterUserPassword` en `true` con alguna de las siguientes operaciones de la API de RDS:

- CreateDBInstance
- ModifyDBInstance
- RestoreDBInstanceFromS3
- RestoreDBInstanceFromSnapshot (solo RDS para Oracle)
- RestoreDBInstanceToPointInTime (solo RDS para Oracle)

Al seleccionar el parámetro `ManageMasterUserPassword` en `true` en estos comandos, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.

Para cifrar el secreto, también puede especificar una clave gestionada por el cliente o utilizar la clave de KMS que proporciona Secrets Manager. Utilice el parámetro `MasterUserSecretKmsKeyId` para especificar una clave administrada por el cliente. El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para especificar una clave en una Cuenta de AWS diferente, debe utilizar la clave de ARN o el alias de ARN. Una vez que RDS administre las credenciales de base de datos para una instancia de base de datos, no se puede cambiar la clave de KMS que se utiliza para cifrar el secreto.

Administración de la contraseña de usuario principal para una base de datos de inquilinos de RDS para Oracle con Secrets Manager

Puede configurar la administración de RDS de la contraseña del usuario maestro en Secrets Manager realizando las siguientes acciones:

- Añadir una base de datos de inquilinos de RDS para Oracle a su instancia de CDB
- Modificación de una base de datos de inquilinos de RDS para Oracle

Puede utilizar la consola de RDS, la AWS CLI o la API de RSD para realizar las acciones anteriores.

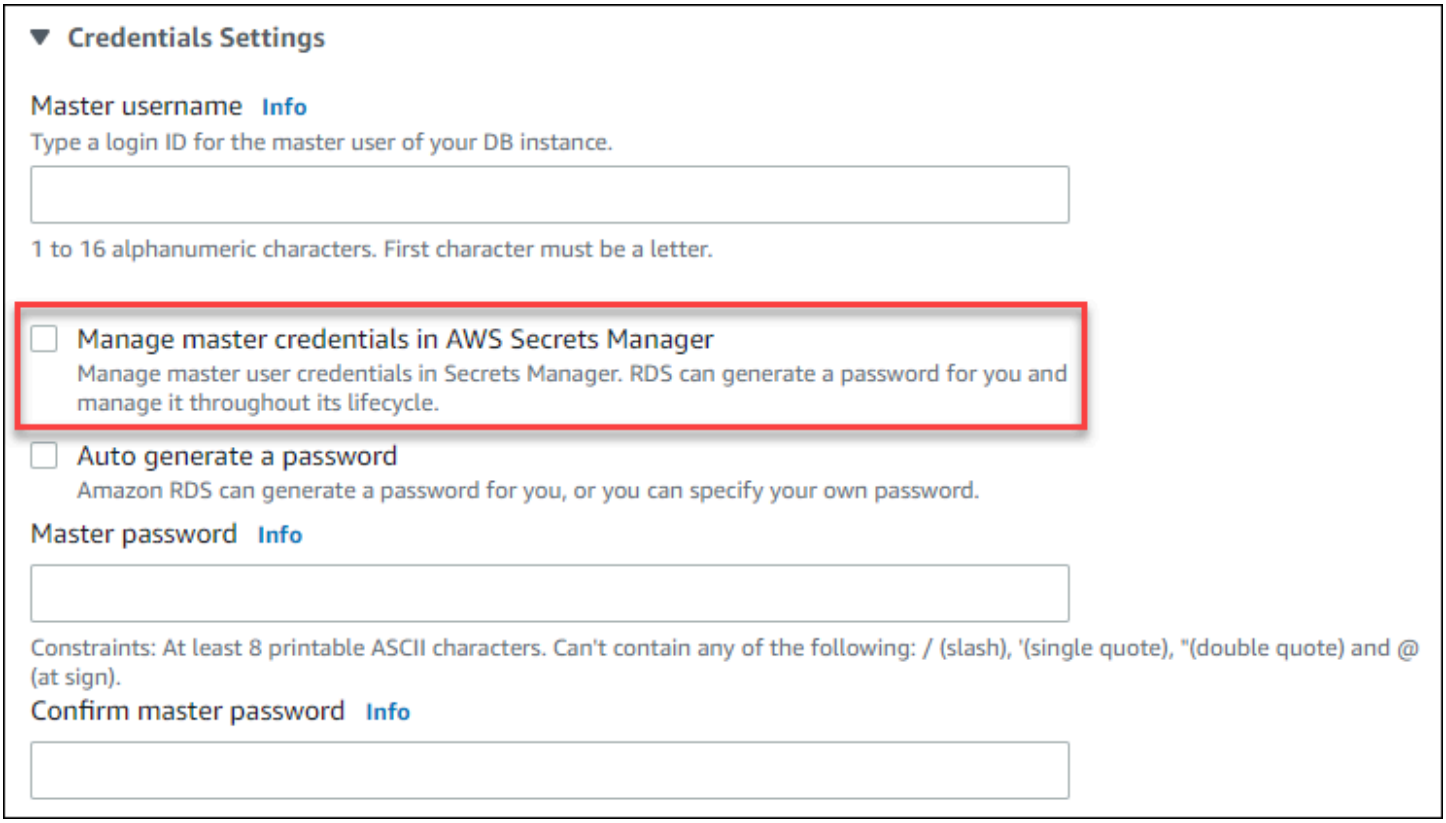
Consola

Siga las instrucciones para crear o modificar una base de datos de inquilinos de RDS para Oracle con la consola de RDS:

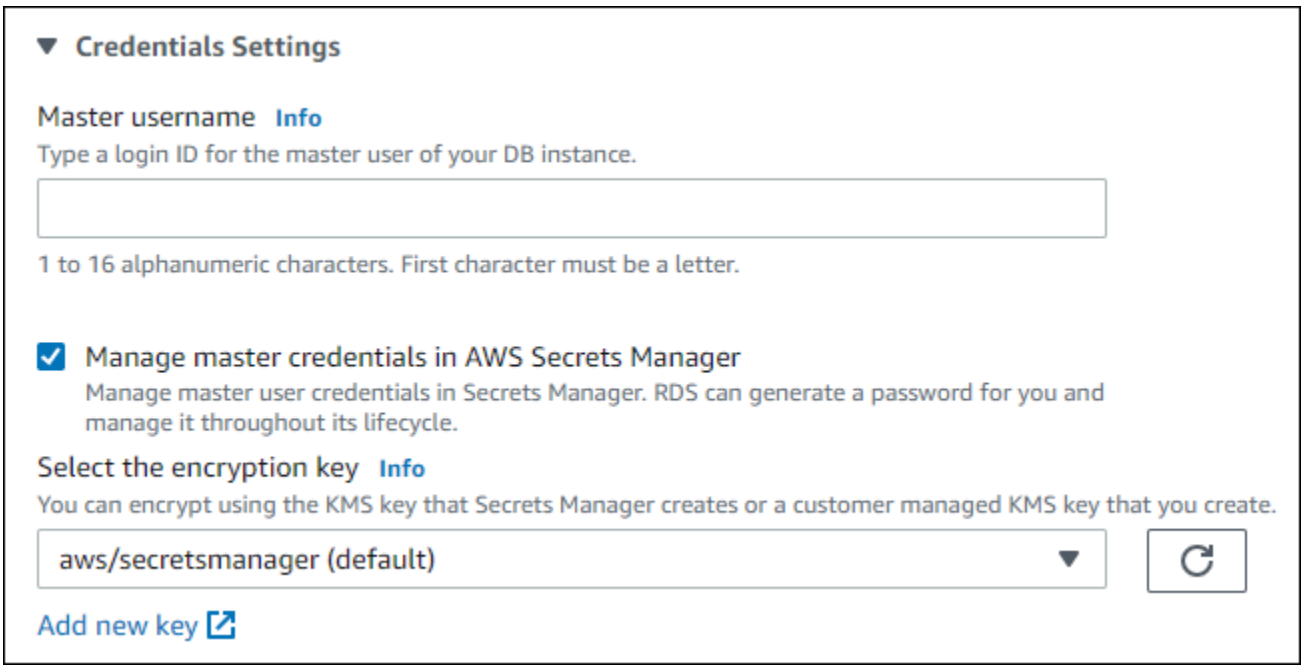
- Añadir una base de datos de inquilinos de RDS para Oracle a su instancia de CDB
- Modificación de una base de datos de inquilinos de RDS para Oracle

Al utilizar la consola de RDS para realizar una de las siguientes operaciones, puede especificar que RDS administre la contraseña principal en Secrets Manager. Al crear una base de datos de inquilinos, seleccione Administrar credenciales principales en AWS Secrets Manager en Configuración de credenciales. Cuando modifique una base de datos de inquilinos, seleccione Administrar las credenciales principales en AWS Secrets Manager en Configuración.

La siguiente imagen es un ejemplo de la configuración de Administrar las credenciales principales en AWS Secrets Manager que se utiliza al crear o restaurar una base de datos de inquilino.



Al seleccionar esta opción, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.



Puede optar por cifrar el secreto con una clave de KMS que proporcione Secrets Manager o con la clave gestionada por el cliente que cree usted. Una vez que RDS administre las credenciales de base de datos para una base de datos de inquilino, no se puede cambiar la clave de KMS que se utiliza para cifrar el secreto.

Puede elegir otros ajustes para cumplir con sus requisitos. Para obtener más información sobre la configuración disponible al crear una base de datos de inquilino, consulte Configuración de instancias de base de datos. Para obtener más información sobre la configuración disponible al modificar una base de datos de inquilino, consulte Configuración de instancias de base de datos.

AWS CLI

Para administrar la contraseña del usuario maestro con RDS en Secrets Manager, especifique la opción `--manage-master-user-password` en uno de los siguientes comandos AWS CLI:

- create-tenant-database
- modify-tenant-database

Al especificar la opción `--manage-master-user-password` en los comandos anteriores, RDS genera la contraseña de usuario principal y la administra durante todo su ciclo de vida en Secrets Manager.

Para cifrar el secreto, también puede especificar una clave gestionada por el cliente o utilizar la clave de KMS que proporciona Secrets Manager. Use la opción `--master-user-secret-kms-key-id` para especificar una clave administrada por el cliente. El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para especificar una clave en una Cuenta de AWS diferente, debe utilizar la clave de ARN o el alias de ARN. Una vez que RDS administre las credenciales de base de datos para una base de datos de inquilino, no se puede cambiar la clave de KMS que se utiliza para cifrar el secreto.

Puede elegir otros ajustes para cumplir con sus requisitos. Para obtener más información sobre la configuración disponible al crear una base de datos de inquilino, consulte create-tenant-database. Para obtener más información sobre la configuración disponible al modificar una base de datos de inquilinos, consulte modify-tenant-database.

En el siguiente ejemplo se crea una base de datos de inquilino de RDS para Oracle y se especifica que RDS administra la contraseña del usuario principal en Secrets Manager. El secreto se cifra mediante la clave de KMS que proporciona Secrets Manager.

Example

Para Linux, macOS o Unix:

```
aws rds create-tenant-database --region us-east-1 \
    --db-instance-identifier my-cdb-inst \
    --tenant-db-name mypdb2 \
    --master-username mypdb2-admin \
    --character-set-name UTF-16 \
    --manage-master-user-password
```

Para Windows:

```
aws rds create-tenant-database --region us-east-1 ^
    --db-instance-identifier my-cdb-inst ^
    --tenant-db-name mypdb2 ^
    --master-username mypdb2-admin ^
    --character-set-name UTF-16 ^
    --manage-master-user-password
```

API de RDS

Para especificar que RDS administre la contraseña del usuario maestro en Secrets Manager, defina el parámetro `ManageMasterUserPassword` en `true` con alguna de las siguientes operaciones de la API de RDS:

- CreateTenantDatabase
- ModifyTenantDatabase

Al seleccionar el parámetro `ManageMasterUserPassword` en `true` en estos comandos, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.

Para cifrar el secreto, también puede especificar una clave gestionada por el cliente o utilizar la clave de KMS que proporciona Secrets Manager. Utilice el parámetro `MasterUserSecretKmsKeyId` para especificar una clave administrada por el cliente. El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para especificar una clave en una Cuenta de AWS diferente, debe utilizar la clave de ARN o el alias de ARN. Una vez que RDS administre las credenciales de base de datos para una base de datos de inquilino, no se puede cambiar la clave de KMS que se utiliza para cifrar el secreto.

Administración de la contraseña de usuario maestra para un clúster de base de datos Multi-AZ con Secrets Manager

Puede configurar la administración de RDS de la contraseña del usuario maestro en Secrets Manager cuando realice las siguientes acciones:

- Creación de un clúster de base de datos multi-AZ para Amazon RDS
- Modificación de un clúster de base de datos multi-AZ para Amazon RDS.

Puede utilizar la consola de RDS, la AWS CLI o la API de RSD para realizar estas acciones.

Consola

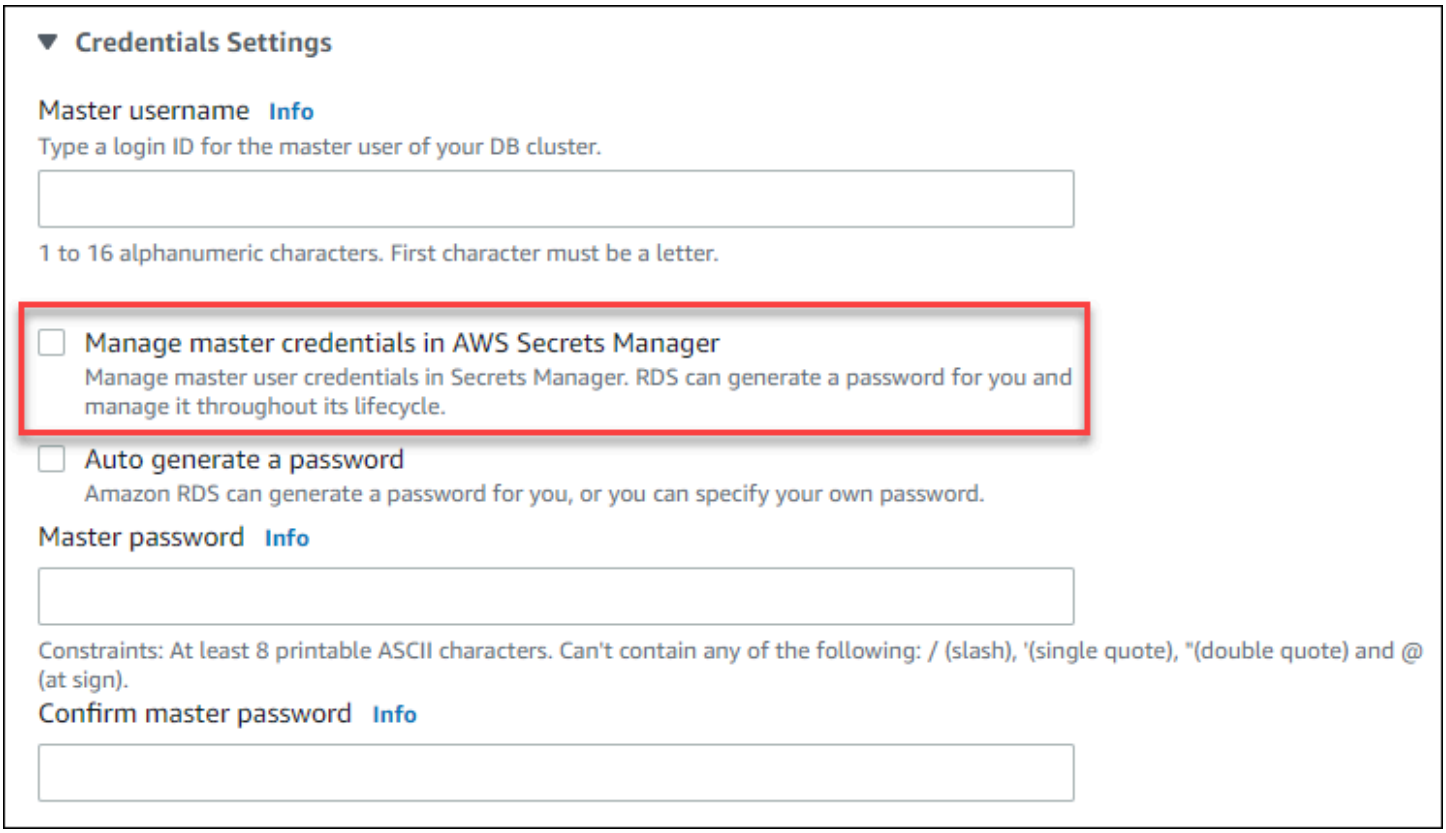
Siga las instrucciones para crear o modificar un clúster de base de datos Multi-AZ con la consola de RDS:

- Creación de un clúster de base de datos

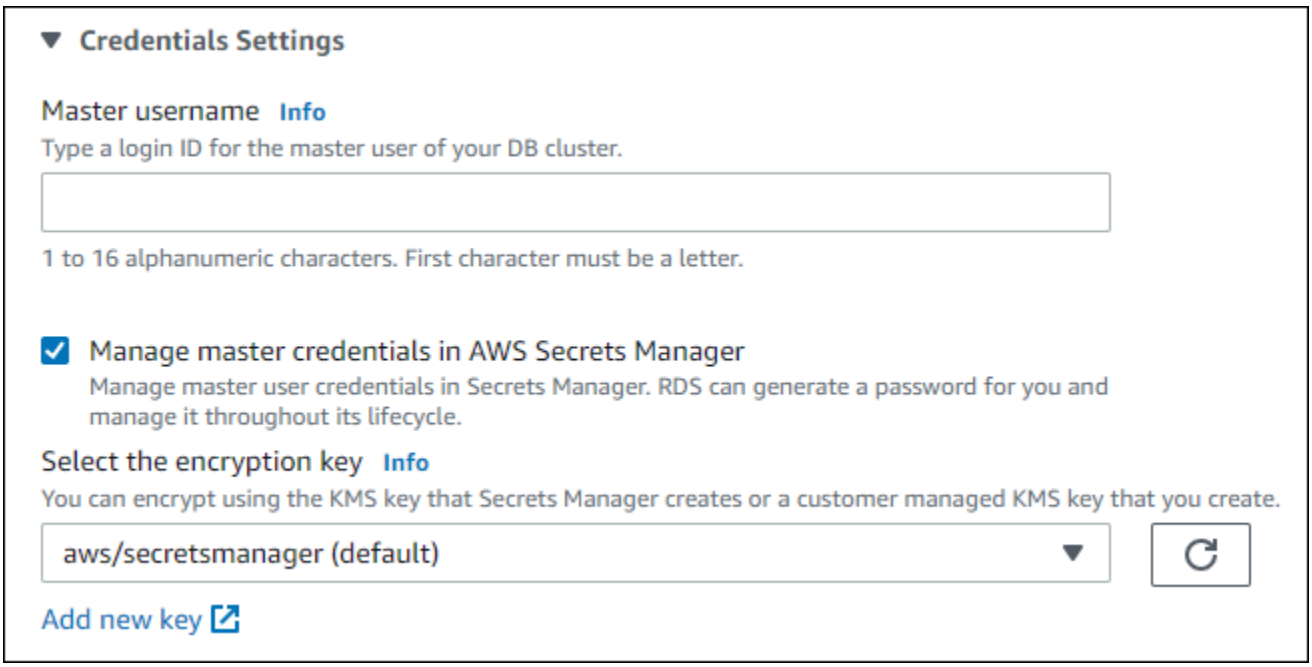
- Modificación de un clúster de base de datos multi-AZ para Amazon RDS.

Al utilizar la consola de RDS para realizar una de estas operaciones, puede especificar que RDS administre la contraseña del usuario maestro en Secrets Manager. Para hacerlo al crear o un clúster de base de datos, seleccione Manage master credentials in AWS Secrets Manager (Administrar las credenciales maestras en AWS Secrets Manager) en Credential settings (Configuración de credenciales). Cuando modifique un clúster de base de datos, seleccione Manage master credentials in AWS Secrets Manager (Administrar las credenciales maestras en AWS Secrets Manager) en Settings (Configuración).

La siguiente imagen es un ejemplo de la configuración Manage master credentials in AWS Secrets Manager (Administrar las credenciales maestras en AWS Secrets Manager) que se utiliza al crear o un clúster de base de datos.



Al seleccionar esta opción, RDS genera la contraseña de usuario maestra y la administra durante todo su ciclo de vida en Secrets Manager.



Puede optar por cifrar el secreto con una clave de KMS que proporcione Secrets Manager o con la clave gestionada por el cliente que cree usted. Una vez que RDS administre las credenciales de la base de datos de un clúster de base de datos, no podrá cambiar la clave de KMS que se usa para cifrar el secreto.

Puede elegir otros ajustes para cumplir con sus requisitos.

Para obtener más información sobre la configuración disponible al crear un clúster de base de datos Multi-AZ, consulte Configuración para la creación de clústeres de base de datos Multi-AZ. Para obtener más información sobre la configuración disponible al modificar un clúster de base de datos Multi-AZ, consulte Configuración para modificarlos clústeres de base de datos Multi-AZ.

AWS CLI

Para administrar la contraseña del usuario maestro con RDS en Secrets Manager, especifique la opción `--manage-master-user-password` en uno de los siguientes comandos:

- create-db-cluster
- modify-db-cluster

Al especificar la opción `--manage-master-user-password` en estos comandos, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.

Para cifrar el secreto, también puede especificar una clave gestionada por el cliente o utilizar la clave de KMS que proporciona Secrets Manager. Use la opción `--master-user-secret-kms-key-id` para especificar una clave administrada por el cliente. El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para especificar una clave en una Cuenta de AWS diferente, debe utilizar la clave de ARN o el alias de ARN. Una vez que RDS administre las credenciales de la base de datos de un clúster de base de datos, no podrá cambiar la clave de KMS que se usa para cifrar el secreto.

Puede elegir otros ajustes para cumplir con sus requisitos.

Para obtener más información sobre la configuración disponible al crear un clúster de base de datos Multi-AZ, consulte Configuración para la creación de clústeres de base de datos Multi-AZ. Para obtener más información sobre la configuración disponible al modificar un clúster de base de datos Multi-AZ, consulte Configuración para modificarlos clústeres de base de datos Multi-AZ.

En este ejemplo se crea un clúster de base de datos Multi-AZ y se especifica que RDS administre la contraseña en Secrets Manager. El secreto se cifra mediante la clave de KMS que proporciona Secrets Manager.

Example

Para Linux, macOS o Unix:

```
aws rds create-db-cluster \
   --db-cluster-identifier mysql-multi-az-db-cluster \
   --engine mysql \
   --engine-version 8.0.39  \
   --backup-retention-period 1  \
   --allocated-storage 4000 \
   --storage-type io1 \
   --iops 10000 \
   --db-cluster-instance-class db.r6gd.xlarge \
   --master-username testUser \
   --manage-master-user-password
```

Para Windows:

```
aws rds create-db-cluster ^
   --db-cluster-identifier mysql-multi-az-db-cluster ^
   --engine mysql ^
```

```
    --engine-version 8.0.39 ^
    --backup-retention-period 1 ^
    --allocated-storage 4000 ^
    --storage-type io1 ^
    --iops 10000 ^
    --db-cluster-instance-class db.r6gd.xlarge ^
    --master-username testUser ^
    --manage-master-user-password
```

API de RDS

Para especificar que RDS administre la contraseña del usuario maestro en Secrets Manager, defina el parámetro `ManageMasterUserPassword` en `true` con alguna de las siguientes operaciones:

- CreateDBCluster
- ModifyDBCluster

Al seleccionar el parámetro `ManageMasterUserPassword` en `true` en una de estas operaciones, RDS genera la contraseña de usuario maestro y la administra durante todo su ciclo de vida en Secrets Manager.

Para cifrar el secreto, también puede especificar una clave gestionada por el cliente o utilizar la clave de KMS que proporciona Secrets Manager. Utilice el parámetro `MasterUserSecretKmsKeyId` para especificar una clave administrada por el cliente. El identificador de la clave de AWS KMS es el ARN de la clave, el identificador de clave, el ARN de alias o el nombre de alias de la clave de KMS. Para especificar una clave en una Cuenta de AWS diferente, debe utilizar la clave de ARN o el alias de ARN. Una vez que RDS administre las credenciales de la base de datos de un clúster de base de datos, no podrá cambiar la clave de KMS que se usa para cifrar el secreto.

Rotación del secreto de contraseña de usuario maestro para una instancia de base de datos

Cuando RDS rota el secreto de contraseña de usuario maestro, Secrets Manager genera una nueva versión de secreto para el secreto existente. La nueva versión del secreto contiene la nueva contraseña de usuario maestra. Amazon RDS cambia la contraseña de usuario maestro para la instancia de base de datos para que coincida con la contraseña de la nueva versión de secreto.

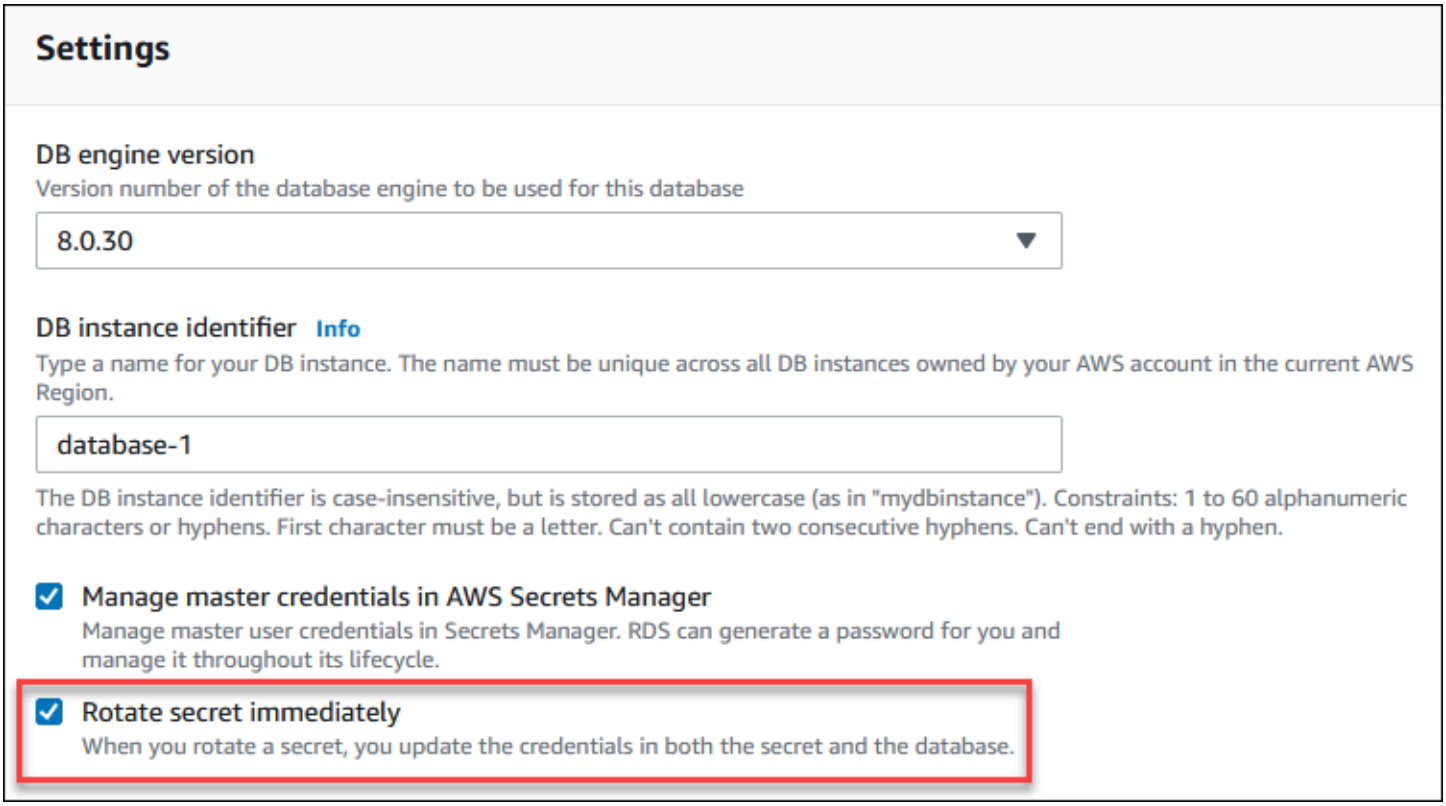
Puede rotar un secreto inmediatamente en lugar de esperar a que se programe una rotación. Para rotar un secreto de contraseña de un usuario maestro en Secrets Manager, modifique la instancia

de base de datos. Para obtener información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Puede cambiar un secreto de contraseña de usuario maestro inmediatamente con la consola de RDS, la AWS CLI de RDS o la API de RDS. La nueva contraseña siempre tiene 28 caracteres y contiene al menos una mayúscula y una minúscula, un número y un signo de puntuación.

Consola

Para rotar un secreto de contraseña de usuario maestro mediante la consola de RDS, modifique la instancia de base de datos y seleccione Rotate secret immediately (Rotar el secreto inmediatamente) en Settings (Configuración).



Siga las instrucciones para modificar una instancia de base de datos con la consola de RDS en Modificación de una instancia de base de datos de Amazon RDS. Debe elegir Apply immediately (Aplicar inmediatamente) en la página de confirmación.

AWS CLI

Para rotar un secreto de contraseña de usuario maestro mediante la AWS CLI, utilice el comando modify-db-instance y especifique la opción `--rotate-master-user-password`. Debe especificar la opción `--apply-immediately` al rotar la contraseña maestra.

En este ejemplo, se rota un secreto de contraseña de usuario maestro.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --rotate-master-user-password \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --rotate-master-user-password ^
    --apply-immediately
```

API de RDS

Puede rotar un secreto de contraseña de usuario maestro mediante la operación ModifyDBInstance y configurar el parámetro `RotateMasterUserPassword` en `true`. Debe establecer el parámetro `ApplyImmediately` en `true` al rotar la contraseña maestra.

Rotación del secreto de contraseña de usuario maestra para un clúster de base de datos Multi-AZ

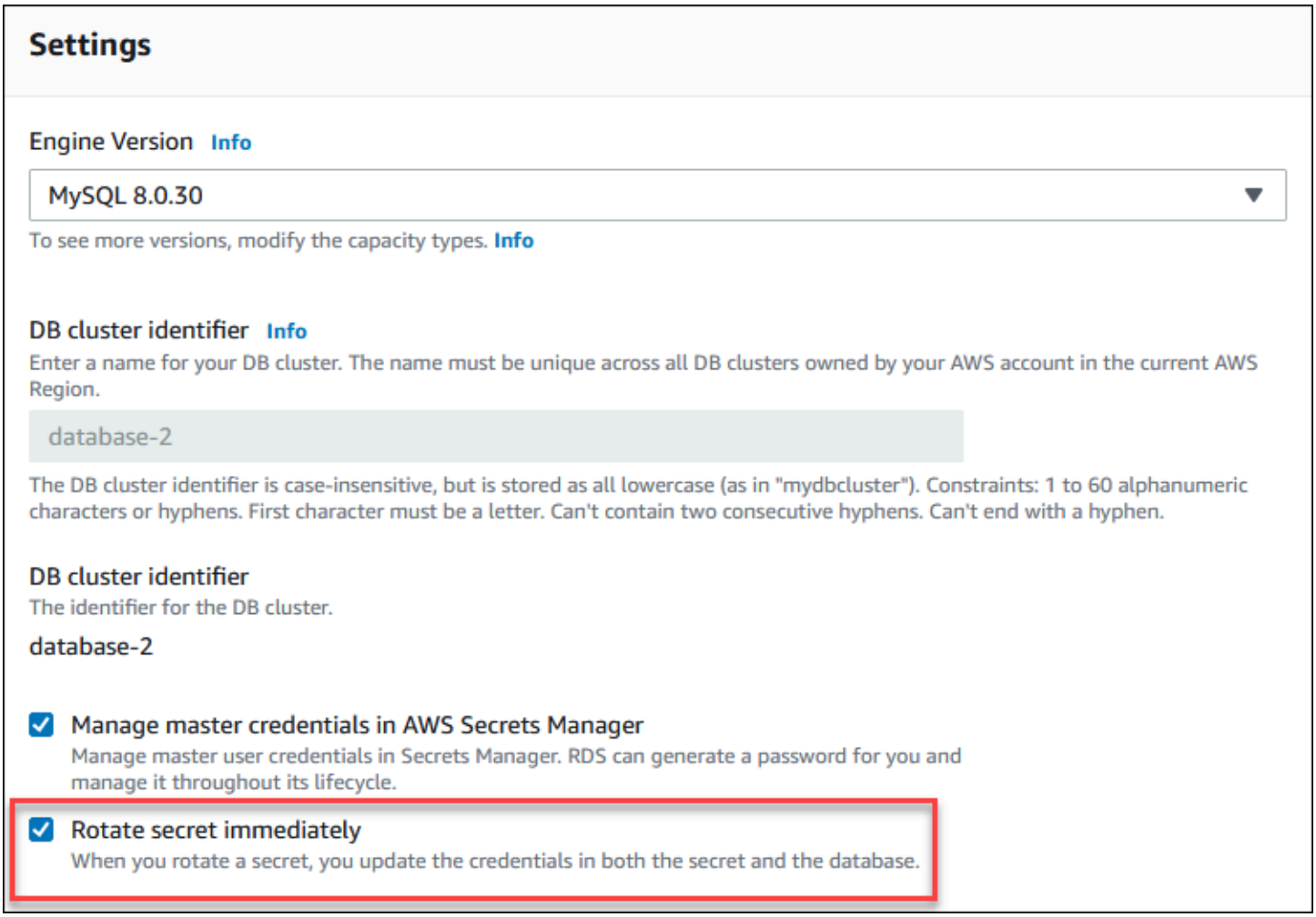
Cuando RDS rota un secreto de contraseña de usuario maestro, Secrets Manager genera una nueva versión de secreto para el secreto existente. La nueva versión del secreto contiene la nueva contraseña de usuario maestra. Amazon RDS cambia la contraseña de usuario maestro para el clúster de base de datos Multi-AZ para que coincida con la contraseña de la nueva versión de secreto.

Puede rotar un secreto inmediatamente en lugar de esperar a que se programe una rotación. Para rotar un secreto de contraseña de usuario maestra en Secrets Manager, modifique el clúster de base de datos Multi-AZ. Para obtener más información sobre la modificación de un clúster de base de datos Multi-AZ, consulte Modificación de un clúster de base de datos multi-AZ para Amazon RDS..

Puede cambiar un secreto de contraseña de usuario maestro inmediatamente con la consola de RDS, la AWS CLI de RDS o la API de RDS. La nueva contraseña siempre tiene 28 caracteres y contiene al menos una mayúscula y una minúscula, un número y un signo de puntuación.

Consola

Para rotar un secreto de contraseña de usuario maestro mediante la consola de RDS, modifique el clúster de base de datos Multi-AZ y seleccione Rotate secret immediately (Rotar el secreto inmediatamente) en Settings (Configuración).



Siga las instrucciones para modificar un clúster de base de datos Multi-AZ con la consola RDS en Modificación de un clúster de base de datos multi-AZ para Amazon RDS.. Debe elegir Apply immediately (Aplicar inmediatamente) en la página de confirmación.

AWS CLI

Para rotar un secreto de contraseña de usuario maestro mediante la AWS CLI, utilice el comando modify-db-cluster y especifique la opción `--rotate-master-user-password`. Debe especificar la opción `--apply-immediately` al rotar la contraseña maestra.

En este ejemplo, se rota un secreto de contraseña de usuario maestro.

Example

Para Linux, macOS o Unix:

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --rotate-master-user-password \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --rotate-master-user-password ^
    --apply-immediately
```

API de RDS

Puede rotar un secreto de contraseña de usuario maestro mediante la operación ModifyDBCluster y estableciendo el parámetro `RotateMasterUserPassword` en `true`. Debe establecer el parámetro `ApplyImmediately` en `true` al rotar la contraseña maestra.

Visualización de los detalles de un secreto para una instancia de base de datos

Puede recuperar sus secretos mediante la consola (https://console.aws.amazon.com/secretsmanager/) o la AWS CLI (comando get-secret-value de Secrets Manager).

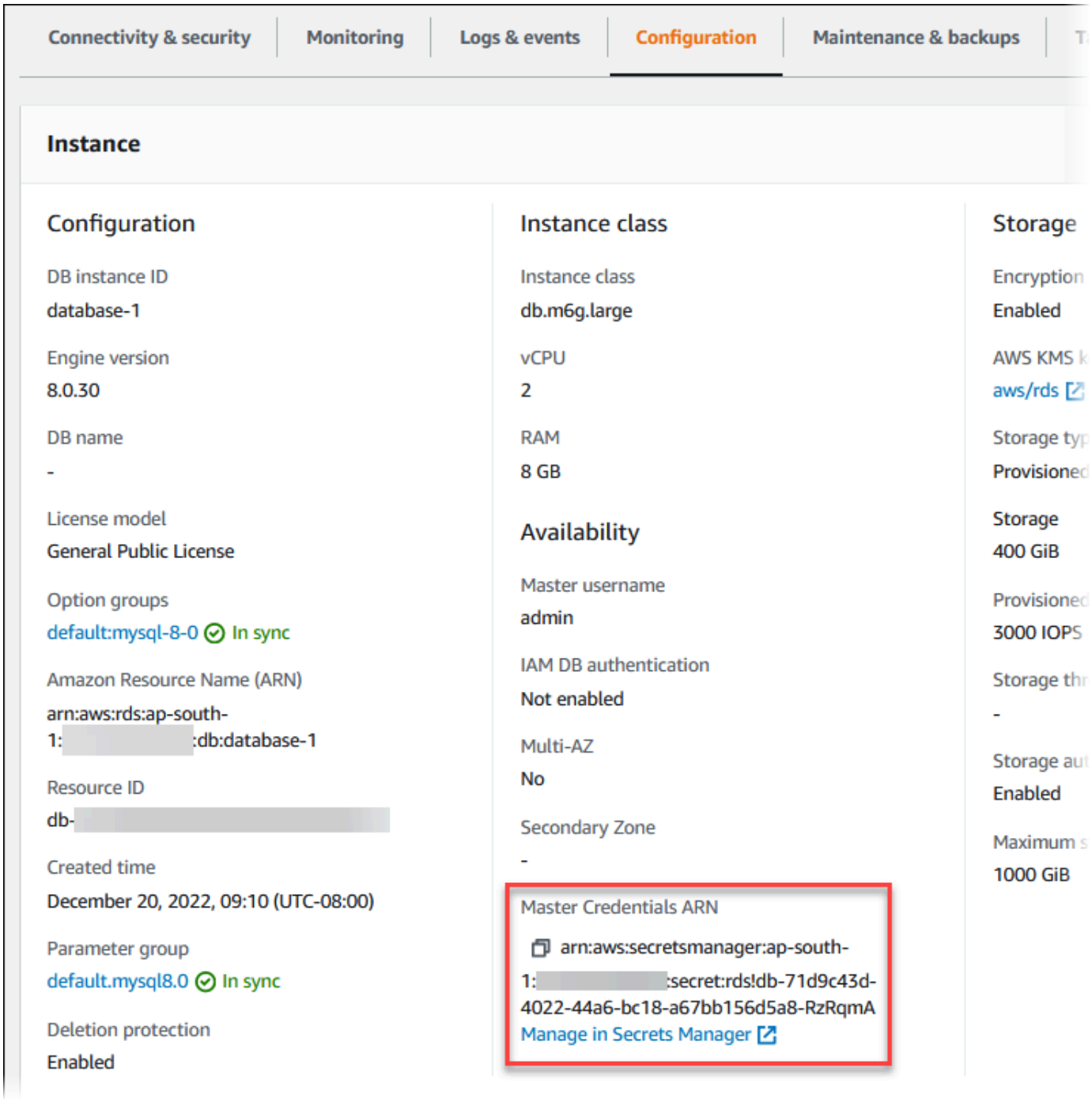
Puede encontrar el nombre de recurso de Amazon (ARN) de un secreto administrado por RDS en Secrets Manager con la consola de RDS, la AWS CLI de RDS o la API de RDS.

Consola

Para ver los detalles de un secreto administrado por RDS en Secrets Manager

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Bases de datos.
3. Seleccione el nombre de la instancia de base de datos para mostrar sus detalles.
4. Elija la pestaña Configuración.

En el Master Credentials ARN (ARN de credenciales maestras), puede ver el ARN secreto.



Puede seguir el enlace Manage in Secrets Manager (Administrar en Secrets Manager) para ver y administrar el secreto en la consola de Secrets Manager.

AWS CLI

Puede utilizar el comando de la CLI de RDS describe-db-instances para buscar la siguiente información sobre un secreto administrado por RDS en Secrets Manager:

- `SecretArn`: ARN del secreto
- `SecretStatus`: estado del secreto

  Otros valores de estado posibles son:

  - `creating`: se está creando el secreto.
  - `active`: el secreto está disponible para su uso y rotación normales.
  - `rotating`: se está rotando el secreto.
  - `impaired`: el secreto se puede usar para acceder a las credenciales de la base de datos, pero no se puede rotar. Un secreto puede tener este estado si, por ejemplo, se cambian los permisos para que RDS ya no pueda acceder al secreto ni a la clave de KMS del secreto.

    Cuando un secreto tiene este estado, puede corregir la condición que provocó el estado. Si corrige la condición que causó el estado, el estado sigue siendo `impaired` hasta la siguiente rotación. De forma alternativa, puede modificar la instancia de base de datos para desactivar la administración automática de las credenciales de la base de datos y, a continuación, volver a modificar la instancia de base de datos para activar la administración automática de las credenciales de la base de datos. Para modificar la instancia de base de datos, use la opción `--manage-master-user-password` en el comando modify-db-instance.
- `KmsKeyId`: ARN de la clave de KMS que se utiliza para cifrar el secreto.

Especifique la opción `--db-instance-identifier` para mostrar el resultado de una instancia de base de datos específica. En este ejemplo se muestra el resultado de un secreto que utiliza una instancia de base de datos.

Example

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

A continuación, se muestra un ejemplo de resultado de un secreto:

```
"MasterUserSecret": {
                "SecretArn": "arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
db-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx",
```

```
                "SecretStatus": "active",
                "KmsKeyId": "arn:aws:kms:eu-
west-1:123456789012:key/0987dcba-09fe-87dc-65ba-ab0987654321"
            }
```

Cuando tenga el ARN secreto, podrá ver los detalles del secreto con el comando get-secret-value de la CLI de Secrets Manager.

En este ejemplo se muestran los detalles del secreto del resultado del ejemplo anterior.

Example

Para Linux, macOS o Unix:

```
aws secretsmanager get-secret-value \
    --secret-id 'arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
db-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx'
```

Para Windows:

```
aws secretsmanager get-secret-value ^
    --secret-id 'arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
db-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx'
```

API de RDS

Puede ver el ARN, el estado y la clave de KMS de un secreto administrado por RDS en Secrets Manager mediante la operación DescribeDBInstances y estableciendo el parámetro `DBInstanceIdentifier` en un identificador de instancia de base de datos. En el resultado se incluyen detalles sobre el secreto.

Cuando tenga el ARN secreto, podrá ver los detalles del secreto con la operación GetSecretValue de Secrets Manager.

Visualización de los detalles de un secreto para un clúster de base de datos Multi-AZ

Puede recuperar sus secretos mediante la consola (https://console.aws.amazon.com/secretsmanager/) o la AWS CLI (comando get-secret-value de Secrets Manager).

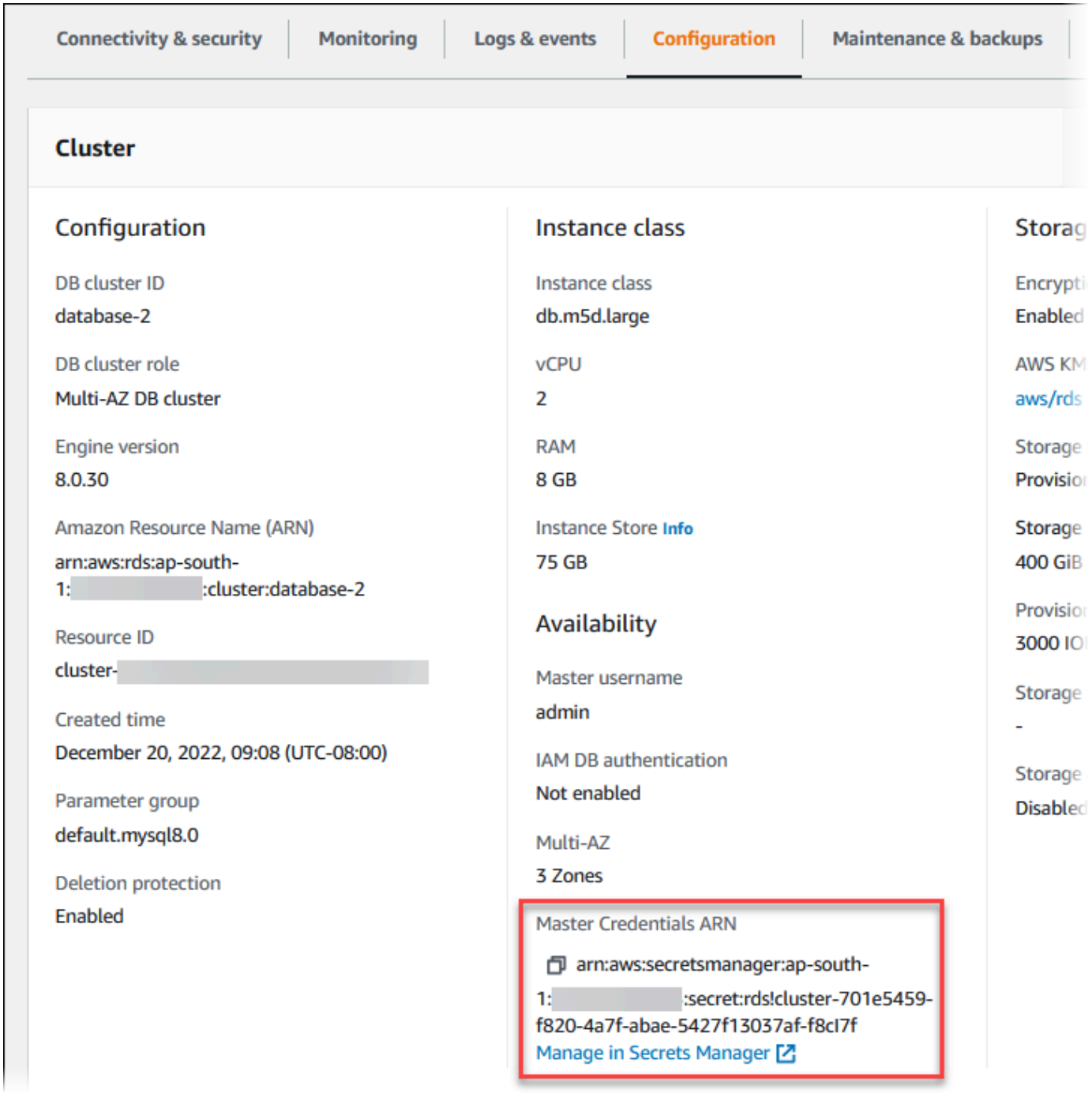
Puede encontrar el nombre de recurso de Amazon (ARN) de un secreto administrado por RDS en Secrets Manager con la consola de RDS, la AWS CLI de RDS o la API de RDS.

Consola

Para ver los detalles de un secreto administrado por RDS en Secrets Manager

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija el nombre del clúster de base de datos Multi-AZ para mostrar sus detalles.
4. Elija la pestaña Configuración.

   En el Master Credentials ARN (ARN de credenciales maestras), puede ver el ARN secreto.



Puede seguir el enlace Manage in Secrets Manager (Administrar en Secrets Manager) para ver y administrar el secreto en la consola de Secrets Manager.

AWS CLI

Puede utilizar el comando describe-db-clusters de la AWS CLI de RDS para buscar la siguiente información sobre un secreto administrado por RDS en Secrets Manager:

- `SecretArn`: ARN del secreto
- `SecretStatus`: estado del secreto

  Otros valores de estado posibles son:

  - `creating`: se está creando el secreto.
  - `active`: el secreto está disponible para su uso y rotación normales.
  - `rotating`: se está rotando el secreto.
  - `impaired`: el secreto se puede usar para acceder a las credenciales de la base de datos, pero no se puede rotar. Un secreto puede tener este estado si, por ejemplo, se cambian los permisos para que RDS ya no pueda acceder al secreto ni a la clave de KMS del secreto.

    Cuando un secreto tiene este estado, puede corregir la condición que provocó el estado. Si corrige la condición que causó el estado, el estado sigue siendo `impaired` hasta la siguiente rotación. De forma alternativa, puede modificar el clúster de base de datos para desactivar la administración automática de las credenciales de la base de datos y, a continuación, volver a modificar el clúster de base de datos para activar la administración automática de las credenciales de la base de datos. Para modificar un clúster de base de datos, use la opción `--manage-master-user-password` en el comando modify-db-cluster.
- `KmsKeyId`: ARN de la clave de KMS que se utiliza para cifrar el secreto.

Especifique la opción `--db-cluster-identifier` para mostrar el resultado de un clúster de base de datos específica. En este ejemplo se muestra el resultado de un secreto que utiliza un clúster de base de datos.

Example

```
aws rds describe-db-clusters --db-cluster-identifier mydbcluster
```

A continuación, se muestra un ejemplo de resultado de un secreto:

```
"MasterUserSecret": {
                "SecretArn": "arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
cluster-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx",
                "SecretStatus": "active",
                "KmsKeyId": "arn:aws:kms:eu-
west-1:123456789012:key/0987dcba-09fe-87dc-65ba-ab0987654321"
            }
```

Cuando tenga el ARN secreto, podrá ver los detalles del secreto con el comando get-secret-value de la CLI de Secrets Manager.

En este ejemplo se muestran los detalles del secreto del resultado del ejemplo anterior.

Example

Para Linux, macOS o Unix:

```
aws secretsmanager get-secret-value \
    --secret-id 'arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
cluster-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx'
```

Para Windows:

```
aws secretsmanager get-secret-value ^
    --secret-id 'arn:aws:secretsmanager:eu-west-1:123456789012:secret:rds!
cluster-033d7456-2c96-450d-9d48-f5de3025e51c-xmJRDx'
```

API de RDS

Puede ver el ARN, el estado y la clave de KMS de un secreto administrado por RDS en Secrets Manager mediante la operación RDS DescribeDBClusters y estableciendo el parámetro `DBClusterIdentifier` en un identificador de clúster de base de datos. En el resultado se incluyen detalles sobre el secreto.

Cuando tenga el ARN secreto, podrá ver los detalles del secreto con la operación GetSecretValue de Secrets Manager.

Visualización de los detalles de un secreto para una base de datos de inquilinos

Puede recuperar sus secretos mediante la consola (https://console.aws.amazon.com/secretsmanager/) o la AWS CLI (comando get-secret-value de Secrets Manager).

Puede encontrar el nombre de recurso de Amazon (ARN) de un secreto administrado por Amazon RDS en AWS Secrets Manager con la consola de Amazon RDS, la AWS CLI o la API de Amazon RDS.

Consola

Visualización de los detalles de un secreto administrado por Amazon RDS en AWS Secrets Manager para una base de datos de inquilinos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos).
3. Elija el nombre de la instancia de base de datos que contiene la base de datos de inquilinos para mostrar sus detalles.
4. Elija la pestaña Configuración.

   En la sección Bases de datos de inquilinos, busque la base de datos del inquilino y consulte su ARN de credenciales maestras.

   Puede seguir el enlace Manage in Secrets Manager (Administrar en Secrets Manager) para ver y administrar el secreto en la consola de Secrets Manager.

AWS CLI

Puede utilizar el comando describe-tenant-databases de la AWS CLI de Amazon RDS para buscar la siguiente información sobre un secreto administrado por Amazon RDS en AWS Secrets Manager para una base de datos de inquilinos:

- `SecretArn`: ARN del secreto
- `SecretStatus`: estado del secreto

  Otros valores de estado posibles son:

  - `creating`: se está creando el secreto.
  - `active`: el secreto está disponible para su uso y rotación normales.
  - `rotating`: se está rotando el secreto.
  - `impaired`: el secreto se puede usar para acceder a las credenciales de la base de datos, pero no se puede rotar. Un secreto puede tener este estado si, por ejemplo, se cambian los permisos para que Amazon RDS ya no pueda acceder al secreto ni a la clave de KMS del secreto.

    Cuando un secreto tiene este estado, puede corregir la condición que provocó el estado. Si corrige la condición que causó el estado, el estado sigue siendo `impaired` hasta la siguiente

rotación. De forma alternativa, puede modificar la base de datos de inquilinos para desactivar la administración automática de las credenciales de la base de datos y, a continuación, volver a modificar la base de datos de inquilinos para activar la administración automática de las credenciales de la base de datos. Para modificar la base de datos de inquilinos, utilice la opción `--manage-master-user-password` en el comando modify-tenant-database.

- `KmsKeyId`: ARN de la clave de KMS que se utiliza para cifrar el secreto.

Especifique la opción `--db-instance-identifier` para mostrar el resultado para bases de datos de inquilinos de una instancia de base de datos específica. También puede especificar la opción `--tenant-db-name` para mostrar el resultado de una base de datos de inquilinos específica. En este ejemplo se muestra el resultado de un secreto que utiliza una base de datos de inquilinos.

Example

```
aws rds describe-tenant-databases \
    --db-instance-identifier database-3 \
    --query "TenantDatabases[0].MasterUserSecret"
```

A continuación, se muestra un ejemplo de resultado de un secreto:

```
{
    "SecretArn": "arn:aws:secretsmanager:us-east-2:123456789012:secret:rds!db-ABC123",
    "SecretStatus": "active",
    "KmsKeyId": "arn:aws:kms:us-east-2:123456789012:key/aa11bb22-####-####-####-
fedcba123456"
}
```

Cuando tenga el ARN secreto, podrá ver los detalles del secreto con el comando get-secret-value de la AWS CLI de Secrets Manager.

En este ejemplo se muestran los detalles del secreto del resultado del ejemplo anterior.

Example

Para Linux, macOS o Unix:

```
aws secretsmanager get-secret-value \
    --secret-id 'arn:aws:secretsmanager:us-east-2:123456789012:secret:rds!db-ABC123'
```

Para Windows:

```
aws secretsmanager get-secret-value ^
    --secret-id 'arn:aws:secretsmanager:us-east-2:123456789012:secret:rds!db-ABC123'
```

API de Amazon RDS

Puede ver el ARN, el estado y la clave de KMS de un secreto administrado por Amazon RDS en AWS Secrets Manager mediante la operación DescribeTenantDatabases y estableciendo el parámetro `DBInstanceIdentifier` en un identificador de instancia de base de datos. También puede establecer el parámetro `TenantDBName` con un nombre de base de datos de inquilinos específico. En el resultado se incluyen detalles sobre el secreto.

Cuando tenga el ARN secreto, podrá ver los detalles del secreto con la operación GetSecretValue de Secrets Manager.

Disponibilidad en regiones y versiones

La disponibilidad y el soporte de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad de versiones y regiones con la integración de Secrets Manager con Amazon RDS, consulte Regiones y motores de bases de datos admitidos para la integración de Secrets Manager con Amazon RDS.

Protección de datos en Amazon RDS

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Relational Database Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon RDS u otros Servicios de AWS mediante la consola, la API, AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Temas

- Protección de datos mediante cifrado
- Privacidad del tráfico entre redes

Protección de datos mediante cifrado

Puede habilitar el cifrado para recursos de bases de datos. También puede cifrar conexiones a instancias de bases de datos.

Temas

- Cifrado de recursos de Amazon RDS

- Administración de AWS KMS key
- Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos
- Rotar certificados SSL/TLS

Cifrado de recursos de Amazon RDS

Amazon RDS puede cifrar sus Amazon RDS instancias de base de datos. Los datos cifrados en reposo incluyen el almacenamiento subyacente de instancias de bases de datos, sus copias de seguridad automatizadas, sus réplicas de lectura y sus instantáneas.

En las instancias de bases de datos de Amazon RDS con cifrado se utiliza el algoritmo de cifrado AES-256 estándar del sector para cifrar los datos en el servidor que aloja instancias de bases de datos de Amazon RDS. Una vez cifrados los datos, Amazon RDS se encarga de la autenticación de acceso y del descifrado de los datos de forma transparente, con un impacto mínimo en el desempeño. No es necesario modificar las aplicaciones cliente de base de datos para utilizar el cifrado.

> **Note**
>
> Para los clústeres de instancias, los datos en tránsito entre el origen y las réplicas de lectura están cifrados, incluso al replicar entre regiones de AWS.

Temas

- Información general del cifrado de los recursos de Amazon RDS
- Cifrar una instancia de base de datos
- Determinar si el cifrado está activado para una instancia de base de datos
- Disponibilidad del cifrado de Amazon RDS
- Cifrado en tránsito
- Limitaciones de las instancias de base de datos cifrados de Amazon RDS

Información general del cifrado de los recursos de Amazon RDS

Las instancias de bases de datos cifradas de Amazon RDS proporcionan una capa adicional de protección de datos al proteger los datos del acceso no autorizado al almacenamiento subyacente. Puede utilizar el cifrado de Amazon RDS para aumentar la protección de datos de las aplicaciones

implementadas en la nube y para cumplir con los requisitos de conformidad para el cifrado en reposo. Para una instancia de base de datos cifrada de Amazon RDS, todos los registros, copias de seguridad e instantáneas están cifrados. Para obtener más información sobre la disponibilidad y las limitaciones del cifrado, consulte Disponibilidad del cifrado de Amazon RDS y Limitaciones de las instancias de base de datos cifrados de Amazon RDS.

Amazon RDS usa una clave de AWS Key Management Service para cifrar estos recursos. AWS KMS combina hardware y software seguros y altamente disponibles para ofrecer un sistema de administración de claves escalado para la nube. Puede utilizar una Clave administrada de AWS, o bien puede o crear claves administradas por el cliente.

Cuando crea una instancia de base de datos cifrada, puede elegir una clave administrada por el cliente o la Clave administrada de AWS para Amazon RDS para cifrar la instancia de base de datos. Si no especifica el identificador de clave para una clave administrada por el cliente, Amazon RDS utiliza la Clave administrada de AWS para la nueva instancia de base de datos. Amazon RDS crea una Clave administrada de AWS para Amazon RDS para su cuenta de AWS. Su cuenta de AWS tiene una Clave administrada de AWS diferente para Amazon RDS para cada región de AWS.

Para administrar las claves administradas por el cliente que se usan para cifrar y descifrar los recursos de Amazon RDS, se utiliza AWS Key Management Service (AWS KMS).

Si utiliza AWS KMS, podrá crear claves administradas por el cliente y definir las políticas que controlan cómo se pueden utilizar las claves administradas por el cliente. AWS KMS es compatible con CloudTrail, lo que permite auditar la utilización de claves de KMS para comprobar que las claves administradas por el cliente se utilizan de forma adecuada. Puede utilizar las claves administradas por el cliente con Amazon Aurora y los servicios de AWS admitidos, como, por ejemplo, Amazon S3, Amazon EBS y Amazon Redshift. Para ver una lista de los servicios integrados con AWS KMS, consulte Integración con los servicios de AWS. Algunas consideraciones sobre el uso de las claves de KMS:

- Una vez que se crea una instancia de base de datos cifrada, no se puede cambiar la clave de KMS que dicha instancia de base de datos utiliza. Por tanto, asegúrese de determinar los requisitos de su clave de KMS antes de crear la instancia de base de datos cifrada.

  Si debe cambiar la clave de cifrado de la instancia de base de datos, cree una instantánea manual de la instancia y habilite el cifrado mientras se copia la instantánea. Para obtener más información, consulte artículo de información de re:Post.
- Si copia una instantánea cifrada, puede utilizar una clave de KMS para cifrar la instantánea de destino diferente de la que se utilizó para cifrar la instantánea de origen.

- Las réplicas de lectura de una instancia cifrada de Amazon RDS deben cifrarse con la misma clave de KMS que la instancia de base de datos primaria cuando ambas están en la misma región de AWS.
- Si la instancia de base de datos primaria y la réplica de lectura se encuentran en regiones de AWS distintas, debe cifrar la réplica de lectura con la clave de KMS de esa región de AWS.
- No se puede compartir una instantánea que se haya cifrado con la Clave administrada de AWS de la cuenta de AWS que compartió la instantánea.
- Amazon RDS también permite cifrar una base de datos Oracle o de SQL Server mediante el cifrado de datos transparente (TDE). Se puede utilizar el TDE con el cifrado RDS en reposo, aunque el uso simultáneo del TDE y el cifrado RDS en reposo podría afectar ligeramente al rendimiento de la base de datos. Debe administrar claves distintas para cada método de cifrado. Para obtener más información acerca de TDE, consulte Cifrado de datos transparente de Oracle o Compatibilidad con el Cifrado de datos transparente en SQL Server.

Important

Amazon RDS pierde el acceso a la clave de KMS para una instancia de base de datos al desactivar la clave de KMS. Si pierde el acceso a una clave de KMS, la instancia de base de datos cifrada entra en el estado `inaccessible-encryption-credentials-recoverable` 2 horas después de la detección en las instancias en las que las copias de seguridad están habilitadas. La instancia de base de datos permanece en este estado durante siete días, durante los cuales se detiene. Es posible que las llamadas a la API realizadas a la instancia de base de datos durante este tiempo no se realicen correctamente. Para recuperar la instancia de base de datos, habilite la clave de KMS y reinicie esta instancia de base de datos. Habilite la clave de KMS desde la AWS Management Console, la AWS CLI o la API de RDS. Reinicie la instancia de base de datos con el comando de la AWS CLI start-db-instance o la AWS Management Console.

El estado `inaccessible-encryption-credentials-recoverable` solo se aplica a instancias de base de datos que pueden detenerse. Este estado recuperable no se aplica a las instancias que no se pueden detener, como las réplicas de lectura y las instancias con réplicas de lectura. Para obtener más información, consulte Limitaciones de la detención de la instancia de base de datos.

Si la instancia de base de datos no se recupera en siete días, pasa al estado de terminal `inaccessible-encryption-credentials`. En este estado, la instancia de base de datos ya no se puede usar y solo puede restaurarla desde una copia de seguridad. Recomendamos que siempre habilite las copias de seguridad para las instancias de bases

de datos cifradas con el fin de protegerse contra la pérdida de los datos cifrados de dichas bases de datos.
Durante la creación de una instancia de base de datos, Amazon RDS comprueba si la entidad principal que realiza la llamada tiene acceso a la clave KMS y genera una concesión a partir de la clave KMS que utiliza durante toda la vida útil de la instancia de base de datos. La revocación del acceso de la entidad principal que realiza la llamada a la clave KMS no afecta a una base de datos en ejecución. Cuando se utilizan claves KMS en situaciones de varias cuentas, como copiar una instantánea a otra cuenta, la clave KMS debe compartirse con la otra cuenta. Si crea una instancia de base de datos a partir de la instantánea sin especificar una clave KMS diferente, la nueva instancia utilizará la clave KMS de la cuenta de origen. La revocación del acceso a la clave después de crear la instancia de base de datos no afecta a la instancia. Sin embargo, la desactivación de la clave afecta a todas las instancias de base de datos cifradas con esa clave. Para evitarlo, especifique una clave diferente durante la operación de copia de la instantánea.
Las instancias de base de datos con copias de seguridad desactivadas permanecen disponibles hasta que los volúmenes se separan del host durante una modificación de la instancia o una recuperación. RDS mueve las instancias al estado `inaccessible-encryption-credentials-recoverable` o al estado `inaccessible-encryption-credentials`, según corresponda.

Para obtener más información acerca de claves de KMS, consulte AWS KMS keys en la Guía para desarrolladores de AWS Key Management Service y Administración de AWS KMS key.

Cifrar una instancia de base de datos

Para cifrar una instancia de base de datos nueva, elija Habilitar el cifrado en la consola de Amazon RDS. Para obtener información sobre la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

Si utiliza el comando create-db-instance de la AWS CLI para crear una instancia de base de datos cifrada, establezca el parámetro `--storage-encrypted`. Si utiliza la operación CreateDBInstance de la API, establezca el parámetro `StorageEncrypted` en true.

Si utiliza el comando AWS CLI de la `create-db-instance` para crear una instancia de base de datos cifrada con una clave administrada por el cliente, establezca el parámetro `--kms-key-id` en cualquier identificador de clave para la clave de KMS. Si utiliza la operación `CreateDBInstance` de

la API de Amazon RDS, establezca el parámetro `KmsKeyId` en cualquier identificador de clave para la clave de KMS. Para utilizar una clave administrada por el cliente en una cuenta de AWS diferente, especifique el ARN de la clave o el ARN del alias.

Determinar si el cifrado está activado para una instancia de base de datos

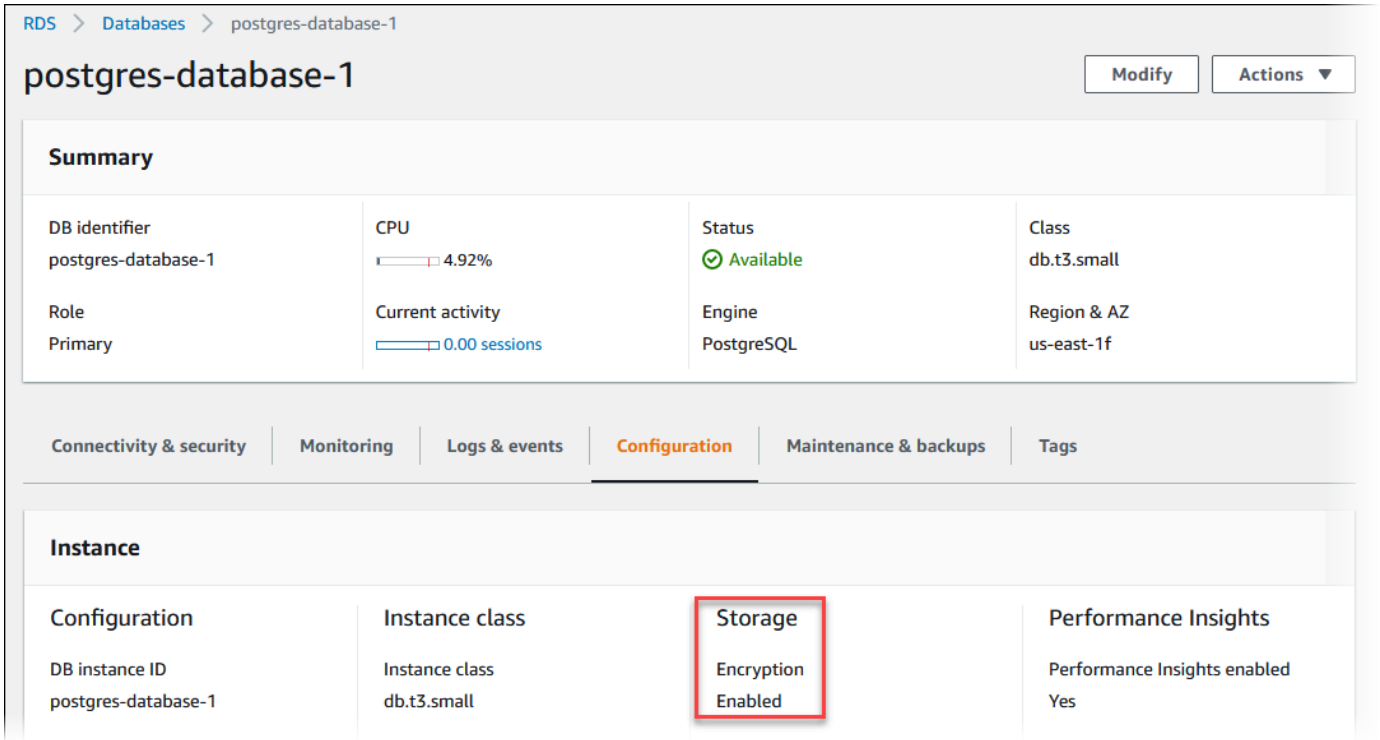
Puede utilizar la AWS Management Console, la AWS CLI o la API de RDS para determinar si el cifrado en reposo está activado para una instancia de base de datos.

Consola

Para determinar si el cifrado en reposo está activado para una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Bases de datos.
3. Elija el nombre de la instancia de base de datos que desea verificar para ver los detalles.
4. Elija la pestaña Configuración y verifique el valor Cifrado en Almacenamiento.

   Muestra Habilitado o No habilitado.



AWS CLI

Para determinar si el cifrado en reposo está activado para una instancia de base de datos mediante el AWS CLI, llame al comando describe-db-instances con la siguiente opción:

- `--db-instance-identifier`: el nombre de la instancia de base de datos.

En el siguiente ejemplo se utiliza una consulta para devolver ya sea `TRUE` o `FALSE` en relación con el cifrado en reposo de la instancia de base de datos `mydb`.

Example

```
aws rds describe-db-instances --db-instance-identifier mydb --query "*[].
{StorageEncrypted:StorageEncrypted}" --output text
```

API de RDS

Para determinar si el cifrado en reposo está activado para una instancia de base de datos mediante la API de Amazon RDS, llame a la operación DescribeDBInstances con el siguiente parámetro:

- `DBInstanceIdentifier`: el nombre de la instancia de base de datos.

Disponibilidad del cifrado de Amazon RDS

Actualmente, el cifrado de Amazon RDS; están disponibles para todos los motores de bases de datos y tipos de almacenamiento.

El cifrado de Amazon RDS está disponible para la mayoría de las clases de instancias de bases de datos. En la tabla siguiente se indican las clases de instancia de base de datos que no admiten el cifrado de Amazon RDS:

Tipo de instancia	Clase de instancia
Uso general (M1)	db.m1.small
	db.m1.medium
	db.m1.large
	db.m1.xlarge

Tipo de instancia	Clase de instancia
Optimizada para memoria (M2)	db.m2.xlarge db.m2.2xlarge db.m2.4xlarge
Ampliable (T2)	db.t2.micro

Cifrado en tránsito

Cifrado en la capa física

Todos los datos que fluyen en las Regiones de AWS a través de la red global de AWS se cifran automáticamente en la capa física antes de salir de las instalaciones seguras de AWS. Todo el tráfico entre las zonas de disponibiliad está cifrado. Las capas adicionales de cifrado, incluidas las que aparecen en esta sección, pueden proporcionar una protección adicional.

Cifrado proporcionado por el emparejamiento de Amazon VPC y el emparejamiento entre regiones de puerta de enlace de tránsito

Todo el tráfico entre regiones que utiliza la interconexión de Amazon VPC y puerta de enlace de tránsito se cifra de forma masiva automáticamente cuando sale de una región. De manera automática, se proporciona una capa adicional de cifrado en la capa física para todo el tráfico antes de dejar las instalaciones seguras de AWS.

Cifrado entre instancias

AWS proporciona conectividad privada y segura entre instancias de bases de datos de todo tipo. Además, en algunos tipos de instancia, se utilizan las capacidades de descarga del hardware Nitro System subyacente para cifrar de manera automática el tráfico en tránsito entre instancias. Este cifrado utiliza algoritmos de encriptación autenticada con datos asociados (AEAD), con cifrado de 256 bits. No hay impacto en el rendimiento de la red. Para admitir este cifrado adicional del tráfico en tránsito entre instancias, se deben cumplir los siguientes requisitos:

- Las instancias utilizan los siguientes tipos de instancias:
  - De uso general: M6i, M6id, M6in, M6idn, M7g
  - Optimizada para memoria: R6i, R6id, R6in, R6idn, R7g, X2idn, X2iedn, X2iezn
- Las instancias se encuentran en la misma Región de AWS.

- Las instancias están en la misma VPC o VPC interconectadas, y el tráfico no pasa a través de un dispositivo o servicio de red virtual, como un equilibrador de carga o una puerta de enlace de tránsito.

Limitaciones de las instancias de base de datos cifrados de Amazon RDS

Existen las siguientes limitaciones para las instancias de Amazon RDS con cifrado de bases de datos:

- Solo se puede cifrar una instancia de base de datos de Amazon RDS al crearla, no después de que se haya creado.

  Sin embargo, debido a que se puede cifrar una copia de una instantánea de base de datos sin cifrar, en la práctica es posible agregar el cifrado a una instancia de base de datos sin cifrar. Es decir, puede crear una instantánea de una instancia de base de datos y, a continuación, crear una copia cifrada de esa instantánea. A continuación, se puede restaurar una instancia de base de datos a partir de la instantánea cifrada y de este modo, se tiene una copia cifrada de la instancia de base de datos original. Para obtener más información, consulte Copia de una instantánea de base de datos para Amazon RDS.
- No puede desactivar el cifrado en una instancia de bases de datos cifrada.
- No puede crear una instantánea cifrada de una instancia de bases de datos sin cifrar.
- Una instantánea de una instancia de bases de datos cifrada debe cifrarse utilizando la misma clave de KMS que la instancia de bases de datos.
- No se puede tener una réplica de lectura cifrada de una instancia de base de datos sin cifrar ni una réplica de lectura sin cifrar de una instancia de base de datos cifrada.
- Las réplicas de lectura cifradas deben cifrarse con la misma clave de KMS que la instancia de base de datos de origen cuando ambas están en la misma región de AWS.
- No se puede restaurar una copia de seguridad ni una instantánea sin cifrar en una instancia de base de datos cifrada.
- Para copiar una instantánea cifrada de una región de AWS en otra, debe especificar la clave de KMS de la región de AWS de destino. Esto se debe a que las claves de KMS son específicas de la región de AWS en la que se crean.

  La instantánea de origen permanece cifrada durante todo el proceso de copia. Amazon RDS utiliza el cifrado de sobre para proteger los datos durante el proceso de copia. Para obtener más

información acerca del cifrado de sobre, consulte Cifrado de sobre en la guía para desarrolladores de AWS Key Management Service.

- No se puede descifrar una instancia de bases de datos cifrada. Sin embargo, puede exportar datos de una instancia de bases de datos cifrada e importar datos a una instancia de bases de datos sin cifrar.

Administración de AWS KMS key

Amazon RDS se integra automáticamente con AWS Key Management Service (AWS KMS) para la administración de claves. Amazon RDS utiliza el cifrado de sobre. Para obtener más información acerca del cifrado de sobre, consulte Cifrado de sobre en la Guía para desarrolladores de AWS Key Management Service.

Puede utilizar dos tipos de claves de AWS KMS para cifrar instancias de bases de datos.

- Si desea tener un control total sobre una clave de KMS, debe crear una clave administrada por el cliente. Para obtener más información acerca de las claves administradas por el cliente, consulte Claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service.
- Las Claves administradas por AWS son las claves de KMS de la cuenta que se crean, administran y utilizan en su nombre por un servicio de AWS integrado con AWS KMS. De forma predeterminada, se utiliza el RDS Clave administrada de AWS (`aws/rds`) para el cifrado. No puede administrar, rotar ni eliminar el RDS Clave administrada de AWS. Para obtener más información acerca de Claves administradas por AWS, consulte Claves administradas por AWS en la Guía para desarrolladores de AWS Key Management Service.

Para administrar las claves KMS usadas para instancias de bases de datos cifradas de Amazon RDS , use AWS Key Management Service (AWS KMS) en la consola de AWS KMS, la AWS CLI o la API de AWS KMS. Para ver los registros de auditoría de cada acción realizada con una clave administrada por AWS o por el cliente, utilice AWS CloudTrail. Para obtener más información sobre la rotación de claves, consulte Rotación de claves de AWS KMS.

Autorización del uso de una clave administrada por el cliente

Cuando RDS utiliza una clave administrada por el cliente en las operaciones criptográficas, actúa en nombre del usuario que está creando o modificando el recurso de RDS .

Para crear un recurso de RDS con una clave administrada por el cliente, un usuario debe tener permisos para llamar a las siguientes operaciones en la clave administrada por el cliente:

- `kms:CreateGrant`
- `kms:DescribeKey`

Puede especificar estos permisos necesarios en una política de claves o en una política de IAM si lo permite la política de claves.

> **Important**
>
> Cuando utiliza instrucciones de denegación explícitas para todos los recursos (*) en políticas de claves de AWS KMS con servicios administrados como Amazon RDS, debe especificar una condición para permitir que la cuenta propietaria del recurso acceda. Es posible que las operaciones produzcan un error sin esta condición, incluso si la regla de denegación incluye excepciones para el usuario de IAM.

> **Tip**
>
> Para seguir el principio de privilegios mínimos, no permita el acceso completo a `kms:CreateGrant`. En su lugar, use la clave de condición kms:ViaService para permitir al usuario crear concesiones en la clave de KMS solo cuando un servicio de AWS haya creado la concesión en nombre del usuario.

Puede hacer que la política de IAM sea más estricta de varias maneras. Por ejemplo, si desea permitir que la clave administrada por el cliente se utilice solo para solicitudes que se originen en RDS , utilice la clave de condición kms:ViaService con el valor `rds.<region>.amazonaws.com`. Además, puede utilizar las claves o valores de Contexto de cifrado de Amazon RDS como condición para utilizar la clave administrada por el cliente para el cifrado.

Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS en la Guía para desarrolladores de AWS Key Management Service y Políticas de claves en AWS KMS.

Contexto de cifrado de Amazon RDS

Cuando RDS utiliza la clave KMS o cuando Amazon EBS utiliza la clave KMS en nombre de RDS , el servicio especifica un contexto de cifrado. El contexto de cifrado es la información autenticada adicional (ADD) que AWS KMS usa para garantizar la integridad de los datos. Cuando se especifica un contexto de cifrado para una operación de cifrado, el servicio debe especificar el mismo contexto de cifrado para la operación de descifrado. De lo contrario, el descifrado produce un error. El contexto de cifrado también se escribe en los registros de AWS CloudTrail para ayudarle a entender por qué se usó una determinada clave KMS. Sus registros de CloudTrail pueden contener numerosas entradas que describen el uso de una clave KMS, pero el contexto de cifrado de cada entrada de registro puede ayudarle a determinar el motivo de ese uso concreto.

Como mínimo, Amazon RDS siempre utiliza el ID de instancia de base de datos para el contexto de cifrado, como en el siguiente ejemplo con formato JSON:

```
{ "aws:rds:db-id": "db-CQYSMDPBRZ7BPMH7Y3RTDG5QY" }
```

Este contexto de cifrado puede ayudarle a identificar la instancia de base de datos para el que se ha utilizado la clave KMS.

Cuando la clave de KMS se usa para una instancia de base de datos y un volumen de Amazon EBS específico, el ID de instancia de base de datos y el ID de volumen de Amazon EBS se usan para el contexto de cifrado, como en el siguiente ejemplo con formato JSON:

```
{
  "aws:rds:db-id": "db-BRG7VYS3SVIFQW7234EJQOM5RQ",
  "aws:ebs:id": "vol-ad8c6542"
}
```

Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos

Puede utilizar la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) desde su aplicación para cifrar una conexión a una base de datos que ejecute Db2, MariaDB, Microsoft SQL Server, MySQL, Oracle o PostgreSQL.

Las conexiones SSL y TLS proporcionan una capa de seguridad al cifrar los datos que circulan entre el cliente y la instancia o clúster de base de datos. Si lo desea, su conexión SSL/TLS puede realizar una verificación de identidad del servidor validando el certificado del servidor instalado en su base de datos. Para solicitar la verificación de la identidad del servidor, siga este proceso general:

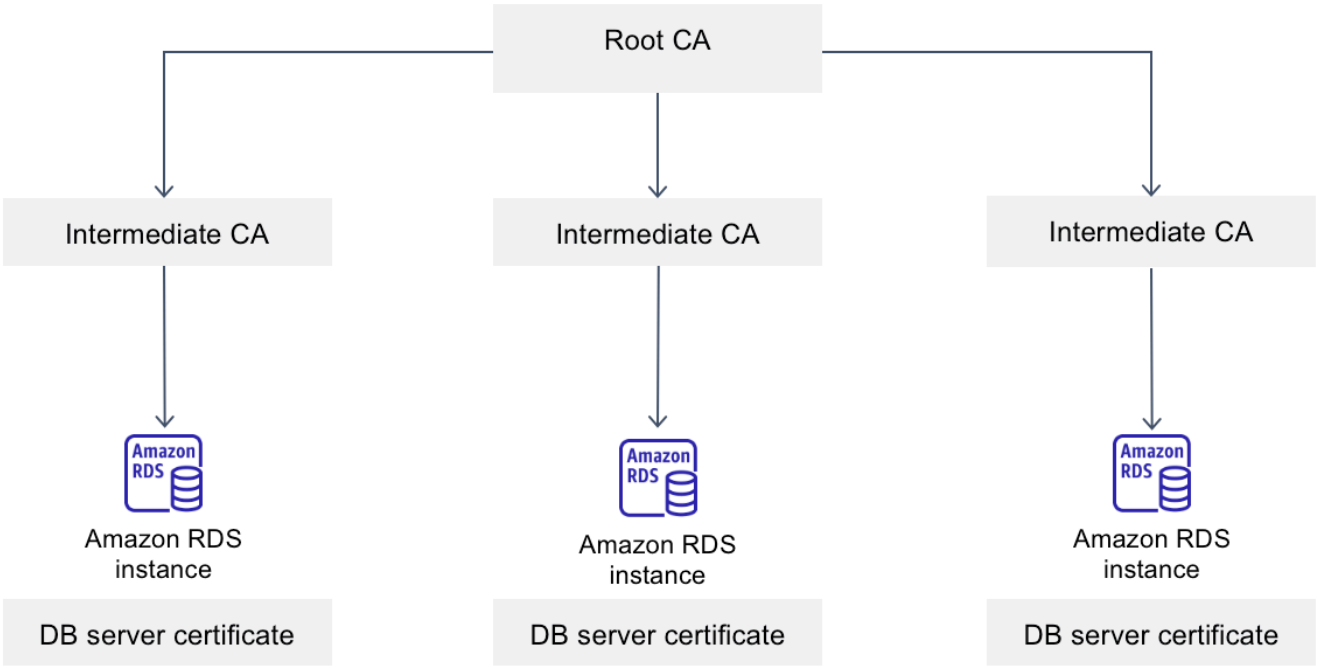
1. Elija la entidad de certificación (CA) que firma el certificado del servidor de base de datos, para su base de datos. Para obtener más información sobre las entidades de certificación, consulte Entidades de certificación.
2. Descargue un paquete de certificados para usarlo cuando se conecte a la base de datos. Para descargar una agrupación de certificados, consulte Agrupaciones de certificados por Región de AWS.

   > **Note**
   >
   > Todos los certificados están disponibles solo para descarga con conexiones SSL/TLS.

3. Conéctese a la base de datos mediante el proceso del motor de base de datos para la implementación de las conexiones SSL/TLS. Cada motor base de datos tiene su propio proceso para implementar SSL/TLS. Para obtener información sobre cómo implementar SSL/TLS para su base de datos, siga el enlace que corresponda a su motor de base de datos:
   - Uso de SSL con una instancia de base de datos de Amazon RDS para Db2
   - Compatibilidad con SSL/TLS para instancias de base de datos de MariaDB en Amazon RDS
   - ???
   - Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS
   - Uso de SSL con una instancia de base de datos de RDS para Oracle
   - Uso de SSL con una instancia de base de datos PostgreSQL

Entidades de certificación

La entidad de certificación (CA) es el certificado que identifica la CA raíz en la parte superior de la cadena de certificados. La CA firma el certificado del servidor de base de datos, que está instalado en cada instancia de base de datos. El certificado del servidor de base de datos identifica la instancia de base de datos como un servidor de confianza.



Amazon RDS proporciona las siguientes CA para firmar el certificado del servidor de base de datos de una base de datos.

Entidad de certificación (CA)	Descripción	Nombre común (NC)
rds-ca-2019	Utiliza una entidad de certificación con el algoritmo de clave privada RSA 2048 y el algoritmo de firma SHA256. Esta CA vence en 2024 y no admite la rotación automática de certificados de servidor. Si utiliza esta CA y desea mantener el mismo estándar, le recomendamos que cambie a la CA rds-ca-rsa2048-g1.	Amazon RDS *region-id entifier* CA 2.019
rds-ca-rsa2048-g1	Utiliza una entidad de certificación con el algoritmo de clave privada RSA 2048 y el algoritmo de firma SHA256 en la mayoría de las Regiones de AWS.	Amazon RDS *region-id entifier* RSA2048 G1

Entidad de certificación (CA)	Descripción	Nombre común (NC)
	En las AWS GovCloud (US) Regions, este certificado utiliza una entidad de certificación con el algoritmo de clave privada RSA 2048 y el algoritmo de firma SHA384. Esta CA sigue siendo válida durante más tiempo que la CA rds-ca-2019. Esta CA admite la rotación automática de certificados de servidor.	
rds-ca-rsa4096-g1	Utiliza una entidad de certificación con el algoritmo de clave privada RSA 4096 y el algoritmo de firma SHA384. Esta CA admite la rotación automática de certificados de servidor.	Amazon RDS *region-identifier* RSA4096 G1
rds-ca-ecc384-g1	Utiliza una entidad de certificación con el algoritmo de clave privada ECC 384 y el algoritmo de firma SHA384. Esta CA admite la rotación automática de certificados de servidor.	Amazon RDS *region-identifier* ECC384 G1

> **Note**
>
> Si utiliza la AWS CLI, puede ver la validez de las entidades de certificación enumeradas anteriormente mediante describe-certificates.

Estos certificados de CA se incluyen en el paquete de certificados regionales y globales. Al utilizar la CA rds-ca-rsa2048-g1, rds-ca-rsa4096-g1 o rds-ca-ecc384-g1 con una instancia de base de datos, RDS administra el certificado del servidor de base de datos en la base de datos. RDS rota el certificado del servidor de base de datos de forma automática antes de que caduque.

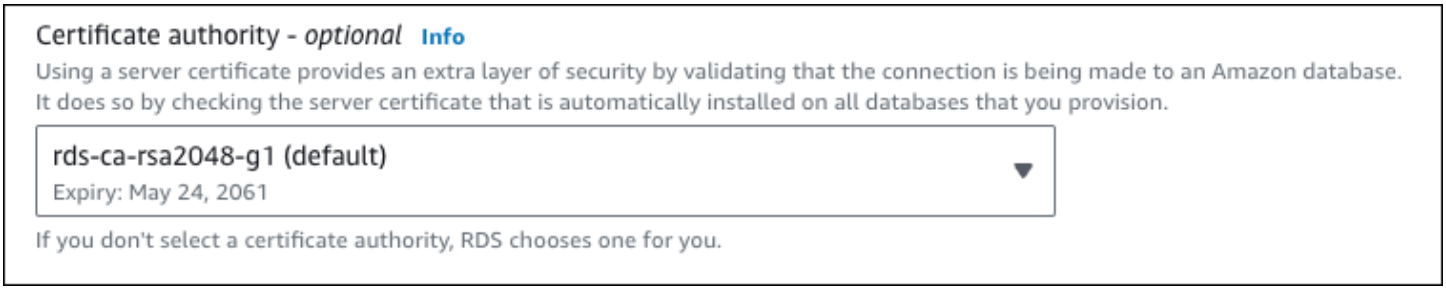
Configuración de la CA para su base de datos

Puede definir la CA para una base de datos con las tareas siguientes:

- Crear una instancia de base de datos o un clúster de base de datos multi-AZ: puede definir la CA al crear una instancia o un clúster de base de datos. Para obtener instrucciones, consulte the section called “Creación de una instancia de base de datos” o the section called “Creación de un clúster de base de datos Multi-AZ”.
- Modificar una instancia de base de datos o un clúster de base de datos multi-AZ: puede configurar la CA de una instancia o un clúster de base de datos modificándola. Para obtener instrucciones, consulte the section called “Modificación de una instancia de base de datos” o the section called “Modificación de un clúster de base de datos Multi-AZ”.

> **Note**
>
> La CA predeterminada está establecida en rds-ca-rsa2048-g1. Puede anular la CA predeterminada para su Cuenta de AWS mediante el comando modify-certificates.

Las CA disponibles dependen del motor de base de datos y de la versión del motor de base de datos. Al utilizar la AWS Management Console, puede elegir la CA mediante la configuración de la Entidad de certificación, tal como se muestra en la siguiente imagen.



La consola solo muestra las CA que están disponibles para le motor de base de datos y la versión del motor de base de datos. Si utiliza la AWS CLI, puede configurar la CA para una instancia de base de datos mediante los comandos create-db-instance o modify-db-instance. Puede configurar la CA para un clúster de base de datos multi-AZ mediante el comando create-db-clúster o modify-db-clúster.

Si utiliza la AWS CLI, puede ver las CA disponibles para su cuenta mediante el comando describe-certificates. Este comando también muestra la fecha de caducidad de cada CA en `ValidTill` en la

salida. Puede buscar las CA que están disponibles para un motor de base de datos y una versión de motor de base de datos específicos mediante el comando describe-db-engine-versions.

El siguiente ejemplo muestra las CA disponibles para la versión predeterminada del motor de base de datos de RDS para PostgreSQL.

```
aws rds describe-db-engine-versions --default-only --engine postgres
```

Su resultado es similar al siguiente. Las CA disponibles se enumeran en `SupportedCACertificateIdentifiers`. El resultado también muestra si la versión del motor de base de datos admite la rotación del certificado sin reiniciarlo en `SupportsCertificateRotationWithoutRestart`.

```
{
    "DBEngineVersions": [
        {
            "Engine": "postgres",
            "MajorEngineVersion": "13",
            "EngineVersion": "13.4",
            "DBParameterGroupFamily": "postgres13",
            "DBEngineDescription": "PostgreSQL",
            "DBEngineVersionDescription": "PostgreSQL 13.4-R1",
            "ValidUpgradeTarget": [],
            "SupportsLogExportsToCloudwatchLogs": false,
            "SupportsReadReplica": true,
            "SupportedFeatureNames": [
                "Lambda"
            ],
            "Status": "available",
            "SupportsParallelQuery": false,
            "SupportsGlobalDatabases": false,
            "SupportsBabelfish": false,
            "SupportsCertificateRotationWithoutRestart": true,
            "SupportedCACertificateIdentifiers": [
                "rds-ca-2019",
                "rds-ca-rsa2048-g1",
                "rds-ca-ecc384-g1",
                "rds-ca-rsa4096-g1"
            ]
        }
    ]
}
```

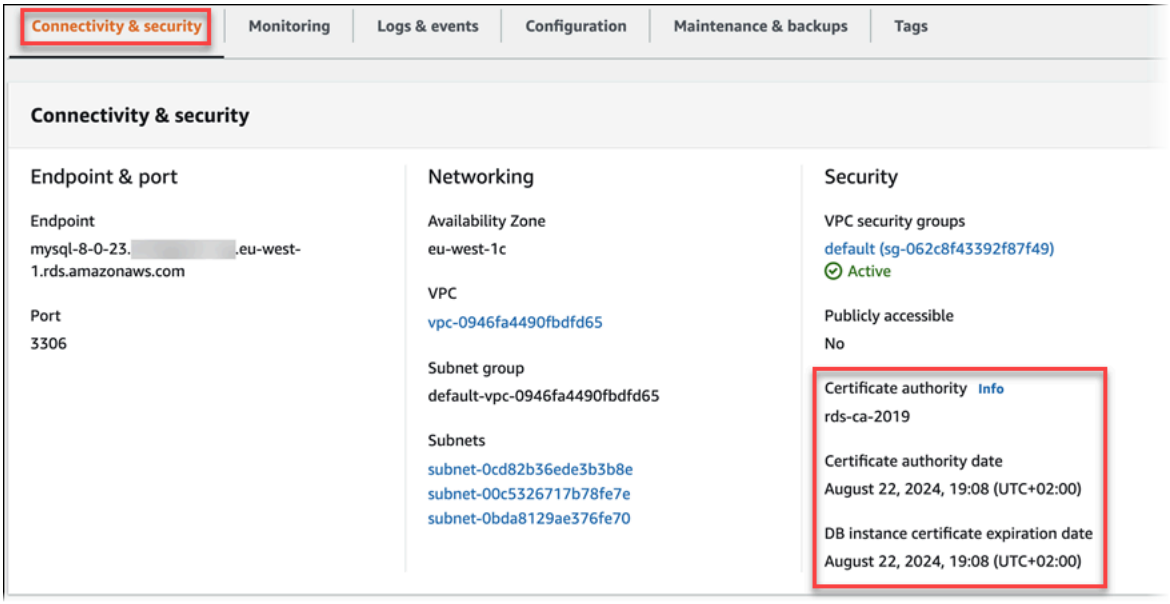
Validez del certificado del servidor de base de datos

La validez del certificado del servidor de base de datos depende del motor de base de datos y de la versión del motor de base de datos. Si la versión del motor de base de datos admite la rotación de certificados sin reinicio, el certificado del servidor de base de datos tiene una validez de 1 año. De no ser así, la validez es de 3 años.

Para obtener más información acerca de la rotación de certificados del servidor de base de datos, consulte Rotación automática de certificados del servidor.

Visualización de la CA de su instancia de base de datos

Puede ver los detalles sobre la CA de una base de datos en la pestaña Conectividad y seguridad de la consola, como se muestra en la siguiente imagen.



Si utiliza la AWS CLI, puede ver los detalles de la CA de una instancia de base de datos mediante el comando describe-db-instances. Puede ver los detalles sobre la CA de un clúster de base de datos multi-AZ mediante el comando describe-db-clústers.

Descarga de agrupaciones de certificados para Amazon RDS

Cuando se conecta a la base de datos con SSL o TLS, la instancia de base de datos requiere un certificado de confianza de Amazon RDS. Seleccione el enlace correspondiente en la siguiente tabla para descargar la agrupación correspondiente a la Región de AWS donde se aloja la base de datos.

Agrupaciones de certificados por Región de AWS

Las agrupaciones de certificados para todas las Regiones de AWS y para regiones de GovCloud (EE. UU.) contienen los siguientes certificados:

- Certificados raíz e intermedios `rds-ca-2019`.
- Certificados CA raíz `rds-ca-rsa2048-g1`, `rds-ca-rsa4096-g1` y `rds-ca-ecc384-g1`. El almacén de confianza de la aplicación solo necesita registrar el certificado CA de raíz.

> **Note**
>
> El proxy de Amazon RDS usa certificados de AWS Certificate Manager (ACM). Si está utilizando RDS Proxy, no es necesario descargar certificados de Amazon RDS ni actualizar aplicaciones que usen conexiones RDS Proxy. Para obtener más información, consulte Uso de TLS/SSL con RDS Proxy.

Para descargar una agrupación de certificados de una Región de AWS, seleccione el enlace de la Región de AWS en la que se aloja la base de datos en la tabla siguiente.

Región de AWS	Paquete de certificados (PEM)	Paquete de certificados (PKCS7)
Cualquier Región de AWS comercial	global-bundle.pem	global-bundle.p7b
EE.UU. Este (Norte de Virginia)	us-east-1-bundle.pem	us-east-1-bundle.p7b
US East (Ohio)	us-east-2-bundle.pem	us-east-2-bundle.p7b
EE.UU. Oeste (Norte de California)	us-west-1-bundle.pem	us-west-1-bundle.p7b
EE.UU. Oeste (Oregón)	us-west-2-bundle.pem	us-west-2-bundle.p7b
Africa (Cape Town)	af-south-1-bundle.pem	af-south-1-bundle.p7b

Región de AWS	Paquete de certificados (PEM)	Paquete de certificados (PKCS7)
Asia Pacific (Hong Kong)	ap-east-1-bundle.pem	ap-east-1-bundle.p7b
Asia-Pacífico (Hyderabad)	ap-south-2-bundle.pem	ap-south-2-bundle.p7b
Asia-Pacífico (Yakarta)	ap-southeast-3-bundle.pem	ap-southeast-3-bundle.p7b
Asia-Pacífico (Melbourne)	ap-southeast-4-bundle.pem	ap-southeast-4-bundle.p7b
Asia Pacific (Bombay)	ap-south-1-bundle.pem	ap-south-1-bundle.p7b
Asia Pacific (Osaka)	ap-northeast-3-bundle.pem	ap-northeast-3-bundle.p7b
Asia Pacífico (Tokio)	ap-northeast-1-bundle.pem	ap-northeast-1-bundle.p7b
Asia Pacific (Seoul)	ap-northeast-2-bundle.pem	ap-northeast-2-bundle.p7b
Asia Pacífico (Singapur)	ap-southeast-1-bundle.pem	ap-southeast-1-bundle.p7b
Asia Pacífico (Sídney)	ap-southeast-2-bundle.pem	ap-southeast-2-bundle.p7b
Canada (Central)	ca-central-1-bundle.pem	ca-central-1-bundle.p7b
Oeste de Canadá (Calgary)	ca-west-1-bundle.pem	ca-west-1-bundle.p7b
Europa (Fráncfort)	eu-central-1-bundle.pem	eu-central-1-bundle.p7b
Europe (Irlanda)	eu-west-1-bundle.pem	eu-west-1-bundle.p7b
Europe (Londres)	eu-west-2-bundle.pem	eu-west-2-bundle.p7b
Europe (Milan)	eu-south-1-bundle.pem	eu-south-1-bundle.p7b
Europe (Paris)	eu-west-3-bundle.pem	eu-west-3-bundle.p7b
Europa (España)	eu-south-2-bundle.pem	eu-south-2-bundle.p7b
Europa (Estocolmo)	eu-north-1-bundle.pem	eu-north-1-bundle.p7b
Europa (Zúrich)	eu-central-2-bundle.pem	eu-central-2-bundle.p7b

Región de AWS	Paquete de certificados (PEM)	Paquete de certificados (PKCS7)
Israel (Tel Aviv)	il-central-1-bundle.pem	il-central-1-bundle.p7b
Medio Oriente (Baréin)	me-south-1-bundle.pem	me-south-1-bundle.p7b
Medio Oriente (EAU)	me-central-1-bundle.pem	me-central-1-bundle.p7b
América del Sur (São Paulo)	sa-east-1-bundle.pem	sa-east-1-bundle.p7b
Cualquier AWS GovCloud (US) Region	global-bundle.pem	global-bundle.p7b
AWS GovCloud (EE. UU. Este)	us-gov-east-1-bundle.pem	us-gov-east-1-bundle.p7b
AWS GovCloud (EE. UU. Oeste)	us-gov-west-1-bundle.pem	us-gov-west-1-bundle.p7b

Visualización del contenido de su certificado de CA

Para comprobar el contenido del paquete de certificados de la CA, utilice el siguiente comando:

```
keytool -printcert -v -file global-bundle.pem
```

Rotar certificados SSL/TLS

Los certificados rds-ca-2019 de la entidad de certificación de Amazon RDS caducaron en agosto de 2024. Si usa o planea usar la capa de conexión segura (SSL) o la seguridad de la capa de transporte (TLS) con la verificación de certificados para conectarse a las instancias de base de datos de RDS o clústeres de base de datos Multi-AZ, considere la posibilidad de utilizar uno de los nuevos certificados de entidad de certificación rds-ca-rsa2048-g1, rds-ca-rsa4096-g1 o rds-ca-ecc384-g1. Si actualmente no utiliza SSL/TLS con verificación de certificados, es posible que aún tenga un certificado de CA caducado y que deba actualizarlo con un certificado de CA nuevo si tiene previsto utilizar SSL/TLS con verificación de certificados para conectarse a sus bases de datos de RDS.

Amazon RDS proporciona nuevos certificados de entidad de certificación como una práctica recomendada de seguridad de AWS. Para obtener información sobre los nuevos certificados y las

regiones de AWS compatibles, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

Para actualizar el certificado de CA de la base de datos, utilice los métodos siguientes:

- Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos
- Actualización del certificado de entidad de certificación mediante la aplicación de mantenimiento

Antes de actualizar sus instancias de base de datos o clústeres de base de datos multi-AZ para usar el nuevo certificado de CA, asegúrese de actualizar sus clientes o aplicaciones que se conectan a sus bases de datos de RDS.

Consideraciones sobre la rotación de certificados

Tenga en cuenta las siguientes situaciones antes de rotar el certificado:

- Amazon RDS Proxy usa certificados de AWS Certificate Manager (ACM). Si utiliza RDS Proxy, al rotar el certificado SSL/TLS, no es necesario que actualice las aplicaciones que utilizan las conexiones de RDS Proxy. Para obtener más información, consulte Uso de TLS/SSL con RDS Proxy.
- Si utiliza la versión 1.15 de una aplicación Go con una instancia de base de datos o clúster de base de datos multi-AZ que se haya creado o actualizado con el certificado rds-ca-2019 antes del 28 de julio de 2020, debe actualizar el certificado de nuevo. Actualice el certificado a rds-ca-rsa2048-g1, rds-ca-rsa4096-g1 o rds-ca-ecc384-g1 en función de su motor .

  Utilice el comando `modify-db-instance` para una instancia de base de datos o el comando `modify-db-cluster` para un clúster de base de datos multi-AZ con el nuevo identificador de certificado de CA. Puede buscar las CA que están disponibles para un motor de base de datos y una versión de motor de base de datos específicos mediante el comando `describe-db-engine-versions`.

  Si creó su base de datos o actualizó su certificado después del 28 de julio de 2020, no se requiere ninguna acción. Para obtener más información, consulte Go GitHub issue #39568.

Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos

En el siguiente ejemplo, se actualiza el certificado de la entidad de certificación de rds-ca-2019 a rds-ca-rsa2048-g1. Puede elegir un certificado diferente. Para obtener más información, consulte Entidades de certificación.

Actualice el almacén de confianza de aplicaciones para reducir el tiempo de inactividad asociado a la actualización del certificado de CA. Para obtener más información acerca de los reinicios asociados a la rotación de certificados de la entidad de certificación, consulte Rotación automática de certificados del servidor.

Actualización del certificado de entidad de certificación modificando la instancia o el clúster de base de datos

1. Descargue el nuevo certificado SSL/TLS como se describe en Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
2. Actualice las aplicaciones para que usen el nuevo certificado SSL/TLS.

   Los métodos para actualizar aplicaciones para nuevos certificados SSL/TLS dependen de sus aplicaciones específicas. Trabaje con sus desarrolladores de aplicaciones para actualizar los certificados SSL/TLS para sus aplicaciones.

   Para obtener información sobre la comprobación de conexiones SSL/TLS y la actualización de cada motor de base de datos, consulte los siguientes temas:

   - Actualización de aplicaciones para la conexión a las instancias de MariaDB con los nuevos certificados SSL/TLS
   - Actualización de aplicaciones para la conexión a las instancias de base de datos de Microsoft SQL Server con los nuevos certificados SSL/TLS
   - Actualización de aplicaciones para la conexión a las instancias de base de datos de MySQL con los nuevos certificados SSL/TLS
   - Actualización de aplicaciones para la conexión a las instancias de base de datos de Oracle con los nuevos certificados SSL/TLS
   - Actualización de aplicaciones para la conexión a las instancias de base de datos de PostgreSQL con los nuevos certificados SSL/TLS

Para obtener el mismo script que actualice un almacén de confianza para un sistema operativo Linux, consulte Script de muestra para la importación de certificados en su almacén de confianza.

> **Note**
>
> El paquete de certificados contiene certificados tanto para la CA antigua como para la nueva, por lo que puede actualizar su aplicación de forma segura y mantener la conectividad durante el período de transición. Si utiliza AWS Database Migration Service para migrar una base de datos a una instancia o clúster de base de datos, recomendamos utilizar el paquete de certificados para garantizar la conectividad durante la migración.

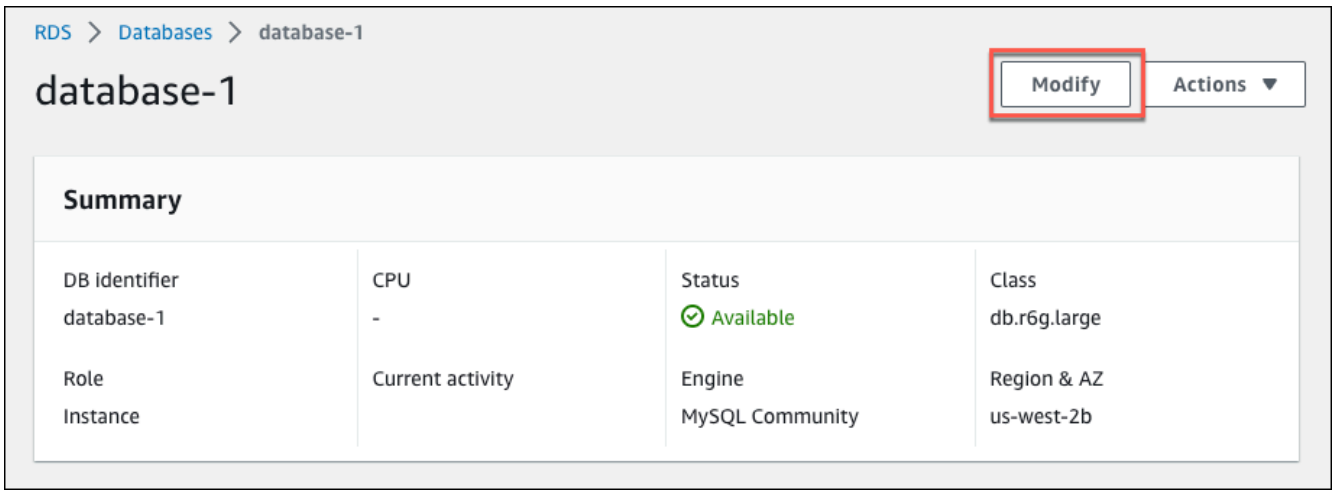
3. Modifique la instancia de base de datos o el clúster de base de datos multi-AZ para cambiar la CA de rds-ca-2019 a rds-ca-rsa2048-g1. Para comprobar si la base de datos requiere un reinicio para actualizar los certificados de CA, utilice el comando describe-db-engine-versions y compruebe el indicador `SupportsCertificateRotationWithoutRestart`.

> **Important**
>
> Si tiene problemas de conectividad después de que el certificado caduque, utilice la opción de aplicación inmediata. Seleccione Apply immediately (Aplicar inmediatamente) en la consola o especifique la opción `--apply-immediately` con la AWS CLI. De manera predeterminada, esta operación está programada para ejecutarse durante su próximo periodo de mantenimiento.
>
> En el caso de las instancias de bases de datos de RDS para Oracle, le recomendamos que reinicie la base de datos de Oracle para evitar errores de conexión.
>
> Para las instancias Multi-AZ de RDS para SQL Server con las opciones AlwaysOn o Mirroring habilitadas, se espera una conmutación por error cuando la instancia se reinicie tras la rotación de certificados.
>
> Para establecer una invalidación para la entidad de certificación de la instancia que sea diferente de la entidad de certificación de RDS predeterminada, utilice el comando de la CLI modify-certificates.

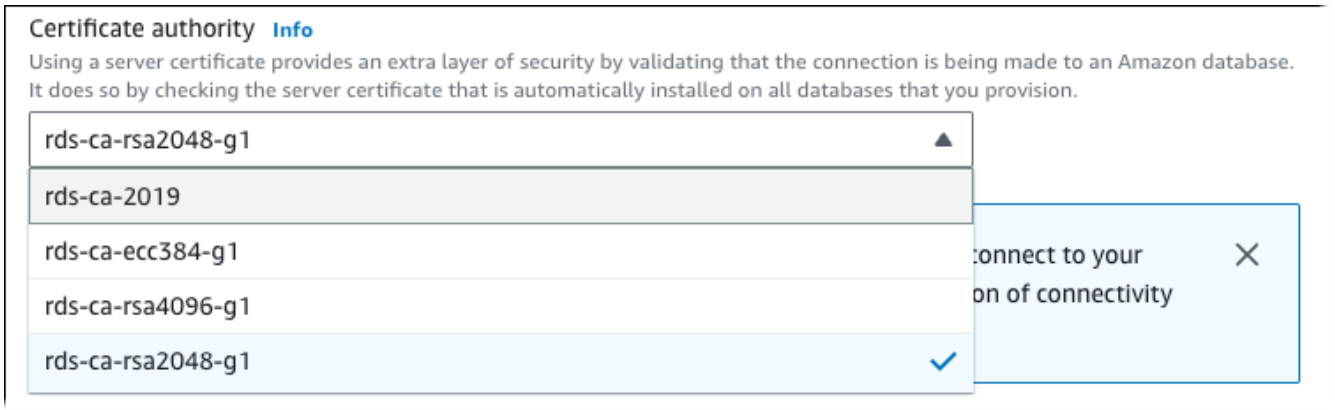
Puede utilizar la AWS Management Console o la AWS CLI para cambiar el certificado de CA de rds-ca-2019 a rds-ca-rsa2048-g1 para una instancia de base de datos o un clúster de base de datos multi-AZ.

Console

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Bases de datos y, a continuación, elija la instancia de base de datos o el clúster de base de datos multi-AZ que desea modificar.
3. Elija Modificar.



4. En la sección Conectividad, elija rds-ca-rsa2048-g1.



5. Elija Continue y consulte el resumen de las modificaciones.
6. Para aplicar los cambios inmediatamente, elija Apply immediately.
7. En la página de confirmación, revise los cambios. Si son correctos, elija Modificar la instancia de base de datos o Modificar el clúster para guardar los cambios.

> **Important**
>
> Cuando programe esta operación, asegúrese de haber actualizado de antemano su tienda de confianza del lado del cliente.

O bien, elija Back (Atrás) para editar los cambios o Cancel (Cancelar) para cancelarlos.

AWS CLI

Para utilizar la AWS CLI para cambiar la CA de rds-ca-2019 a rds-ca-rsa2048-g1 para una instancia de base de datos o un clúster de base de datos multi-AZ, llame al comando modify-db-instance o modify-db-clúster. Especifique el identificador de instancia o clúster de base de datos y la opción `--ca-certificate-identifier`.

Utilice el parámetro `--apply-immediately` para aplicar la actualización inmediatamente. De manera predeterminada, esta operación está programada para ejecutarse durante su próximo periodo de mantenimiento.

> **Important**
>
> Cuando programe esta operación, asegúrese de haber actualizado de antemano su tienda de confianza del lado del cliente.

Example

instancia de base de datos

En el siguiente ejemplo, se modifica `mydbinstance` al establecer el certificado de CA en `rds-ca-rsa2048-g1`.

Para Linux, macOS o:Unix

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --ca-certificate-identifier rds-ca-rsa2048-g1
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --ca-certificate-identifier rds-ca-rsa2048-g1
```

> **Note**
>
> Si su instancia requiere reinicio, puede utilizar el comando de la CLI modify-db-instance y especificar la opción `--no-certificate-rotation-restart`.

Example

Clúster de base de datos multi-AZ

En el siguiente ejemplo, se modifica `mydbcluster` al establecer el certificado de CA en `rds-ca-rsa2048-g1`.

Para Linux, macOS o:Unix

```
aws rds modify-db-cluster \
    --db-cluster-identifier mydbcluster \
    --ca-certificate-identifier rds-ca-rsa2048-g1
```

En:Windows

```
aws rds modify-db-cluster ^
    --db-cluster-identifier mydbcluster ^
    --ca-certificate-identifier rds-ca-rsa2048-g1
```

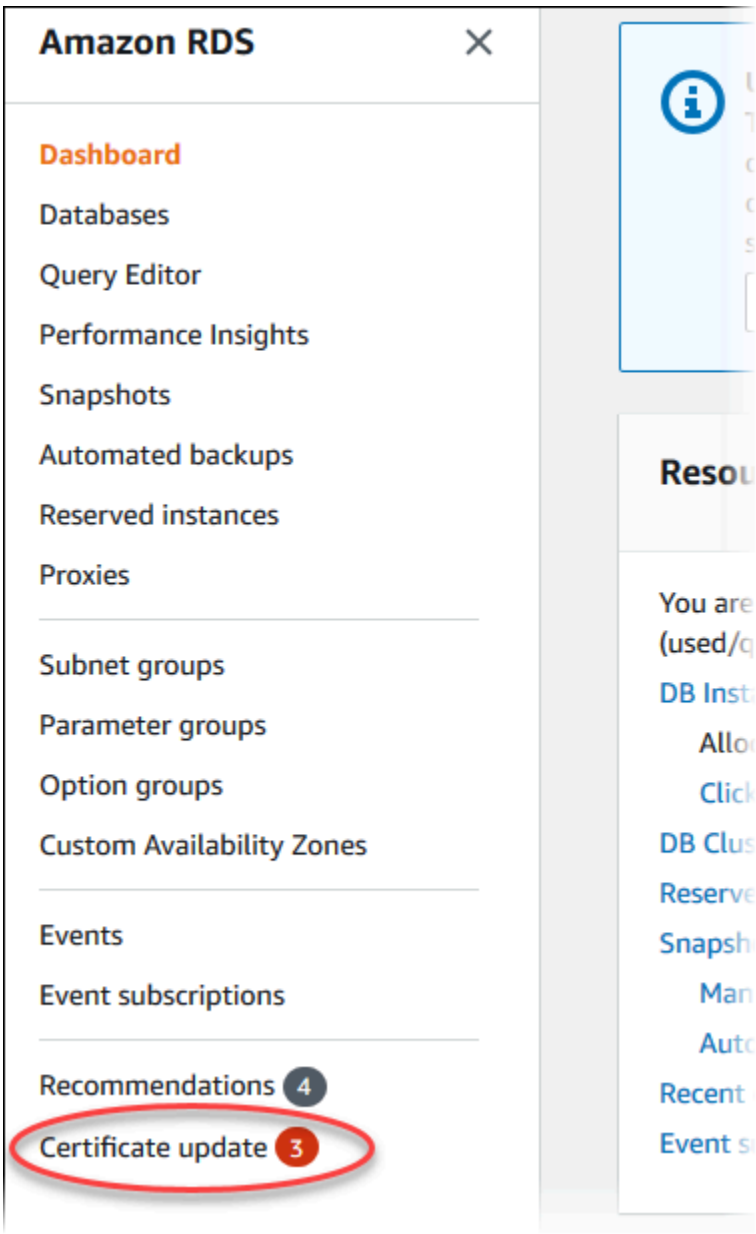
Actualización del certificado de entidad de certificación mediante la aplicación de mantenimiento

Realice los siguientes pasos para actualizar el certificado de CA aplicando el mantenimiento.

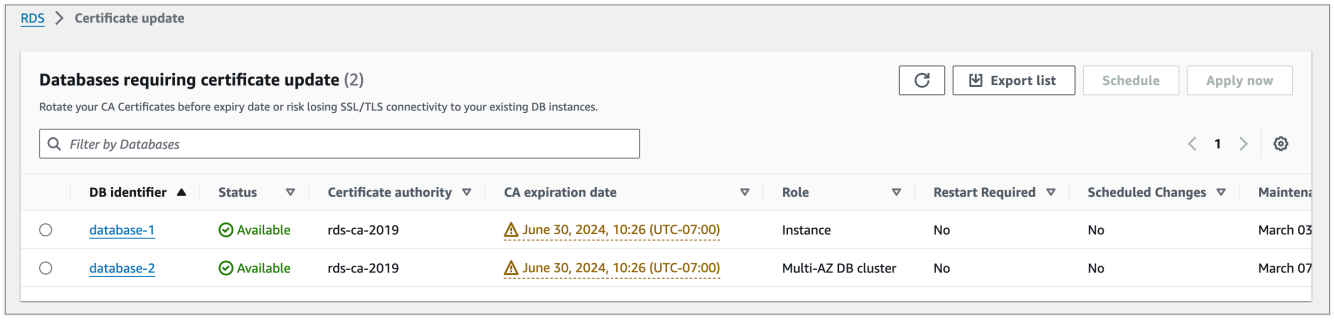
Console

Actualización del certificado de CA aplicando el mantenimiento

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Actualización del certificado.



Se muestra la página Bases de datos que requieren actualización de certificados.



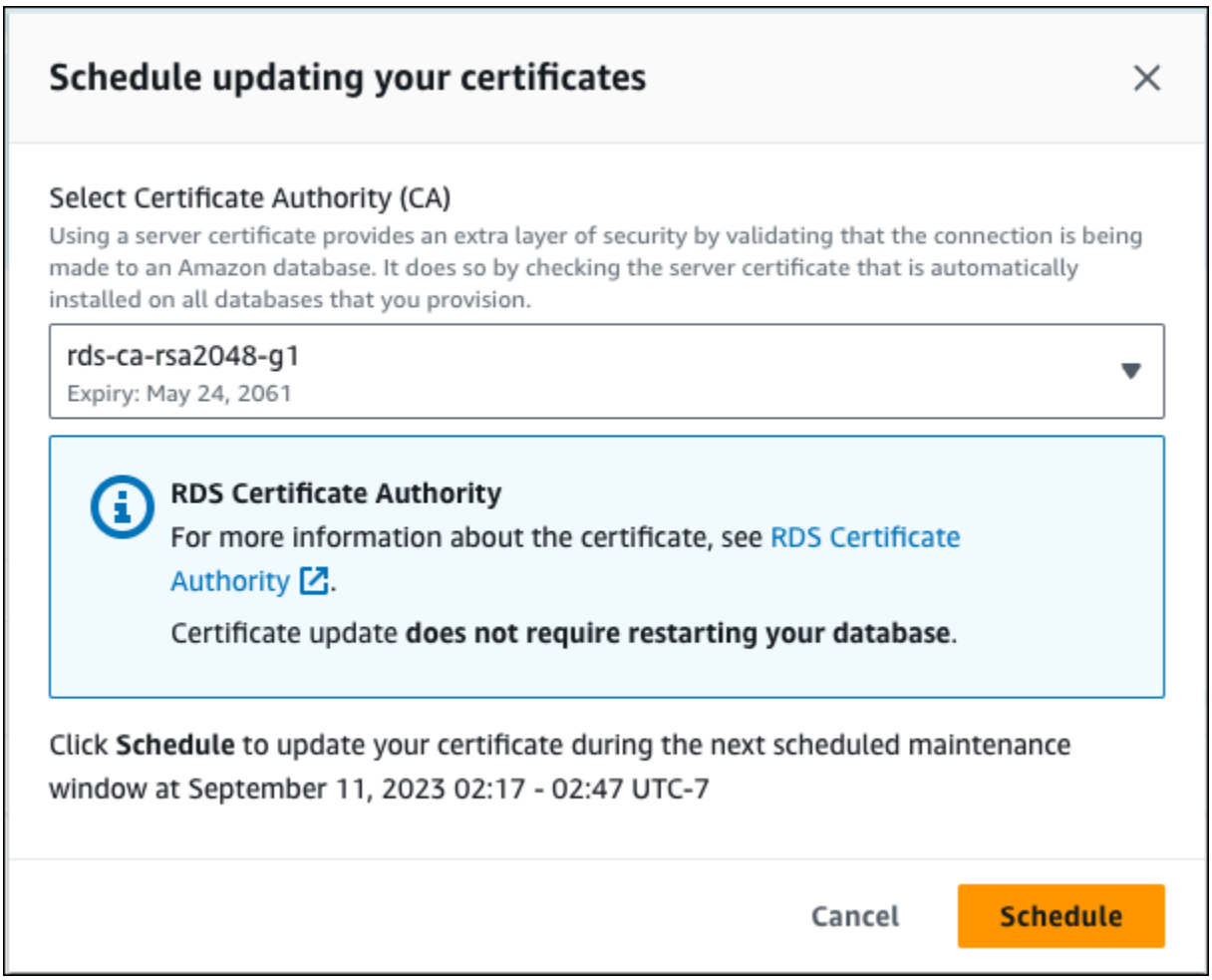
> **Note**
>
> Esta página solo muestra las instancias y clústeres de base de datos de la Región de AWS actual. Si tiene instancias de base de datos en más de una Región de AWS, consulte esta página en cada Región de AWS para ver todas las instancias de base de datos con certificados SSL/TLS antiguos.

3. Elija la instancia de base de datos o el clúster de base de datos multi-AZ que desea actualizar.

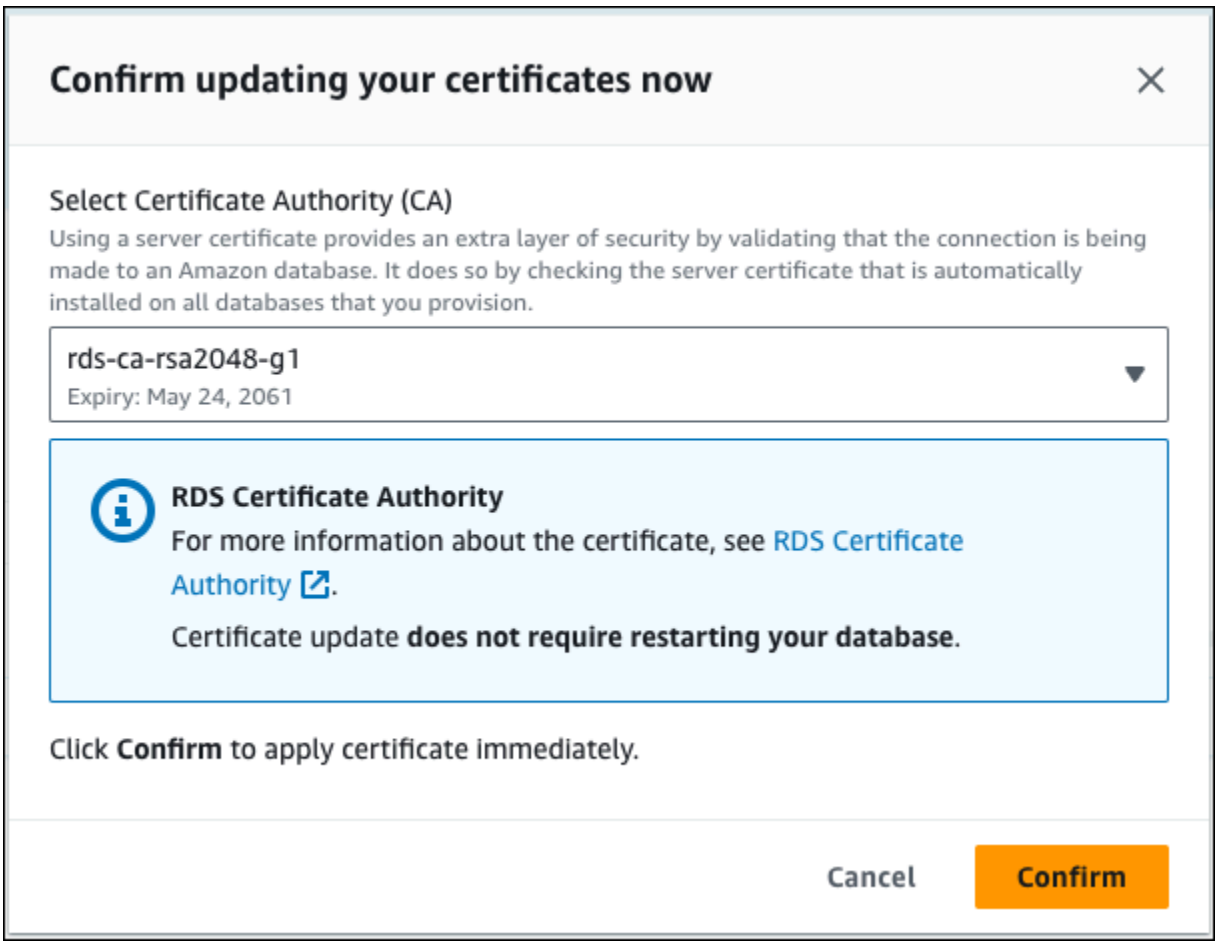
   Elija Programación para programar la rotación de certificados para la siguiente ventana de mantenimiento. Para aplicar la rotación inmediatamente, elija Aplicar ahora.

   > **Important**
   >
   > Si tiene problemas de conectividad después de que el certificado caduque, utilice la opción Aplicar ahora.

4. a. Si elige Programación, se le solicitará que confirme la rotación del certificado de CA. Este mensaje también indica el período programado para la actualización.



b. Si elige Aplicar ahora, se le solicita que confirme la rotación del certificado de CA.



> **Important**
>
> Antes de programar la rotación de certificados de CA en la base de datos, actualice las aplicaciones cliente que utilicen SSL/TLS y el certificado de servidor para conectarse. Estas actualizaciones son específicas de su motor de base de datos. Después de actualizar estas aplicaciones cliente, puede confirmar la rotación del certificado de CA.

Para continuar, seleccione la casilla de verificación y, a continuación, seleccione Confirm (Confirmar).

5. Repita los pasos 3 y 4 para cada instancia y clúster de base de datos que desee actualizar.

Rotación automática de certificados del servidor

Si su CA raíz admite la rotación automática de certificados del servidor, RDS administra automáticamente la rotación del certificado del servidor de base de datos. RDS utiliza la misma CA raíz para esta rotación automática, por lo que no es necesario descargar un nuevo paquete de CA. Consulte Entidades de certificación.

La rotación y la validez del certificado del servidor de base de datos dependen del motor de base de datos:

- Si su motor de base de datos admite la rotación sin reinicio, RDS rota automáticamente el certificado del servidor de base de datos sin que usted tenga que realizar ninguna acción. RDS intenta rotar el certificado del servidor de base de datos en el período de mantenimiento que prefiera a la mitad de la vida del certificado del servidor de base de datos. El nuevo certificado del servidor de base de datos es válido durante 12 meses.
- Si su motor de base de datos no admite la rotación sin reinicio, RDS le notificará un evento de mantenimiento al menos 6 meses antes de que caduque el certificado del servidor de base de datos. El nuevo certificado del servidor de base de datos es válido durante 36 meses.

Utilice el comando describe-db-engine-versions e inspeccione el indicador `SupportsCertificateRotationWithoutRestart` para identificar si la versión del motor de base de datos admite la rotación del certificado sin reinicio. Para obtener más información, consulte Configuración de la CA para su base de datos.

Script de muestra para la importación de certificados en su almacén de confianza

A continuación se muestran scripts de shell de ejemplo que importan el paquete de certificados a un almacén de confianza.

Cada script de shell de muestra utiliza keytool, que forma parte del kit de desarrollo de Java (JDK). Para obtener información sobre la instalación de JDK, consulte la Guía de instalación de JDK.

Linux

A continuación se muestra un ejemplo de script de intérprete de comandos que importa el paquete de certificados a un almacén de confianza en un sistema operativo Linux.

```
mydir=tmp/certs
```

```
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi truststore=${mydir}/rds-truststore.jks storepassword=changeit

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem">
 ${mydir}/global-bundle.pem
awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
 {split_after=1}{print > "rds-ca-" n+1 ".pem"}' < ${mydir}/global-bundle.pem

for CERT in rds-ca-*; do alias=$(openssl x509 -noout -text -in $CERT | perl -ne
 'next unless /Subject:/; s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -
keystore ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep Alias |
 cut -d " " -f3- | while read alias
do expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword} -
alias "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

macOS

A continuación se muestra un ejemplo de script de intérprete de comandos que importa el paquete de certificados a un almacén de confianza en macOS.

```
mydir=tmp/certs
if [ ! -e "${mydir}" ]
then
mkdir -p "${mydir}"
fi truststore=${mydir}/rds-truststore.jks storepassword=changeit

curl -sS "https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem">
 ${mydir}/global-bundle.pem
```

```
split -p "-----BEGIN CERTIFICATE-----" ${mydir}/global-bundle.pem rds-ca-

for CERT in rds-ca-*; do alias=$(openssl x509 -noout -text -in $CERT | perl -ne
 'next unless /Subject:/; s/.*(CN=|CN = )//; print')
  echo "Importing $alias"
  keytool -import -file ${CERT} -alias "${alias}" -storepass ${storepassword} -
keystore ${truststore} -noprompt
  rm $CERT
done

rm ${mydir}/global-bundle.pem

echo "Trust store content is: "

keytool -list -v -keystore "$truststore" -storepass ${storepassword} | grep Alias |
 cut -d " " -f3- | while read alias
do expiry=`keytool -list -v -keystore "$truststore" -storepass ${storepassword} -
alias "${alias}" | grep Valid | perl -ne 'if(/until: (.*?)\n/) { print "$1\n"; }'`
   echo " Certificate ${alias} expires in '$expiry'"
done
```

Privacidad del tráfico entre redes

Las conexiones están protegidas entre Amazon RDS y las aplicaciones en las instalaciones y entre Amazon RDS y otros recursos de AWS dentro de la misma región de AWS.

Tráfico entre el servicio y las aplicaciones y clientes locales

Tiene dos opciones de conectividad entre su red privada y AWS:

- Una conexión de Site-to-Site VPN de AWS. Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN?
- Una conexión de AWS Direct Connect. Para obtener más información, consulte ¿Qué es AWS Direct Connect?

Accederá a Amazon RDS a través de la red mediante las operaciones de la API publicadas por AWS. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.

- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Administración de la identidad y el acceso en Amazon RDS

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los gestionadores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién se puede autenticar (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de Amazon RDS. IAM es un servicio de Servicio de AWS que se puedes utilizar sin cargo adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Amazon RDS con IAM
- Ejemplos de políticas basadas en identidad para Amazon RDS
- Políticas administradas por AWS para Amazon RDS
- Actualizaciones de Amazon RDS a políticas administradas por AWS
- Prevención de los problemas del suplente confuso entre servicios
- Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL
- Solución de problemas de identidades y accesos en Amazon RDS

Público

La forma en que utiliza AWS Identity and Access Management (IAM) difiere en función del trabajo que realiza en Amazon RDS.

Usuario de servicio: si utiliza el servicio Amazon RDS para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon RDS para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica en Amazon RDS, consulte Solución de problemas de identidades y accesos en Amazon RDS.

Administrador de servicio: si está a cargo de los recursos de –Amazon RDS en su empresa, probablemente tenga acceso completo a Amazon RDS. Su trabajo consiste en determinar qué a

características y recursos de Amazon RDS deben acceder sus empleados. A continuación, debe enviar solicitudes a su administrador de para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Amazon RDS, consulte Cómo funciona Amazon RDS con IAM.

Administrador: si es un administrador de IAM, es posible que quiera conocer información sobre cómo escribir políticas para administrar el acceso a Amazon RDS. Para ver ejemplos de políticas basadas en la identidad de Amazon RDS que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidad para Amazon RDS.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de un origen de identidad. AWS IAM Identity Center Los usuarios (de IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso de AWS. Para obtener más información sobre el inicio de sesión en AWS, consulta Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Autenticación multifactor de AWS en IAM, en la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de gestionador, utilicen la federación con un proveedor de identidades para acceder a los Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de un origen de identidad. Cuando identidades federadas acceden a Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propio origen de identidades para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulte ¿Qué es IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de AWSque dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Puede autenticar en si instancia utilizando autenticación de base de datos de IAM.

La autenticación de base de datos de IAM funciona con los siguientes motores de base de datos:

- RDS para MariaDB
- RDS para MySQL
- RDS para PostgreSQL

Para obtener más información sobre la autenticación en su instancia con IAM, consulte Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL.

Roles de IAM

Un rol de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un rol de IAM en la AWS Management Console cambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Permisos de usuario temporales: un usuario puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad

al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puede acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.

- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Reenviar sesiones de acceso: cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Rol vinculado a los servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del

servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecuten en una instancia de EC2 y realicen solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información acerca del uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en vez de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades de IAM o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad (usuario raíz, usuario o rol de IAM) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Un administrador puede utilizar las políticas para especificar quién tiene acceso a los recursos de AWS y qué acciones se pueden realizar en dichos recursos. Cada entidad de IAM (conjunto de permisos o rol) comienza sin permisos. En otras palabras, de forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe adjuntarle una política de permisos. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como por ejemplo, un conjunto de permisos o un rol. Estas políticas controlan qué acciones puede realizar dicha identidad, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único conjunto de permisos o un rol. Las políticas administradas son políticas independientes que puede asociar a varios conjuntos de permisos o roles de su cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Para obtener información sobre las políticas administradas de AWS que son específicas de Amazon RDS, consulte Políticas administradas por AWS para Amazon RDS.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad (conjunto de permisos o rol). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de sus permisos. Las políticas basadas en recursos que especifiquen el conjunto de permisos o rol en el campo `Principal` no están restringidos por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP

limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del conjunto de permisos o rol y las políticas de la sesión. Los permisos también puede proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulta Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon RDS con IAM

Antes de utilizar IAM para administrar el acceso a Amazon RDS, debe saber qué características de IAM están disponibles para usar con Amazon RDS.

En la siguiente tabla, encontrará las características de IAM que puede usar con Amazon RDS:

Característica de IAM	Compatibilidad de Amazon RDS
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No

Característica de IAM	Compatibilidad de Amazon RDS
Control de acceso basado en atributos (ABAC) (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una perspectiva general de cómo funciona Amazon RDS y otros servicios de AWS con IAM, consulte los servicios de AWS que funcionan con IAM en la guía del usuario de IAM.

Temas

- Políticas de Amazon RDS basadas en identidades
- Políticas basadas en recursos de Amazon RDS
- Acciones de política de Amazon RDS
- Recursos de políticas de Amazon RDS
- Claves de condición de políticas para Amazon RDS
- Listas de control de acceso (ACL) de Amazon RDS
- Control de acceso basado en atributos (ABAC) en políticas con etiquetas de Amazon RDS
- Uso de credenciales temporales con Amazon RDS
- Sesiones de acceso directo para Amazon RDS
- Roles de servicio para Amazon RDS
- Roles vinculados a servicios para Amazon RDS

Políticas de Amazon RDS basadas en identidades

Admite las políticas basadas en identidad: sí.

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué

condiciones. Para obtener más información sobre cómo crear una política basada en identidades, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas de Amazon RDS basadas en identidades

Para ver ejemplos de políticas basadas en identidad de Amazon RDS, consulte Ejemplos de políticas basadas en identidad para Amazon RDS.

Políticas basadas en recursos de Amazon RDS

Admite políticas basadas en recursos: no.

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los gestionadores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales puedes incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un gestionador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de política de Amazon RDS

Admite las acciones de política: sí.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de Amazon RDS utilizan el siguiente prefijo antes de la acción: `rds:`. Por ejemplo, para conceder a alguien permiso para eliminar un punto de enlace de Amazon RDS con la operación de la API `DescribeDBInstances` de `rds:DescribeDBInstances`, incluya la acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Amazon RDS define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones de en una única instrucción, sepárelas con comas del siguiente modo.

```
"Action": [
      "rds:action1",
      "rds:action2"
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción.

```
"Action": "rds:Describe*"
```

Para ver una lista de las acciones de Amazon RDS, consulte Acciones definidas por Amazon RDS en la referencia de autorizaciones de servicio.

Recursos de políticas de Amazon RDS

Admite los recursos de políticas: sí.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

El recurso de instancia de base de datos tiene el siguiente nombre de recurso de Amazon (ARN).

```
arn:${Partition}:rds:${Region}:${Account}:{ResourceType}/${Resource}
```

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Por ejemplo, para especificar la instancia de base de datos `dbtest` en su instrucción, utilice el siguiente ARN.

```
"Resource": "arn:aws:rds:us-west-2:123456789012:db:dbtest"
```

Para especificar todas las instancias de base de datos que pertenecen a una cuenta específica, utilice el carácter comodín (*).

```
"Resource": "arn:aws:rds:us-east-1:123456789012:db:*"
```

Algunas operaciones de API de RDS, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, utilice el carácter comodín (*).

```
"Resource": "*"
```

En muchas operaciones de la API de Amazon RDS se utilizan varios recursos. Por ejemplo, `CreateDBInstance` crea una instancia de base de datos. Puede especificar que un usuario de debe usar un grupo de seguridad y un grupo de parámetros específicos al crear una instancia de base de datos. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
      "resource1",
      "resource2"
```

Para ver una lista de las acciones de Amazon RDS, consulte Recursos definidos por Amazon RDS en la referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon RDS.

Claves de condición de políticas para Amazon RDS

Admite claves de condición de políticas específicas del servicio: sí.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Amazon RDS define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Todas las operaciones de API de RDS admiten la clave de condición `aws:RequestedRegion`.

Para ver una lista de las claves de condición de Amazon RDS, consulte Claves de condición de Amazon RDS en la referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon RDS.

Listas de control de acceso (ACL) de Amazon RDS

Admite las listas de control de acceso (ACL): no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) en políticas con etiquetas de Amazon RDS

Admite las etiquetas de control de acceso basado en atributos (ABAC) en las políticas: sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puedes adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos en función de los atributos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Para obtener más información acerca del etiquetado de recursos de Amazon RDS, consulte Especificación de condiciones: uso de etiquetas personalizadas. Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Conceda permiso para acciones en un recurso con una etiqueta específica con dos valores diferentes..

Uso de credenciales temporales con Amazon RDS

Admite credenciales temporales: sí.

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulta Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio a un rol de IAM (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puedes usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Amazon RDS

Admite sesiones de acceso directo: sí.

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que

desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Roles de servicio para Amazon RDS

Admite roles de servicio: sí.

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon RDS. Edite los roles de servicio solo cuando Amazon RDS proporcione orientación para hacerlo.

Roles vinculados a servicios para Amazon RDS

Admite roles vinculados al servicio: sí.

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo usar los roles vinculados a servicios de Amazon RDS, consulte Uso de roles vinculados a servicios de Amazon RDS.

Ejemplos de políticas basadas en identidad para Amazon RDS

De forma predeterminada, los conjuntos de permisos y roles no tienen permiso para crear ni modificar recursos de Amazon RDS. Tampoco pueden realizar tareas mediante la AWS Management

Console, la AWS CLI o la API de AWS. Un administrador debe crear políticas de IAM que concedan conjuntos de permisos y permisos de roles para realizar operaciones de API concretas en los recursos especificados necesarios. El administrador debe asociar esas políticas a los conjuntos de permisos o roles que necesiten esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Mediante la consola de Amazon RDS
- Permisos necesarios para usar la consola
- Cómo permitir a los usuarios consultar sus propios permisos
- Políticas de permisos para crear, modificar y eliminar recursos en Amazon RDS
- Políticas de ejemplo: uso de claves de condición
- Especificación de condiciones: uso de etiquetas personalizadas
- Concesión de permisos para etiquetar recursos de Amazon RDS durante la creación

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos de Amazon RDS de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comienza con las políticas administradas por AWSy continúa con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de tarea, utiliza las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas gestionadas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se

pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesite usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para obtener una mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de Amazon RDS

Para acceder a la consola de Amazon RDS, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y consultar los detalles sobre los recursos de Amazon RDS en su cuenta de Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Para asegurarse de que esas entidades puedan seguir usando la consola de Amazon RDS, asocie también la siguiente política administrada por AWS a las entidades.

```
AmazonRDSReadOnlyAccess
```

Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Permisos necesarios para usar la consola

Para que un usuario pueda trabajar con la consola, debe tener un conjunto mínimo de permisos. Estos permisos permiten al usuario describir los recursos de Amazon RDS de su cuenta de AWS y proporcionar otra información relacionada, incluida información de red y seguridad de Amazon EC2.

Si crea una política de IAM que sea más restrictiva que el mínimo de permisos necesarios, la consola no funciona del modo esperado para los usuarios con esa política de IAM. Para asegurarse de que esos usuarios puedan seguir usando la consola, asocie también la política administrada `AmazonRDSReadOnlyAccess` al usuario, según se explica en Administración de acceso mediante políticas.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de Amazon RDS.

La siguiente política concede acceso completo a todos los recursos de Amazon RDS para la cuenta de AWS raíz:

```

AmazonRDSFullAccess

```

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Políticas de permisos para crear, modificar y eliminar recursos en Amazon RDS

En las siguientes secciones, encontrará ejemplos de políticas de permisos para otorgar y limitar el acceso a los recursos:

Permitir a un usuario crear en instancias de base de datos en una cuenta de AWS

A continuación, se muestra el ejemplo de una política que permite que la cuenta con el ID `123456789012` pueda crear instancias de base de datos para su cuenta AWS. La política requiere que el nombre de la nueva instancia de base de datos comience por `test`. La nueva instancia de base de datos también debe utilizar el motor de base de datos MySQL y la clase de instancia de base de datos `db.t2.micro`. Además, la nueva instancia de base de datos debe usar un grupo de

opciones y un grupo de parámetros de base de datos que comience por `default` y debe utilizar el grupo de subred `default`.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowCreateDBInstanceOnly",
         "Effect": "Allow",
         "Action": [
            "rds:CreateDBInstance"
         ],
         "Resource": [
            "arn:aws:rds:*:123456789012:db:test*",
            "arn:aws:rds:*:123456789012:og:default*",
            "arn:aws:rds:*:123456789012:pg:default*",
            "arn:aws:rds:*:123456789012:subgrp:default"
         ],
         "Condition": {
            "StringEquals": {
               "rds:DatabaseEngine": "mysql",
               "rds:DatabaseClass": "db.t2.micro"
            }
         }
      }
   ]
}
```

En la política se incluye una sola instrucción que especifica los siguientes permisos para el usuario de:

- La política permite a la cuenta crear una instancia de base de datos utilizando la operación CreateDBInstance de la API (esto también se aplica al comando create-db-instance de la AWS CLI y a la AWS Management Console).
- El elemento `Resource` especifica que el usuario puede realizar acciones en o con recursos. Puede especificar los recursos mediante un nombre de recurso de Amazon (ARN). Este ARN incluye el nombre del servicio al que pertenece el recurso (`rds`), la región AWS (`*` indica cualquier región de este ejemplo), el número de cuenta de AWS (`123456789012` es el número de cuenta en

este ejemplo) y el tipo de recurso. Para obtener más información acerca de la creación de nombres ARN, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

El elemento `Resource` del ejemplo especifica las siguientes restricciones políticas en los recursos del usuario:

- El identificador de instancias de bases de datos para la nueva instancia de base de datos debe comenzar por `test` (por ejemplo, `testCustomerData1`, `test-region2-data`).
- El grupo de opciones de la nueva instancia de base de datos debe empezar por `default`.
- El grupo de parámetros de base de datos de la nueva instancia de base de datos debe empezar por `default`.
- El grupo de subred de la nueva instancia de base de datos debe ser el grupo de subred `default`.

- El elemento `Condition` especifica que el motor de base de datos debe ser MySQL, mientras que la clase de instancia de base de datos debe ser `db.t2.micro`. El elemento `Condition` especifica las condiciones en las que se debe aplicar una política. Puede añadir permisos o restricciones adicionales mediante el elemento `Condition`. Para obtener más información acerca de cómo especificar condiciones, consulte Claves de condición de políticas para Amazon RDS. Este ejemplo especifica el estado del `rds:DatabaseEngine` y la `rds:DatabaseClass`. Para obtener más información acerca de los valores de estado válidos para `rds:DatabaseEngine`, consulte la lista bajo el parámetro `Engine` en CreateDBInstance. Para obtener información acerca de los valores de estado válidos para `rds:DatabaseClass`, consulte Motores de base de datos compatibles para clases de instancia de base de datos.

La política no especifica el elemento `Principal`, ya que en una política basada en la identidad no se especifica el elemento principal que obtiene el permiso. Al asociar una política a un usuario, el usuario es la entidad principal implícita. Cuando se asocia una política de permisos a un rol de IAM, la entidad principal identificada en la política de confianza del rol obtiene los permisos.

Para ver una lista de las acciones de Amazon RDS, consulte Acciones definidas por Amazon RDS en la referencia de autorizaciones de servicio.

Permitir que un usuario realice cualquier acción Describe con cualquier recurso de RDS

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por `Describe`. Estas acciones muestran información acerca de un recurso de RDS, como una instancia de base de datos. El carácter de comodín (*) en el elemento `Resource` indica

que las acciones están permitidas para todos los recursos de Amazon RDS que pertenecen a la cuenta.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowRDSDescribe",
         "Effect": "Allow",
         "Action": "rds:Describe*",
         "Resource": "*"
      }
   ]
}
```

Permitirle al usuario crear una instancia de base de datos que use los grupos de parámetros de base de datos y de subredes especificados

La política de permisos siguiente otorga permisos para permitir que el usuario solo pueda crear una instancia de base de datos que use el grupo de parámetros de base de datos `mydbpg` y el grupo de subredes de base de datos `mydbsubnetgroup`.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": "rds:CreateDBInstance",
         "Resource": [
            "arn:aws:rds:*:*:pg:mydbpg",
            "arn:aws:rds:*:*:subgrp:mydbsubnetgroup"
         ]
      }
   ]
```

```
}
```

Conceda permiso para acciones en un recurso con una etiqueta específica con dos valores diferentes.

Puede utilizar las condiciones de su política basada en la identidad para controlar el acceso a los recursos de Amazon RDS basados en etiquetas. La siguiente política da permiso para aplicar la operación de API `CreateDBSnapshot` en instancias de base de datos con la etiqueta `stage` establecida en `development` o `test`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowAnySnapshotName",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:snapshot:*"
      },
      {
         "Sid":"AllowDevTestToCreateSnapshot",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
```

```
}
```

La siguiente política da permiso para aplicar la operación de API `ModifyDBInstance` en instancias de base de datos con la etiqueta `stage` establecida en `development` o `test`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowChangingParameterOptionSecurityGroups",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource": [
            "arn:aws:rds:*:123456789012:pg:*",
            "arn:aws:rds:*:123456789012:secgrp:*",
            "arn:aws:rds:*:123456789012:og:*"
         ]
      },
      {
         "Sid":"AllowDevTestToModifyInstance",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

Evitar que un usuario elimine una instancia de base de datos

La siguiente política de permisos concede permisos para impedir que un usuario elimine una instancia de base de datos específica. Por ejemplo, puede servir para impedir la eliminación de instancias de base de datos de producción a cualquier usuario que no sea un administrador.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "DenyDelete1",
         "Effect": "Deny",
         "Action": "rds:DeleteDBInstance",
         "Resource": "arn:aws:rds:us-west-2:123456789012:db:my-mysql-instance"
      }
   ]
}
```

Denegar todo el acceso a un recurso

Puede denegar explícitamente el acceso a un recurso. Las políticas de denegación tienen prioridad sobre las políticas de permiso. La política siguiente niega explícitamente a un usuario la capacidad de administrar un recurso:

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": "rds:*",
         "Resource": "arn:aws:rds:us-east-1:123456789012:db:mydb"
      }
```

```
    ]
}
```

Políticas de ejemplo: uso de claves de condición

Los siguientes ejemplos muestran cómo puede usar claves de condición en las políticas de permisos de IAM para Amazon RDS.

Ejemplo 1: conceder permiso para crear una instancia de base de datos que utilice un motor de base de datos específico y no sea Multi-AZ.

La siguiente política utiliza una clave de condición de RDS y permite al usuario crear solamente instancias de base de datos que utilizan el motor de base de datos MySQL y no utilizan Multi-AZ. El elemento `Condition` indica el requisito de que el motor de base de datos sea MySQL.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "AllowMySQLCreate",
         "Effect": "Allow",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "rds:DatabaseEngine": "mysql"
            },
            "Bool": {
               "rds:MultiAz": false
            }
         }
      }
   ]
}
```

Ejemplo 2: denegar permiso explícitamente para crear instancias de base de datos para determinadas clases de instancia de base de datos y crear instancias de base de datos que utilizan IOPS provisionadas

La siguiente política deniega permiso explícitamente para crear instancias de base de datos que utilizan las clases de instancia de base de datos `r3.8xlarge` y `m4.10xlarge`, que son las clases

de instancia de base de datos más costosas y de mayor tamaño. Esta política también evita que los usuarios creen instancias de base de datos que utilizan IOPS provisionadas, las cuales tienen un costo adicional.

Al denegarse permiso explícitamente se sustituye a cualquier otro permiso concedido. Esto garantiza que las identidades no obtengan accidentalmente permisos que el usuario no desee conceder nunca.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "DenyLargeCreate",
         "Effect": "Deny",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "rds:DatabaseClass": [
                  "db.r3.8xlarge",
                  "db.m4.10xlarge"
               ]
            }
         }
      },
      {
         "Sid": "DenyPIOPSCreate",
         "Effect": "Deny",
         "Action": "rds:CreateDBInstance",
         "Resource": "*",
         "Condition": {
            "NumericNotEquals": {
               "rds:Piops": "0"
            }
         }
      }
   ]
}
```

Ejemplo 3: limitar el conjunto de claves y valores de etiquetas que se pueden usar para etiquetar un recurso

En la siguiente política se usa una clave condicional de RDS y permite añadir una etiqueta con la clave `stage` a un recurso con los valores `test`, `qa` y `production`.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource"
         ],
         "Resource": "*",
         "Condition": {
            "streq": {
               "rds:req-tag/stage": [
                  "test",
                  "qa",
                  "production"
               ]
            }
         }
      }
   ]
}
```

Especificación de condiciones: uso de etiquetas personalizadas

Amazon RDS admite la especificación de condiciones en una política de IAM que utiliza etiquetas personalizadas.

Por ejemplo, suponga que añade una etiqueta con el nombre `environment` a sus instancias de base de datos con valores como `beta`, `staging`, `production`, etc. Si lo hace, puede crear una política que restrinja a ciertos usuarios en instancias de bases de datos basándose en el valor de la etiqueta `environment`.

> **Note**
>
> Los identificadores de etiquetas personalizados distinguen entre mayúsculas y minúsculas.

En la tabla siguiente, se enumeran los identificadores de etiqueta de RDS que puede usar en un elemento `Condition`.

Identificador de etiqueta de RDS	Se aplica a
`db-tag`	Instancias de base de datos, incluidas las réplicas de lectura
`snapshot-tag`	Instantáneas de base de datos
`ri-tag`	Instancias de base de datos reservadas
`og-tag`	Grupos de opciones de base de datos
`pg-tag`	Grupos de parámetros de base de datos
`subgrp-tag`	Grupos de subred de base de datos
`es-tag`	Suscripciones de eventos
`cluster-tag`	Clústeres de base de datos
`cluster-pg-tag`	Grupos de parámetros de clúster de bases de datos
`cluster-snapshot-tag`	Instantáneas de clúster de bases de datos

La sintaxis de una condición de etiqueta personalizada es la siguiente:

```
"Condition":{"StringEquals":{"rds:rds-tag-identifier/tag-name":
["value"]} }
```

Por ejemplo, el elemento `Condition` siguiente se aplica a instancias de base de datos con una etiqueta llamada `environment` y un valor de etiqueta `production`.

```
"Condition":{"StringEquals":{"rds:db-tag/environment": ["production"]} }
```

Para obtener información acerca de la creación etiquetas, consulte Etiquetado de los recursos de y Amazon RDS.

> **Important**
>
> Si administra el acceso a sus recursos de RDS mediante el etiquetado, recomendamos que proteja el acceso a las etiquetas. Puede administrar el acceso a etiquetas creando políticas para las acciones `AddTagsToResource` y `RemoveTagsFromResource`. Por ejemplo, la política siguiente deniega a los usuarios la posibilidad de agregar o quitar etiquetas para todos los recursos. A continuación, puede crear políticas para permitir que usuarios específicos agreguen o quiten etiquetas.
>
> ```
> {
>    "Version":"2012-10-17",
>    "Statement":[
>       {
>          "Sid":"DenyTagUpdates",
>          "Effect":"Deny",
>          "Action":[
>             "rds:AddTagsToResource",
>             "rds:RemoveTagsFromResource"
>          ],
>          "Resource":"*"
>       }
>    ]
> }
> ```

Para ver una lista de las acciones de Amazon RDS, consulte Acciones definidas por Amazon RDS en la referencia de autorizaciones de servicio.

Políticas de ejemplo: uso de etiquetas personalizadas

Los siguientes ejemplos muestran cómo puede usar etiquetas personalizadas en las políticas de permisos de IAM para Amazon RDS. Para obtener más información sobre cómo agregar etiquetas a un recurso de Amazon RDS, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

> **Note**
>
> Todos los ejemplos utilizan la región us-west-2 y contienen identificadores de cuenta ficticios.

Ejemplo 1: conceda permiso para acciones en un recurso con una etiqueta específica con dos valores diferentes.

La siguiente política da permiso para aplicar la operación de API `CreateDBSnapshot` en instancias de base de datos con la etiqueta `stage` establecida en `development` o `test`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowAnySnapshotName",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:snapshot:*"
      },
      {
         "Sid":"AllowDevTestToCreateSnapshot",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBSnapshot"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

La siguiente política da permiso para aplicar la operación de API `ModifyDBInstance` en instancias de base de datos con la etiqueta `stage` establecida en `development` o `test`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowChangingParameterOptionSecurityGroups",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource":" [
            "arn:aws:rds:*:123456789012:pg:*",
            "arn:aws:rds:*:123456789012:secgrp:*",
            "arn:aws:rds:*:123456789012:og:*"
         ]
      },
      {
         "Sid":"AllowDevTestToModifyInstance",
         "Effect":"Allow",
         "Action":[
            "rds:ModifyDBInstance"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:*",
         "Condition":{
            "StringEquals":{
                "rds:db-tag/stage":[
                  "development",
                  "test"
               ]
            }
         }
      }
   ]
}
```

Ejemplo 2: deniegue explícitamente permiso para crear una instancia de base de datos que utilice grupos de parámetros de base de datos especificados.

La siguiente política deniega explícitamente permiso para crear una instancia de base de datos que utilice grupos de parámetros de base de datos con valores de etiqueta específicos. Podría aplicar esta política si necesita que se utilice siempre un grupo de parámetros de base de datos específico, creado por el cliente, al crear instancias de base de datos. Las políticas que utilizan `Deny` suelen aplicarse para restringir el acceso concedido por una política más amplia.

Al denegarse permiso explícitamente se sustituye a cualquier otro permiso concedido. Esto garantiza que las identidades no obtengan accidentalmente permisos que el usuario no desee conceder nunca.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyProductionCreate",
         "Effect":"Deny",
         "Action":"rds:CreateDBInstance",
         "Resource":"arn:aws:rds:*:123456789012:pg:*",
         "Condition":{
            "StringEquals":{
               "rds:pg-tag/usage":"prod"
            }
         }
      }
   ]
}
```

Ejemplo 3: conceda permiso para acciones en una instancia de base de datos con un nombre de instancia cuyo prefijo sea un nombre de usuario.

La siguiente política da permiso para llamar a cualquier API (salvo `AddTagsToResource` o `RemoveTagsFromResource`) en una instancia de base de datos cuyo prefijo sea un nombre de usuario y que tenga una etiqueta llamada `stage` igual a `devo` o que no tenga ninguna etiqueta llamada `stage`.

La línea `Resource` en la política identifica un recurso por su nombre de recurso de Amazon (ARN). Para obtener más información sobre el uso de ARN con recursos de Amazon RDS, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowFullDevAccessNoTags",
         "Effect":"Allow",
         "NotAction":[
            "rds:AddTagsToResource",
            "rds:RemoveTagsFromResource"
         ],
         "Resource":"arn:aws:rds:*:123456789012:db:${aws:username}*",
         "Condition":{
            "StringEqualsIfExists":{
               "rds:db-tag/stage":"devo"
            }
         }
      }
   ]
}
```

Concesión de permisos para etiquetar recursos de Amazon RDS durante la creación

Algunas operaciones de la API de RDS le permiten especificar etiquetas durante la creación del recurso. Puede utilizar etiquetas de recursos para implementar el control basado en atributos (ABAC). Para obtener más información, consulte ¿Qué es ABAC para AWS? y Control del acceso a los recursos de AWS mediante etiquetas.

Para permitir que los usuarios etiqueten los recursos durante su creación, es preciso que tengan permisos para utilizar la acción que crea el recurso, por ejemplo `rds:CreateDBInstance`. Si se especifican etiquetas en la acción de creación, RDS realiza una autorización adicional en la acción `rds:AddTagsToResource` para verificar que los usuarios tengan permisos para crear etiquetas. Por lo tanto, los usuarios también deben tener permisos explícitos para usar la acción `rds:AddTagsToResource`.

En la definición de la política de IAM para la acción `rds:AddTagsToResource`, puede utilizar la clave de condición `aws:RequestTag` para requerir etiquetas en una solicitud de etiquetado de un recurso.

Por ejemplo, la siguiente política permite a los usuarios crear instancias de base de datos y aplicar etiquetas durante la creación de instancias de base de datos, pero solo con claves de etiqueta específicas (`environment` o `project`):

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "rds:CreateDBInstance"
           ],
           "Resource": "*"
       },
       {
           "Effect": "Allow",
           "Action": [
               "rds:AddTagsToResource"
           ],
           "Resource": "*",
           "Condition": {
               "StringEquals": {
                   "aws:RequestTag/environment": ["production", "development"],
                   "aws:RequestTag/project": ["dataanalytics", "webapp"]
               },
               "ForAllValues:StringEquals": {
                   "aws:TagKeys": ["environment", "project"]
               }
           }
       }
   ]
}
```

Esta política deniega cualquier solicitud de creación de instancias de base de datos que incluya etiquetas distintas de las etiquetas `environment` o `project`, o que no especifique ninguna de estas etiquetas. Además, los usuarios deben especificar valores para las etiquetas que coincidan con los valores permitidos en la política.

La siguiente política permite a los usuarios crear clústeres de base de datos y aplicar cualquier etiqueta durante la creación, excepto la etiqueta `environment=prod`:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
```

```
            "Action": [
                "rds:CreateDBCluster"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:AddTagsToResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/environment": "prod"
                }
            }
        }
    ]
}
```

Acciones de la API de RDS compatibles para etiquetar durante la creación

Las siguientes acciones de la API de RDS admiten el etiquetado al crear un recurso. Para estas acciones, puede especificar etiquetas al crear el recurso:

- `CreateBlueGreenDeployment`
- `CreateCustomDBEngineVersion`
- `CreateDBCluster`
- `CreateDBClusterEndpoint`
- `CreateDBClusterParameterGroup`
- `CreateDBClusterSnapshot`
- `CreateDBInstance`
- `CreateDBInstanceReadReplica`
- `CreateDBParameterGroup`
- `CreateDBProxy`
- `CreateDBProxyEndpoint`
- `CreateDBSecurityGroup`
- `CreateDBShardGroup`

- `CreateDBSnapshot`
- `CreateDBSubnetGroup`
- `CreateEventSubscription`
- `CreateGlobalCluster`
- `CreateIntegration`
- `CreateOptionGroup`
- `CreateTenantDatabase`
- `CopyDBClusterParameterGroup`
- `CopyDBClusterSnapshot`
- `CopyDBParameterGroup`
- `CopyDBSnapshot`
- `CopyOptionGroup`
- `RestoreDBClusterFromS3`
- `RestoreDBClusterFromSnapshot`
- `RestoreDBClusterToPointInTime`
- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceFromS3`
- `RestoreDBInstanceToPointInTime`
- `PurchaseReservedDBInstancesOffering`

Si utiliza la AWS CLI o la API para crear un recurso con etiquetas, el parámetro `Tags` se utiliza para aplicar etiquetas a los recursos durante la creación.

En el caso de estas acciones de la API, si se produce un error al etiquetar, el recurso no se crea y se produce un error en la solicitud. Esto garantiza que los recursos se creen con etiquetas o, de lo contrario, no se creen sin las etiquetas correspondientes.

Políticas administradas por AWS para Amazon RDS

Para añadir permisos a conjuntos de permisos y roles, es más fácil utilizar políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le brinden a su equipo solo los permisos necesarios. Para comenzar rápidamente, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información acerca de las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los Servicios de AWS mantienen y actualizan las políticas administradas por AWS. No puede cambiar los permisos en las políticas administradas de AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (conjuntos de permisos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWScuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan permisos de una política administrada por AWS, por lo que las actualizaciones de políticas no deterioran los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada por `ReadOnlyAccess` AWS proporciona acceso de solo lectura a todos los recursos y a Servicios de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

Temas

- Política administrada por:AWS AmazonRDSReadOnlyAccess
- Política administrada por:AWS AmazonRDSFullAccess
- Política administrada por:AWS AmazonRDSDataFullAccess
- Política administrada por:AWS AmazonRDSEnhancedMonitoringRole
- Política administrada por:AWS AmazonRDSPerformanceInsightsReadOnly
- Política administrada por AWS: AmazonRDSPerformanceInsightsFullAccess
- Política administrada por:AWS AmazonRDSDirectoryServiceAccess
- Política administrada por:AWS AmazonRDSServiceRolePolicy

- Política administrada por:AWS AmazonRDSCustomServiceRolePolicy
- Política administrada de:AWS AmazonRDSCustomInstanceProfileRolePolicy
- Política administrada de:AWS AmazonRDSPreviewServiceRolePolicy
- Política administrada de:AWS AmazonRDSBetaServiceRolePolicy

Política administrada por:AWS AmazonRDSReadOnlyAccess

Esta política permite acceso de solo lectura a Amazon RDS mediante la AWS Management Console.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `rds`: permite a las entidades principales describir los recursos de Amazon RDS y enumerar las etiquetas de los recursos de Amazon RDS.
- `cloudwatch`: permite a las entidades principales obtener estadísticas de métricas de Amazon CloudWatch.
- `ec2`: permite a las entidades principales describir las zonas de disponibilidad y los recursos de red.
- `logs`: permite a las entidades principales describir los flujos de registro de CloudWatch Logs de los grupos de registros y obtener eventos de registro de CloudWatch Logs.
- `devops-guru`: permite a las entidades principales describir los recursos que incluyen la cobertura de Amazon DevOps Guru, que se especifica mediante nombres de pila o etiquetas de recursos de CloudFormation.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSReadOnlyAccess en la Guía de referencia de políticas administradas de AWS.

Política administrada por:AWS AmazonRDSFullAccess

Esta política proporciona acceso completo a Amazon RDS mediante la AWS Management Console.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `rds`: permite a las entidades principales obtener acceso completo a Amazon RDS.

- `application-autoscaling`: permite a las entidades principales describir y administrar los objetivos y las políticas de escalado de Application Auto Scaling.
- `cloudwatch`: permite a las entidades principales obtener estadísticas métricas de CloudWatch y administrar alarmas de CloudWatch.
- `ec2`: permite a las entidades principales describir las zonas de disponibilidad y los recursos de red.
- `logs`: permite a las entidades principales describir los flujos de registro de CloudWatch Logs de los grupos de registros y obtener eventos de registro de CloudWatch Logs.
- `outposts`: permite a las entidades principales obtener tipos de instancias AWS Outposts.
- `pi`: permite a las entidades principales obtener métricas de Información sobre rendimiento.
- `sns`: permite a las entidades principales acceder a las suscripciones y temas de Amazon Simple Notification Service (Amazon SNS), y publicar mensajes de Amazon SNS.
- `devops-guru`: permite a las entidades principales describir los recursos que incluyen la cobertura de Amazon DevOps Guru, que se especifica mediante nombres de pila o etiquetas de recursos de CloudFormation.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSFullAccess en la Guía de referencia de políticas administradas de AWS.

Política administrada por:AWS AmazonRDSDataFullAccess

Esta política permite tener acceso completo para utilizar la API de datos y el editor de consultas en los clústeres de Aurora Serverless en una Cuenta de AWS determinada. Esta política permite a la Cuenta de AWS obtener el valor de un secreto de AWS Secrets Manager.

Puede adjuntar la política de `AmazonRDSDataFullAccess` a las identidades de IAM.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `dbqms`: permite a las entidades principales acceder, crear, eliminar, describir y actualizar consultas. El Database Query Metadata Service (`dbqms`) es un servicio únicamente interno. Proporciona sus consultas recientes y guardadas para el editor de consultas en la AWS Management Console para varios servicios de Servicios de AWS, incluido Amazon RDS.
- `rds-data`: permite a las entidades principales ejecutar instrucciones SQL en bases de datos de Aurora Serverless.

- `secretsmanager`: permite a las entidades principales obtener el valor de un secreto de AWS Secrets Manager.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSDataFullAccess en la Guía de referencia de políticas administradas de AWS.

Política administrada por:AWS AmazonRDSEnhancedMonitoringRole

Esta política proporciona acceso a registros de Amazon Cloudwatch para Supervisión mejorada de Amazon RDS.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `logs`: permite a las entidades principales crear grupos de registros y políticas de retención de CloudWatch Logs, y crear y describir flujos de registro de CloudWatch Logs de los grupos de registro. También permite a las entidades principales poner y obtener eventos de registro de CloudWatch Logs.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSEnhancedMonitoringRole en la Guía de referencia de políticas administradas de AWS.

Política administrada por:AWS AmazonRDSPerformanceInsightsReadOnly

Esta política proporciona acceso de solo lectura a Información sobre rendimiento de Amazon RDS para instancias de base de datos de Amazon RDS y clústeres de base de datos de Amazon Aurora.

Ahora, esta política incluye `Sid` (ID de instrucción) como identificador en las instrucciones de la política.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `rds`: permite a las entidades principales describir instancias de base de datos de Amazon RDS y clústeres de base de datos de Amazon Aurora
- `pi`: permite a las entidades principales realizar llamadas a la API de Información sobre rendimiento de Amazon RDS y acceder a las métricas de Información sobre rendimiento.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSPerformanceInsightsReadOnly en la Guía de referencia de políticas administradas de AWS.

Política administrada por AWS: AmazonRDSPerformanceInsightsFullAccess

Esta política proporciona acceso completo a Información de rendimiento de Amazon RDS para instancias de base de datos de Amazon RDS y clústeres de base de datos de Amazon Aurora.

Ahora, esta política incluye `Sid` (ID de instrucción) como identificador en las instrucciones de la política.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `rds`: permite a las entidades principales describir instancias de base de datos de Amazon RDS y clústeres de base de datos de Amazon Aurora
- `pi`: permite a los entidades principales realizar llamadas a la API de Información de rendimiento de Amazon RDS y crear, ver y eliminar informes de análisis de rendimiento.
- `cloudwatch`: permite a las entidades principales enumerar todas las métricas de Amazon CloudWatch y obtener estadísticas y datos de las métricas.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSPerformanceInsightsFullAccess en la Guía de referencia de políticas administradas de AWS.

Política administrada por:AWS AmazonRDSDirectoryServiceAccess

Esta política permite a Amazon RDS realizar llamadas al AWS Directory Service.

Detalles de los permisos

Esta política incluye el siguiente permiso:

- `ds`: permite a las entidades principales describir directorios y autorización de control de AWS Directory Service a los directorios de AWS Directory Service.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSDirectoryServiceAccess en la Guía de referencia de políticas administradas de AWS.

Política administrada por:AWS AmazonRDSServiceRolePolicy

No puede adjuntar la política `AmazonRDSServiceRolePolicy` a sus entidades de IAM. Esta política está adjunta a un rol vinculado a servicios que permite a Amazon RDS realizar acciones en su nombre. Para obtener más información, consulte Permisos de roles vinculados a servicios de Amazon RDS.

Política administrada por:AWS AmazonRDSCustomServiceRolePolicy

No puede adjuntar la política `AmazonRDSCustomServiceRolePolicy` a sus entidades de IAM. Esta política está asociada a un rol vinculado a servicios que permite que Amazon RDS llame a los servicios de AWS en nombre de sus recursos de base de datos de RDS.

Esta política incluye los permisos siguientes:

- `ec2`: permite a RDS Custom realizar operaciones de copia de seguridad en la instancia de base de datos, lo que proporciona capacidades de restauración en un momento dado.
- `secretsmanager`: permite a RDS Custom gestionar los secretos específicos de la instancia de base de datos creados por RDS Custom.
- `cloudwatch`: permite a RDS Custom cargar registros y métricas de instancias de base de datos a CloudWatch a través del agente de CloudWatch.
- `events`,:`sqs` permite a RDS Custom enviar y recibir información de estado sobre la instancia de base de datos.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSCustomServiceRolePolicy en la Guía de referencia de políticas administradas de AWS.

Política administrada de:AWS AmazonRDSCustomInstanceProfileRolePolicy

No debe adjuntar `AmazonRDSCustomInstanceProfileRolePolicy` a sus entidades IAM. Solo debe adjuntarse a un rol de perfil de instancia que se utilice para conceder permisos a su instancia de base de datos de Amazon RDS Custom para realizar diversas acciones de automatización y tareas de administración de bases de datos. Transfiera el perfil de instancia como parámetro

`custom-iam-instance-profile` durante la creación de la instancia de RDS Custom; RDS Custom asociará este perfil de instancia a su instancia de base de datos.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `ssm`, `ssmmessages`,:`ec2messages` permite que RDS Custom se comunique, ejecute la automatización y mantenga a los agentes en la instancia de base de datos a través de Systems Manager.
- `ec2`,:`s3` permite a RDS Custom realizar operaciones de copia de seguridad en la instancia de base de datos, lo que proporciona capacidades de restauración en un momento dado.
- `secretsmanager`: permite a RDS Custom gestionar los secretos específicos de la instancia de base de datos creados por RDS Custom.
- `cloudwatch`,:`logs` permite a RDS Custom cargar registros y métricas de instancias de base de datos a CloudWatch a través del agente de CloudWatch.
- `events`,:`sqs` permite a RDS Custom enviar y recibir información de estado sobre la instancia de base de datos.
- `kms`: permite a RDS Custom utilizar una clave KMS específica de la instancia para cifrar los secretos y los objetos de S3 que gestiona RDS Custom.

Para obtener más información sobre esta política, lo que incluye el documento de políticas de JSON, consulte AmazonRDSCustomInstanceProfileRolePolicy, en la Guía de referencia de la política administrada de AWS.

Política administrada de:AWS AmazonRDSPreviewServiceRolePolicy

No debe adjuntar `AmazonRDSPreviewServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado a servicios que permite que Amazon RDS llame a los servicios de AWS en nombre de sus recursos de base de datos de RDS. Para obtener más información, consulte Rol vinculado a servicios para Amazon RDS Preview.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `ec2`: permite a las entidades principales describir las zonas de disponibilidad y los recursos de red.

- `secretsmanager`: permite a las entidades principales obtener el valor de un secreto de AWS Secrets Manager.
- `cloudwatch,:logs` permite a Amazon RDS cargar registros y métricas de instancias de base de datos a CloudWatch a través del agente de CloudWatch.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSDataFullAccess en la Guía de referencia de políticas administradas de AWS.

Política administrada de:AWS AmazonRDSBetaServiceRolePolicy

No debe adjuntar `AmazonRDSBetaServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado a servicios que permite que Amazon RDS llame a los servicios de AWS en nombre de sus recursos de base de datos de RDS. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Beta.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `ec2`: permite a Amazon RDS realizar operaciones de copia de seguridad en la instancia de base de datos, lo que proporciona capacidades de restauración en un momento dado.
- `secretsmanager`: permite a Amazon RDS gestionar los secretos específicos de la instancia de base de datos creados por Amazon RDS.
- `cloudwatch,:logs` permite a Amazon RDS cargar registros y métricas de instancias de base de datos a CloudWatch a través del agente de CloudWatch.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSBetaServiceRolePolicy en la Guía de referencia de políticas administradas de AWS.

Actualizaciones de Amazon RDS a políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Amazon RDS desde que este servicio comenzó a hacer un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de la API de Amazon RDS.

Cambio	Descripción	Fecha
Política administrada de:AWS AmazonRDSPreviewServiceRolePolicy: actualización de una política actual	Amazon RDS ha eliminado el permiso `sns:Publish` de `AmazonRDSPreviewServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSPreview`. Para obtener más información, consulte Política administrada de:AWS AmazonRDSPreviewServiceRolePolicy.	7 de agosto de 2024
Política administrada de:AWS AmazonRDSBetaServiceRolePolicy: actualización de una política actual	Amazon RDS ha eliminado el permiso `sns:Publish` de `AmazonRDSBetaServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSBeta`. Para obtener más información, consulte Política administrada de:AWS AmazonRDSBetaServiceRolePolicy.	7 de agosto de 2024
Permisos de roles vinculados a servicios para Amazon RDS Custom: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del	18 de julio de 2024

Cambio	Descripción	Fecha
	rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . Gracias a los permisos, RDS Custom puede comunicarse con los servicios de Amazon RDS en otra Región de AWS y copiar imágenes de EC2. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	
Política administrada por:AWS AmazonRDSServiceRolePolicy: actualización de una política actual	Amazon RDS ha eliminado el permiso `sns:Publish` de `AmazonRDSServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDS` . Para obtener más información, consulte Política administrada por:AWS AmazonRDSServiceRolePolicy.	2 de julio de 2024

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios para Amazon RDS Custom: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . Este nuevo permiso permite a RDS Custom asociar un rol de servicio como perfil de instancia a una instancia de RDS Custom. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	19 de abril de 2024

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: actualización de una política actual	Amazon RDS agregó un nuevo permiso a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado al servicio `AWSServiceRoleForRDSCustom` para permitir que RDS Custom para SQL Server modifique el tipo de instancia de host de la base de datos subyacente. RDS también agregó el permiso `ec2:DescribeInstanceTypes` para obtener información sobre el tipo de instancia para el host de la base de datos. Para obtener más información, consulte Políticas administradas por AWS para Amazon RDS.	8 de abril de 2024

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: política nueva	Amazon RDS agregó una nueva política administrada denominada `AmazonRDSCustomInstanceProfileRolePolicy` para permitir a RDS Custom realizar acciones de automatización y tareas de administración de bases de datos a través de un perfil de instancia de EC2. Para obtener más información, consulte Políticas administradas por AWS para Amazon RDS.	27 de febrero de 2024
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha agregado nuevos ID de instrucciones a la `AmazonRDSServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDS` . Para obtener más información, consulte Permisos de roles vinculados a servicios de Amazon RDS.	19 de enero de 2024

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: actualización de políticas existentes	Las políticas administradas `AmazonRDSPerformanceInsightsReadOnly` y `AmazonRDSPerformanceInsightsFullAccess` incluyen ahora `Sid` (ID de instrucción) como identificador en las instrucciones de la política. Para obtener más información, consulte Política administrada por:AWS AmazonRDS PerformanceInsightsReadOnly y Política administrada por AWS: AmazonRDS PerformanceInsightsFullAccess.	23 de octubre de 2023
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom`. Estos nuevos permisos permiten que RDS Custom para Oracle cree, modifique y elimine reglas administradas de EventBridge. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	20 de septiembre de 2023

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la política administrada `AmazonRDSFullAccess`. Los permisos le permiten generar, ver y eliminar el informe de análisis de rendimiento durante un período de tiempo. Para obtener más información sobre la configuración de políticas de acceso para la Información de rendimiento, consulte Configuración de directivas de acceso para información sobre rendimiento	17 de agosto de 2023

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: nueva política y actualización de la política existente	Amazon RDS ha añadido nuevos permisos a la política administrada `AmazonRDSPerformanceInsightsReadOnly` y una nueva política administrada denominada `AmazonRDSPerformanceInsightsFullAccess`. Estos permisos le permiten analizar la Información de rendimiento durante un período de tiempo, ver los resultados del análisis junto con las recomendaciones y eliminar los informes. Para obtener más información sobre la configuración de políticas de acceso para la Información de rendimiento, consulte Configuración de directivas de acceso para información sobre rendimiento	16 de agosto de 2023

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . Estos nuevos permisos permiten que RDS Custom para Oracle utilice instantáneas de bases de datos. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	23 de junio de 2023
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . Estos nuevos permisos permiten que RDS Custom para Oracle utilice instantáneas de bases de datos. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	23 de junio de 2023

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . Estos nuevos permisos permiten a RDS Custom crear interfaces de red. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	30 de mayo de 2023
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . Estos nuevos permisos permiten a RDS Custom llamar a Amazon EBS para comprobar la cuota de almacenamiento. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	18 de abril de 2023

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS Custom ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` para su integración con Amazon SQS. RDS Custom debe integrarse con Amazon SQS para crear y administrar las colas de SQS en la cuenta del cliente. Los nombres de las colas de SQS siguen el formato `do-not-delete-rds-custom-[identifier]` y se etiquetan con `Amazon RDS Custom`. El permiso para `ec2:CreateSnapshot` también se ha añadido para permitir a RDS Custom crear copias de seguridad de los volúmenes asociados a la instancia. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	6 de abril de 2023

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: actualización de una política actual	Amazon RDS ha añadido el espacio de nombres de Amazon CloudWatch `ListMetrics` a `AmazonRDSFullAccess` y `AmazonRDSReadOnlyAccess`. Este espacio de nombres es necesario para que Amazon RDS publique métricas de uso de recursos específicas. Para obtener más información, consulte Overview of managing access permissions to your CloudWatch resources (Información general sobre la administración de los permisos de acceso a los recursos de CloudWatch) en la Guía del usuario de Amazon CloudWatch.	4 de abril de 2023

Cambio	Descripción	Fecha
Políticas administradas por AWS para Amazon RDS: actualización de una política actual	Amazon RDS ha añadido un nuevo permiso a las políticas administradas `AmazonRDSFullAccess` y `AmazonRDSReadOnlyAccess` para permitirle visualizar resultados de Amazon DevOps Guru en la consola de RDS. Este permiso es necesario para poder mostrar los resultados de DevOps Guru. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	30 de marzo de 2023

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDS` para su integración con AWS Secrets Manager. RDS debe integrarse con Secrets Manager para administrar las contraseñas de los usuarios maestros en Secrets Manager. El secreto utiliza una convención de nomenclatura reservada y restringe las actualizaciones de los clientes. Para obtener más información, consulte Administración de contraseñas con Amazon RDS y AWS Secrets Manager.	22 de diciembre de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos a la `AmazonRDSCustomServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSCustom` . RDS Custom admite clústeres de bases de datos. Estos nuevos permisos de la política permiten a RDS Custom llamar a Servicios de AWS en nombre de sus clústeres de bases de datos. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon RDS Custom.	9 de noviembre de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos al rol vinculado a un servicio `AWSServiceRoleForRDS` de integración con AWS Secrets Manager. La integración con Secrets Manager es necesaria para que el correo electrónico de SQL Server Reporting Services (SSRS) funcione en RDS. El correo electrónico de SSRS crea un secreto en nombre del cliente. El secreto utiliza una convención de nomenclatura reservada y restringe las actualizaciones de los clientes. Para obtener más información, consulte Uso del correo electrónico de SSRS para enviar informes.	26 de agosto de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos espacios de nombres de Amazon CloudWatch a `AmazonRDSPreviewServiceRolePolicy` para `PutMetricData` . Este espacio de nombres es necesario para que Amazon RDS publique métricas de uso de recursos. Para obtener más información, consulte Uso de claves de condición para limitar el acceso a los espacios de nombres de CloudWatch en la guía del usuario de Amazon CloudWatch.	7 de junio de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos espacios de nombres de Amazon CloudWatch a `AmazonRDSBetaServiceRolePolicy` para `PutMetricData` . Este espacio de nombres es necesario para que Amazon RDS publique métricas de uso de recursos. Para obtener más información, consulte Uso de claves de condición para limitar el acceso a los espacios de nombres de CloudWatch en la guía del usuario de Amazon CloudWatch.	7 de junio de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos espacios de nombres de Amazon CloudWatch a `AWSServiceRoleForRDS` para `PutMetricData` . Este espacio de nombres es necesario para que Amazon RDS publique métricas de uso de recursos. Para obtener más informaci ón, consulte Uso de claves de condición para limitar el acceso a los espacios de nombres de CloudWatch en la guía del usuario de Amazon CloudWatch.	22 de abril de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos permisos al rol vinculado al servicio de `AWSServiceRoleForRDS` para administrar los permisos de los grupos de IP propiedad del cliente y las tablas de enrutamiento de puerta de enlace local (LGW-RTB). Estos permisos son necesarios para que RDS on Outposts realice una replicación Multi-AZ en toda la red local de Outposts. Para obtener más información, consulte Trabajo con implementaciones Multi-AZ para Amazon RDS on AWS Outposts.	19 de abril de 2022

Cambio	Descripción	Fecha
Políticas basadas en identidades: actualización de una política actual	Amazon RDS ha añadido un nuevo permiso a la política administrada por `AmazonRDSFullAccess` para describir los permisos en LGW-RTB. Este permiso es necesario para que RDS on Outposts realice una replicación Multi-AZ en toda la red local de Outposts. Para obtener más información, consulte Trabajo con implementaciones Multi-AZ para Amazon RDS on AWS Outposts.	19 de abril de 2022
Políticas administradas por AWS para Amazon RDS: política nueva	Amazon RDS ha añadido una nueva política administrada llamada `AmazonRDSPerformanceInsightsReadOnly` para permitir que Amazon RDS llame a servicios de AWS en nombre de sus instancias de bases de datos. Para obtener más información sobre la configuración de políticas de acceso para la Información de rendimiento, consulte Configuración de directivas de acceso para información sobre rendimiento	10 de marzo de 2022

Cambio	Descripción	Fecha
Permisos de roles vinculados a servicios de Amazon RDS: actualización de una política actual	Amazon RDS ha añadido nuevos espacios de nombres de Amazon CloudWatch a `AWSServiceRoleForRDS` para `PutMetricData` . Estos espacios de nombres son necesarios para Amazon DocumentDB (compatible con MongoDB) y Amazon Neptune para publicar métricas de CloudWatch. Para obtener más informaci ón, consulte Uso de claves de condición para limitar el acceso a los espacios de nombres de CloudWatch en la guía del usuario de Amazon CloudWatch.	4 de marzo de 2022
Permisos de roles vinculados a servicios para Amazon RDS Custom: política nueva	Amazon RDS ha agregado un nuevo rol vinculado al servicio llamado `AWSServic eRoleForRDSCustom` para permitir que RDS Custom llame a Servicios de AWS en nombre de las instancias de bases de datos.	26 de octubre de 2021
Amazon RDS ha comenzado a hacer un seguimiento de los cambios	Amazon RDS ha comenzado a realizar un seguimiento de los cambios en sus políticas administradas por AWS.	26 de octubre de 2021

Prevención de los problemas del suplente confuso entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa.

La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que pueden ayudarlo a proteger sus datos en todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta. Para obtener más información, consulte El problema del suplente confuso en la Guía del usuario de IAM.

A fin de limitar los permisos que Amazon RDS da a otro servicio para un recurso específico, le recomendamos utilizar las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos.

En algunos casos, el valor de `aws:SourceArn` no contiene el ID de la cuenta, por ejemplo, al utilizar el nombre de recurso de Amazon (ARN) para un bucket de Simple Storage Service (Amazon S3). En estos casos, asegúrese de utilizar ambas claves de contexto de condición global para limitar los permisos. En algunos casos, se utilizan las claves de contexto de condición global y el valor de `aws:SourceArn` contiene el ID de la cuenta. En estos casos, asegúrese de que el valor de `aws:SourceAccount` y la cuenta en `aws:SourceArn` utilicen el mismo ID de cuenta cuando se utilizan en la misma instrucción de política. Si quiere que solo se asocie un recurso al acceso entre servicios, utilice `aws:SourceArn`. Si quiere permitir que cualquier recurso de esa cuenta de AWS se asocie al uso entre servicios, utilice `aws:SourceAccount`.

Asegúrese de que el valor de `aws:SourceArn` sea un ARN para un tipo de recurso de Amazon RDS. Para obtener más información, consulte Nombres de recursos de Amazon (ARN) en Amazon RDS.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. En algunos casos, es posible que no sepa el ARN completo del recurso o que esté especificando varios recursos. En estos casos, utilice la clave de condición de contexto global de `aws:SourceArn` con comodines (*) para las partes desconocidas del ARN. Un ejemplo es `arn:aws:rds:*:123456789012:*`.

En el ejemplo siguiente, se muestra cómo se pueden utilizar las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount` en Amazon RDS para evitar el problema del suplente confuso.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "rds.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:rds:us-east-1:123456789012:db:mydbinstance"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Para ver más ejemplos de las políticas que utilizan las claves de contexto de condición global de `aws:SourceArn` y `aws:SourceAccount`, consulte las siguientes secciones:

- Concesión de permisos para publicar notificaciones en un tema de Amazon SNS
- Creación manual de un rol de IAM para la copia de seguridad y la restauración nativas
- Configuración de la autenticación de Windows para las instancias de base de datos de SQL Server
- Requisitos previos para la integración de RDS for SQL Server con S3
- Creación manual de un rol de IAM para SQL Server Audit
- Configuración de permisos IAM para la integración de RDS para Oracle con Amazon S3
- Configuración del acceso a un bucket de Amazon S3 (importación de PostgreSQL)
- Configuración del acceso a un bucket de Amazon S3 (exportación de PostgreSQL)

Autenticación de bases de datos de IAM para MariaDB, MySQL, and PostgreSQL

Puede autenticar en su instancia mediante la autenticación de base de datos de AWS Identity and Access Management (IAM). La autenticación de base de datos de IAM funciona con MariaDB, MySQL y PostgreSQL. Con este método de autenticación, no es necesario usar una contraseña al conectarse a una instancia. En su lugar, puede usar un token de autenticación.

Un token de autenticación es una cadena única de caracteres que genera Amazon RDS bajo demanda. Los tokens de autenticación se generan mediante AWS Signature versión 4. Cada token tiene una vida útil de 15 minutos. No es necesario almacenar credenciales de usuario en la base de datos, ya que la autenticación se administra de forma externa mediante IAM. También puede seguir utilizando la autenticación de base de datos estándar. El token solo se utiliza para la autenticación y no afecta a la sesión después de establecerse.

La autenticación de bases de datos de IAM proporciona los siguientes beneficios:

- El tráfico de red hacia y desde la base de datos se cifra mediante Secure Socket Layer (SSL) o Transport Layer Security (TLS). Para obtener más información sobre el uso de SSL/TLS con Amazon RDS, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
- Puede usar IAM para administrar de forma centralizada el acceso a sus recursos de base de datos, en lugar de administrar el acceso individualmente en cada instancia.
- Para las aplicaciones que se ejecutan en Amazon EC2, puede usar las credenciales del perfil específicas de la instancia de EC2 para obtener acceso a su base de datos en lugar de una contraseña, para mayor seguridad.

En general, considere la posibilidad de utilizar la autenticación de base de datos de IAM cuando sus aplicaciones creen menos de 200 conexiones por segundo y no desee administrar los nombres de usuario y las contraseñas directamente en el código de la aplicación.

El controlador JDBC de Amazon Web Services (AWS) admite la autenticación de base de datos de IAM. Para obtener más información, consulte AWS IAM Authentication Plugin en el repositorio GitHub del controlador JDBC de Amazon Web Services (AWS).

El controlador de Python de Amazon Web Services (AWS) admite la autenticación de base de datos de IAM. Para obtener más información, consulte AWS IAM Authentication Plugin en el repositorio GitHub del controlador de Python de Amazon Web Services (AWS).

Consulte los siguientes temas para aprender a utilizar el proceso de configuración de IAM para la autenticación de bases de datos:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM
- Conexión a la instancia con la autenticación de IAM

Disponibilidad en regiones y versiones

La disponibilidad y el soporte de las características varía según las versiones específicas de cada motor de base de datos. Para obtener más información sobre la disponibilidad de motor, versión y región con Amazon RDS y la autenticación de base de datos de IAM, consulte Regiones y motores de base de datos admitidos para autenticación de base de datos IAM en Amazon RDS.

Soporte de CLI y SDK

La autenticación de bases de datos de IAM está disponible para la AWS CLI y para los siguientes SDK de AWS específicos para cada lenguaje:

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go
- AWS SDK para Java
- AWS SDK para JavaScript
- AWS SDK para PHP
- AWS SDK para Python (Boto3)
- AWS SDK para Ruby

Restricciones a la autenticación de bases de datos de IAM

Si utiliza la autenticación de base de datos de IAM, se aplicarán las siguientes limitaciones:

- La autenticación de bases de datos de IAM limita las conexiones a 200 conexiones por segundo.

  Las conexiones que utilizan el mismo token de autenticación no se limitan. Se recomienda reutilizar los tokens de autenticación siempre que sea posible.

- Actualmente, la autenticación de base de datos de IAM no admite todas las claves de contexto de condición global.

  Para obtener más información sobre las claves de condición globales, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.
- Para PostgreSQL, si se agrega el rol de IAM (`rds_iam`) a un usuario (incluido el usuario maestro de RDS), la autenticación de IAM tiene prioridad sobre la autenticación de la contraseña, por lo que el usuario debe iniciar sesión como un usuario de IAM.
- Para PostgreSQL, Amazon RDS no admite habilitar los métodos de autenticación de IAM y Kerberos al mismo tiempo.
- En el caso de PostgreSQL, no puede utilizar la autenticación de IAM para establecer una conexión de replicación.
- No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.
- CloudWatch y CloudTrail no registran la autenticación de IAM. Estos servicios no rastrean las llamadas a la API `generate-db-auth-token` que autorizan a la función de IAM a habilitar la conexión a la base de datos.
- La autenticación de la base de datos de IAM requiere recursos informáticos en la instancia de la base de datos. Debe tener entre 300 MiB y 1000 MiB de memoria adicional en la base de datos para obtener una conectividad fiable. Para ver la memoria necesaria para la carga de trabajo, compare la columna RES de los procesos RDS en la lista de procesos de supervisión mejorada antes y después de habilitar la autenticación de bases de datos de IAM. Consulte Visualización de métricas OS en la consola de RDS.

  Si está utilizando una instancia de clase ampliable, evite quedarse sin memoria mediante la reducción de la memoria utilizada por otros parámetros como búferes y caché en la misma cantidad.
- En el caso de RDS para MySQL, no puede utilizar la autenticación basada en contraseñas para un usuario de base de datos que configure con la autenticación de IAM.
- La autenticación de base de datos de IAM no es compatible con RDS en Outposts para ningún motor.

Recomendaciones para la autenticación de base de datos de IAM

Recomendamos lo siguiente cuando se utiliza la autenticación de base de datos de IAM:

- Utilice la autenticación de base de datos de IAM cuando la aplicación necesite menos de 200 conexiones nuevas por segundo para la autenticación de bases de datos de IAM.

  Los motores de base de datos que funcionan con Amazon RDS no imponen ninguna restricción a los intentos de autenticación por segundo. Sin embargo, al usar la autenticación de bases de datos de IAM, su aplicación debe generar un token de autenticación. A continuación, su aplicación usa ese token para conectarse a la instancia. Si supera el límite máximo de nuevas conexiones por segundo, la sobrecarga adicional de la autenticación de bases de datos de IAM puede dar lugar a la limitación controlada de las conexiones.

  Considere la posibilidad de utilizar la agrupación de conexiones en sus aplicaciones para mitigar la creación constante de conexiones. Esto puede reducir la sobrecarga de la autenticación de bases de datos de IAM y permitir que las aplicaciones reutilicen las conexiones existentes. De forma alternativa, también puede utilizar RDS Proxy para estos casos de uso. RDS Proxy tiene costos adicionales. Consulte los precios de RDS Proxy.
- El tamaño de un token de autenticación de base de datos de IAM depende de muchos factores, como la cantidad de etiquetas de IAM, las políticas de servicio de IAM, las longitudes del ARN y otras propiedades de IAM y de la base de datos. El tamaño mínimo de este token suele ser de aproximadamente 1 KB, pero puede ser mayor. Dado que este token se utiliza como contraseña en la cadena de conexión a la base de datos mediante la autenticación de IAM, debe asegurarse de que ni el controlador de la base de datos (por ejemplo, ODBC) ni ninguna herramienta limiten ni trunquen de otro modo este token debido a su tamaño. Un token truncado provocará un error en la validación de autenticación que realiza la base de datos e IAM.
- Si utiliza credenciales temporales al crear un token de autenticación de base de datos de IAM, las credenciales temporales deben seguir siendo válidas cuando utilice el token de autenticación de base de datos de IAM para realizar una solicitud de conexión.

Claves de contexto de condición globales de AWS admitidas

La autenticación de base de datos de IAM no admite el siguiente subconjunto de claves de contexto de condición globales de AWS.

- `aws:Referer`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`

- `aws:UserAgent`
- `aws:VpcSourceIp`

Para obtener más información, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Activación y desactivación de la autenticación de bases de datos de IAM

De forma predeterminada, la autenticación de bases de datos de IAM está deshabilitada en las instancias de base de datos. Puede activar o desactivar la autenticación de bases de datos de IAM mediante la AWS Management Console, la AWS CLI o la API.

Puede habilitar la autenticación de base de datos de IAM cuando realice una de las siguientes acciones:

- Para crear una nueva instancia de base de datos con la autenticación de base de datos de IAM activada, consulte Creación de una instancia de base de datos de Amazon RDS.
- Para modificar una instancia de base de datos para activar la autenticación de base de datos de IAM, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Para restaurar una instancia de bases de datos a partir de una instantánea con la autenticación de base de datos de IAM activada, consulte Restauración a una instancia de base de datos.
- Para restaurar una instancia de base de datos a un momento dado con la autenticación de base de datos de IAM habilitada, consulte Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

La autenticación de IAM para instancias de base de datos PostgreSQL exige que el valor de SSL sea 1. No puede habilitar la autenticación de IAM para una instantánea de base de datos PostgreSQL si el valor de SSL es 0. No puede cambiar el valor de SSL a 0 si la autenticación de IAM está habilitada para una instancia de base de datos PostgreSQL.

Consola

Cada flujo de trabajo de creación o modificación tiene una sección Database authentication (Autenticación de base de datos), donde puede activar o desactivar la autenticación de base de datos de IAM. En esa sección, elija Password and IAM database authentication (Autenticación de bases de datos con contraseña e IAM) para activar la autenticación de base de datos de IAM.

Para activar o desactivar la autenticación de IAM para una instancia existente

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia que desea modificar.

> **Note**
>
> Asegúrese de que la instancia de base de datos sea compatible con la autenticación de IAM. Compruebe los requisitos de compatibilidad en Disponibilidad en regiones y versiones.

4. Elija Modify.
5. En la sección Database authentication (Autenticación de base de datos), elija Password and IAM database authentication (Autenticación de bases de datos con contraseña e IAM) para activar la autenticación de base de datos de IAM. Elija Autenticación con contraseña o Contraseña y autenticación Kerberos para deshabilitar la autenticación de IAM.
6. También puede elegir habilitar la publicación de registros de autenticación de bases de datos de IAM en Registros de CloudWatch. En Exportaciones de registros, elija la opción registro iam-db-auth-error. La publicación de los registros en Registros de CloudWatch consume almacenamiento y se generan cargos por dicho almacenamiento. Asegúrese de eliminar los Registros de CloudWatch que ya no necesite.
7. Elija Continue.
8. Para aplicar los cambios inmediatamente, elija Immediately (Inmediatamente) en la sección Scheduling of modifications (Programación de modificaciones).
9. Elija Modify DB instance (Modificar instancia de base de datos) .

AWS CLI

Para crear una instancia de base de datos nueva con la autenticación de IAM mediante la AWS CLI, use el comando `create-db-instance`. Especifique la opción `--enable-iam-database-authentication`, como se muestra en el siguiente ejemplo.

```
aws rds create-db-instance \
    --db-instance-identifier mydbinstance \
    --db-instance-class db.m3.medium \
```

```
    --engine MySQL \
    --allocated-storage 20 \
    --master-username masterawsuser \
    --manage-master-user-password \
    --enable-iam-database-authentication
```

Para actualizar una instancia de base de datos existente para que tenga o no tenga autenticación de IAM, utilice el comando AWS CLI de la `modify-db-instance`. Especifique la opción `--enable-iam-database-authentication` o `--no-enable-iam-database-authentication`, como proceda.

> **Note**
>
> Asegúrese de que la instancia de base de datos sea compatible con la autenticación de IAM. Compruebe los requisitos de compatibilidad en Disponibilidad en regiones y versiones.

De forma predeterminada, Amazon RDS realiza la modificación durante el siguiente periodo de mantenimiento. Si desea invalidar esto y habilitar la autenticación de bases de datos de IAM lo antes posible, use el parámetro `--apply-immediately`.

En el siguiente ejemplo se muestra cómo habilitar inmediatamente la autenticación de IAM para una instancia de base de datos existente.

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --apply-immediately \
    --enable-iam-database-authentication
```

Si restaura una instancia, use uno de los siguientes comandos de AWS CLI:

- `restore-db-instance-to-point-in-time`
- `restore-db-instance-from-db-snapshot`

De forma predeterminada, la configuración de la autenticación de bases de datos de IAM será la de la instantánea de origen. Para cambiar esta configuración, establezca la opción `--enable-iam-database-authentication` o `--no-enable-iam-database-authentication`, como proceda.

API de RDS

Para crear una instancia de base de datos nueva con la autenticación de IAM mediante la API, use la operación de la API `CreateDBInstance`. Defina el parámetro `EnableIAMDatabaseAuthentication` como `true`.

Para actualizar una instancia de base de datos existente para que tenga o no tenga autenticación de IAM, utilice la operación de la API `ModifyDBInstance`. Establezca el parámetro `EnableIAMDatabaseAuthentication` en `true` para habilitar la autenticación de IAM o en `false` para deshabilitarla.

> **Note**
>
> Asegúrese de que la instancia de base de datos sea compatible con la autenticación de IAM. Compruebe los requisitos de compatibilidad en Disponibilidad en regiones y versiones.

Si restaura una instancia, use una de las siguientes operaciones de la API:

- `RestoreDBInstanceFromDBSnapshot`
- `RestoreDBInstanceToPointInTime`

De forma predeterminada, la configuración de la autenticación de bases de datos de IAM será la de la instantánea de origen. Para cambiar esta configuración, establezca el parámetro `EnableIAMDatabaseAuthentication` en `true` para habilitar la autenticación de IAM o `false` para deshabilitarla.

Creación y uso de una política de IAM para el acceso a bases de datos de IAM

Para permitir a un usuario o rol conectarse a su instancia de base de datos, debe crear una política de IAM. Después de eso, puede asociar la política a un conjunto de permisos o un rol.

> **Note**
>
> Para obtener más información acerca de las políticas de IAM, consulte Administración de la identidad y el acceso en Amazon RDS.

La siguiente política de ejemplo permite a un usuario conectarse a una instancia de base de datos mediante la autenticación de bases de datos de IAM.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:1234567890:dbuser:db-ABCDEFGHIJKL01234/
db_user"
         ]
      }
   ]
}
```

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:1234567890:dbuser:cluster-
ABCDEFGHIJKL01234/db_user"
         ]
      }
   ]
}
```

> **Important**
>
> Un usuario con permisos de administrador puede acceder a las instancias de base de datos sin permiso explícito en una política de IAM. Si desea restringir el acceso del administrador a los de instancias de base de datos, puede crear un rol de IAM con los permisos privilegiados menores y asignarlo al administrador.

> **Note**
>
> No confunda el prefijo `rds-db:` con otros prefijos de operación de la API de RDS que empiezan por `rds:`. Puede usar el prefijo `rds-db:` y la acción `rds-db:connect` solo para la autenticación de bases de datos de IAM. No son válidos en ningún otro contexto.

La política de ejemplo incluye una sola instrucción con los siguientes elementos:

- `Effect`: especifique `Allow` para conceder acceso a la instancia. Si no permite el acceso de forma explícita, el acceso se deniega de forma predeterminada.
- `Action`: especifique `rds-db:connect` para permitir las conexiones a la instancia.
- `Resource`: especifique un nombre de recurso de Amazon (ARN) que describa una cuenta de base de datos en una instancia. El formato del ARN es el siguiente.

```
arn:aws:rds-db:region:account-id:dbuser:DbiResourceId/db-user-name
```

  En este formato, reemplace lo siguiente:

  - *`region`* es la región de AWS para la instancia y . En la política de ejemplo, la región de AWS es `us-east-2`.
  - *`account-id`* es el número de cuenta de AWS para la instancia y . En la política de ejemplo, el número de cuenta es `1234567890`. El usuario debe estar en la misma cuenta que la cuenta de la instancia de base de datos.

    Para realizar el acceso entre cuentas, cree un rol de IAM con la política que se muestra arriba en la cuenta para la instancia de base de datos y permita que su otra cuenta asuma el rol.

- *DbiResourceId* es el identificador de la instancia. Este identificador es único para una región de AWS y nunca cambia. En la política de ejemplo, el identificador es db-ABCDEFGHIJKL01234.

  Para buscar un ID de recurso de instancia en la AWS Management Console de Amazon RDS, elija la instancia para ver los detalles. A continuación, elija la pestaña Configuration (Configuración). El Resource ID (ID de recurso) se muestra en la sección Configuration (Configuración).

  También puede usar el comando de la AWS CLI para enumerar los identificadores e ID de recurso para todas sus instancias y de base de datos en la región de AWS actual, como se muestra a continuación.

  ```
  aws rds describe-db-instances --query "DBInstances[*].
  [DBInstanceIdentifier,DbiResourceId]"
  ```

  Si utiliza Amazon Aurora, especifique un `DbClusterResourceId` en lugar de un `DbiResourceId`. Para obtener más información, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM en la Guía del usuario de Amazon Aurora.

  > **Note**
  >
  > Si se está conectando a una base de datos a través del proxy de RDS, especifique el ID del recurso proxy; por ejemplo, `prx-ABCDEFGHIJKL01234`. Para obtener información sobre el uso de la autenticación de bases de datos de IAM con el proxy de RDS, consulte Conexión a un proxy mediante autenticación de IAM.

- *db-user-name* es el nombre de la cuenta de base de datos que se asociará a la autenticación de IAM. En la política de ejemplo, la cuenta de base de datos es `db_user`.

Puede crear otros ARN que admitan diversos patrones de acceso. La siguiente política permite el acceso a dos cuentas de base de datos diferentes en una instancia de base de datos.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:db-ABCDEFGHIJKL01234/
jane_doe",
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:db-ABCDEFGHIJKL01234/
mary_roe"
         ]
      }
   ]
}
```

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:cluster-
ABCDEFGHIJKL01234/jane_doe",
             "arn:aws:rds-db:us-east-2:123456789012:dbuser:cluster-
ABCDEFGHIJKL01234/mary_roe"
         ]
      }
   ]
}
```

La siguiente política usa el carácter "*" a fin de buscar coincidencias con todas las instancias y de base de datos y cuentas de base de datos para una cuenta de AWS y una región de AWS determinadas.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds-db:connect"
            ],
            "Resource": [
                "arn:aws:rds-db:us-east-2:1234567890:dbuser:*/*"
            ]
        }
    ]
}
```

La siguiente política busca coincidencias con todas las instancias y de base de datos para una cuenta de AWS y una región de AWS determinadas. Sin embargo, la política solo concede acceso a instancias de base de datos que tienen una cuenta de base de datos `jane_doe`.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
             "rds-db:connect"
         ],
         "Resource": [
```

```
            "arn:aws:rds-db:us-east-2:123456789012:dbuser:*/jane_doe"
        ]
      }
   ]
}
```

El usuario o el rol solo tiene acceso a las mismas bases de datos que el usuario de la base de datos. Por ejemplo, suponga que su instancia tiene una base de datos denominada dev y otra llamada test. Si el usuario de base de datos `jane_doe` solo tiene acceso a dev, cualquier usuario o rol que obtenga acceso a esa instancia de base de datos con el usuario `jane_doe` también tendrá acceso únicamente a dev. Esta restricción del acceso también se aplica a otros objetos de la base de datos tales como tablas, vistas, etc.

Un administrador debe crear políticas de IAM que concedan permisos a las entidades para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe asociar esas políticas a los conjuntos de permisos o roles que necesiten esos permisos. Para ver algunos ejemplos de políticas, consulte Ejemplos de políticas basadas en identidad para Amazon RDS.

Asociación de una política de IAM a un conjunto de permisos o un rol

Tras crear una política de IAM que permita la autenticación de bases de datos, es necesario asociar la política a un conjunto de permisos o un rol. Para ver un tutorial acerca de este tema, consulte Crear y asociar su primera política administrada por el cliente en la Guía del usuario de IAM.

Mientras realiza el tutorial, puede usar uno de los ejemplos de política mostrados en esta sección como punto de partida y adaptarlo a sus necesidades. Al final del tutorial, tiene un conjunto de permisos con una política asociada que puede utilizar la acción `rds-db:connect`.

> **Note**
>
> Puede asignar varios conjuntos de permisos o roles a la misma cuenta de usuario de base de datos. Por ejemplo, suponga que su política de IAM ha especificado el siguiente ARN del recurso.
>
> ```
> arn:aws:rds-db:us-east-2:123456789012:dbuser:db-12ABC34DEFG5HIJ6KLMNOP78QR/
> jane_doe
> ```

Si adjunta la política a los usuarios Jane, Bob y Diego, cada uno de esos usuarios puede conectarse a la instancia de base de datos especificado por medio de la cuenta de la base de datos de `jane_doe`.

Creación de cuentas de base de datos utilizando autenticación de IAM

Con la autenticación de bases de datos de IAM, no es necesario asignar contraseñas de la base de datos a las cuentas de usuario creadas. Si quita un usuario asignado a una cuenta de base de datos, también debe quitar la cuenta de base de datos con la instrucción `DROP USER`.

> **Note**
>
> El nombre de usuario utilizado para la autenticación de IAM debe coincidir con el nombre de usuario en la base de datos.

Temas

- Uso de la autenticación de IAM con MariaDB y MySQL
- Uso de la autenticación de IAM con PostgreSQL

Uso de la autenticación de IAM con MariaDB y MySQL

Con MariaDB y MySQL, `AWSAuthenticationPlugin` gestiona la autenticación. Se trata de un complemento proporcionado por AWS que funciona perfectamente con IAM para autenticar a sus usuarios. Conecte al de instancias de base de datos como usuario maestro o como usuario diferente que pueda crear usuarios y conceder privilegios. Tras la conexión, lance la instrucción `CREATE USER`, tal como se muestra en el siguiente ejemplo.

```
CREATE USER 'jane_doe' IDENTIFIED WITH AWSAuthenticationPlugin AS 'RDS';
```

La cláusula `IDENTIFIED WITH` permite que MariaDB y MySQL usen `AWSAuthenticationPlugin` para autenticar la cuenta de base de datos (`jane_doe`). La cláusula de `AS 'RDS'` hace referencia al método de autenticación. Asegúrese de que el nombre de usuario de la base de datos especificado

sea igual a un recurso de la política de IAM para el acceso a la base de datos de IAM. Para obtener más información, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM.

> **Note**
>
> Si ve el siguiente mensaje, significa que el complemento proporcionado por AWS no está disponible para la instanciay actual.
> `ERROR 1524 (HY000): Plugin 'AWSAuthenticationPlugin' is not loaded`
> Para identificar este error, verifique que usa una configuración admitida y que ha habilitado la autenticación de bases de datos de IAM en su instancia. Para obtener más información, consulte Disponibilidad en regiones y versiones y Activación y desactivación de la autenticación de bases de datos de IAM.

Después de crear una cuenta mediante `AWSAuthenticationPlugin`, puede administrarla de la misma forma que otras cuentas de base de datos. Por ejemplo, puede modificar los privilegios de cuenta con las instrucciones `GRANT` y `REVOKE`, o bien modificar diversos atributos de cuenta con la instrucción `ALTER USER`.

El tráfico de la red de la base de datos se cifra mediante SSL/TLS cuando se utiliza IAM. Para permitir las conexiones SSL, modifique la cuenta de usuario con el siguiente comando.

```
ALTER USER 'jane_doe'@'%' REQUIRE SSL;
```

Uso de la autenticación de IAM con PostgreSQL

Para usar la autenticación de IAM con PostgreSQL, conéctese a la instancia de base de datos como usuario maestro o como usuario diferente que pueda crear usuarios y conceder privilegios. Tras la conexión, cree usuarios de base de datos y, a continuación, concédales el rol `rds_iam` tal como se muestra en el siguiente ejemplo.

```
CREATE USER db_userx;
GRANT rds_iam TO db_userx;
```

Asegúrese de que el nombre de usuario de la base de datos especificado sea igual a un recurso de la política de IAM para el acceso a la base de datos de IAM. Para obtener más información, consulte Creación y uso de una política de IAM para el acceso a bases de datos de IAM. Debe conceder el

rol `rds_iam` para utilizar la autenticación de IAM. También puede utilizar suscripciones anidadas o concesiones indirectas del rol.

Conexión a la instancia con la autenticación de IAM

Con la autenticación de bases de datos de IAM, puede usar un token de autenticación al conectarse a su instancia. Un token de autenticación es una cadena de caracteres que usa en lugar de una contraseña. Después de generar un token de autenticación, será válido durante 15 minutos antes de caducar. Si intenta conectarse mediante un token caducado, la solicitud de conexión se deniega.

Todos los tokens de autenticación deben ir acompañados de una firma válida, mediante AWS Signature versión 4. (Para obtener más información, consulte Proceso de firma Signature Version 4 en la Referencia general de AWS.). AWS CLI y un SDK de AWS, como AWS SDK para Java o AWS SDK para Python (Boto3), pueden firmar automáticamente cada token que cree.

Puede utilizar un token de autenticación cuando se conecte a Amazon RDS desde otro servicio de AWS, como AWS Lambda. Al utilizar un token, puede evitar introducir una contraseña en el código. De forma opcional, puede usar un SDK de AWS para crear y firmar mediante programación un token de autenticación.

Una vez que tenga un token de autenticación de IAM firmado, podrá conectarse a una instancia de base de datos de Amazon RDS. A continuación, puede aprender cómo hacer esto mediante una herramienta de línea de comandos o un SDK de AWS, como AWS SDK para Java o AWS SDK para Python (Boto3).

Para obtener más información, consulte las siguientes entradas del blog:

- Use IAM authentication to connect with SQL Workbench/J to Aurora MySQL or Amazon RDS for MySQL
- Using IAM authentication to connect with pgAdmin Amazon Aurora PostgreSQL or Amazon RDS para PostgreSQL (Usar la autenticación de IAM para conectar pgAdmin con Amazon Aurora PostgreSQL o Amazon RDS para PostgreSQL)

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM

- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM

Temas

- Conexión a su de instancia de base de datos mediante la autenticación IAM con los controladores de AWS
- Conexión a su instancia con autenticación de IAM desde la línea de comandos: AWS CLI y cliente de MySQL
- Conexión a su instancia desde la línea de comandos: AWS CLI y psql Client
- Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para .NET
- Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para Go
- Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para Java
- Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para Python (Boto3)

Conexión a su de instancia de base de datos mediante la autenticación IAM con los controladores de AWS

El conjunto de controladores de AWS se ha diseñado para permitir tiempos de transición y conmutación por error más rápidos y autenticarse con AWS Secrets Manager, AWS Identity and Access Management (IAM) e identidad federada. Los controladores de AWS se basan en la supervisión del estado de la instancia de base de datos y en el conocimiento de la topología de la instancia para determinar quién es el nuevo escritor. Este enfoque reduce los tiempos de transición y conmutación por error a segundos de un solo dígito, en comparación con las decenas de segundos de los controladores de código abierto.

Para obtener más información sobre los controladores de AWS, consulte el controlador de idioma correspondiente de su instancia de base de datos RDS para MariaDB, RDS para MySQL o RDS para PostgreSQL.

> **Note**
>
> Las únicas características que se admiten con RDS para MariaDB son la autenticación con AWS Secrets Manager, AWS Identity and Access Management (IAM) y la identidad federada.

Conexión a su instancia con autenticación de IAM desde la línea de comandos: AWS CLI y cliente de MySQL

Puede conectarse desde la línea de comando a una instancia de base de datos de Amazon RDScon AWS CLI y la herramienta de línea de comandos de `mysql` como se describe a continuación.

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM

> **Note**
>
> Para obtener información sobre cómo conectarse a la base de datos mediante SQL Workbench/J con la autenticación IAM, consulte la publicación de blog Use IAM authentication to connect with SQL Workbench/J to Aurora MySQL or Amazon RDS for MySQL.

Temas

- Generación de un token de autenticación de IAM
- Conexión a su instancia

Generación de un token de autenticación de IAM

En el siguiente ejemplo se muestra cómo obtener un token de autenticación firmado mediante la AWS CLI.

```
aws rds generate-db-auth-token \
   --hostname rdsmysql.123456789012.us-west-2.rds.amazonaws.com \
   --port 3306 \
   --region us-west-2 \
   --username jane_doe
```

En el ejemplo, los parámetros son los siguientes:

- `--hostname`: el nombre de host de la instancia a los que desea obtener acceso.
- `--port`: el número de puerto que se utiliza para conectarse a la instancia.
- `--region`: la región de AWS en la que se ejecuta la instancia
- `--username`: la cuenta de base de datos a la que desea acceder.

Los primeros caracteres del token tienen un aspecto similar al siguiente.

```
rdsmysql.123456789012.us-west-2.rds.amazonaws.com:3306/?
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

Conexión a su instancia

El formato general para conectarse se muestra a continuación.

```
mysql --host=hostName --port=portNumber --ssl-ca=full_path_to_ssl_certificate --enable-
cleartext-plugin --user=userName --password=authToken
```

Los parámetros son los siguientes:

- `--host`: el nombre de host de la instancia a los que desea obtener acceso.
- `--port`: el número de puerto que se utiliza para conectarse a la instancia.
- `--ssl-ca`: la ruta completa al archivo de certificado SSL que contiene la clave pública

  Para obtener más información sobre la compatibilidad con SSL/TLS para MariaDB, consulte Compatibilidad con SSL/TLS para instancias de base de datos de MariaDB en Amazon RDS.

  Para obtener más información sobre la compatibilidad con SSL/TLS para MySQL, consulte Compatibilidad de SSL/TLS con instancias de bases de datos de MySQL en Amazon RDS.

Para descargar un certificado SSL, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

- `--enable-cleartext-plugin`: un valor que especifica que `AWSAuthenticationPlugin` debe usarse para esta conexión.

  Si está utilizando un cliente MariaDB, la opción `--enable-cleartext-plugin` no es necesaria.
- `--user`: la cuenta de base de datos a la que desea acceder.
- `--password`: un token de autenticación de IAM firmado.

El token de autenticación consta de varios cientos de caracteres. Puede ser difícil de tratar en la línea de comando. Una forma de solucionar esto es guardar el token en una variable de entorno y, a continuación, usar esa variable al conectarse. En el siguiente ejemplo se muestra una forma de realizar esta alternativa. En el ejemplo, */sample_dir/* es la ruta completa al archivo de certificado SSL que contiene la clave pública.

```
RDSHOST="mysqldb.123456789012.us-east-1.rds.amazonaws.com"
TOKEN="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 3306 --region us-
west-2 --username jane_doe )"

mysql --host=$RDSHOST --port=3306 --ssl-ca=/sample_dir/global-bundle.pem --enable-
cleartext-plugin --user=jane_doe --password=$TOKEN
```

Al conectarse mediante `AWSAuthenticationPlugin`, la conexión está protegida mediante SSL. Para verificar esto, escriba lo siguiente en el símbolo del sistema `mysql>`.

```
show status like 'Ssl%';
```

En las siguientes líneas de la salida aparecen más detalles.

```
+---------------+-------------+
| Variable_name | Value

                                                                    |

+---------------+-------------+
| ...           | ...
```

```
| Ssl_cipher     | AES256-SHA

                                                                    |
| ...            | ...
| Ssl_version    | TLSv1.1

                                                                    |
| ...            | ...
+----------------------------+
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Conexión a su instancia desde la línea de comandos: AWS CLI y psql Client

Puede conectarse desde la línea de comando a una instancia de base de datos de Amazon RDS para PostgreSQL con AWS CLI y la herramienta de línea de comandos psql como se describe a continuación.

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM

> **Note**
>
> Para obtener información acerca de cómo conectarse a la base de datos mediante pgAdmin con la autenticación IAM, consulte la entrada de blog Use IAM authentication to connect with pgAdmin to Amazon Aurora PostgreSQL or Amazon RDS for PostgreSQL (Usar la autenticación de IAM para conectarse con pgAdmin a Amazon Aurora PostgreSQL o Amazon RDS for PostgreSQL).

Temas

- Generación de un token de autenticación de IAM

- Conexión a una instancia de base de datos de PostgreSQL en Amazon RDS

Generación de un token de autenticación de IAM

El token de autenticación consta de varios cientos de caracteres por que puede ser difícil de tratar en la línea de comando. Una forma de solucionar esto es guardar el token en una variable de entorno y, a continuación, usar esa variable al conectarse. En el siguiente ejemplo se muestra cómo usar la AWS CLI para obtener un token de autenticación firmado mediante el comando `generate-db-auth-token` y almacenarlo en una variable de entorno `PGPASSWORD`.

```
export RDSHOST="rdspostgres.123456789012.us-west-2.rds.amazonaws.com"
export PGPASSWORD="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 5432 --
region us-west-2 --username jane_doe )"
```

En el ejemplo, los parámetros para el comando `generate-db-auth-token` son los siguientes:

- `--hostname`: el nombre de host de la instancia de base de datos a los que desea obtener acceso.
- `--port`: el número de puerto que se utiliza para conectarse a la instancia.
- `--region`: la región de AWS en la que se ejecuta la instancia
- `--username`: la cuenta de base de datos a la que desea acceder.

Los primeros caracteres del token generado tienen un aspecto similar al siguiente.

```
rdspostgres.123456789012.us-west-2.rds.amazonaws.com:5432/?
Action=connect&DBUser=jane_doe&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Expires=900...
```

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

Conexión a una instancia de base de datos de PostgreSQL en Amazon RDS

El formato general para usar psql para conectarse se muestra a continuación.

```
psql "host=hostName port=portNumber sslmode=verify-full
 sslrootcert=full_path_to_ssl_certificate dbname=DBName user=userName
 password=authToken"
```

Los parámetros son los siguientes:

- `host`: el nombre de host de la instancia de base de datos a los que desea obtener acceso.
- `port`: el número de puerto que se utiliza para conectarse a la instancia.
- `sslmode`: el modo de SSL que se debe utilizar.

  Cuando se utiliza `sslmode=verify-full`, la conexión SSL verifica el punto de conexión de la instancia con respecto al punto de enlace del certificado SSL.
- `sslrootcert`: la ruta completa al archivo de certificado SSL que contiene la clave pública

  Para obtener más información, consulte Uso de SSL con una instancia de base de datos PostgreSQL.

  Para descargar un certificado SSL, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.
- `dbname`: la base de datos a la que desea obtener acceso.
- `user`: la cuenta de base de datos a la que desea acceder.
- `password`: un token de autenticación de IAM firmado.

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

El siguiente ejemplo muestra el uso de psql para conectarse. En el ejemplo, psql utiliza la variable de entorno `RDSHOST` para el host y la variable de entorno `PGPASSWORD` para el token generado. Además, */sample_dir/* es la ruta completa al archivo de certificado SSL que contiene la clave pública.

```
export RDSHOST="rdspostgres.123456789012.us-west-2.rds.amazonaws.com"
export PGPASSWORD="$(aws rds generate-db-auth-token --hostname $RDSHOST --port 5432 --
region us-west-2 --username jane_doe )"
```

```
psql "host=$RDSHOST port=5432 sslmode=verify-full sslrootcert=/sample_dir/global-
bundle.pem dbname=DBName user=jane_doe password=$PGPASSWORD"
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para .NET

Puede conectarse a una instancia de base de datos de RDS for MariaDB, MySQL o PostgreSQL con el AWS SDK para .NET como se describe a continuación.

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM

Ejemplos

En los siguientes ejemplos de código, se muestra cómo se genera un token de autenticación y cómo se utiliza para conectarse a una instancia.

Para ejecutar este ejemplo de código, necesita AWS SDK para .NET, que se encuentra en el sitio de AWS. Los paquetes `AWSSDK.CORE` y `AWSSDK.RDS` son necesarios. Para conectarse a una instancia de base de datos, use el conector de base de datos .NET para el motor de base de datos, como MySqlConnector para MariaDB o MySQL, o Npgsql para PostgreSQL.

Este código se conecta a una instancia de base de datos de MariaDB o MySQL. Modifique los valores de las siguientes variables según sea necesario:

- `server`: el punto de enlace de la instancia que desea acceder
- `user`: la cuenta de base de datos a la que desea acceder.
- `database`: la base de datos a la que desea obtener acceso.
- `port`: el número de puerto que se utiliza para conectarse a la instancia.
- `SslMode`: el modo de SSL que se debe utilizar.

Cuando se utiliza `SslMode=Required`, la conexión SSL verifica el punto de conexión de la instancia con respecto al punto de enlace del certificado SSL.

- `SslCa`: la ruta completa al certificado SSL de Amazon RDS

  Para descargar un certificado, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

```
using System;
using System.Data;
using MySql.Data;
using MySql.Data.MySqlClient;
using Amazon;

namespace ubuntu
{
  class Program
  {
    static void Main(string[] args)
    {
      var pwd =
 Amazon.RDS.Util.RDSAuthTokenGenerator.GenerateAuthToken(RegionEndpoint.USEast1,
 "mysqldb.123456789012.us-east-1.rds.amazonaws.com", 3306, "jane_doe");
      // for debug only Console.Write("{0}\n", pwd);  //this verifies the token is
 generated

      MySqlConnection conn = new MySqlConnection($"server=mysqldb.123456789012.us-
east-1.rds.amazonaws.com;user=jane_doe;database=mydB;port=3306;password={pwd};SslMode=Required;
      conn.Open();

      // Define a query
      MySqlCommand sampleCommand = new MySqlCommand("SHOW DATABASES;", conn);

      // Execute a query
      MySqlDataReader mysqlDataRdr = sampleCommand.ExecuteReader();
```

```
      // Read all rows and output the first column in each row
      while (mysqlDataRdr.Read())
        Console.WriteLine(mysqlDataRdr[0]);

      mysqlDataRdr.Close();
      // Close connection
      conn.Close();
    }
  }
}
```

Este código se conecta a una instancia de base de datos de PostgreSQL.

Modifique los valores de las siguientes variables según sea necesario:

- `Server`: el punto de enlace de la instancia que desea acceder
- `User ID`: la cuenta de base de datos a la que desea acceder.
- `Database`: la base de datos a la que desea obtener acceso.
- `Port`: el número de puerto que se utiliza para conectarse a la instancia.
- `SSL Mode`: el modo de SSL que se debe utilizar.

  Cuando se utiliza `SSL Mode=Required`, la conexión SSL verifica el punto de conexión de la instancia con respecto al punto de enlace del certificado SSL.
- `Root Certificate`: la ruta completa al certificado SSL de Amazon RDS

  Para descargar un certificado, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

```
using System;
using Npgsql;
using Amazon.RDS.Util;
```

```
namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            var pwd =
 RDSAuthTokenGenerator.GenerateAuthToken("postgresmydb.123456789012.us-
east-1.rds.amazonaws.com", 5432, "jane_doe");
// for debug only Console.Write("{0}\n", pwd);  //this verifies the token is generated

            NpgsqlConnection conn = new
 NpgsqlConnection($"Server=postgresmydb.123456789012.us-east-1.rds.amazonaws.com;User
 Id=jane_doe;Password={pwd};Database=mydb;SSL Mode=Require;Root
 Certificate=full_path_to_ssl_certificate");
            conn.Open();

            // Define a query
                   NpgsqlCommand cmd = new NpgsqlCommand("select count(*) FROM
 pg_user", conn);

            // Execute a query
            NpgsqlDataReader dr = cmd.ExecuteReader();

            // Read all rows and output the first column in each row
            while (dr.Read())
                Console.Write("{0}\n", dr[0]);

            // Close connection
            conn.Close();
        }
    }
}
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para Go

Puede conectarse a una instancia de base de datos de RDS for MariaDB, MySQL o PostgreSQL con el AWS SDK para Go como se describe a continuación.

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM

Ejemplos

Para ejecutar estos ejemplos de código, necesita AWS SDK para Go, que se encuentra en el sitio de AWS.

Modifique los valores de las siguientes variables según sea necesario:

- `dbName`: la base de datos a la que desea obtener acceso.
- `dbUser`: la cuenta de base de datos a la que desea acceder.
- `dbHost`: el punto de enlace de la instancia que desea acceder

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

- `dbPort`: el número de puerto que se utiliza para conectarse a la instancia.
- `region`: la región de AWS en la que se ejecuta la instancia

Además, debe asegurarse de que las bibliotecas importadas en el código de muestra existen en el sistema.

> **Important**
>
> En los ejemplos de esta sección se utiliza el código siguiente para proporcionar credenciales que tienen acceso a una base de datos desde un entorno local:
> `creds := credentials.NewEnvCredentials()`
> Si accede a una base de datos desde un servicio de AWS, como Amazon EC2 o Amazon ECS, puede reemplazar el código por el siguiente código:
> `sess := session.Must(session.NewSession())`

```
creds := sess.Config.Credentials
```

Si realiza este cambio, asegúrese de agregar la siguiente importación:

```
"github.com/aws/aws-sdk-go/aws/session"
```

Temas

- Conexión mediante la autenticación de IAM y el V2 AWS SDK para Go
- Conexión mediante la autenticación de IAM y el V1 AWS SDK para Go

Conexión mediante la autenticación de IAM y el V2 AWS SDK para Go

Se puede conectar a unclúster de base de datos mediante la autenticación de IAM y el V2AWS SDK para Go.

En los siguientes ejemplos de código, se muestra cómo se genera un token de autenticación y cómo se utiliza para conectarse a una instancia.

Este código se conecta a una instancia de base de datos de MariaDB o MySQL.

```
package main

import (
     "context"
     "database/sql"
     "fmt"

     "github.com/aws/aws-sdk-go-v2/config"
     "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
     _ "github.com/go-sql-driver/mysql"
)

func main() {

     var dbName string = "DatabaseName"
     var dbUser string = "DatabaseUser"
     var dbHost string = "mysqldb.123456789012.us-east-1.rds.amazonaws.com"
     var dbPort int = 3306
     var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
     var region string = "us-east-1"

    cfg, err := config.LoadDefaultConfig(context.TODO())
```

```
    if err != nil {
     panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
     context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
     panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
        dbUser, authenticationToken, dbEndpoint, dbName,
    )

    db, err := sql.Open("mysql", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Este código se conecta a una instancia de base de datos de PostgreSQL.

```
package main

import (
     "context"
     "database/sql"
     "fmt"

     "github.com/aws/aws-sdk-go-v2/config"
     "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
     _ "github.com/lib/pq"
)

func main() {

     var dbName string = "DatabaseName"
     var dbUser string = "DatabaseUser"
```

```
     var dbHost string = "postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
     var dbPort int = 5432
     var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
     var region string = "us-east-1"

    cfg, err := config.LoadDefaultConfig(context.TODO())
    if err != nil {
     panic("configuration error: " + err.Error())
    }

    authenticationToken, err := auth.BuildAuthToken(
     context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
    if err != nil {
     panic("failed to create authentication token: " + err.Error())
    }

    dsn := fmt.Sprintf("host=%s port=%d user=%s password=%s dbname=%s",
        dbHost, dbPort, dbUser, authenticationToken, dbName,
    )

    db, err := sql.Open("postgres", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Conexión mediante la autenticación de IAM y el V1 AWS SDK para Go

Conexión a una instancia mediante la autenticación de IAM y el V1 AWS SDK para Go

En los siguientes ejemplos de código, se muestra cómo se genera un token de autenticación y cómo se utiliza para conectarse a una instancia.

Este código se conecta a una instancia de base de datos de MariaDB o MySQL.

```
package main
```

```
import (
    "database/sql"
    "fmt"
    "log"

    "github.com/aws/aws-sdk-go/aws/credentials"
    "github.com/aws/aws-sdk-go/service/rds/rdsutils"
    _ "github.com/go-sql-driver/mysql"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "mysqldb.123456789012.us-east-1.rds.amazonaws.com"
    dbPort := 3306
    dbEndpoint := fmt.Sprintf("%s:%d", dbHost, dbPort)
    region := "us-east-1"

    creds := credentials.NewEnvCredentials()
    authToken, err := rdsutils.BuildAuthToken(dbEndpoint, region, dbUser, creds)
    if err != nil {
        panic(err)
    }

    dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
        dbUser, authToken, dbEndpoint, dbName,
    )

    db, err := sql.Open("mysql", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Este código se conecta a una instancia de base de datos de PostgreSQL.

```
package main
```

```
import (
 "database/sql"
 "fmt"

 "github.com/aws/aws-sdk-go/aws/credentials"
 "github.com/aws/aws-sdk-go/service/rds/rdsutils"
 _ "github.com/lib/pq"
)

func main() {
    dbName := "app"
    dbUser := "jane_doe"
    dbHost := "postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
    dbPort := 5432
    dbEndpoint := fmt.Sprintf("%s:%d", dbHost, dbPort)
    region := "us-east-1"

    creds := credentials.NewEnvCredentials()
    authToken, err := rdsutils.BuildAuthToken(dbEndpoint, region, dbUser, creds)
    if err != nil {
        panic(err)
    }

    dsn := fmt.Sprintf("host=%s port=%d user=%s password=%s dbname=%s",
        dbHost, dbPort, dbUser, authToken, dbName,
    )

    db, err := sql.Open("postgres", dsn)
    if err != nil {
        panic(err)
    }

    err = db.Ping()
    if err != nil {
        panic(err)
    }
}
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para Java

Puede conectarse a una instancia de base de datos de RDS for MariaDB, MySQL o PostgreSQL con el AWS SDK para Java como se describe a continuación.

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM
- Configurar el SDK de AWS para Java

Para ver ejemplos de cómo usar el SDK para Java 2.x, consulte Ejemplos de Amazon RDS que utilizan SDK para Java 2.x. También puede utilizar el contenedor JDBC avanzado de AWS; consulte la documentación del contenedor JDBC avanzado de AWS.

Temas

- Generación de un token de autenticación de IAM
- Creación manual de un token de autenticación de IAM
- Conexión a su instancia

Generación de un token de autenticación de IAM

Si escribe programas mediante AWS SDK para Java, puede obtener un token de autenticación firmado mediante la clase `RdsIamAuthTokenGenerator`. El uso de esta clase requiere que proporcione las credenciales de AWS. Para hacer esto, puede crear una instancia de la clase `DefaultAWSCredentialsProviderChain`. `DefaultAWSCredentialsProviderChain` usa la primera clave de acceso y clave secreta de AWS que encuentra en la cadena predeterminada de proveedores de credenciales. A fin de obtener más información acerca de las claves de acceso de AWS, consulte Administración de claves de acceso para usuarios.

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

Tras crear una instancia de `RdsIamAuthTokenGenerator`, puede llamar al método `getAuthToken` para obtener un token firmado. Proporcione la región de AWS el nombre de host, el número de puerto y el nombre de usuario. En el siguiente ejemplo de código se ilustra cómo hacerlo.

```
package com.amazonaws.codesamples;

import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.services.rds.auth.GetIamAuthTokenRequest;
import com.amazonaws.services.rds.auth.RdsIamAuthTokenGenerator;

public class GenerateRDSAuthToken {

    public static void main(String[] args) {

     String region = "us-west-2";
     String hostname = "rdsmysql.123456789012.us-west-2.rds.amazonaws.com";
     String port = "3306";
     String username = "jane_doe";

     System.out.println(generateAuthToken(region, hostname, port, username));
    }

   static String generateAuthToken(String region, String hostName, String port, String
 username) {

     RdsIamAuthTokenGenerator generator = RdsIamAuthTokenGenerator.builder()
      .credentials(new DefaultAWSCredentialsProviderChain())
      .region(region)
      .build();

     String authToken = generator.getAuthToken(
      GetIamAuthTokenRequest.builder()
      .hostname(hostName)
      .port(Integer.parseInt(port))
      .userName(username)
      .build());
```

```
     return authToken;
    }

}
```

Creación manual de un token de autenticación de IAM

En Java, la forma más sencilla de generar un token de autenticación es usar `RdsIamAuthTokenGenerator`. Esta clase crea automáticamente un token de autenticación y, a continuación, lo firma mediante AWS Signature versión 4. Para obtener más información, consulte Proceso de firma Signature Version 4 en la Referencia general de AWS.

Sin embargo, también puede crear y firmar un token de autenticación manualmente, como se muestra en el siguiente ejemplo de código.

```
package com.amazonaws.codesamples;

import com.amazonaws.SdkClientException;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.auth.SigningAlgorithm;
import com.amazonaws.util.BinaryUtils;
import org.apache.commons.lang3.StringUtils;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.nio.charset.Charset;
import java.security.MessageDigest;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.SortedMap;
import java.util.TreeMap;

import static com.amazonaws.auth.internal.SignerConstants.AWS4_TERMINATOR;
import static com.amazonaws.util.StringUtils.UTF8;

public class CreateRDSAuthTokenManually {
    public static String httpMethod = "GET";
    public static String action = "connect";
    public static String canonicalURIParameter = "/";
    public static SortedMap<String, String> canonicalQueryParameters = new TreeMap();
    public static String payload = StringUtils.EMPTY;
    public static String signedHeader = "host";
```

```
    public static String algorithm = "AWS4-HMAC-SHA256";
    public static String serviceName = "rds-db";
    public static String requestWithoutSignature;

    public static void main(String[] args) throws Exception {

        String region = "us-west-2";
        String instanceName = "rdsmysql.123456789012.us-west-2.rds.amazonaws.com";
        String port = "3306";
        String username = "jane_doe";

        Date now = new Date();
        String date = new SimpleDateFormat("yyyyMMdd").format(now);
        String dateTimeStamp = new
SimpleDateFormat("yyyyMMdd'T'HHmmss'Z'").format(now);
       DefaultAWSCredentialsProviderChain creds = new
DefaultAWSCredentialsProviderChain();
    String awsAccessKey = creds.getCredentials().getAWSAccessKeyId();
    String awsSecretKey = creds.getCredentials().getAWSSecretKey();
       String expiryMinutes = "900";

       System.out.println("Step 1:  Create a canonical request:");
       String canonicalString = createCanonicalString(username, awsAccessKey, date,
dateTimeStamp, region, expiryMinutes, instanceName, port);
       System.out.println(canonicalString);
       System.out.println();

       System.out.println("Step 2:  Create a string to sign:");
       String stringToSign = createStringToSign(dateTimeStamp, canonicalString,
awsAccessKey, date, region);
       System.out.println(stringToSign);
       System.out.println();

       System.out.println("Step 3:  Calculate the signature:");
       String signature = BinaryUtils.toHex(calculateSignature(stringToSign,
newSigningKey(awsSecretKey, date, region, serviceName)));
       System.out.println(signature);
       System.out.println();

       System.out.println("Step 4:  Add the signing info to the request");

       System.out.println(appendSignature(signature));
       System.out.println();
```

```
    }

    //Step 1: Create a canonical request date should be in format YYYYMMDD and dateTime
 should be in format YYYYMMDDTHHMMSSZ
    public static String createCanonicalString(String user, String accessKey, String
 date, String dateTime, String region, String expiryPeriod, String hostName, String
 port) throws Exception {
        canonicalQueryParameters.put("Action", action);
        canonicalQueryParameters.put("DBUser", user);
        canonicalQueryParameters.put("X-Amz-Algorithm", "AWS4-HMAC-SHA256");
        canonicalQueryParameters.put("X-Amz-Credential", accessKey + "%2F" + date +
"%2F" + region + "%2F" + serviceName + "%2Faws4_request");
        canonicalQueryParameters.put("X-Amz-Date", dateTime);
        canonicalQueryParameters.put("X-Amz-Expires", expiryPeriod);
        canonicalQueryParameters.put("X-Amz-SignedHeaders", signedHeader);
        String canonicalQueryString = "";
        while(!canonicalQueryParameters.isEmpty()) {
            String currentQueryParameter = canonicalQueryParameters.firstKey();
            String currentQueryParameterValue =
 canonicalQueryParameters.remove(currentQueryParameter);
            canonicalQueryString = canonicalQueryString + currentQueryParameter + "=" +
 currentQueryParameterValue;
            if (!currentQueryParameter.equals("X-Amz-SignedHeaders")) {
                canonicalQueryString += "&";
            }
        }
        String canonicalHeaders = "host:" + hostName + ":" + port + '\n';
        requestWithoutSignature = hostName + ":" + port + "/?" + canonicalQueryString;

        String hashedPayload = BinaryUtils.toHex(hash(payload));
        return httpMethod + '\n' + canonicalURIParameter + '\n' + canonicalQueryString
 + '\n' + canonicalHeaders + '\n' + signedHeader + '\n' + hashedPayload;

    }

    //Step 2: Create a string to sign using sig v4
    public static String createStringToSign(String dateTime, String canonicalRequest,
 String accessKey, String date, String region) throws Exception {
        String credentialScope = date + "/" + region + "/" + serviceName + "/
aws4_request";
        return algorithm + '\n' + dateTime + '\n' + credentialScope + '\n' +
 BinaryUtils.toHex(hash(canonicalRequest));

    }
```

```
    //Step 3: Calculate signature
    /**
     * Step 3 of the &AWS; Signature version 4 calculation. It involves deriving
     * the signing key and computing the signature. Refer to
     * http://docs.aws.amazon
     * .com/general/latest/gr/sigv4-calculate-signature.html
     */
    public static byte[] calculateSignature(String stringToSign,
                                            byte[] signingKey) {
        return sign(stringToSign.getBytes(Charset.forName("UTF-8")), signingKey,
                SigningAlgorithm.HmacSHA256);
    }

    public static byte[] sign(byte[] data, byte[] key,
                          SigningAlgorithm algorithm) throws SdkClientException {
        try {
            Mac mac = algorithm.getMac();
            mac.init(new SecretKeySpec(key, algorithm.toString()));
            return mac.doFinal(data);
        } catch (Exception e) {
            throw new SdkClientException(
                    "Unable to calculate a request signature: "
                            + e.getMessage(), e);
        }
    }

    public static byte[] newSigningKey(String secretKey,
                                   String dateStamp, String regionName, String
serviceName) {
        byte[] kSecret = ("AWS4" + secretKey).getBytes(Charset.forName("UTF-8"));
        byte[] kDate = sign(dateStamp, kSecret, SigningAlgorithm.HmacSHA256);
        byte[] kRegion = sign(regionName, kDate, SigningAlgorithm.HmacSHA256);
        byte[] kService = sign(serviceName, kRegion,
                SigningAlgorithm.HmacSHA256);
        return sign(AWS4_TERMINATOR, kService, SigningAlgorithm.HmacSHA256);
    }

    public static byte[] sign(String stringData, byte[] key,
                        SigningAlgorithm algorithm) throws SdkClientException {
        try {
            byte[] data = stringData.getBytes(UTF8);
            return sign(data, key, algorithm);
        } catch (Exception e) {
```

```
            throw new SdkClientException(
                    "Unable to calculate a request signature: "
                            + e.getMessage(), e);
        }
    }

    //Step 4: append the signature
    public static String appendSignature(String signature) {
        return requestWithoutSignature + "&X-Amz-Signature=" + signature;
    }

    public static byte[] hash(String s) throws Exception {
        try {
            MessageDigest md = MessageDigest.getInstance("SHA-256");
            md.update(s.getBytes(UTF8));
            return md.digest();
        } catch (Exception e) {
            throw new SdkClientException(
                    "Unable to compute hash while signing request: "
                            + e.getMessage(), e);
        }
    }
}
```

Conexión a su instancia

El siguiente ejemplo de código muestra cómo generar un token de autenticación y, a continuación, usarlo para conectarse a una instancia que ejecuta MariaDB o MySQL.

Para ejecutar este ejemplo de código, necesita AWS SDK para Java, que se encuentra en el sitio de AWS. Además, necesitará lo siguiente:

- MySQL Connector/J. Este ejemplo de código se ha probado con `mysql-connector-java-5.1.33-bin.jar`.
- Un certificado intermedio para Amazon RDS que es específico de una región de AWS. (Para obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.) En tiempo de ejecución, el cargador de clases busca el certificado en el mismo directorio que este ejemplo de código Java, de modo que el cargador de clases pueda encontrarlo.
- Modifique los valores de las siguientes variables según sea necesario:
  - `RDS_INSTANCE_HOSTNAME`: el nombre de anfitrión de la instancia que desea acceder.

- `RDS_INSTANCE_PORT`: el número de puerto usado para conectarse a la instancia de PostgreSQL.
- `REGION_NAME`: la región de AWS en la que se ejecuta la instancia.
- `DB_USER`: la cuenta de base de datos a la que desea acceder.
- `SSL_CERTIFICATE`: un certificado de SSL para Amazon RDS que es específico de una región de AWS.

  Para descargar un certificado para su región de AWS, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos. Coloque el certificado SSL en el mismo directorio que este archivo de programa Java, de modo que el cargador de clases pueda encontrar el certificado en tiempo de ejecución.

En este ejemplo de código, se obtienen las credenciales de AWS de la cadena predeterminada de proveedores de credenciales.

> **Note**
>
> Especifique una contraseña para `DEFAULT_KEY_STORE_PASSWORD` que no sea la que se muestra aquí como práctica recomendada de seguridad.

```
package com.amazonaws.samples;

import com.amazonaws.services.rds.auth.RdsIamAuthTokenGenerator;
import com.amazonaws.services.rds.auth.GetIamAuthTokenRequest;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.auth.AWSStaticCredentialsProvider;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.security.KeyStore;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
```

```
import java.sql.Statement;
import java.util.Properties;

import java.net.URL;

public class IAMDatabaseAuthenticationTester {
    //&AWS; Credentials of the IAM user with policy enabling IAM Database Authenticated
 access to the db by the db user.
    private static final DefaultAWSCredentialsProviderChain creds = new
 DefaultAWSCredentialsProviderChain();
    private static final String AWS_ACCESS_KEY =
 creds.getCredentials().getAWSAccessKeyId();
    private static final String AWS_SECRET_KEY =
 creds.getCredentials().getAWSSecretKey();

    //Configuration parameters for the generation of the IAM Database Authentication
 token
    private static final String RDS_INSTANCE_HOSTNAME = "rdsmysql.123456789012.us-
west-2.rds.amazonaws.com";
    private static final int RDS_INSTANCE_PORT = 3306;
    private static final String REGION_NAME = "us-west-2";
    private static final String DB_USER = "jane_doe";
    private static final String JDBC_URL = "jdbc:mysql://" + RDS_INSTANCE_HOSTNAME +
 ":" + RDS_INSTANCE_PORT;

    private static final String SSL_CERTIFICATE = "rds-ca-2019-us-west-2.pem";

    private static final String KEY_STORE_TYPE = "JKS";
    private static final String KEY_STORE_PROVIDER = "SUN";
    private static final String KEY_STORE_FILE_PREFIX = "sys-connect-via-ssl-test-
cacerts";
    private static final String KEY_STORE_FILE_SUFFIX = ".jks";
    private static final String DEFAULT_KEY_STORE_PASSWORD = "changeit";

    public static void main(String[] args) throws Exception {
        //get the connection
        Connection connection = getDBConnectionUsingIam();

        //verify the connection is successful
        Statement stmt= connection.createStatement();
        ResultSet rs=stmt.executeQuery("SELECT 'Success!' FROM DUAL;");
        while (rs.next()) {
             String id = rs.getString(1);
            System.out.println(id); //Should print "Success!"
```

```
        }

        //close the connection
        stmt.close();
        connection.close();

        clearSslProperties();

    }

    /**
     * This method returns a connection to the db instance authenticated using IAM
 Database Authentication
     * @return
     * @throws Exception
     */
    private static Connection getDBConnectionUsingIam() throws Exception {
        setSslProperties();
        return DriverManager.getConnection(JDBC_URL, setMySqlConnectionProperties());
    }

    /**
     * This method sets the mysql connection properties which includes the IAM Database
 Authentication token
     * as the password. It also specifies that SSL verification is required.
     * @return
     */
    private static Properties setMySqlConnectionProperties() {
        Properties mysqlConnectionProperties = new Properties();
        mysqlConnectionProperties.setProperty("verifyServerCertificate","true");
        mysqlConnectionProperties.setProperty("useSSL", "true");
        mysqlConnectionProperties.setProperty("user",DB_USER);
        mysqlConnectionProperties.setProperty("password",generateAuthToken());
        return mysqlConnectionProperties;
    }

    /**
     * This method generates the IAM Auth Token.
     * An example IAM Auth Token would look like follows:
     * btusi123.cmz7kenwo2ye.rds.cn-north-1.amazonaws.com.cn:3306/?
Action=connect&DBUser=iamtestuser&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Date=20171003T010726Z&X-Amz-SignedHeaders=host&X-Amz-Expires=899&X-Amz-
Credential=AKIAPFXHGVDI5RNFO4AQ%2F20171003%2Fcn-north-1%2Frds-db%2Faws4_request&X-Amz-
Signature=f9f45ef96c1f770cdad11a53e33ffa4c3730bc03fdee820cfdf1322eed15483b
```

```
     * @return
     */
    private static String generateAuthToken() {
        BasicAWSCredentials awsCredentials = new BasicAWSCredentials(AWS_ACCESS_KEY,
AWS_SECRET_KEY);

        RdsIamAuthTokenGenerator generator = RdsIamAuthTokenGenerator.builder()
                .credentials(new
AWSStaticCredentialsProvider(awsCredentials)).region(REGION_NAME).build();
        return generator.getAuthToken(GetIamAuthTokenRequest.builder()

.hostname(RDS_INSTANCE_HOSTNAME).port(RDS_INSTANCE_PORT).userName(DB_USER).build());
    }

    /**
     * This method sets the SSL properties which specify the key store file, its type
and password:
     * @throws Exception
     */
    private static void setSslProperties() throws Exception {
        System.setProperty("javax.net.ssl.trustStore", createKeyStoreFile());
        System.setProperty("javax.net.ssl.trustStoreType", KEY_STORE_TYPE);
        System.setProperty("javax.net.ssl.trustStorePassword",
DEFAULT_KEY_STORE_PASSWORD);
    }

    /**
     * This method returns the path of the Key Store File needed for the SSL
verification during the IAM Database Authentication to
     * the db instance.
     * @return
     * @throws Exception
     */
    private static String createKeyStoreFile() throws Exception {
        return createKeyStoreFile(createCertificate()).getPath();
    }

    /**
     *  This method generates the SSL certificate
     * @return
     * @throws Exception
     */
    private static X509Certificate createCertificate() throws Exception {
        CertificateFactory certFactory = CertificateFactory.getInstance("X.509");
```

```
        URL url = new File(SSL_CERTIFICATE).toURI().toURL();
        if (url == null) {
            throw new Exception();
        }
        try (InputStream certInputStream = url.openStream()) {
            return (X509Certificate) certFactory.generateCertificate(certInputStream);
        }
    }

    /**
     * This method creates the Key Store File
     * @param rootX509Certificate - the SSL certificate to be stored in the KeyStore
     * @return
     * @throws Exception
     */
    private static File createKeyStoreFile(X509Certificate rootX509Certificate) throws
 Exception {
        File keyStoreFile = File.createTempFile(KEY_STORE_FILE_PREFIX,
 KEY_STORE_FILE_SUFFIX);
        try (FileOutputStream fos = new FileOutputStream(keyStoreFile.getPath())) {
            KeyStore ks = KeyStore.getInstance(KEY_STORE_TYPE, KEY_STORE_PROVIDER);
            ks.load(null);
            ks.setCertificateEntry("rootCaCertificate", rootX509Certificate);
            ks.store(fos, DEFAULT_KEY_STORE_PASSWORD.toCharArray());
        }
        return keyStoreFile;
    }

    /**
     * This method clears the SSL properties.
     * @throws Exception
     */
    private static void clearSslProperties() throws Exception {
           System.clearProperty("javax.net.ssl.trustStore");
           System.clearProperty("javax.net.ssl.trustStoreType");
           System.clearProperty("javax.net.ssl.trustStorePassword");
    }

}
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Conexión la instancia de base de datos mediante la autenticación de IAM y el AWS SDK para Python (Boto3)

Puede conectarse a una instancia de base de datos de RDS for MariaDB, MySQL o PostgreSQL con el AWS SDK para Python (Boto3) como se describe a continuación.

Requisitos previos

A continuación, se muestran requisitos previos para conectarse al de instancia de base de datos mediante la autenticación de IAM:

- Activación y desactivación de la autenticación de bases de datos de IAM
- Creación y uso de una política de IAM para el acceso a bases de datos de IAM
- Creación de cuentas de base de datos utilizando autenticación de IAM

Además, debe asegurarse de que las bibliotecas importadas en el código de muestra existen en el sistema.

Ejemplos

Los ejemplos de código utilizan perfiles para credenciales compartidas. Para obtener información acerca de la especificación de credenciales, consulte Credenciales en la documentación de AWS SDK para Python (Boto3).

En los siguientes ejemplos de código, se muestra cómo se genera un token de autenticación y cómo se utiliza para conectarse a una instancia.

Para ejecutar este ejemplo de código, necesita AWS SDK para Python (Boto3), que se encuentra en el sitio de AWS.

Modifique los valores de las siguientes variables según sea necesario:

- `ENDPOINT`: el punto de enlace de la instancia que desea acceder
- `PORT`: el número de puerto que se utiliza para conectarse a la instancia.
- `USER`: la cuenta de base de datos a la que desea acceder.
- `REGION`: la región de AWS en la que se ejecuta la instancia
- `DBNAME`: la base de datos a la que desea obtener acceso.
- `SSLCERTIFICATE`: la ruta completa al certificado SSL de Amazon RDS

Para `ssl_ca`, especifique un certificado SSL. Para descargar un certificado SSL, consulte Uso de SSL/TLS para cifrar una conexión a una instancia o clúster de base de datos.

> **Note**
>
> No puede utilizar un registro DNS personalizado de Route 53 en lugar del punto de conexión de la instancia de base de datos para generar el token de autenticación.

Este código se conecta a una instancia de base de datos de MariaDB o MySQL.

Antes de ejecutar este código, siga las instrucciones del índice del paquete de Python para instalar el controlador PyMySQL.

```
import pymysql
import sys
import boto3
import os

ENDPOINT="mysqldb.123456789012.us-east-1.rds.amazonaws.com"
PORT="3306"
USER="jane_doe"
REGION="us-east-1"
DBNAME="mydb"
os.environ['LIBMYSQL_ENABLE_CLEARTEXT_PLUGIN'] = '1'

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='default')
client = session.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USER,
 Region=REGION)

try:
    conn =
 pymysql.connect(auth_plugin_map={'mysql_clear_password':None},host=ENDPOINT,
 user=USER, password=token, port=PORT, database=DBNAME, ssl_ca='SSLCERTIFICATE',
 ssl_verify_identity=True, ssl_verify_cert=True)
    cur = conn.cursor()
    cur.execute("""SELECT now()""")
    query_results = cur.fetchall()
```

```
    print(query_results)
except Exception as e:
    print("Database connection failed due to {}".format(e))
```

Este código se conecta a una instancia de base de datos de PostgreSQL.

Antes de ejecutar este código, instale `psycopg2` y siga las instrucciones en Psycopg documentation (Documentación de Psycopg).

```
import psycopg2
import sys
import boto3
import os

ENDPOINT="postgresmydb.123456789012.us-east-1.rds.amazonaws.com"
PORT="5432"
USER="jane_doe"
REGION="us-east-1"
DBNAME="mydb"

#gets the credentials from .aws/credentials
session = boto3.Session(profile_name='RDSCreds')
client = session.client('rds')

token = client.generate_db_auth_token(DBHostname=ENDPOINT, Port=PORT, DBUsername=USER,
 Region=REGION)

try:
    conn = psycopg2.connect(host=ENDPOINT, port=PORT, database=DBNAME, user=USER,
 password=token, sslrootcert="SSLCERTIFICATE")
    cur = conn.cursor()
    cur.execute("""SELECT now()""")
    query_results = cur.fetchall()
    print(query_results)
except Exception as e:
    print("Database connection failed due to {}".format(e))
```

Si desea conectarse a una instancia de base de datos a través de un proxy, consulte Conexión a un proxy mediante autenticación de IAM.

Solución de problemas de autenticación de bases de datos de IAM

A continuación, encontrará ideas para la solución de problemas comunes de autenticación de bases de datos de IAM e información sobre los registros y métricas de CloudWatch para la autenticación de base de datos de IAM.

Exportación de registros de errores de autenticación de bases de datos de IAM a Registros de CloudWatch

Los registros de errores de autenticación de bases de datos de IAM se almacenan en el host de base de datos y puede exportar estos registros a la cuenta de Registros de CloudWatch. Utilice los registros y métodos de solución de esta página para solucionar los problemas de autenticación de bases de datos de IAM.

Puede habilitar la exportación de registros a Registros de CloudWatch desde la consola, la AWS CLI y la API de RDS. Para obtener instrucciones sobre la consola, consulte Publicación de registros de base de datos en registros de Amazon Cloudwatch.

Para exportar los registros de errores de autenticación de bases de datos de IAM a Registros de CloudWatch al crear una instancia de base de datos desde la AWS CLI, utilice el siguiente comando:

```
aws rds create-db-instance --db-instance-identifier mydbinstance \
--region us-east-1 \
--db-instance-class db.t3.large \
--allocated-storage 50 \
--engine postgres \
--engine-version 16 \
--port 5432 \
--master-username master \
--master-user-password password \
--publicly-accessible \
--enable-iam-database-authentication \
--enable-cloudwatch-logs-exports=iam-db-auth-error
```

Para exportar los registros de errores de autenticación de bases de datos de IAM a Registros de CloudWatch al modificar una instancia de base de datos desde la AWS CLI, utilice el siguiente comando:

```
aws rds modify-db-instance --db-instance-identifier mydbinstance \
--region us-east-1 \
```

```
--cloudwatch-logs-export-configuration '{"EnableLogTypes":["iam-db-auth-error"]}'
```

Para verificar si la instancia de base de datos está exportando los registros de autenticación de base de datos de IAM a Registros de CloudWatch, compruebe si el parámetro `EnabledCloudwatchLogsExports` está establecido en `iam-db-auth-error` en la salida del comando `describe-db-instances`.

```
aws rds describe-db-instances --region us-east-1 --db-instance-identifier mydbinstance
            ...
             "EnabledCloudwatchLogsExports": [
                "iam-db-auth-error"
            ],
            ...
```

Métricas de CloudWatch de autenticación de bases de datos de IAM

Amazon RDS proporciona métricas casi en tiempo real sobre la autenticación de bases de datos de IAM a la cuenta de Amazon CloudWatch. En la siguiente tabla se enumeran las métricas de autenticación de bases de datos de IAM disponibles mediante CloudWatch:

Métrica	Descripción
`IamDbAuthConnectionRequests`	Número total de solicitudes de conexión realizadas con autenticación de bases de datos de IAM.
`IamDbAuthConnectionSuccess`	Número total de solicitudes de autenticación de bases de datos de IAM correctamente realizadas.
`IamDbAuthConnectionFailure`	Número total de solicitudes de autenticación de bases de datos de IAM con error.
`IamDbAuthConnectionFailureInvalidToken`	Número total de solicitudes de autenticación de bases de datos de IAM con error debido a un token no válido.

Métrica	Descripción
`IamDbAuthConnectionFailureInsufficientPermissions`	Número total de solicitudes de autenticación de bases de datos de IAM con error debido a políticas o permisos incorrectos.
`IamDbAuthConnectionFailureThrottling`	Número total de solicitudes de autenticación de bases de datos de IAM con error debido a la limitación de la autenticación de bases de datos de IAM.
`IamDbAuthConnectionFailureServerError`	Número total de solicitudes de autenticación de bases de datos de IAM con error debido a un error interno del servidor en la característica de autenticación de bases de datos de IAM.

Problemas y soluciones comunes de

Es posible que se encuentre con los siguientes problemas al utilizar la autenticación de bases de datos de IAM. Utilice los pasos de corrección de la tabla para resolver los problemas:

Error	Métricas	Causa	Solución

`[ERROR] Failed to authenticate the connection request for user` *`db_user`* `because the provided token is malformed or otherwise invalid. (Status Code: 400, Error Code: InvalidToken)`	`IamDbAuthConnectionFailure`
	
	`IamDbAuthConnectionFailureInvalidToken`
		El token de autenticación de bases de datos de IAM en la solicitud de conexión no es un token SigV4a válido o no tiene el formato correcto.	Compruebe la estrategia de generación de tokens en la aplicación. En algunos casos, asegúrese de que pasa el token con un formato válido. Si se trunca el token (o se aplica un formato de cadena incorrecto), el token no será válido.

Error	Métricas	Causa	Solución

`[ERROR] Failed to authenticate the connection request for user db_user because the token age is longer than 15 minutes. (Status Code: 400, Error Code:ExpiredToken)`	`IamDbAuthConnectionFailure`
	
	`IamDbAuthConnectionFailureInvalidToken`
		El token de autenticación de bases de datos de IAM ha caducado. Los tokens solo son válidos durante 15 minutos.	Compruebe la lógica de almacenamiento en caché de tokens o de reutilización de tokens en la aplicación. No debe reutilizar tokens que tengan más de 15 minutos.

Error	Métricas	Causa	Solución

`[ERROR] Failed to authorize the connection request for user` *db_user* `because the IAM policy assumed by the caller 'arn:aws:sts::123456789012:assumed-role/ <RoleName>/ <RoleSession>' is not authorized to perform `rds-db:connect` on the DB instance. (Status Code: 403, Error Code:NotAuthorized)`	`IamDbAuthConnectionFailure`
	
	`IamDbAuthConnectionFailureInsufficientPermissions`
		Este error es posible que se deba a las siguientes razones:
		• La política de IAM que asume la aplicación no autoriza la acción `rds-db:connect` .
		• Está asumiendo el rol o la política incorrectos para que *db_user* se conecte a la base de datos.
		• Está asumiendo la política correcta para *db_user*, pero no se está conectando a la base de datos correcta.
			Verifique el rol o la política de IAM que está asumiendo en la aplicación. Asegúrese de que asume la misma política para generar el token que para conectarse a la base de datos.

Error	Métricas	Causa	Solución

`[ERROR] Failed to authorize the connection request for user db_user due to IAM DB authentication throttling. (Status Code: 429, Error Code: ThrottlingException)`	`IamDbAuthConnectionFailure`
	
	`IamDbAuthConnectionFailureThrottling`
		Está realizando demasiadas solicitudes de conexión a la base de datos en un corto período de tiempo. El límite de limitación de autenticación de bases de datos de IAM es de 200 conexiones por segundo.	Reduzca la velocidad de establecimiento de nuevas conexiones con la autenticación de IAM. Considere implementar la agrupación de conexiones mediante Proxy de RDS para reutilizar las conexiones establecidas en la aplicación.

`[ERROR] Failed to authorize the connection request for user db_user due to an internal IAM DB authentication error. (Status Code: 500, Error Code: InternalError)`	`IamDbAuthConnectionFailure`
	
	`IamDbAuthConnectionFailureThrottling`
		Se ha producido un error interno al autorizar la conexión de la base de datos con la autenticación de bases de datos de IAM.	Póngase en contacto con https://aws.amazon.com/premiumsupport/ para investigar el problema.

Solución de problemas de identidades y accesos en Amazon RDS

Utilice la información siguiente para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Amazon RDS e IAM.

Temas

- No tengo autorización para realizar una acción en Amazon RDS
- No estoy autorizado a realizar la operación iam:PassRole

- Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon RDS.

No tengo autorización para realizar una acción en Amazon RDS

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

En el siguiente ejemplo, el error se produce cuando el usuario `mateojackson`, intenta utilizar la consola para ver detalles sobre un *`widget`*, pero no tiene permisos `rds:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 rds:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `rds:`*`GetWidget`*.

No estoy autorizado a realizar la operación iam:PassRole

Si recibe un error que indica que no está autorizado para llevar a cabo la acción `iam:PassRole`, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión. Pida a la persona que actualice sus políticas de forma que pueda transferir un rol a Amazon RDS.

Algunos servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon RDS. Sin embargo, la acción requiere que el servicio cuente con permisos otorgados por un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, Mary pide a su administrador que actualice sus políticas para que pueda realizar la acción `iam:PassRole`.

Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon RDS.

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Amazon RDS admite estas características, consulte Cómo funciona Amazon RDS con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a cuentas de AWS de terceros, consulte Proporcionar acceso a cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobe cómo proporcionar acceso mediante una identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Registro y monitoreo en Amazon RDS

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon RDS y las soluciones de AWS. Debe recopilar datos de supervisión de todas las partes de la solución de AWS para que pueda depurar un error multipunto de una forma más fácil si se produce. AWS proporciona varias herramientas para supervisar los recursos de Amazon RDS y responder a posibles incidentes:

Alarmas de Amazon CloudWatch

Con las alarmas de Amazon CloudWatch, puede ver una métrica determinada durante el periodo especificado. Si la métrica supera un límite determinado, se envía una notificación a un tema de Amazon SNS o a una política de AWS Auto Scaling. Las alarmas de CloudWatch no invocan acciones simplemente porque se encuentren en determinado estado. En su lugar, el estado debe haber cambiado y debe mantenerse durante el número de periodos especificado.

AWS CloudTrailRegistros de

CloudTrail proporciona un registro de las acciones que realiza un usuario, un rol o un servicio de AWS en Amazon RDS . CloudTrail captura todas las llamadas a la API para Amazon RDS como eventos, incluidas las llamadas procedentes de la consola y de las llamadas de código a operaciones de la API de Amazon RDS. Mediante la información que recopila CloudTrail, puede determinar la solicitud que se envió a Amazon RDS , la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y detalles adicionales. Para obtener más información, consulte Supervisión de llamadas a la API de Amazon RDS en AWS CloudTrail.

Enhanced Monitoring (Monitorización mejorada)

Amazon RDS proporciona métricas en tiempo real para el sistema operativo (SO) en el que se ejecuta la instancia . Puede ver las métricas de la instancia de bases de datos con la consola o usar la salida JSON de la supervisión mejorada de Registros de Amazon CloudWatch en un sistema de supervisión de su elección. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.

Amazon RDS Performance Insights

La información de rendimiento amplía las características de supervisión existentes de Amazon RDS para ilustrar el rendimiento de la base de datos y le ayuda a analizar cualquier problema que le afecte. Con el panel de Performance Insights, puede visualizar la carga de la base de datos y filtrarla por esperas, instrucciones SQL, hosts o usuarios. Para obtener más información, consulte Monitoreo de la carga de base de datos con Performance Insights en Amazon RDS.

Registros de la base de datos

Puede ver, descargar y monitorizar los registros de base de datos usando la AWS Management Console, la AWS CLI o la API de RDS. Para obtener más información, consulte Supervisión de archivos de registro de Amazon RDS.

Recomendaciones de Amazon RDS

Amazon RDS proporciona recomendaciones automatizadas de recursos de la base de datos. Estas recomendaciones proporcionan instrucciones de las prácticas recomendadas mediante el análisis de los datos de rendimiento, uso y configuración de la instancia de bases de datos. Para obtener más información, consulte Recomendaciones para Amazon RDS.

Notificación de eventos de Amazon RDS

Amazon RDS usa Amazon Simple Notification Service (Amazon SNS) para proporcionar una notificación cuando se produce un evento de Amazon RDS . Estas notificaciones pueden realizarse con cualquier método que admita Amazon SNS para una región de AWS, como un email, un mensaje de texto o una llamada a un punto de enlace HTTP. Para obtener más información, consulte Uso de notificaciones de eventos de Amazon RDS.

AWS Trusted Advisor

Trusted Advisor aprovecha las prácticas recomendadas aprendidas al atender a cientos de miles de clientes de AWS. Trusted Advisor inspecciona su entorno de AWS y realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el rendimiento y la disponibilidad del sistema o ayudar a cerrar deficiencias de seguridad. Todos los clientes de AWS tienen acceso a cinco comprobaciones de Trusted Advisor. Los clientes con un plan de soporte Business o Enterprise pueden ver todas las comprobaciones de Trusted Advisor.

Trusted Advisor cuenta con las siguientes comprobaciones relacionadas con Amazon RDS :

- Instancias de bases de datos inactivas de Amazon RDS
- Riesgo de acceso de grupos de seguridad de Amazon RDS
- Copias de seguridad de Amazon RDS
- Multi-AZ de Amazon RDS

Para obtener más información acerca de estas comprobaciones, consulte Prácticas recomendadas de Trusted Advisor (verificaciones).

Para obtener más información acerca de la supervisión de Amazon RDS , consulte Supervisión de métricas en una instancia de Amazon RDS.

Validación de la conformidad en Amazon RDS

Auditores externos evalúan la seguridad y la conformidad de Amazon RDS como parte de varios programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de AWS servicios en el ámbito de programas de cumplimiento específicos, consulte los AWS servicios en ámbito por programa de cumplimiento. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de cumplimiento al utilizar Amazon RDS está determinada por la confidencialidad de los datos, los objetivos de cumplimiento de la organización, y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento de normas:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones que cumplan los requisitos de HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- AWS Config: este servicio de AWS evalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y la normativa.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

Resiliencia en Amazon RDS

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, Amazon RDS ofrece características que lo ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

Copia de seguridad y restauración

Amazon RDS crea y guarda copias de seguridad automatizadas de la instancia de base de datos. Amazon RDS crea una instantánea del volumen de almacenamiento de la instancia de base de datos; para ello, hace una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales.

Amazon RDS crea copias de seguridad automatizadas de la instancia de base de datos durante el periodo de copia de seguridad de la instancia de base de datos. Amazon RDS guarda las copias de seguridad automatizadas de la instancia de base de datos en función del periodo de retención de copia de seguridad especificado. Si es necesario, puede restaurar su base de datos a cualquier momento dado durante el periodo de retención de copia de seguridad. También puede crear una copia de seguridad de su instancia de base de datos manualmente mediante la creación de una instantánea de base de datos.

Puede crear una instancia de base de datos restaurando esta instantánea de base de datos como una solución de recuperación de desastres si falla la instancia de base de datos de origen.

Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

Replicación

Amazon RDS usa la funcionalidad de replicación integrada de los motores de base de datos de MariaDB, MySQL, Oracle y PostgreSQL para crear un tipo especial de instancia de base de datos,

llamada réplica de lectura, a partir de una instancia de base de datos de origen. Las actualizaciones realizadas en la instancia de base de datos de origen se copian de forma asíncrona en la réplica de lectura. Puede reducir la carga de la instancia de base de datos de origen dirigiendo las consultas de lectura de sus aplicaciones a la réplica de lectura. Las réplicas de lectura le permiten ajustar la escala de manera elástica por encima de las restricciones de capacidad de una instancia de base de datos para las cargas de trabajo de las bases de datos con operaciones intensivas de lectura. Puede promocionar una réplica de lectura en la instancia independiente como solución de recuperación de desastres si la instancia de base de datos de origen sufre un error. En algunos motores de base de datos, Amazon RDS también admite otras opciones de replicación.

Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.

Conmutación por error

Amazon RDS proporciona alta disponibilidad y compatibilidad con la conmutación por error para las instancias de base de datos con despliegues Multi-AZ. Amazon RDS usa varias tecnologías diferentes para proporcionar compatibilidad con la conmutación por error. los despliegues Multi-AZ de instancias de base de datos de Oracle, PostgreSQL, MySQL y MariaDB usan la tecnología de conmutación por error de Amazon. Las instancias de base de datos de SQL Server utilizan Creación de reflejos de base de datos (Database Mirroring, DBM) de SQL Server.

Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.

Seguridad de la infraestructura en Amazon RDS

Como se trata de un servicio administrado, Amazon Relational Database Service está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWSprotege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a Amazon RDS a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Además, Amazon RDS ofrece características para ayudar a admitir la seguridad de la infraestructura.

Grupos de seguridad

Los grupos de seguridad controlan el acceso del tráfico entrante y saliente a una instancia de base de datos. De forma predeterminada, el acceso de red está deshabilitado para una instancia de base de datos. Puede especificar reglas en un grupo de seguridad que permitan el acceso desde un rango de direcciones IP, un puerto o un grupo de seguridad. Una vez configuradas las reglas de entrada, se aplican las mismas reglas a todas las instancias de base de datos que estén asociadas a ese grupo de seguridad.

Para obtener más información, consulte Control de acceso con grupos de seguridad.

Public accessibility (Accesibilidad pública)

Cuando lance una instancia de base de datos dentro de una nube privada virtual (VPC, por sus siglas en inglés) basada en el servicio de Amazon VPC, podrá activar o desactivar la accesibilidad

pública para esa instancia de base de datos. Para designar si la instancia de base de datos que se crea tiene un nombre de DNS que se resuelve en una dirección IP pública, utilice el parámetro Public accessibility (Accesibilidad pública). Con este parámetro podrá especificar si hay acceso público a la instancia de base de datos. Es posible modificar una instancia de base de datos para activar o desactivar la accesibilidad pública modificando el parámetro Public accessibility (Accesibilidad pública).

Para obtener más información, consulte Cómo ocultar una instancia de base de datos en una VPC desde Internet..

> **Note**
>
> Si la instancia de base de datos se encuentra en una VPC pero no es accesible públicamente, también puede usar una conexión AWS Site-to-Site VPN o una conexión de AWS Direct Connect para acceder a ella desde una red privada. Para obtener más información, consulte Privacidad del tráfico entre redes.

La API de Amazon RDS y los puntos de enlace de la VPC de tipo interfaz (AWS PrivateLink)

Puede establecer una conexión privada entre los puntos de enlace de la VPC y la API de Amazon RDS mediante la creación de un punto de enlace de la VPC de tipo interfaz. Puntos de enlace de tipo interfaz con tecnología de AWS PrivateLink.

AWS PrivateLink permite acceder de forma privada a las operaciones de la API de Amazon RDS sin una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN o una conexión de AWS Direct Connect. Las instancias de bases de datos de su VPC no necesitan direcciones IP públicas para comunicarse con los puntos de conexión de la API de Amazon RDS para lanzar, modificar o terminar instancias de base de datos. Las instancias de bases de datos tampoco necesitan direcciones IP públicas para utilizar ninguna de las operaciones de la API de RDS disponibles. El tráfico entre la VPC y Amazon RDS no sale de la red de Amazon.

Cada punto de enlace de la interfaz está representado por una o más interfaces de red elásticas en las subredes. Para obtener más información sobre las interfaces de red elásticas, consulte Interfaces de red elásticas en la Guía del usuario de Amazon EC2.

Para obtener más información sobre puntos de enlace de la VPC, consulte Puntos de enlace de la VPC de tipo interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC. Para obtener información sobre las operaciones de la API de RDS, consulte la referencia de la API de Amazon RDS.

No necesita un punto de conexión de VPC de la interfaz para conectarse con una instancia de base de datos. Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC.

Consideraciones para los puntos de enlace de VPC

Antes de configurar un punto de enlace de la VPC de tipo interfaz para los puntos de enlace de la API de Amazon RDS, asegúrese de revisar Propiedades y limitaciones de puntos de enlace de interfaz en la Guía del usuario de Amazon VPC.

Todas las operaciones de la API de RDS relevantes para la administración de los recursos de Amazon RDS están disponibles desde la VPC mediante el uso de AWS PrivateLink.

Las políticas de puntos de enlace de VPC son compatibles con los puntos de enlace de API de RDS. De forma predeterminada, se permite el acceso completo a las operaciones de API de RDS a través

del punto de enlace. Para obtener más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la guía del usuario de Amazon VPC.

Disponibilidad

La API de Amazon RDS actualmente admite puntos de enlace de la VPC en las siguientes regiones de AWS:

- US East (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- Oeste de Canadá (Calgary
- China (Pekín)
- China (Ningxia)
- Europa (Fráncfort)
- Europa (Zúrich)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- Europa (Milán)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)

- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (EE. UU. Oeste)

Creación de un punto de enlace de la VPC de interfaz para Amazon RDS API

Puede crear un punto de enlace de la VPC para la API de Amazon RDS mediante la consola de Amazon VPC o AWS Command Line Interface (AWS CLI). Para más información, consulte Creación de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto de enlace de la VPC para Amazon RDS API mediante el uso del nombre del servicio `com.amazonaws.region.rds`.

Salvo en las regiones de AWS en China, si habilita un DNS privado para el punto de enlace, podrá realizar solicitudes de la API a Amazon RDS con el punto de enlace de la VPC mediante el nombre de DNS predeterminado de la región de AWS, por ejemplo `rds.us-east-1.amazonaws.com`. En las regiones de China (Pekín) y China (Ningxia) de AWS, puede realizar solicitudes de la API con el punto de enlace de la VPC mediante `rds-api.cn-north-1.amazonaws.com.cn` y `rds-api.cn-northwest-1.amazonaws.com.cn`, respectivamente.

Para más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Creación de una política de punto de enlace de la VPC para la Amazon RDS API

Puede asociar una política de punto de enlace con el punto de enlace de la VPC que controla el acceso a la Amazon RDS API. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la guía del usuario de Amazon VPC.

Ejemplo: política de punto de enlace de la VPC para acciones de la Amazon RDS API

A continuación, se muestra un ejemplo de una política de punto de enlace para la Amazon RDS API. Cuando se asocia a un punto de enlace, esta política concede acceso a las acciones de la Amazon RDS API enumeradas para todos las entidades principales de todos los recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "rds:CreateDBInstance",
            "rds:ModifyDBInstance",
            "rds:CreateDBSnapshot"
         ],
         "Resource":"*"
      }
   ]
}
```

Ejemplo: política de punto de enlace de la VPC que deniega todo el acceso desde una cuenta de AWS especificada

La siguiente política de punto de enlace de la VPC deniega a la cuenta de AWS 123456789012 todo el acceso a los recursos mediante el punto de enlace. La política permite todas las acciones de otras cuentas.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": { "AWS": [ "123456789012" ] }
     }
```

```
    ]
}
```

Prácticas recomendadas de seguridad para Amazon RDS

Utilice cuentas de AWS Identity and Access Management (IAM) para controlar el acceso a las operaciones de la API de Amazon RDS, especialmente operaciones que crean, modifican o eliminan recursos de Amazon RDS . Dichos recursos incluyen instancias de base de datos, grupos de seguridad y grupos de parámetros. Utilice también IAM para controlar acciones que realizan acciones administrativas comunes como copias de seguridad y restauración de instancias de base de datos.

- Cree un usuario individual para cada persona que administre recursos de Amazon RDS , incluido usted mismo. No utilice las credenciales raíz de AWS para administrar los recursos de Amazon RDS .
- Asigne a cada usuario el conjunto mínimo de permisos requerido para realizar sus tareas.
- Use los grupos de IAM para administrar con eficacia los permisos para varios usuarios.
- Rote con regularidad sus credenciales de IAM.
- Configure AWS Secrets Manager para rotar automáticamente los secretos para Amazon RDS . Para obtener más información, consulte Rotación de sus secretos de AWS Secrets Manager en la guía del usuario de AWS Secrets Manager. También puede recuperar mediante programación las credenciales desde AWS Secrets Manager. Para obtener más información, consulte Recuperar el valor secreto en la guía del usuario de AWS Secrets Manager.

Para obtener más información acerca de la seguridad de Amazon RDS , consulte Seguridad en Amazon RDS. Para obtener más información acerca de IAM, consulte AWS Identity and Access Management. Para obtener información acerca de las prácticas recomendadas de IAM, consulte Prácticas recomendadas de IAM.

AWS Security Hub utiliza controles de seguridad para evaluar las configuraciones de los recursos y los estándares de seguridad para ayudarlo a cumplir varios marcos de conformidad. Para obtener más información sobre el uso de Security Hub para evaluar los recursos de Lambda, consulte Amazon Relational Database Service controls (Controles de Amazon Relational Database Service) en la Guía del usuario de AWS Security Hub.

Puede supervisar el uso de RDS en relación con las prácticas recomendadas de seguridad con Security Hub. Para obtener más información, consulte ¿Qué es AWS Security Hub?.

Utilice la AWS Management Console, la AWS CLI o la API de RDS para cambiar la contraseña para el usuario maestro. Si usa otra herramienta, como un cliente de SQL, para cambiar la contraseña del usuario maestro, podría provocar involuntariamente la revocación de privilegios para el usuario.

Control de acceso con grupos de seguridad

Los grupos de seguridad de VPC controlan el acceso del tráfico entrante y saliente de una instancia de base de datos. De forma predeterminada, el acceso de red está desactivado para una instancia de base de datos. Puede especificar reglas en un grupo de seguridad que permitan el acceso desde un rango de direcciones IP, un puerto o un grupo de seguridad. Una vez configuradas las reglas de entrada, se aplican las mismas reglas a todas las instancias de base de datos que estén asociadas a ese grupo de seguridad. Puede especificar hasta 20 reglas en un grupo de seguridad.

Información general de los grupos de seguridad de VPC

Cada regla de grupo de seguridad de VPC permite a un origen específico acceder a una instancia de base de datos de una VPC asociada a ese grupo de seguridad de VPC. El origen puede ser un rango de direcciones (por ejemplo, 203.0.113.0/24), u otro grupo de seguridad de VPC. Cuando se especifica un grupo de seguridad de VPC como origen, se permite el tráfico entrante procedente de todas las instancias, normalmente servidores de aplicaciones, que utilizan el grupo de seguridad de VPC. Los grupos de seguridad de VPC pueden tener reglas que rijan el tráfico entrante y saliente. Sin embargo, las reglas de tráfico saliente normalmente no se aplican a instancias de bases de datos. Las reglas de tráfico saliente solo se aplican si la instancia de base de datos actúa como cliente. Por ejemplo, las reglas de tráfico saliente se aplican a una base de datos Oracle con enlaces a la base de datos saliente. Debe utilizar la API de Amazon EC2 o la opción Security Group (Grupo de seguridad) de la consola de VPC para crear grupos de seguridad de VPC.

Cuando cree reglas para el grupo de seguridad de la VPC que permitan el acceso a las instancias de la VPC, debe especificar un puerto para cada rango de direcciones a las que la regla permite el acceso. Por ejemplo, si desea habilitar el acceso Secure Shell (SSH) a las instancias de la VPC, puede crear una regla que permita el acceso al puerto TCP 22 para el rango de direcciones especificado.

Puede configurar varios grupos de seguridad de VPC que permitan el acceso a puertos distintos para las distintas instancias de la VPC. Por ejemplo, puede crear un grupo de seguridad de VPC que permita el acceso al puerto TCP 80 para los servidores web de la VPC. A continuación, puede crear otro grupo de seguridad de la VPC que permita el acceso al puerto TCP 3306 para las instancias de base de datos de RDS para MySQL en la VPC.

Para obtener más información sobre los grupos de seguridad de VPC, consulte Grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

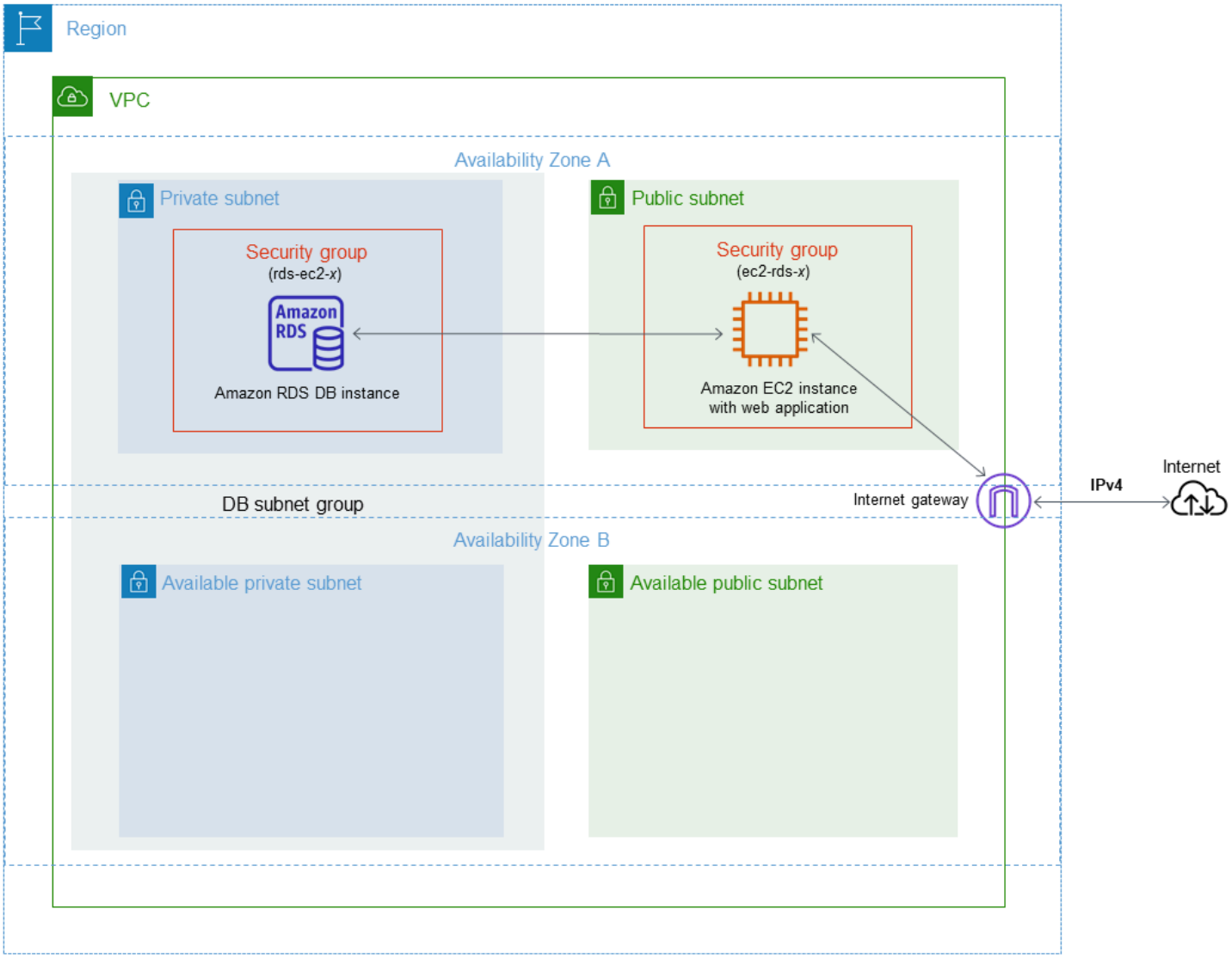
> **Note**
>
> Si la instancia de la base de datos se encuentra en una VPC pero no es accesible públicamente, también puede usar una conexión AWS Site-to-Site VPN o una conexión de AWS Direct Connect para acceder desde una red privada. Para obtener más información, consulte Privacidad del tráfico entre redes.

Escenario de grupos de seguridad

Un uso común de instancia de base de datos en una VPC es compartir datos con un servidor de aplicaciones que se ejecuta en una instancia de Amazon EC2 de la misma VPC, al que obtiene acceso desde una aplicación cliente situada fuera de la VPC. Para este escenario, se utilizan las páginas de RDS y VPC de la AWS Management Console o las operaciones de la API de RDS y EC2 para crear las instancias y los grupos de seguridad necesarios:

1. Cree un grupo de seguridad de VPC (por ejemplo, `sg-0123ec2example`) y defina reglas de entrada que utilicen las direcciones IP de la aplicación cliente como origen. Este grupo de seguridad permite que la aplicación cliente se conecte a las instancias EC2 de una VPC que utilice este grupo de seguridad.
2. Cree una instancia EC2 para la aplicación y añada la instancia EC2 al grupo de seguridad de VPC (`sg-0123ec2example`) que creó en el paso anterior.
3. Cree un segundo grupo de seguridad de VPC (por ejemplo, `sg-6789rdsexample`) y cree una regla nueva especificando el grupo de seguridad de VPC que creó en el paso 1 (`sg-0123ec2example`) como origen.
4. Cree una instancia nueva de base de datos y agregue la instancia de base de datos al grupo de seguridad de la VPC (`sg-6789rdsexample`) que creó en el paso anterior. Cuando cree la instancia de base de datos, utilice el mismo número de puerto que especificó para la regla de grupo de seguridad de VPC (`sg-6789rdsexample`) que creó en el paso 3.

En el siguiente diagrama se muestra este escenario.



Para obtener instrucciones detalladas acerca de la configuración de una VPC para este escenario, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4). Para obtener más información acerca del uso de una VPC, consulte VPC de Amazon y Amazon RDS.

Creación de un grupo de seguridad de VPC

Puede crear un grupo de seguridad de VPC para una instancia de base de datos mediante la consola de VPC. Para obtener información sobre la creación de un grupo de seguridad, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad y Grupos de seguridad en la Guía del usuario de Amazon Virtual Private Cloud.

Asociación de un grupo de seguridad con una instancia de base de datos

Puede asociar un grupo de seguridad con una instancia de base de datos mediante la opción Modify (Modificar) de la consola de RDS, la API de Amazon RDS `ModifyDBInstance` o el comando `modify-db-instance` de AWS CLI.

El siguiente ejemplo de la CLI asocia un grupo de seguridad de VPC específico y elimina los grupos de seguridad de base de datos de la instancia de base de datos.

```
aws rds modify-db-instance --db-instance-identifier dbName --vpc-security-group-ids sg-ID
```

Para obtener información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS. Para consideraciones relativas al grupo de seguridad al restaurar una instancia de base de datos a partir de una instantánea de base de datos, consulte Consideraciones relativas al grupo de seguridad.

> **Note**
>
> La consola de RDS muestra diferentes nombres de reglas de grupos de seguridad para la base de datos si el valor del puerto está configurado en un valor no predeterminado.

En el caso de instancias de bases de datos de RDS para Oracle, se pueden asociar grupos de seguridad adicionales rellenando la configuración de opciones de grupos de seguridad para las opciones Oracle Enterprise Manager Database Express (OEM), Oracle Management Agent for Enterprise Manager Cloud Control (OEM Agent) y Oracle Secure Sockets Layer. En este caso, tanto los grupos de seguridad asociados a la instancia de base de datos como la configuración de las opciones se aplican a la instancia de base de datos. Para obtener más información acerca de estos grupos de opciones, consulte Oracle Enterprise Manager, Oracle Management Agent para Enterprise Manager Cloud Control y Capa de conexión segura de Oracle.

Privilegios de la cuenta de usuario maestro

Cuando se crea una instancia nueva de base de datos, el usuario maestro predeterminado que se utiliza obtiene determinados privilegios para esa instancia de bases de datos. No se puede cambiar el nombre de usuario maestro después de crear la instancia de base de datos.

Important

Le recomendamos encarecidamente que no utilice el usuario maestro directamente en sus aplicaciones. En lugar de ello, es mejor ceñirse a la práctica recomendada de utilizar un usuario de base de datos creado con los privilegios mínimos necesarios para su aplicación.

Note

Si elimina los permisos para el usuario maestro de forma accidental, puede restaurarlos modificando la instancia de base de datos y estableciendo una nueva contraseña para el usuario maestro. Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS .

En la siguiente tabla se muestran los privilegios y los roles de base de datos que obtiene el usuario maestro para cada uno de los motores de bases de datos.

Motor de base de datos	Privilegio del sistema	Rol de base de datos
RDS para Db2	El usuario maestro se asigna al grupo `masterdba` y se le asigna el `master_user_role` . `SYSMON`, `DBADM` con `DATAACCESS` Y `ACCCESSCTRL` , `BINDADD`, `CONNECT`, `CREATETAB` , `CREATE_SECURE_OBJECT` , `EXPLAIN`, `IMPLICIT_SCHEMA` , `LOAD`, `SQLADM`, `WLMADM`	`DBA`,`DBA_RESTRICTED` , `DEVELOPER` ,`ROLE_NULLID_PACKAGES` , `ROLE_PROCEDURES` ,`ROLE_TABLESPACES` Para obtener más información, consulte Roles predeterminados de Amazon RDS para Db2.

Motor de base de datos	Privilegio del sistema	Rol de base de datos
RDS para MariaDB	`SELECT,INSERT,UPDATE,DELETE, CREATE,DROP,RELOAD, PROCESS,REFERENCES ,INDEX, ALTER,SHOW DATABASES ,CREATE TEMPORARY TABLES ,LOCK TABLES, EXECUTE,REPLICATION CLIENT,CREATE VIEW ,SHOW VIEW,CREATE ROUTINE, ALTER ROUTINE,CREATE USER, EVENT,TRIGGER,REPLICATION SLAVE` A partir de la versión 11.4 de RDS para MariaDB, el usuario maestro también obtiene el privilegio `SHOW CREATE ROUTINE`.	—
RDS para MySQL 8.0 y versiones posteriores	`SELECT,INSERT,UPDATE, DELETE,CREATE,DROP, RELOAD,PROCESS, REFERENCES ,INDEX,ALTER, SHOW DATABASES ,CREATE TEMPORARY TABLES,LOCK TABLES,EXECUTE, REPLICATION SLAVE ,REPLICATION CLIENT , CREATE VIEW,SHOW VIEW,CREATE ROUTINE,ALTER ROUTINE,CREATE USER,EVENT,TRIGGER, CREATE ROLE,DROP ROLE, APPLICATION_PASSWORD_ADMIN , ROLE_ADMIN ,SET_USER_ID , XA_RECOVER_ADMIN`	`rds_superuser_role` Para obtener más información acerca de `rds_superuser_role` , consulte Modelo de privilegios basado en roles de RDS para MySQL.
Versiones de RDS para MySQL anteriores a 8.0.36	`SELECT,INSERT,UPDATE, DELETE,CREATE,DROP, RELOAD,PROCESS, REFERENCES ,INDEX,ALTER, SHOW DATABASES ,CREATE TEMPORARY TABLES,LOCK TABLES,EXECUTE, REPLICATION CLIENT ,CREATE VIEW, SHOW VIEW,CREATE ROUTINE,ALTER ROUTINE,CREATE USER,EVENT, TRIGGER,REPLICATION SLAVE`	—

Motor de base de datos	Privilegio del sistema	Rol de base de datos
RDS para PostgreSQL	`CREATE ROLE,CREATE DB, PASSWORD VALID UNTIL INFINITY,CREATE EXTENSION ,ALTER EXTENSION ,DROP EXTENSION ,CREATE TABLESPACE ,ALTER <OBJECT> OWNER,CHECKPOINT , PG_CANCEL_BACKEND( ) , PG_TERMINATE_BACKEND() ,SELECT PG_STAT_REPLICATION ,EXECUTE PG_STAT_STATEMENTS_RESET() ,OWN POSTGRES_ FDW_HANDLER() ,OWN POSTGRES_FDW_VALIDATOR() ,OWN POSTGRES_FDW , EXECUTE PG_BUFFERCACHE_PAGES() ,SELECT PG_BUFFERCACHE`	`RDS_SUPERUSER` Para obtener más información acerca de RDS_SUPERUSER, consulte Descripción de los roles y permisos de PostgreSQL.

Motor de base de datos	Privilegio del sistema	Rol de base de datos
RDS para Oracle	ADMINISTER DATABASE TRIGGER ,ALTER DATABASE LINK,ALTER PUBLIC DATABASE LINK, AUDIT SYSTEM,CHANGE NOTIFICATION , DROP ANY DIRECTORY ,EXEMPT ACCESS POLICY,EXEMPT IDENTITY POLICY,EXEMPT REDACTION POLICY,FLASHBACK ANY TABLE, GRANT ANY OBJECT PRIVILEGE ,RESTRICTED SESSION ,SELECT ANY TABLE,UNLIMITED TABLESPACE	DBA **Note** El rol DBA está exento de los siguientes privilegios: ALTER DATABASE,ALTER SYSTEM, CREATE ANY DIRECTORY ,CREATE EXTERNAL JOB,CREATE PLUGGABLE DATABASE, GRANT ANY PRIVILEGE ,GRANT ANY ROLE,READ ANY FILE GROUP
Amazon RDS for Microsoft SQL Server	ADMINISTER BULK OPERATIONS ,ALTER ANY CONNECTION ,ALTER ANY CREDENTIAL , ALTER ANY EVENT SESSION,ALTER ANY LINKED SERVER,ALTER ANY LOGIN,ALTER ANY SERVER AUDIT,ALTER ANY SERVER ROLE, ALTER SERVER STATE,ALTER TRACE, CONNECT SQL,CREATE ANY DATABASE, VIEW ANY DATABASE,VIEW ANY DEFINITION ,VIEW SERVER STATE,ALTER ON ROLE SQLAgentOperatorRole	DB_OWNER (rol de nivel de base de datos), PROCESSADMIN (rol de nivel de servidor), SETUPADMIN (rol de nivel de servidor), SQLAgentUserRole (rol de nivel de base de datos)

Uso de roles vinculados a servicios de Amazon RDS

Amazon RDS utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM) Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon RDS. Los roles vinculados a servicios están predefinidos por Amazon RDS e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica el uso de Amazon RDS porque ya no tendrá que agregar manualmente los permisos necesarios. Amazon RDS define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Amazon RDS puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Las funciones se pueden eliminar únicamente después de eliminar primero sus recursos relacionados. De esta forma, se protegen los recursos de Amazon RDS, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios de Amazon RDS

Amazon RDS utiliza el rol vinculado al servicio denominado AWSServiceRoleForRDS para permitir que Amazon RDS llame a servicios de AWS en nombre de sus instancias de base de datos.

El rol vinculado al servicio AWSServiceRoleForRDS confía en que los siguientes servicios asuman el rol:

- `rds.amazonaws.com`

Este rol vinculado al servicio tiene una política de permisos adjunta llamada `AmazonRDSServiceRolePolicy`, que le otorga permisos para operar en su cuenta.

Para obtener más información sobre esta política, incluido el documento de política de JSON, consulte AmazonRDSServiceRolePolicy en la Guía de referencia de políticas administradas de AWS.

Note

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Si aparece el siguiente mensaje de error:
Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
Asegúrese de que tiene habilitados los permisos siguientes:

```
{
    "Action": "iam:CreateServiceLinkedRole",
    "Effect": "Allow",
    "Resource": "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName":"rds.amazonaws.com"
        }
    }
}
```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de Amazon RDS

No necesita crear manualmente un rol vinculado a un servicio. Cuando crea una instancia de base de datos, Amazon RDS vuelve a crear por usted el rol vinculado al servicio.

Important

Si utilizaba el servicio Amazon RDS antes del 1 de diciembre de 2017, cuando comenzó a admitir roles vinculados a servicios, entonces Amazon RDS creó el rol AWSServiceRoleForRDS en su cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de AWS.

Si elimina este rol vinculado a servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea una instancia de base de datos, Amazon RDS vuelve a crear por usted el rol vinculado al servicio.

Modificación de un rol vinculado a un servicio de Amazon RDS

Amazon RDS no permite editar el rol vinculado al servicio AWSServiceRoleForRDS. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de Amazon RDS

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe eliminar todas las instancias para poder eliminar el rol vinculado al servicio.

Limpiar un rol vinculado a un servicio

Antes de poder utilizar IAM para eliminar un rol vinculado a un servicio, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza.

Para comprobar si el rol vinculado a un servicio tiene una sesión activa en la consola de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, elija Roles. Luego, elija el nombre (no la casilla de verificación) del rol AWSServiceRoleForRDS.
3. En la página Resumen del rol seleccionado, elija la pestaña Acceso reciente.
4. En la pestaña Acceso reciente, revise la actividad reciente del rol vinculado a servicios.

> **Note**
>
> Si no está seguro de si Amazon RDS utiliza el rol AWSServiceRoleForRDS, puede intentar eliminar el rol para comprobarlo. Si el servicio está utilizando el rol, este no podrá eliminarse y podrá ver las regiones de AWS en las que se está utilizando. Si el rol se está utilizando, debe esperar que la sesión finalice para poder eliminarlo. No se puede revocar la sesión de un rol vinculado a un servicio.

Si desea eliminar el rol AWSServiceRoleForRDS, primero debe eliminar sus instancias de base de datos totales.

Eliminación de todas las instancias

Use alguno de estos procedimientos para eliminar cada una de sus instancias.

Para eliminar una instancia (consola)

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, seleccione Databases (Bases de datos).
3. Elija la instancia que desea eliminar.
4. En Actions (Acciones), elija Delete (Eliminar).
5. Si aparece el mensaje Create final Snapshot? (¿Crear instantánea final?), elija Yes (Sí) o No.
6. Si eligió Yes (Sí) en el paso anterior, en Final snapshot name (Nombre de instantánea final) escriba el nombre de la instantánea final.
7. Elija Eliminar.

Para eliminar una instancia (CLI)

Consulte `delete-db-instance` en la referencia de comandos de AWS CLI.

Para eliminar una instancia (API)

Consulte `DeleteDBInstance` en la Amazon RDS API Reference.

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar el rol vinculado al servicio AWSServiceRoleForRDS. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Permisos de roles vinculados a servicios para Amazon RDS Custom

Amazon RDS Custom utiliza el rol vinculado al servicio llamado `AWSServiceRoleForRDSCustom` para permitir que RDS Custom llame a los servicios de AWS en nombre de sus recursos de base de datos de RDS.

El rol vinculado al servicio AWSServiceRoleForRDSCustom confía en los siguientes servicios para asumir el rol:

- `custom.rds.amazonaws.com`

Este rol vinculado al servicio tiene una política de permisos adjunta llamada `AmazonRDSCustomServiceRolePolicy` que le otorga permisos para operar en su cuenta.

Crear, editar o eliminar el rol vinculado a servicios para RDS Custom funciona igual que para Amazon RDS. Para obtener más información, consulte Política administrada por:AWS AmazonRDSCustomServiceRolePolicy.

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Si aparece el siguiente mensaje de error:
> Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
> Asegúrese de que tiene habilitados los permisos siguientes:
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/custom.rds.amazonaws.com/
> AmazonRDSCustomServiceRolePolicy",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"custom.rds.amazonaws.com"
>         }
>     }
> }
> ```
>
> Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Permisos de roles vinculados a servicios para Amazon RDS Beta

Amazon RDS utiliza el rol vinculado al servicio llamado `AWSServiceRoleForRDSBeta` para que Amazon RDS pueda llamar a los servicios AWS en nombre de sus recursos de base de datos de RDS.

El rol vinculado al servicio AWSServiceRoleForRDSBeta depende de los siguientes servicios para asumir el rol:

- `rds.amazonaws.com`

Este rol vinculado al servicio tiene una política de permisos adjunta llamada `AmazonRDSBetaServiceRolePolicy` que le otorga permisos para operar en su cuenta. Para obtener más información, consulte Política administrada de:AWS AmazonRDSBetaServiceRolePolicy.

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Si aparece el siguiente mensaje de error:
> Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
> Asegúrese de que tiene habilitados los permisos siguientes:
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/custom.rds.amazonaws.com/
> AmazonRDSBetaServiceRolePolicy",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"custom.rds.amazonaws.com"
>         }
>     }
> }
> ```
>
> Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Rol vinculado a servicios para Amazon RDS Preview

Amazon RDS utiliza el rol vinculado al servicio llamado `AWSServiceRoleForRDSPreview` para que Amazon RDS pueda llamar a los servicios AWS en nombre de sus recursos de base de datos de RDS.

El rol vinculado al servicio AWSServiceRoleForRDSPreview depende de los siguientes servicios para asumir el rol:

- `rds.amazonaws.com`

Este rol vinculado al servicio tiene una política de permisos adjunta llamada `AmazonRDSPreviewServiceRolePolicy` que le otorga permisos para operar en su cuenta. Para obtener más información, consulte Política administrada de:AWS AmazonRDSPreviewServiceRolePolicy.

> **Note**
>
> Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o función) crear, editar o eliminar la descripción de una función vinculada a un servicio. Si aparece el siguiente mensaje de error:
> Unable to create the resource. Verify that you have permission to create service linked role. Otherwise wait and try again later.
> Asegúrese de que tiene habilitados los permisos siguientes:
>
> ```
> {
>     "Action": "iam:CreateServiceLinkedRole",
>     "Effect": "Allow",
>     "Resource": "arn:aws:iam::*:role/aws-service-role/custom.rds.amazonaws.com/
> AmazonRDSPreviewServiceRolePolicy",
>     "Condition": {
>         "StringLike": {
>             "iam:AWSServiceName":"custom.rds.amazonaws.com"
>         }
>     }
> }
> ```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

VPC de Amazon y Amazon RDS

Amazon Virtual Private Cloud (Amazon VPC) hace posible lanzar recursos de AWS, como instancias de base de datos de Amazon RDS, en una nube privada virtual (VPC).

Cuando utilice una VPC, puede controlar todos los aspectos del entorno de red virtual. Puede elegir su propio rango de direcciones IP, crear subredes y configurar listas de enrutamiento y control de acceso. Es posible ejecutar la instancia de base de datos en una VPC sin ningún coste adicional.

Las cuentas tienen una VPC predeterminada. Todas las nuevas instancias de bases de datos se crean en la VPC predeterminada, a menos que se especifique lo contrario.

Temas

- Uso de una instancia de base de datos en una VPC
- Actualización de la VPC para una instancia de base de datos
- Escenarios de acceso a una instancia de base de datos en una VPC
- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4)
- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (modo de pila doble)
- Traslado de una instancia de base de datos que no está en una VPC a una VPC

A continuación, encontrará una discusión acerca de la funcionalidad de la VPC relevante a instancias de base de datos de Amazon RDS. Para obtener más información sobre Amazon VPC, consulte la guía de introducción de Amazon VPC y la guía del usuario de Amazon VPC.

Uso de una instancia de base de datos en una VPC

Su instancia de base de datos debe estar dentro de la nube privada virtual (VPC). Una VPC es una red virtual aislada lógicamente de otras redes virtuales en la nube de AWS. Amazon VPC le permite lanzar recursos de AWS, como una instanciaAmazon Aurora o una instancia de Amazon EC2, en una VPC. La VPC puede ser una VPC predeterminada que viene con la cuenta o una que se haya creado en ella. Todas las VPC están asociadas a la cuenta de AWS.

La VPC predeterminada tiene tres subredes que se pueden utilizar para aislar recursos dentro de la VPC. La VPC predeterminada también tiene una gateway de Internet que se puede utilizar para proporcionar acceso a los recursos situados dentro de la VPC desde fuera de la VPC.

Para obtener una lista de los escenarios relacionados con las instancias de bases de datos de Amazon RDS dentro y fuera de una VPC, consulte Escenarios de acceso a una instancia de base de datos en una VPC.

Temas

- Uso de una instancia de base de datos en una VPC
- Uso de los grupos de subredes de base de datos
- Subredes compartidas
- Direccionamiento IP de Amazon RDS
- Cómo ocultar una instancia de base de datos en una VPC desde Internet.
- Creación de una instancia de base de datos en una VPC

En los siguientes tutoriales se explica cómo crear una VPC que se puede utilizar en un escenario de Amazon RDS habitual:

- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4)
- Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (modo de pila doble)

Uso de una instancia de base de datos en una VPC

A continuación se ofrecen algunos consejos para utilizar una instancia de base de datos en una VPC:

- La VPC debe tener dos subredes como mínimo. Estas subredes deben estar en dos zonas de disponibilidad distintas de la Región de AWS en la que desea implementar la instancia de base de datos. Una subred es un segmento del rango de direcciones IP de una VPC que puede especificar y que le permite agrupar instancias de base de datos según sus necesidades operativas y de seguridad.

  Para implementaciones Multi-AZ, si se define una subred para dos o más zonas de disponibilidad de una región de Región de AWS, Amazon RDS podrá crear una instancia en espera en otra zona de disponibilidad si fuera necesario. Asegúrese de hacerlo incluso para las implementaciones Single-AZ, por si desea convertirlas en implementaciones Multi-AZ en algún momento.

> **Note**
>
> El grupo de subredes de base de datos para una zona local puede tener solo una subred.

- Si desea que una instancia de base de datos de la VPC sea accesible públicamente, debe activar los atributos DNS hostnames y DNS resolution.
- La VPC debe tener un grupo de subredes de base de datos que haya creado. Para crear un grupo de subredes de base de datos, especifique las subredes que ha creado. Amazon RDS elige una subred y una dirección IP dentro de ese grupo de subredes para asociarlas con su instancia de base de datos. La instancia de base de datos utiliza la zona de disponibilidad que contiene la subred.
- La VPC debe tener un grupo de seguridad de VPC que permita el acceso a la instancia de base de datos.

  Para obtener más información, consulte Escenarios de acceso a una instancia de base de datos en una VPC.
- Los bloques de CIDR de cada una de las subredes deben ser lo suficientemente grandes como para acomodar direcciones IP de repuesto para que Amazon RDS las use durante las actividades de mantenimiento, incluyendo la conmutación por error y el escalado de recursos de computación. Por ejemplo, un rango como 10.0.0/24 y 10.0.2.0/24 suele ser lo suficientemente grande.
- El atributo instance tenancy de una VPC puede definirse como default o dedicated. Todas las VPC predeterminadas tienen el atributo de tenencia de instancia definido como default, y una VPC predeterminada puede admitir cualquier clase de instancia de base de datos.

  Si opta por tener la instancia de base de datos en una VPC dedicada cuyo atributo de tenencia de instancia está establecido en dedicado, la clase de instancia de base de datos de la instancia debe ser uno de los tipos aprobados de instancia dedicada de Amazon EC2. Por ejemplo, la instancia dedicada r5.large de EC2 corresponde a la clase de instancia de base de datos r5.large. Para obtener información acerca de la tenencia de instancias en una VPC, consulte Instancias dedicadas en la Guía del usuario de Amazon Elastic Compute Cloud.

  Para obtener más información acerca de los tipos de instancias que puede haber en una instancia dedicada, consulte Instancias dedicadas de Amazon EC2 en la página de precios de Amazon EC2.

> **Note**
>
> Cuando establece el atributo de tenencia de instancia en dedicado para una instancia de base de datos, no garantiza que la instancia de base de datos se ejecute en un host dedicado.

- Cuando se asigna un grupo de opciones a una instancia de base de datos, se asocia a la VPC de la instancia de base de datos. Esta vinculación significa que no se puede utilizar el grupo de opciones asignado a una instancia de base de datos si se intenta restaurar la instancia de base de datos en una VPC distinta.
- Si restaura una instancia de base de datos en una VPC diferente, asegúrese de asignar el grupo de opciones predeterminado a la instancia de base de datos, asignar un grupo de opciones que esté vinculado a esa VPC, o crear un grupo de opciones nuevo y asignarlo a la instancia de base de datos. Con las opciones persistentes o permanentes, como TDE de Oracle, debe crear un grupo de opciones nuevo que incluya la opción persistente o permanente cuando restaure una instancia de base de datos en una VPC diferente.

Uso de los grupos de subredes de base de datos

Las subredes son segmentos del rango de direcciones IP de una VPC que se definen para agrupar recursos de acuerdo con las necesidades operativas y de seguridad. Un grupo de subredes de base de datos es una colección de subredes (normalmente privadas) que se crean en una VPC y que después se asignan a las instancias de bases de datos. Un grupo de subredes de base de datos le permite especificar una VPC específica al crear instancias de bases de datos utilizando la AWS CLI o la API de RDS. Si utiliza la consola, solo puede elegir la VPC y los grupos de subredes que desea utilizar.

Cada grupo de subredes de base de datos debe tener subredes como mínimo en dos zonas de disponibilidad de una Región de AWS determinada. Cuando crea una instancia de base de datos en una VPC, debe elegir un grupo de subredes de base de datos. Desde el grupo de subred de base de datos, Amazon RDS elige una subred y una dirección IP dentro de esa subred para asociarla con la de base de datos. La base de datos utiliza la zona de disponibilidad que contiene la subred. Amazon RDS siempre asigna una dirección IP desde una subred que tiene espacio de dirección IP libre.

Si falla la instancia de base de datos principal de una implementación multi-AZ, Amazon RDS puede promocionar la instancia en espera correspondiente y, posteriormente, crear una nueva instancia en espera utilizando una dirección IP de la subred de una de las otras zonas de disponibilidad.

Las subredes de un grupo de subredes de base de datos son públicas o privadas. Las subredes son públicas o privadas, en función de la configuración que establezca para sus listas de control de acceso a la red (ACL de red) y tablas de enrutamiento. Para que una instancia de base de datos sea accesible públicamente, todas las subredes del grupo de subredes de base de datos deben ser públicas. Si una subred asociada a una instancia de base de datos de acceso público cambia de pública a privada, eso puede afectar a la disponibilidad de la instancia.

Para crear un grupo de subredes de base de datos que admita el modo de pila doble, asegúrese de que cada subred que agregue al grupo de subredes de base de datos tenga un bloque de CIDR de protocolo de Internet versión 6 (IPv6) asociado. Para obtener más información, consulte Direccionamiento IP de Amazon RDS y el tema sobre cómo migrar a IPv6 en la Guía del usuario de Amazon VPC.

> **Note**
>
> El grupo de subredes de base de datos para una zona local puede tener solo una subred.

Cuando Amazon RDS crea una instancia de base de datos en una VPC, asigna una interfaz de red a la instancia de base de datos utilizando una dirección IP del grupo de subredes de base de datos. Sin embargo, le recomendamos que utilice el nombre del sistema de nombres de dominio (DNS) para conectarse a la instancia de base de datos. Se recomienda hacerlo porque la dirección IP subyacente cambia durante la conmutación por error.

> **Note**
>
> Para cada instancia de base de datos que ejecute en una VPC, asegúrese de reservar al menos una dirección en cada subred del grupo de subredes de base de datos para que la utilice Amazon RDS para las acciones de recuperación.

Subredes compartidas

Puede crear una instancia de base de datos en una VPC compartida.

Algunas consideraciones a tener en cuenta al utilizar las VPC compartidas:

- Puede mover una instancia de base de datos de una subred de VPC compartida a una subred de VPC no compartida y viceversa.

- Los participantes de una VPC compartida deben crear un grupo de seguridad en la VPC que les permita crear una instancia de base de datos.
- Los propietarios y los participantes de una VPC compartida pueden acceder a la base de datos mediante consultas SQL. Sin embargo, solo el creador de un recurso puede realizar llamadas a la API en el recurso.

Direccionamiento IP de Amazon RDS

Las direcciones IP permiten que los recursos de la VPC se comuniquen entre sí y con otros recursos a través de Internet. Amazon RDS admite los protocolos de direcciones IPv4 e IPv6. De forma predeterminada, Amazon RDS y Amazon VPC utilizan el protocolo de direccionamiento IPv4. No puedes desactivar este comportamiento. Al crear una VPC, debe especificar un bloque de CIDR IPv4 (un intervalo de direcciones IPv4 privadas). De manera opcional, puede asignar un bloque de CIDR IPv6 a su VPC y sus subredes y asignar direcciones IPv6 de dicho bloque a instancias de base de datos de su subred

La compatibilidad con el protocolo IPv6 amplía el número de direcciones IP admitidas. Al utilizar el protocolo IPv6, se asegura de tener suficientes direcciones disponibles para el futuro crecimiento de Internet. Los recursos de RDS nuevos y existentes pueden utilizar direcciones IPv4 e IPv6 dentro de su VPC. Configurar, proteger y traducir el tráfico de red entre los dos protocolos utilizados en diferentes partes de una aplicación puede provocar sobrecarga operativa. Puede estandarizar el protocolo IPv6 para los recursos de Amazon RDS para simplificar la configuración de la red.

Temas

- Direcciones IPv4
- Direcciones IPv6
- Modo de pila doble

Direcciones IPv4

Al crear una VPC, debe especificar un rango de direcciones IPv4 para la VPC como bloque de CIDR como `10.0.0.0/16`. Un grupo de subredes de base de datos define el rango de direcciones IP de este bloque de CIDR que puede utilizar una instancia de base de datos. Esta dirección IP puede ser privada o pública.

Una dirección IPv4 privada es una dirección IP a la que no se puede obtener acceso desde Internet. Se pueden usar direcciones IPv4 privadas para la comunicación entre la instancia de la base de datos y otros recursos, como instancias de Amazon EC2, en la misma VPC. Cada instancia de base de datos tiene una dirección IP privada para la comunicación en la VPC.

Una dirección IP pública es una dirección IPv4 a la que se puede acceder desde Internet. Se pueden usar direcciones públicas para la comunicación entre la instancia de la base de datos y los recursos en Internet, como un cliente SQL. Debe controlar si una instancia de base de datos recibe una dirección IP pública.

Para ver un tutorial que muestra cómo crear una VPC con solo direcciones IPv4 privadas que puede utilizar con un escenario habitual de Amazon RDS, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).

Direcciones IPv6

De manera opcional, puede asociar un bloque de CIDR IPv6 a su VPC y sus subredes y asignar direcciones IPv6 desde dicho bloque a los recursos de su VPC. Cada dirección IPv6 es única a nivel mundial.

El bloque de CIDR IPv6 de su VPC se asigna automáticamente de entre el grupo de direcciones IPv6 de Amazon. Usted no puede elegir el rango.

Al conectarse a una dirección IPv6, asegúrese de que se cumplan las siguientes condiciones:

- El cliente se ha configurado de manera que se permita el tráfico de la base de datos a través de IPv6.
- Los grupos de seguridad de RDS utilizados por la instancia de base de datos están configurados correctamente para permitir el tráfico de cliente a la base de datos a través de IPv6.
- La pila del sistema operativo de cliente permite el tráfico en la dirección IPv6. Además, los controladores y bibliotecas del sistema operativo están configurados para elegir el punto de conexión de la instancia de base de datos predeterminado correcto (IPv4 o IPv6).

Para obtener más información sobre IPv6, consulte el tema sobre direccionamiento IP en la Guía del usuario de Amazon VPC.

Modo de pila doble

Cuando una instancia de base de datos puede comunicarse a través de los protocolos de direcciones tanto IPv4 como IPv6, se ejecuta en modo de pila doble. Por lo tanto, los recursos

pueden comunicarse con la instancia de base de datos a través de IPv4, IPv6 o ambos. RDS deshabilita el acceso a la puerta de enlace de Internet para los puntos de conexión IPv6 de instancias de base de datos en modo de pila doble. RDS hace esto para garantizar que los puntos de conexión IPv6 sean privados y solo se pueda acceder a ellos desde la VPC.

Temas

- Modo de pila doble y grupos de subredes de base de datos
- Utilización de instancias de base de datos en modo de pila doble
- Modificación de instancias de base de datos de solo IPv4 para utilizar el modo de pila doble
- Disponibilidad en regiones y versiones
- Limitaciones de instancias de base de datos de red de pila doble

Para ver un tutorial donde se muestra cómo crear una VPC con las direcciones IPv4 y IPv6 que puede utilizar en un escenario habitual de Amazon RDS, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (modo de pila doble).

Modo de pila doble y grupos de subredes de base de datos

Para utilizar el modo de pila doble, asegúrese de que cada subred del grupo de subredes de base de datos que asocie a la instancia de base de datos tenga un bloque de CIDR de IPv6 asociado. Puede crear un nuevo grupo de subredes de base de datos o modificar un grupo existente de subredes de base de datos para cumplir este requisito. Cuando una instancia de base de datos esté en modo de pila doble, los clientes podrán conectarse como siempre. Asegúrese de que los firewalls de seguridad del cliente y los grupos de seguridad de instancias de base de datos RDS estén configurados correctamente para permitir el tráfico a través de IPv6. Para conectarse, los clientes utilizan el punto de conexión de la instancia de base de datos. Las aplicaciones de cliente pueden especificar qué protocolo prefieren al conectarse a una base de datos. En modo de pila doble, la instancia de base de datos detecta el protocolo de red preferido del cliente (IPv4 o IPv6) y utiliza ese protocolo para la conexión.

Si un grupo de subredes de base de datos deja de admitir el modo de pila doble debido a la eliminación de subredes o a la disociación de CIDR, existe el riesgo de que se produzca un estado de red incompatible para las instancias de base de datos asociadas al grupo de subredes de base de datos. Además, no puede utilizar el grupo de subredes de base de datos al crear una instancia nueva de base de datos en modo de pila doble.

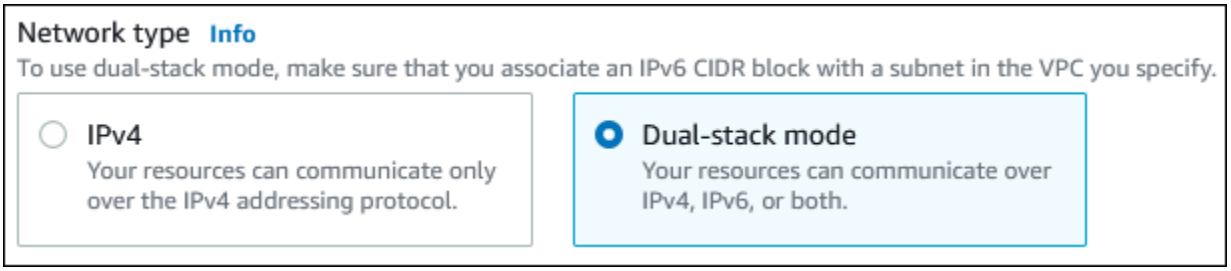
Para determinar si un grupo de subredes de base de datos admite el modo de pila doble mediante la AWS Management Console, consulte Network type (Tipo de red) en la página de detalles del grupo de subredes de base de datos. Para determinar si un grupo de subredes de base de datos admite el modo de pila doble mediante la AWS CLI, ejecute el comando describe-db-subnet-groups y la vista `SupportedNetworkTypes` en la salida.

Las réplicas de lectura se tratan como instancias de base de datos independientes y pueden tener un tipo de red diferente al de la instancia de base de datos principal. Si cambia el tipo de red de la instancia de base de datos principal de una réplica de lectura, la réplica de lectura no se verá afectada. Al restaurar una instancia de base de datos, puede restaurarla a cualquier tipo de red compatible.

Utilización de instancias de base de datos en modo de pila doble

Al crear o modificar una instancia de base de datos, puede especificar que el modo de pila doble permita que los recursos se comuniquen con su instancia de base de datos a través de IPv4, IPv6 o ambos.

Al utilizar la AWS Management Console para crear o modificar una instancia de base de datos, puede especificar el modo de pila doble en la sección Network type (Tipo de red). En la imagen siguiente se muestra la sección Network type (Tipo de red) en la consola.



Si utiliza la AWS CLI para crear o modificar una instancia de base de datos, establezca la opción `--network-type` en `DUAL` para utilizar el modo de pila doble. Si utiliza la API de RDS para crear o modificar una instancia de base de datos, establezca el parámetro `NetworkType` en `DUAL` para utilizar el modo de pila doble. Al modificar el tipo de red de una instancia de base de datos, puede haber un tiempo de inactividad. Si el modo de pila doble no es compatible con la versión del motor de base de datos o el grupo de subredes de base de datos especificados, se devuelve el error `NetworkTypeNotSupported`.

Para obtener más información acerca de la creación de una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS. Para obtener más información acerca

de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Para determinar si una instancia de base de datos está en modo de pila doble mediante la consola, consulte Network type (Tipo de red) en la pestaña Connectivity & security (Conectividad y seguridad) de la instancia de base de datos.

Modificación de instancias de base de datos de solo IPv4 para utilizar el modo de pila doble

Puede modificar la instancia de base de datos solo IPv4 para utilizar el modo de pila doble. Para ello, cambie el tipo de red de la instancia de base de datos. La modificación podría dar lugar a un tiempo de inactividad.

Se recomienda cambiar el tipo de red de las instancias de base de datos de Amazon RDS durante un período de mantenimiento. Actualmente, no se admite la configuración del tipo de red de las nuevas instancias en el modo de doble pila. Puede configurar el tipo de red manualmente mediante el comando `modify-db-instance` .

Antes de modificar una instancia de base de datos para utilizar el modo de pila doble, asegúrese de que su grupo de subredes de base de datos admite el modo de pila doble. Si el grupo de subredes de base de datos asociado a la instancia de base de datos no admite el modo de pila doble, especifique otro grupo de subredes de base de datos que lo admita cuando modifique la instancia de base de datos. La modificación del grupo de subredes de base de datos de una instancia de base de datos puede provocar un tiempo de inactividad.

Si modifica el grupo de subredes de base de datos de una instancia de base de datos antes de cambiar la instancia de base de datos para utilizar el modo de doble pila, asegúrese de que el grupo de subredes de base de datos sea válido para la instancia de base de datos antes y después del cambio.

Para instancias Single-AZ de RDS para PostgreSQL, RDS para MySQL, RDS para Oracle y RDS para MariaDB, le recomendamos que llame al comando modify-db-instance solo con el parámetro `--network-type` con el valor `DUAL` para cambiar la red al modo de doble pila. Si se añaden otros parámetros junto con el parámetro `--network-type` en la misma llamada a la API, se podría producir un tiempo de inactividad. Para modificar varios parámetros, asegúrese de que la modificación del tipo de red se haya completado correctamente antes de enviar otra solicitud de `modify-db-instance` con otros parámetros.

Las modificaciones del tipo de red para instancias de base de datos multi-AZ de RDS para PostgreSQL, RDS para MySQL, RDS para Oracle y RDS para MariaDB provocan un breve tiempo de

inactividad y producen una conmutación por error si solo utiliza el parámetro `--network-type` o si combina parámetros en un comando modify-db-instance.

Las modificaciones del tipo de red en instancias de base de datos single-AZ o multi-AZ de RDS para SQL Server provocan un tiempo de inactividad si solo se usa el parámetro `--network-type` o si se combinan parámetros en un comando `modify-db-instance`. Las modificaciones del tipo de red provocan una conmutación por error en una instancia multi-AZ de SQL Server.

Si no puede conectarse a la instancia de base de datos después del cambio, asegúrese de que los firewalls de seguridad de la base de datos y del cliente y las tablas de enrutamiento se hayan configurado correctamente para permitir el tráfico a la base de datos de la red seleccionada (IPv4 o IPv6). Es posible que también tenga que modificar los parámetros, las bibliotecas o los controladores del sistema operativo para conectarse mediante una dirección IPv6.

Cuando modifique una instancia de base de datos para utilizar el modo de pila doble, no puede haber un cambio pendiente de una implementación single-AZ a una implementación multi-AZ, ni de una implementación multi-AZ a una implementación single-AZ.

Para modificar una instancia de base de datos solo IPv4 para utilizar el modo de pila doble

1. Modifique un grupo de subredes de base de datos para admitir el modo de pila doble o cree un grupo de subredes de base de datos que admita el modo de pila doble:

   a. Asocie un bloque de CIDR IPv6 a su VPC.

      Para obtener más información, consulte el tema Agregue un bloque CIDR de IPv6 a su VPC en la Guía del usuario de Amazon VPC.

   b. Adjunte el bloque de CIDR IPv6 a todas las subredes de su grupo de subredes de base de datos.

      Para obtener más información, consulte el tema Agregue un bloque CIDR de IPv6 a su subred en la Guía del usuario de Amazon VPC.

   c. Confirme que el grupo de subredes de base de datos admita el modo de pila doble.

      Si utiliza la AWS Management Console, seleccione el grupo de subredes de base de datos y asegúrese de que el valor Supported network types (Tipos de redes compatibles) sea Dual, IPv4 (Doble, IPv4).

      Si utiliza la AWS CLI, ejecute el comando describe-db-subnet-groups y asegúrese de que el valor `SupportedNetworkType` de la instancia de base de datos sea `Dual, IPv4`.

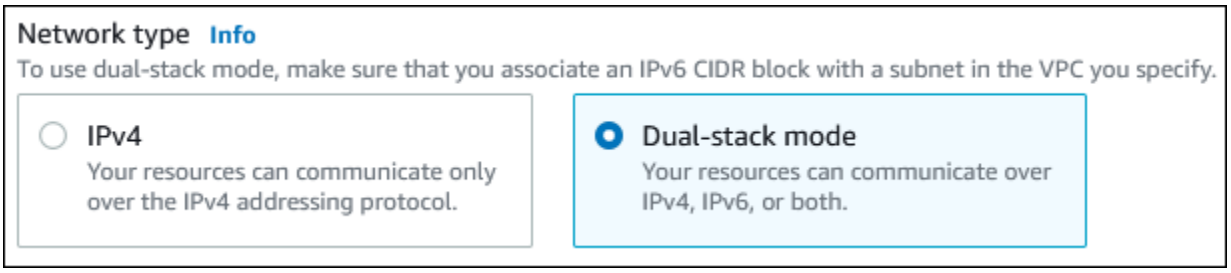
2. Modifique el grupo de seguridad asociado a la instancia de base de datos para permitir conexiones IPv6 a la base de datos o cree un nuevo grupo de seguridad que permita conexiones IPv6.

   Para obtener instrucciones, consulte el tema sobre cómo crear un grupo de seguridad en la Guía del usuario de Amazon VPC.

3. Modifique el clúster base de datos para admitir el modo de pila doble. Para ello, defina Network type (Tipo de red) en Dual-stack mode (Modo de pila doble).

   Si utiliza la consola, asegúrese de que la siguiente configuración sea correcta:

   - Network type (Tipo de red): Dual-stack mode (Modo de pila doble)



   - DB subnet group (Grupo de subredes de base de datos): el grupo de subredes de base de datos que configuró en un paso anterior
   - Security group (Grupo de seguridad): la seguridad que configuró en el paso anterior

   Si utiliza la AWS CLI, asegúrese de que la siguiente configuración sea correcta:

   - `--network-type` – `dual`
   - `--db-subnet-group-name`: el grupo de subredes de base de datos que configuró en un paso anterior
   - `--vpc-security-group-ids`: el grupo de seguridad de la VPC que configuró en un paso anterior

   Por ejemplo:

```
aws rds modify-db-instance --db-instance-identifier my-instance --network-type
 "DUAL"
```

4. Confirme que la instancia de base de datos admite el modo de pila doble.

Si utiliza la consola, elija la pestaña Connectivity & security (Conectividad y seguridad) (Configuración) para el clúster de base de datos. En esa pestaña, asegúrese de que el valor de Network type (Tipo de red) es Dual-stack mode (Modo de pila doble).

Si utiliza la AWS CLI, ejecute al comando describe-db-instances y asegúrese de que el valor `NetworkType` de la instancia de base de datos sea `dual`.

Ejecute el comando `dig` en el punto de conexión de la instancia de base de datos del para identificar la dirección IPv6 que tiene asociada.

```
dig db-instance-endpoint AAAA
```

Utilice el punto de conexión de la instancia de escritor (no la dirección IPv6) para conectarse a la instancia de base de datos.

Disponibilidad en regiones y versiones

La disponibilidad de las características varía según las versiones específicas de cada motor de base de datos y entre Regiones de AWS. Para obtener más información sobre la disponibilidad de versiones y regiones con el modo de pila doble, consulte Regiones y motores de bases de datos admitidos para el modo de doble pila en Amazon RDS.

Limitaciones de instancias de base de datos de red de pila doble

Las siguientes limitaciones se aplican a las instancias de base de datos de red de pila doble:

- Las instancias de base de datos no pueden utilizar el protocolo IPv6 exclusivamente. Pueden utilizar IPv4 exclusivamente o utilizar el protocolo IPv4 y IPv6 (modo de pila doble).
- Amazon RDS no admite subredes IPv6 nativas.
- Las instancias de base de datos que utilizan el modo de pila doble deben ser de tipo privado. No pueden ser accesibles públicamente.
- Para RDS for SQL Server, las instancias de base de datos en modo de pila doble que utilizan puntos de conexión de escucha de grupos de disponibilidad Always On AGs solo presentan direcciones IPv4.
- No puede utilizar RDS Proxy con instancias de base de datos en modo de pila doble.
- No puede utilizar el modo de pila doble con RDS en instancias de base de datos de AWS Outposts.

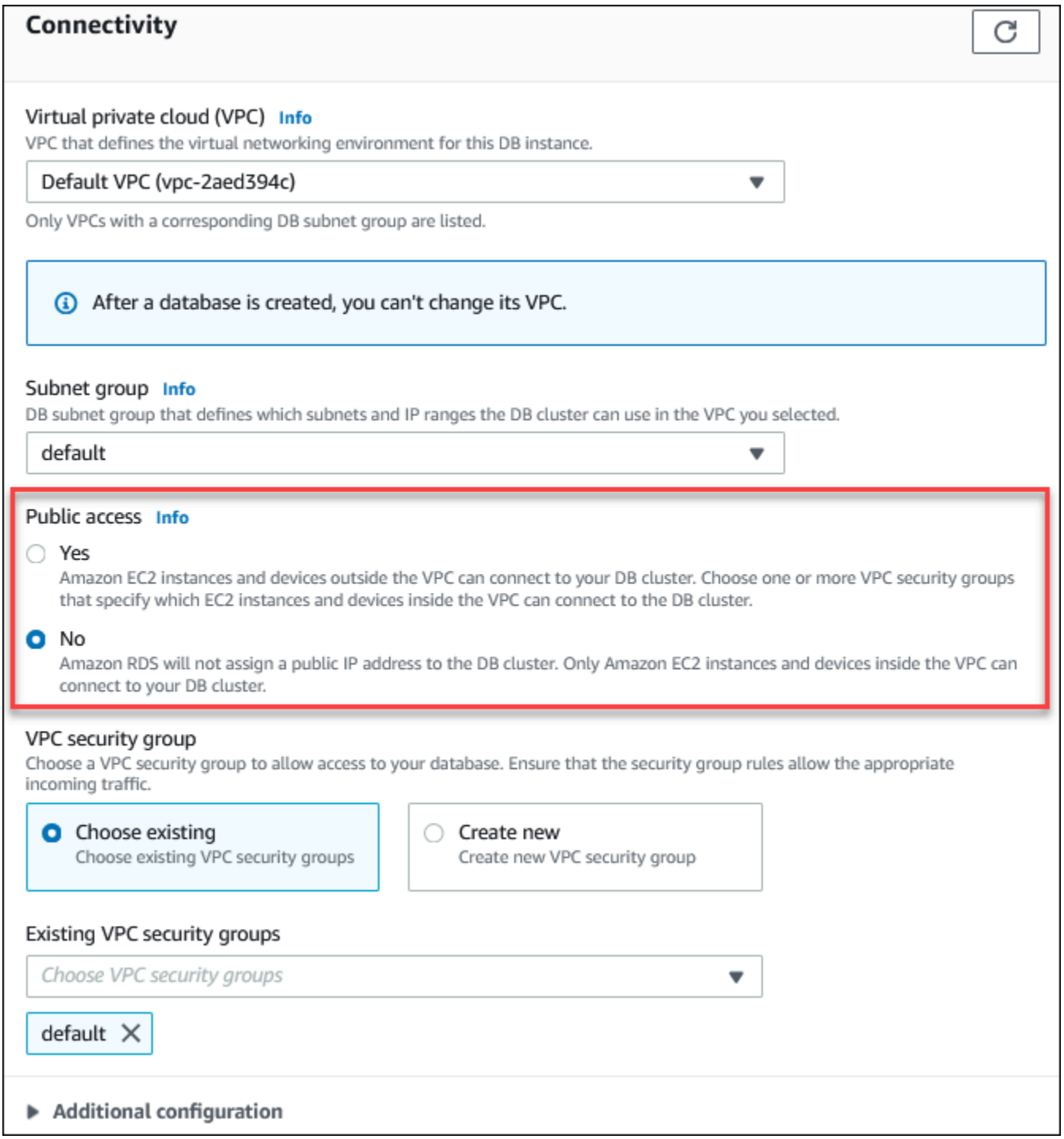
- No puede utilizar el modo de pila doble con instancias de base de datos en una zona local.

Cómo ocultar una instancia de base de datos en una VPC desde Internet.

Un escenario común de Amazon RDS consiste en tener una VPC en la que hay una instancia de Amazon EC2 con una aplicación web abierta al público y una instancia de base de datos con una base de datos que no es de acceso público. Por ejemplo, puede crear una VPC que tenga una subred pública y una subred privada. Las instancias de EC2 que funcionan como servidores web se pueden implementar en la subred pública. Los clústeres de base de datos se implementan en la subred privada. En una implementación de este tipo, solo los servidores web tienen acceso a las instancias de bases de datos. Para ver una ilustración de este escenario, consulte Acceso a una instancia de base de datos en una VPC desde una instancia de Amazon EC2 de la misma VPC.

Cuando lanza una instancia de base de datos dentro de una VPC, la instancia de base de datos tiene una dirección IP privada para el tráfico dentro de la VPC. Esta dirección IP privada no es accesible públicamente. Puede utilizar la opción Public access (Acceso público) para designar si la instancia de base de datos también tiene una dirección IP pública además de la dirección IP privada. Si la instancia se designa como de acceso público, su punto de conexión DNS se resuelve en la dirección IP privada desde dentro de la VPC. Se resuelve en la dirección IP pública desde fuera de la VPC. Acceso a el clúster de base de datos está controlado en última instancia por el grupo de seguridad que utiliza. No se permite el acceso público si el grupo de seguridad asignado a la instancia de la base de datos no incluye reglas de entrada que lo permitan. Además, para que una instancia de base de datos sea accesible públicamente, las subredes del grupo de subredes de base de datos deben tener una puerta de enlace de Internet. Para obtener más información, consulte No puede conectarse a la instancia de base de datos de Amazon RDS.

Es posible modificar una instancia de base de datos para activar o desactivar la accesibilidad pública modificando la opción Public access (Acceso público). En la ilustración siguiente se muestra la opción Public access (Acceso público) en la sección Additional connectivity configuration (Configuración de conectividad adicional). Para definir la opción, abra la sección Additional connectivity configuration (Configuración de conectividad adicional) en la sección Connectivity (Conectividad).



Para obtener información sobre cómo modificar una instancia de base de datos para establecer la opción Public access (Acceso público), consulte Modificación de una instancia de base de datos de Amazon RDS.

Creación de una instancia de base de datos en una VPC

Los siguientes procedimientos le ayudan a crear una instancia de base de datos en una VPC. Para utilizar la VPC predeterminada, puede comenzar con el paso 2, y utilizar la VPC y el grupo de subredes de la base de datos que ya se han creado para usted. Si desea crear una VPC adicional, puede crear una VPC nueva.

> **Note**
>
> Si desea que una instancia de base de datos de la VPC sea accesible públicamente, debe actualizar la información de DNS para la VPC activando los atributos DNS hostnames y DNS resolution de la VPC. Para obtener información acerca de cómo actualizar la información de DNS para una instancia de VPC, consulte Actualización de la compatibilidad de DNS para su VPC.

Siga estos pasos para crear una instancia de base de datos en una VPC:

- Paso 1: Crear una VPC
- Paso 2: Crear un grupo de subredes de base de datos
- Paso 3: Crear un grupo de seguridad de VPC
- Paso 4: Crear la instancia de base de datos en la VPC

Paso 1: Crear una VPC

Cree una VPC con subredes en al menos dos zonas de disponibilidad. Utilizará estas subredes cuando cree un grupo de subredes de base de datos. Si tiene una VPC predeterminada, se crea automáticamente una subred en cada zona de disponibilidad de la Región de AWS.

Para obtener más información, consulte Creación de una VPC con subredes públicas y privadas o Creación de una VPC en la Guía del usuario de Amazon VPC.

Paso 2: Crear un grupo de subredes de base de datos

Un grupo de subredes de base de datos es una colección de subredes (normalmente privadas) que se crean para una VPC y que después se asignan a las instancias de bases de datos. Un grupo de subredes de base de datos le permite especificar una VPC específica al crear instancias de bases

de datos utilizando la AWS CLI o API. Si utiliza la consola, solo puede elegir la VPC y las subredes que desea utilizar. Cada grupo de subredes de base de datos debe tener como mínimo una subred en al menos dos zonas de disponibilidad de la Región de AWS. Como práctica recomendada, cada grupo de subredes de base de datos debería tener al menos una subred por cada una de las zonas de disponibilidad en la Región de AWS.

Para las implementaciones Multi-AZ, si se define una subred para todas las zonas de disponibilidad de una Región de AWS, Amazon RDS podría crear una réplica en espera en otra zona de disponibilidad si fuera necesario. Puede seguir esta práctica recomendada incluso para las implementaciones Single-AZ, ya que quizá las convierta en implementaciones Multi-AZ en un futuro.

Para que una instancia de base de datos sea accesible públicamente, las subredes del grupo de subredes de base de datos deben tener una puerta de enlace de Internet. Para obtener más información sobre las puertas de enlace de Internet, consulte Conectar subredes a Internet por medio de una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.

> **Note**
>
> El grupo de subredes de base de datos para una zona local puede tener solo una subred.

Cuando crea una instancia de base de datos en una VPC, debe elegir un grupo de subredes de base de datos. Amazon RDS elige una subred y una dirección IP dentro de esa subred para asociarla con la instancia de base de datos. Si no existen grupos de subredes de base de datos, Amazon RDS crea un grupo de subredes predeterminado cuando se crea una instancia de base de datos. Amazon RDS crea y asocia una interfaz de red elástica a su instancia de base de datos con esa dirección IP. La instancia de base de datos utiliza la zona de disponibilidad que contiene la subred.

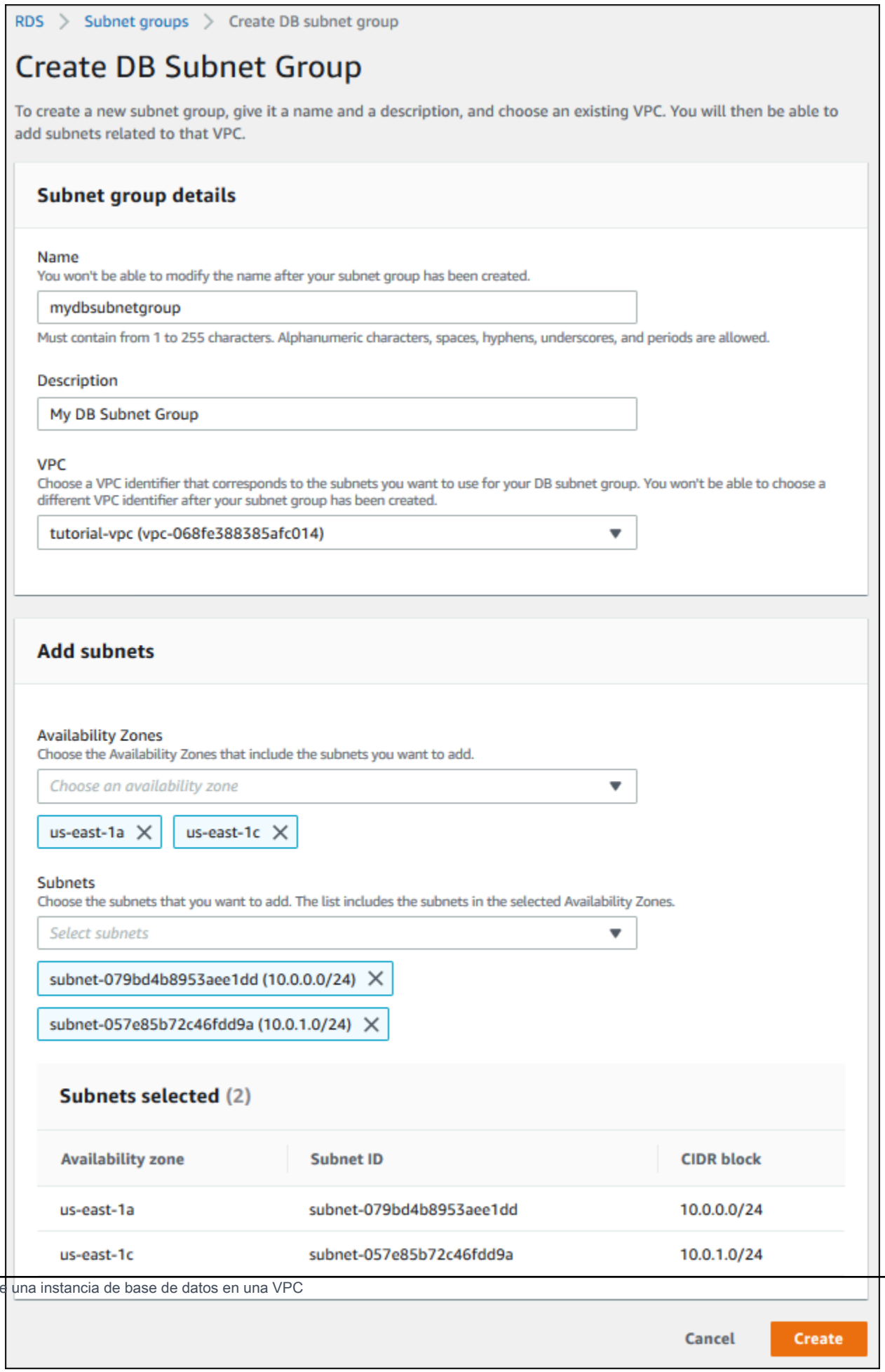
Para implementaciones Multi-AZ, si se define una subred para dos o más zonas de disponibilidad de una región de Región de AWS, Amazon RDS podrá crear una instancia en espera en otra zona de disponibilidad si fuera necesario. Debe hacerlo incluso para las implementaciones Single-AZ, por si desea convertirlos en implementaciones Multi-AZ en algún momento.

En este paso, debe crear un grupo de subredes de base de datos y debe agregar las subredes que creó para la VPC.

Para crear un grupo de subredes de base de datos

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

2. En el panel de navegación, elija Subnet groups.
3. Elija Create DB Subnet Group.
4. En Name, escriba el nombre del grupo de subredes de base de datos.
5. En Description, escriba la descripción del grupo de opciones de base de datos.
6. Para la VPC, elija la VPC predeterminada o la VPC que ha creado.
7. En la sección Agregar subredes, elija las zonas de disponibilidad que incluyen las subredes en Zonas de disponibilidad, y, a continuación, elija las subredes en Subredes.


RDS > Subnet groups > Create DB subnet group
Create DB Subnet Group
To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.
Subnet group details
Name
You won't be able to modify the name after your subnet group has been created.
mydbsubnetgroup
Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.
Description
My DB Subnet Group
VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.
tutorial-vpc (vpc-068fe388385afc014)
Add subnets
Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone
us-east-1a
us-east-1c
Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.
Select subnets
subnet-079bd4b8953aee1dd (10.0.0.0/24)
subnet-057e85b72c46fdd9a (10.0.1.0/24)
Subnets selected (2)
Availability zone
Subnet ID
CIDR block
us-east-1a
subnet-079bd4b8953aee1dd
10.0.0.0/24
us-east-1c
subnet-057e85b72c46fdd9a
10.0.1.0/24
Cancel
Create

> **Note**
>
> Si ha habilitado una zona local, puede elegir un grupo de zonas de disponibilidad en la página Create DB subnet group (Crear grupo de subredes de base de datos). En este caso, elija Availability Zone group (Grupo de zonas de disponibilidad), Availability Zones (Zonas de disponibilidad)y Subnets (Subredes).

8. Seleccione Create (Crear).

   El nuevo grupo de subredes de base de datos aparece en la lista de grupos de subredes de base de datos de la consola de RDS. Puede elegir el grupo de subredes de base de datos para ver los detalles, incluidas todas las subredes asociadas al grupo, en el panel de detalles de la parte inferior de la ventana.

Paso 3: Crear un grupo de seguridad de VPC

Antes de crear la instancia de base de datos, debe crear un grupo de seguridad de VPC para asociarlo a la instancia de base de datos. Si no crea un grupo de seguridad de VPC, puede utilizar el grupo de seguridad predeterminado cuando cree una instancia de base de datos. Para obtener instrucciones sobre cómo crear un grupo de seguridad para la instancia de base de datos, consulte Creación de un grupo de seguridad de VPC para una instancia de base de datos privada o consulte Controlar el tráfico hacia los recursos mediante grupos de seguridad en la Guía del usuario de Amazon VPC.

Paso 4: Crear la instancia de base de datos en la VPC

En este paso, se crea una instancia de base de datos y se utiliza el nombre de la VPC, el grupo de subredes de base de datos y el grupo de seguridad de VPC creados en los pasos anteriores.

> **Note**
>
> Si desea que una instancia de base de datos de la VPC sea accesible públicamente, debe activar los atributos DNS hostnames y DNS resolution de la VPC. Para obtener más información, consulte Atributos de DNS para su VPC en la Guía del usuario de Amazon VPC.

Para obtener más información sobre cómo crear una instancia de base de datos, consulte Creación de una instancia de base de datos de Amazon RDS.

Cuando la sección Connectivity (Conectividad) se lo pida, introduzca el nombre de la VPC, el grupo de subredes de base de datos y el grupo de seguridad de la VPC.

Actualización de la VPC para una instancia de base de datos

Puede utilizar la AWS Management Console para trasladar una instancia de base de datos a otra VPC.

Para obtener más información acerca de la modificación de una instancia de base de datos , consulte Modificación de una instancia de base de datos de Amazon RDS. En la sección Connectivity (Conectividad) de la página de modificación, que se muestra a continuación, ingrese el nuevo grupo de subredes de base de datos en el campo DB Subnet group (Grupo de subredes de base de datos). El grupo de subredes nuevo debe ser un grupo de subredes de una VPC nueva.



No puede cambiar la VPC de una instancia de base de datos si se cumplen las siguientes condiciones:

- La instancia de base de datos se encuentra en varias zonas de disponibilidad. Puede convertir la instancia de base de datos en una única zona de disponibilidad, trasladarla a una nueva VPC y, a continuación, convertirla de nuevo en una instancia de base de datos Multi-AZ. Para obtener más información, consulte Configuración y administración de una implementación multi-AZ para Amazon RDS.
- La instancia de base de datos tiene una o varias réplicas de lectura. Puede quitar las réplicas de lectura, trasladar la instancia de base de datos a una nueva VPC y, a continuación, volver a agregar las réplicas de lectura. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.
- La instancia de base de datos es una réplica de lectura. Puede promocionar la réplica de lectura y, a continuación, trasladar la instancia de base de datos independiente a una nueva VPC. Para

obtener más información, consulte Promoción de una réplica de lectura para convertirla en una instancia de base de datos independiente.

- El grupo de subredes de la VPC de destino no tiene subredes en la zona de disponibilidad de la instancia de base de datos. Puede agregar subredes en la zona de disponibilidad de la instancia de base de datos al grupo de subredes de base de datos y, a continuación, trasladar la instancia de base de datos a la nueva VPC. Para obtener más información, consulte Uso de los grupos de subredes de base de datos.

Escenarios de acceso a una instancia de base de datos en una VPC

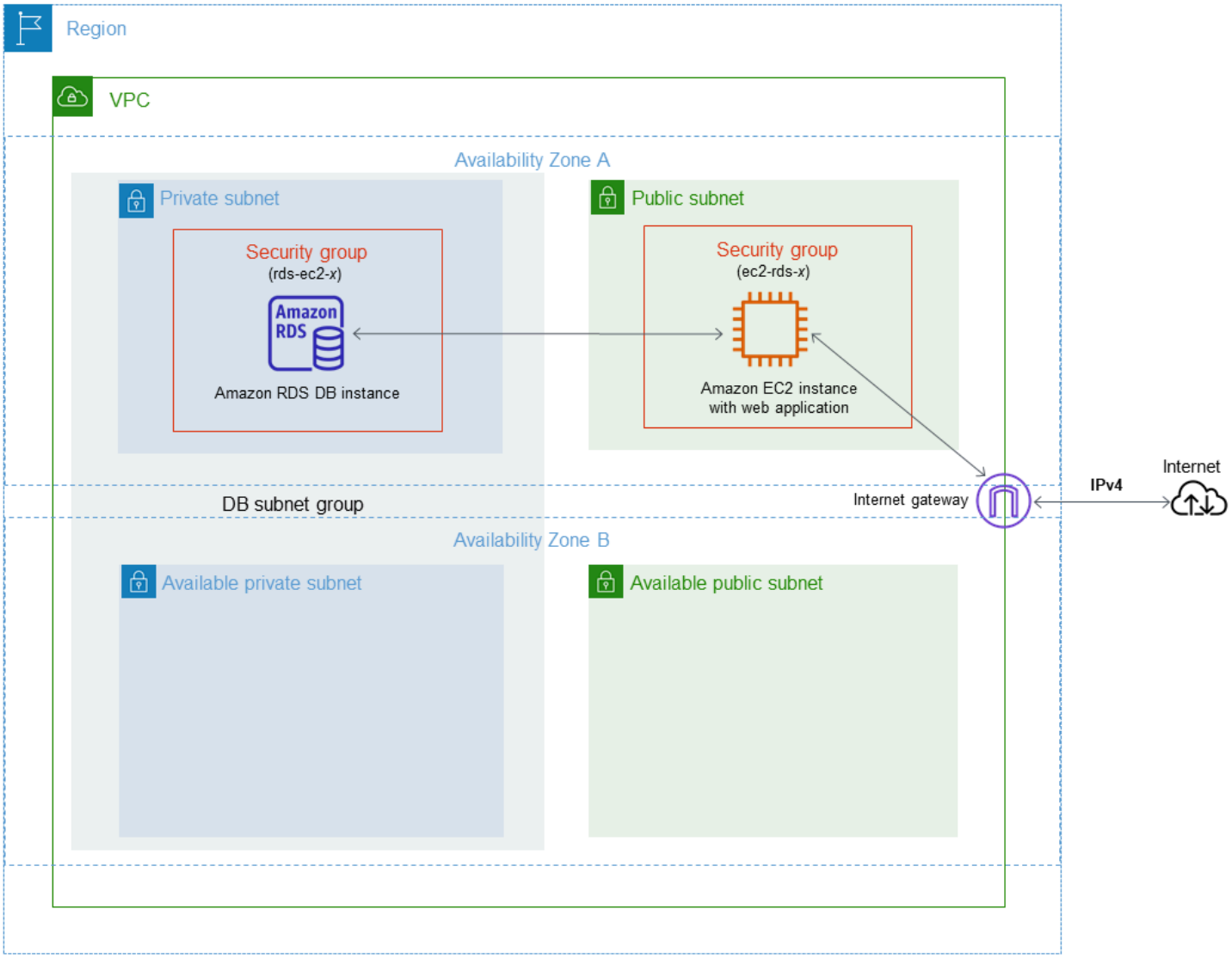
Amazon RDS admite los siguientes escenarios para acceder a una instancia de base de datos en una VPC:

- Una instancia de Amazon EC2 de la misma VPC
- Una instancia EC2 de otra VPC
- Una aplicación cliente a través de Internet
- Una red privada

Acceso a una instancia de base de datos en una VPC desde una instancia de Amazon EC2 de la misma VPC

Un uso común de una instancia de base de datos en una VPC es compartir datos con un servidor de aplicaciones que se ejecuta en una instancia de Amazon EC2 de la misma VPC.

En el siguiente diagrama se muestra este escenario.



La forma más sencilla de administrar el acceso entre instancias EC2 e instancias de bases de datos en la misma VPC es la siguiente:

- Cree el grupo de seguridad de VPC al que pertenecerán las instancias de bases de datos. Este grupo de seguridad se puede utilizar para restringir el acceso a las instancias de bases de datos. Por ejemplo, puede crear una regla personalizada para este grupo de seguridad. Esto puede permitir el acceso TCP utilizando el puerto que asignó a la instancia de base de datos cuando lo creó y una dirección IP que utiliza para acceder a la instancia de base de datos para el desarrollo u otras finalidades.
- Cree el grupo de seguridad de VPC al que pertenecerán las instancias EC2 (clientes y servidores web). Este grupo de seguridad puede, si es necesario, permitir el acceso a la instancia EC2 desde Internet a través de la tabla de enrutamiento de la VPC. Por ejemplo, puede establecer reglas en

este grupo de seguridad para permitir el acceso mediante TCP a la instancia EC2 a través del puerto 22.

- Cree reglas personalizadas en el grupo de seguridad para las instancias de bases de datos que permitan las conexiones desde el grupo de seguridad que creó para las instancias EC2. Estas reglas podrían permitir a cualquier miembro del grupo de seguridad acceder a las instancias de base de datos.

Hay una subred pública y privada adicional en una zona de disponibilidad independiente. Un grupo de subredes de base de datos de RDS requiere una subred en al menos dos zonas de disponibilidad. La subred adicional facilita el cambio a una implementación de instancia de base de datos multi-AZ en el futuro.

Para ver un tutorial que muestra cómo crear una VPC con subredes públicas y privadas para este escenario, consulte Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4).

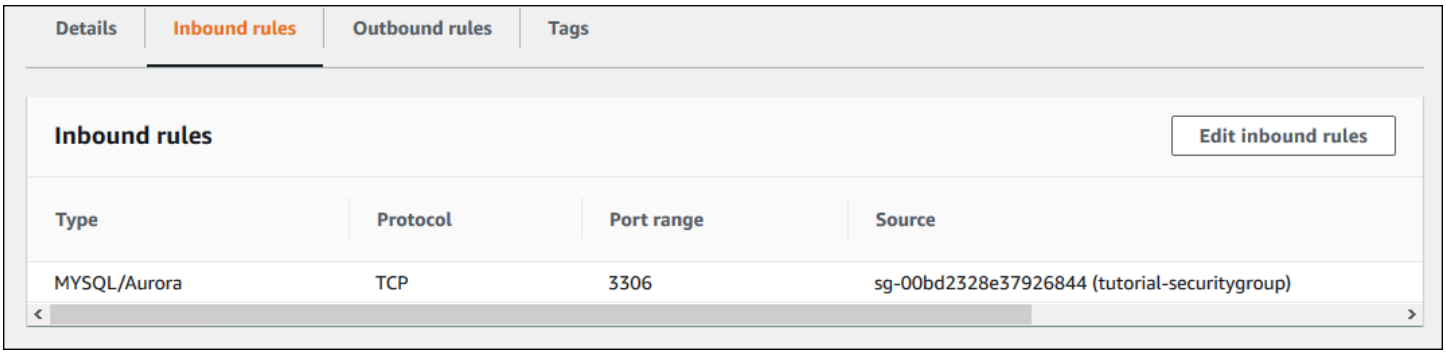
> **Tip**
>
> Puede configurar la conectividad de red entre una instancia de Amazon EC2 y una instancia de base de datos automáticamente al crear la instancia de base de datos. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2.

Para crear una regla en un grupo de seguridad de VPC que permita establecer conexiones desde otro grupo de seguridad, haga lo siguiente:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Elija o cree el grupo de seguridad al que desea que puedan tener acceso los miembros de otro grupo de seguridad. En el escenario anterior, este es el grupo de seguridad que utiliza para las instancias de base de datos. Elija la pestaña Inbound Rules (Reglas de entrada) y, a continuación, elija Edit inbound rules (Editar reglas de entrada).
4. En la página Edit inbound rules (Editar reglas de entrada), elija Add Rule (Agregar regla).
5. En Type (Tipo), elija la entrada que corresponda al puerto que utilizó al crear la instancia de base de datos, como MySQL/Aurora.

6. En el cuadro Origen, comience a escribir el ID del grupo de seguridad, que enumera los grupos de seguridad coincidentes. Elija el grupo de seguridad cuyos miembros desea que tengan acceso a los recursos protegidos por este grupo de seguridad. En el escenario anterior, este es el grupo de seguridad que utiliza para su instancia EC2.
7. Si es necesario, repita los pasos para el protocolo TCP creando una regla con Todo TCP en el campo Tipo y con el grupo de seguridad en el campo Origen. Si va a utilizar el protocolo UDP, cree una regla con All UDP (Todo UDP) en el campo Type (Tipo) y con el grupo de seguridad en el campo Source (Origen).
8. Seleccione Guardar reglas.

La siguiente pantalla muestra una regla de entrada con un grupo de seguridad para su origen.

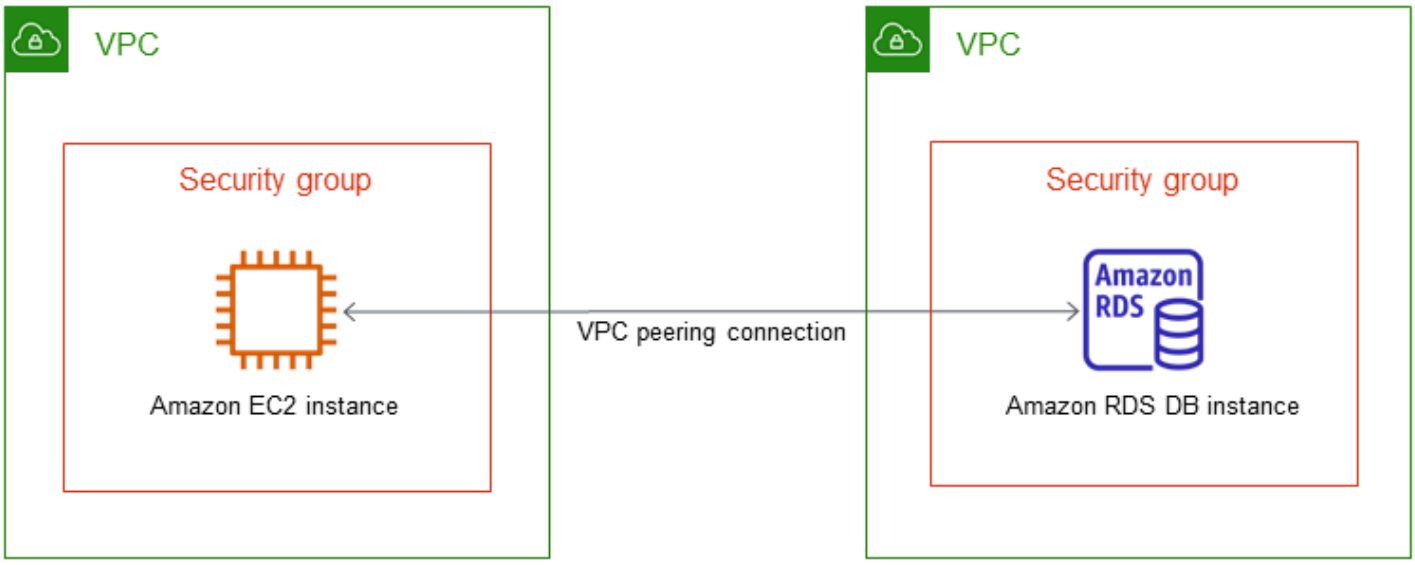


Para obtener más información sobre cómo conectarse a la instancia de base de datos desde su instancia de EC2, consulte Conexión a una instancia de base de datos de Amazon RDS .

Acceso a una instancia de base de datos en una VPC desde una instancia EC2 de otra VPC

Cuando una instancia de base de datos está en una VPC que no coincide con la de la instancia EC2 que se está utilizando para obtener acceso a ella, puede usar la interconexión con VPC para obtener acceso a la instancia de base de datos.

En el siguiente diagrama se muestra este escenario.

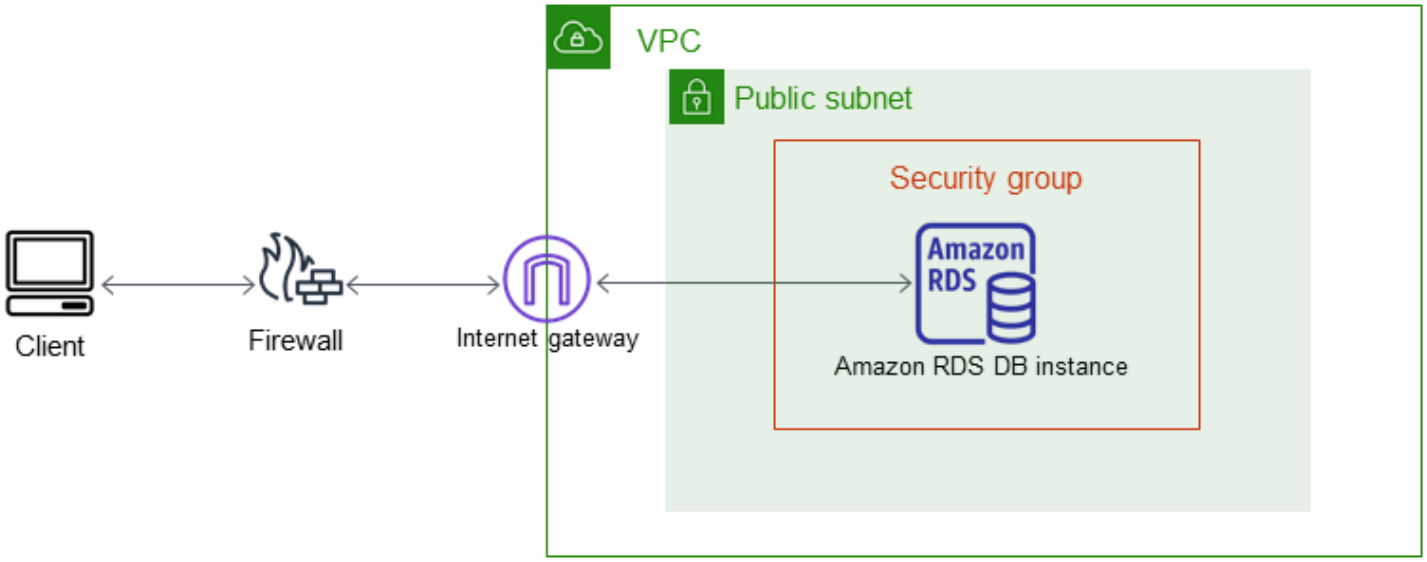


Una conexión de emparejamiento de VPC es una conexión de redes entre dos VPC que permite direccionar el tráfico entre ellas mediante direcciones IP privadas. Los recursos de ambas VPC se pueden comunicar entre sí siempre que se encuentren en la misma red. Puede crear una conexión de emparejamiento de VPC entre sus propias VPC, con una VPC de otra cuenta de AWS o con una VPC de otra Región de AWS. Para obtener más información sobre las interconexiones de VPC, consulte Interconexión con VPC en la Guía de usuario de Amazon Virtual Private Cloud.

Acceso a una instancia de base de datos en una VPC desde una aplicación cliente a través de internet

Para acceder a una instancia de base de datos en una VPC desde una aplicación cliente a través de internet, configure una VPC con una subred pública única y una puerta de enlace de Internet para permitir la comunicación a través de internet.

En el siguiente diagrama se muestra este escenario.



Recomendamos la siguiente configuración:

- Una VPC de tamaño /16 (por ejemplo, CIDR: 10.0.0.0/16). Este tamaño proporciona 65 536 direcciones IP privadas.
- Una subred de tamaño /24 (por ejemplo, CIDR: 10.0.0.0/24). Este tamaño proporciona 256 direcciones IP privadas.
- Una instancia de base de datos de Amazon RDS que se ha asociado a la VPC y a la subred. Amazon RDS asigna una dirección IP de la subred a la instancia de base de datos.
- Una gateway de Internet que conecte la VPC a Internet y a otros productos de AWS.
- Un grupo de seguridad asociado a la instancia de base de datos. Las reglas de entrada del grupo de seguridad permiten a la aplicación cliente obtener acceso a la instancia de base de datos.

Para obtener información acerca de la creación de una instancia de base de datos en una VPC, consulte Creación de una instancia de base de datos en una VPC.

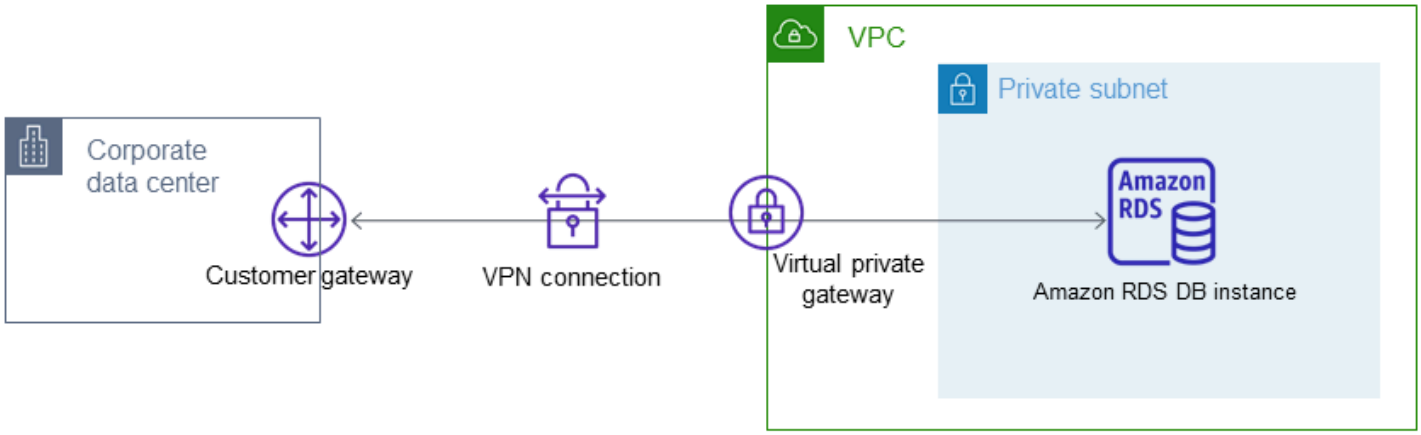
Una instancia de base de datos en una VPC a la que se accede mediante una red privada

Si su instancia de base de datos no es accesible públicamente, tiene las siguientes opciones para acceder a ella desde una red privada:

- Una conexión de Site-to-Site VPN de AWS. Para obtener más información, consulte ¿Qué es AWS Site-to-Site VPN?

- Una conexión de AWS Direct Connect. Para obtener más información, consulte ¿Qué es AWS Direct Connect?
- Una conexión de AWS Client VPN. Para obtener más información, consulte ¿Qué es AWS Client VPN?

El siguiente diagrama muestra un escenario con una conexión de Site-to-site VPN AWS.

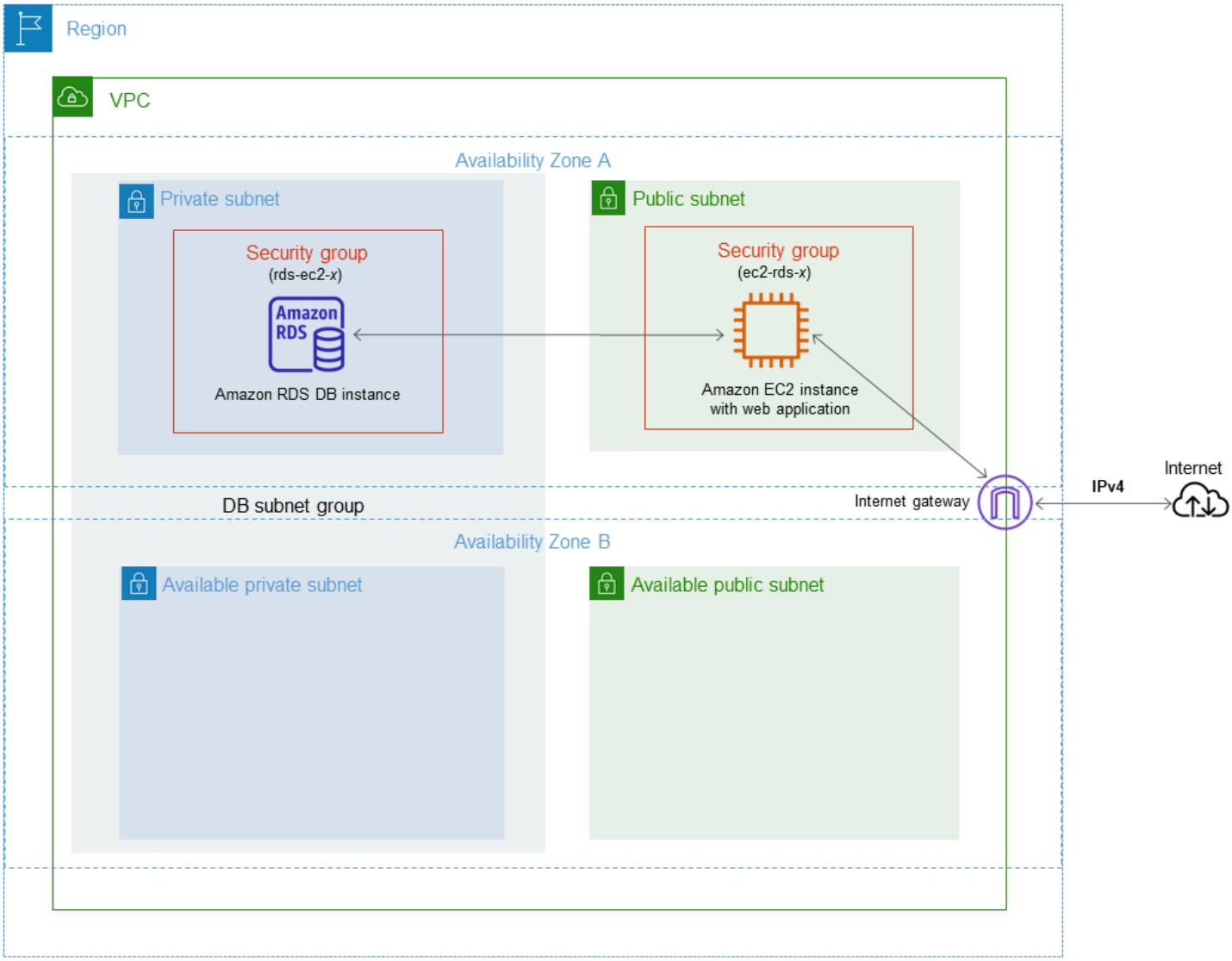


Para obtener más información, consulte Privacidad del tráfico entre redes.

Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (solo IPv4)

Un escenario común incluye una instancia de base de datos en una nube privada virtual (VPC) basada en el servicio Amazon VPC. Esta VPC comparte datos con un servidor web que se ejecuta en la misma VPC. En este tutorial se crea la VPC para este escenario.

En el siguiente diagrama se muestra este escenario. Para obtener información acerca de otros escenarios, consulte Escenarios de acceso a una instancia de base de datos en una VPC.



Su instancia de bases de datos debe estar disponible únicamente para su servidor web, y no para la Internet pública. Además, cree de una VPC con subredes públicas y privadas. El servidor web está alojado en la subred pública, para que pueda obtener acceso a la red pública de internet. La

instancia de base de datos se aloja en una subred privada. El servidor web puede conectarse a la instancia de base de datos porque se aloja en la misma VPC. Sin embargo, la instancia de base de datos no está disponible en la red pública de internet, lo que proporciona mayor seguridad.

Este tutorial configura una subred pública y privada adicional en una zona de disponibilidad independiente. En el tutorial no se utilizan estas subredes. Un grupo de subredes de base de datos de RDS requiere una subred en al menos dos zonas de disponibilidad. La subred adicional facilita el cambio a una implementación de instancia de base de datos multi-AZ en el futuro.

En este tutorial se describe la configuración de una VPC para de instancias de bases de datos de Amazon RDS. Para ver un tutorial que muestra cómo crear un servidor web para este escenario de la VPC, consulte Explicación: crear un servidor web y una instancia de base de datos de Amazon RDS. Para obtener más información sobre Amazon VPC, consulte la guía de introducción de Amazon VPC y la guía del usuario de Amazon VPC.

> **Tip**
>
> Puede configurar la conectividad de red entre una instancia de Amazon EC2 y una instancia de base de datos automáticamente al crear la instancia de base de datos. La configuración de red es similar a la que se describe en este tutorial. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2.

Creación de una VPC con subredes públicas y privadas

Utilice el siguiente procedimiento para crear una VPC con subredes públicas y privadas.

Para crear una VPC y las subredes

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En la esquina superior derecha de la AWS Management Console, elija la región en la que desea crear la VPC. En este ejemplo se utiliza la región EE.UU. Oeste (Oregón).
3. En la esquina superior izquierda, elija VPC Dashboard (Panel de control VPC). Para comenzar a crear una VPC, elija Create VPC (Crear una VPC).
4. En Resources to create (Recursos para crear), en VPC settings (Configuración VPC), elija VPC and more (VPC y más).
5. En VPC settings (Configuración de la VPC), establezca estos valores:

- Name tag auto-generation (Generación automática de etiquetas de nombre): **`tutorial`**
- IPv4 CIDR block (Bloque de CIDR IPv4): **`10.0.0.0/16`**
- IPv6 CIDR block (Bloque de CIDR IPv6): ningún bloque de CIDR IPv6
- Tenancy (Tenencia): predeterminada
- Number of Availability Zones (AZs) (Número de zonas de disponibilidad): 2
- Customize AZs (Personalizar AZ): conserve los valores predeterminados.
- Number of public subnet (Número de subredes públicas): 2
- Number of private subnets (Número de subredes privadas): 2
- Customize subnets CIDR blocks (Personalizar bloques CIDR de subredes): conserve los valores predeterminados.
- NAT gateways ($) (Puertas de enlace NAT): ninguna
- VPC endpoints (Puntos de conexión de VPC): ninguna
- DNS options (Opciones de DNS): conserve los valores predeterminados.

> **Note**
>
> Amazon RDS requiere al menos dos subredes en dos zonas de disponibilidad diferentes para admitir implementaciones de instancias de base de datos multi-AZ. En este tutorial se crea una implementación Single-AZ, pero el requisito facilita la conversión a una implementación de instancia de base de datos Multi-AZ en el futuro.

6. Seleccione Creación de VPC.

Creación de un grupo de seguridad de VPC para un servidor web público

Primero debe crear un grupo de seguridad para el acceso público. Para conectarse a instancias de EC2 públicas en su VPC, añada reglas de entrada a su grupo de seguridad de VPC. Permiten que el tráfico se conecte desde Internet.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).

3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:

   - Security group name (Nombre de grupo de seguridad: **`tutorial-securitygroup`**
   - Description: **`Tutorial Security Group`**
   - VPC: elija la VPC que creó en el paso anterior, por ejemplo, vpc-***`identificador`***(tutorial-vpc)

4. Agregar reglas de entrada al grupo de seguridad

   a. Determine la dirección IP que usará para conectarse a las instancias de EC2 mediante Secure Shell (SSH). Para determinar su dirección IP pública, en una ventana o pestaña distinta del navegador, puede utilizar el servicio en https://checkip.amazonaws.com. Un ejemplo de dirección IP es `203.0.113.25/32`.

      En muchos casos, puede conectarse a través de un proveedor de servicios de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, busque el rango de direcciones IP utilizadas por los ordenadores cliente.

      > **Warning**
      >
      > Si utiliza `0.0.0.0/0` para el acceso SSH, permita que todas las direcciones IP accedan a sus instancias públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo debe autorizar una dirección IP específica o un intervalo de direcciones para acceder a sus instancias mediante SSH.

   b. En la sección Inbound rules (Reglas de entrada), elija Add rule (agregar regla).

   c. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el acceso SSH a la instancia de Amazon EC2. Si lo hace, puede conectarse a la instancia de Amazon EC2 para instalar el servidor web y otras utilidades. También puede conectarse a su instancia de EC2 para cargar contenido para el servidor web.

      - Tipo: **`SSH`**
      - Origen: la dirección IP o el rango de direcciones del Paso a, por ejemplo **`203.0.113.25/32`**.

   d. Seleccione Add rule (Agregar regla).

e. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el acceso HTTP al servidor web.

- Tipo: **HTTP**
- Origen: **0.0.0.0/0**

5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

   Anote el ID del grupo de seguridad, ya que lo necesitará más tarde en este tutorial.

Creación de un grupo de seguridad de VPC para una instancia de base de datos privada

Para que una instancia de base de datos sea privada, debe crear un segundo grupo de seguridad para el acceso privado. Para conectarse a instancias de base de datos privada en la VPC, agregue reglas de entrada al grupo de seguridad de la VPC que permitan el tráfico solo desde el servidor web.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Security group name (Nombre de grupo de seguridad: **tutorial-db-securitygroup**
   - Description: **Tutorial DB Instance Security Group**
   - VPC: elija la VPC que creó en el paso anterior, por ejemplo, vpc-***identificador***(tutorial-vpc)
4. Agregar reglas de entrada al grupo de seguridad
   a. En la sección Inbound rules (Reglas de entrada), elija Add rule (gregar regla).
   b. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el tráfico de MySQL en el puerto 3306 desde la instancia de Amazon EC2. Si lo hace, podrá conectarse desde su servidor web a su instancia de base de datos. Si lo hace, puede almacenar y recuperar datos en la base de datos desde la aplicación web.
      - Tipo: **MySQL/Aurora**

- Source (Origen): el identificador del grupo de seguridad tutorial-securitygroup que creó anteriormente en este tutorial, por ejemplo, sg-9edd5cfb.

5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

Creación de un grupo de subredes de base de datos

Un grupo de subredes de base de datos es una colección de subredes que se crea en una VPC y que después se asigna a las instancias de bases de datos. Un grupo de subredes de base de datos le permite especificar una VPC específica al crear instancias de bases de datos.

Para crear un grupo de subredes de base de datos

1. Identifique las subredes privadas de la base de datos en la VPC.

   a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

   b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Subnets (Subredes).

   c. Observe los ID de subred de las subredes denominadas tutorial-subred-private1-us-west-2a ytutorial-subnet-private2-us-west-2b.

      Necesitará los ID de subred cuando cree el grupo de subredes de base de datos.

2. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

   Asegúrese de conectarse a la consola de Amazon RDS, no a la consola de Amazon VPC.

3. En el panel de navegación, elija Subnet groups.

4. Elija Create DB Subnet Group (Crear grupo de subredes de base de datos).

5. En la página Create DB subnet group (Crear grupo de subredes de base de datos), establezca estos valores en Subnet group details (Detalles del grupo de subredes):

   - Name: **`tutorial-db-subnet-group`**
   - Description: **`Tutorial DB Subnet Group`**
   - VPC: tutorial-vpc (vpc-***`identificador`***)

6. En la sección Agregar subredes elija las Zonas de disponibilidad y Subredes.

   Para este tutorial, elija us-west-2a y us-west-2b en Availability Zones (Zonas de disponibilidad). En Subnets (Subredes), elija las subredes privadas que identificó en el paso anterior.

7. Seleccione Crear.

   El nuevo grupo de subredes de base de datos aparece en la lista de grupos de subredes de base de datos de la consola de RDS. Puede elegir el grupo de subredes de base de datos para ver los detalles en el panel de detalles de la parte inferior de la ventana. Estos detalles incluyen todas las subredes asociadas al grupo.

> **Note**
>
> Si creó esta VPC para completar Explicación: crear un servidor web y una instancia de base de datos de Amazon RDS, cree el de la instancia de base de datos siguiendo las instrucciones que se indican en Crear una instancia de base de datos de Amazon RDS .

Eliminación de la VPC

Después de crear la VPC y otros recursos para este tutorial, puede eliminarlos si ya no son necesarios.

> **Note**
>
> Si agregó recursos en la VPC que creó para este tutorial, es posible que primero tenga que eliminar estos para poder eliminar la VPC. Por ejemplo, estos recursos pueden incluir instancias de Amazon EC2 o instancias de base de datos de Amazon RDS. Para obtener más información, consulte Eliminación de la VPC en la Guía del usuario de Amazon VPC.

Para eliminar una VPC y los recursos relacionados

1. Elimine el grupo de subred de base de datos.
   a. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
   b. En el panel de navegación, elija Subnet groups.
   c. Seleccione el grupo de subred de base de datos que desea eliminar, como tutorial-db-subnet-group.
   d. Elija Eliminar y, a continuación, elija Eliminar en la ventana de confirmación.
2. Anote el ID de la VPC.

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione VPCs.
c. En la lista, identifique la VPC que creó, como, por ejemplo, tutorial-vpc.
d. Anote el ID de la VPC que ha creado. Necesitará el ID de la VPC en pasos posteriores.

3. Elimine los grupos de seguridad.

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
b. Seleccione Panel de control de VPC y, a continuación, seleccione Grupos de seguridad.
c. Seleccione el grupo de seguridad de la instancia de base de datos de Amazon RDS, como, por ejemplo, tutorial-db-securitygroup.
d. En Actions (Acciones), elija Delete security groups (Eliminar grupos de seguridad) y, a continuación, seleccione Delete (Eliminar) en la página de confirmación.
e. En la página Grupos de seguridad, seleccione el grupo de seguridad para la instancia de Amazon EC2, como, por ejemplo, tutorial-securitygroup.
f. En Actions (Acciones), elija Delete security groups (Eliminar grupos de seguridad) y, a continuación, seleccione Delete (Eliminar) en la página de confirmación.

4. Eliminación de la VPC

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione VPCs.
c. Seleccione la VPC que desea eliminar, como, por ejemplo tutorial-vpc.
d. En Actions (Acciones), elija Delete VPC (Eliminar VPC).

   La página de confirmación muestra otros recursos asociados a la VPC que también se eliminarán, incluidas las subredes asociadas a ella.
e. En la página de confirmación, introduzca **`delete`** y elija Eliminar.

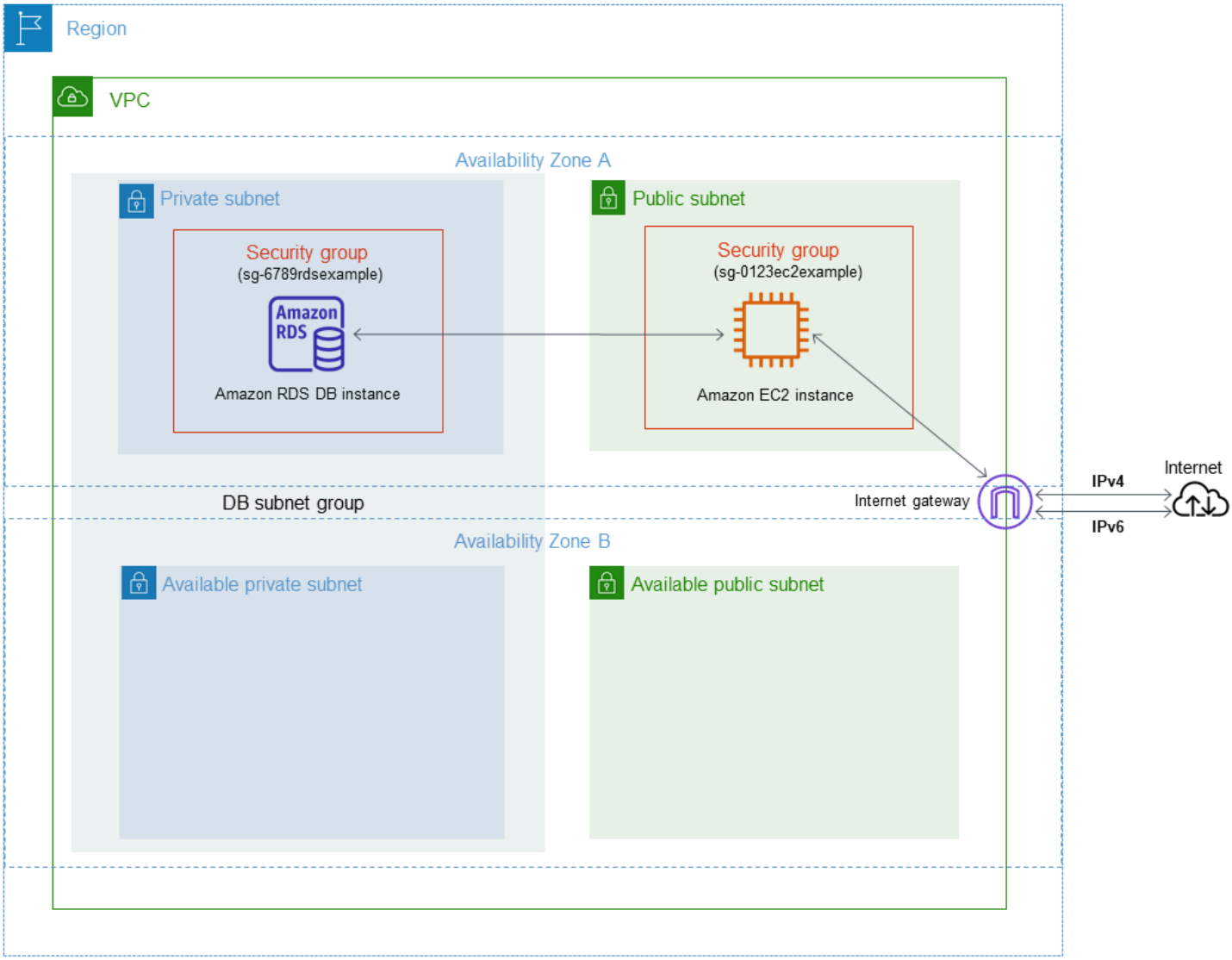
Tutorial: Creación de una VPC para utilizarla con una instancia de base de datos (modo de pila doble)

Un escenario común incluye una instancia de base de datos en una nube privada virtual (VPC) basada en el servicio Amazon VPC. Esta VPC comparte datos con una instancia de Amazon EC2 pública que se ejecuta en la misma VPC.

En este tutorial, creará la VPC para este escenario que funciona con una base de datos que se ejecuta en modo de pila doble. Modo de doble pila para permitir la conexión a través del protocolo de direccionamiento IPv6. Para obtener más información sobre el direccionamiento de IP, consulte Direccionamiento IP de Amazon RDS.

Las instancias de red de doble pila se admiten en la mayoría de las regiones. Para obtener más información, consulte Disponibilidad en regiones y versiones. Para ver las limitaciones del modo de doble pila, consulte Limitaciones de instancias de base de datos de red de pila doble.

En el siguiente diagrama se muestra este escenario.



Para obtener información acerca de otros escenarios, consulte Escenarios de acceso a una instancia de base de datos en una VPC.

Su instancia de bases de datos debe estar disponible únicamente para su instancia de Amazon EC2, y no para la Internet pública. Además, cree de una VPC con subredes públicas y privadas. La instancia de Amazon EC2 está alojada en la subred pública, para que pueda acceder a la red pública de internet. La instancia de base de datos se aloja en una subred privada. La instancia de Amazon EC2 se puede conectar a la instancia de base de datos porque se aloja en la misma VPC. Sin embargo, la instancia de base de datos no está disponible en la red pública de internet, lo que proporciona mayor seguridad.

Este tutorial configura una subred pública y privada adicional en una zona de disponibilidad independiente. En el tutorial no se utilizan estas subredes. Un grupo de subredes de base de datos

de RDS requiere una subred en al menos dos zonas de disponibilidad. La subred adicional facilita el cambio a una implementación de instancia de base de datos multi-AZ en el futuro.

Para crear una instancia de base de datos que utilice el modo de pila doble, especifique Dual-stack mode (Modo pila doble) en el ajuste Network type (Tipo de red). También puede modificar una instancia de base de datos con el mismo ajuste. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS y Modificación de una instancia de base de datos de Amazon RDS.

En este tutorial se describe la configuración de una VPC para de instancias de bases de datos de Amazon RDS. Para obtener más información acerca de Amazon VPC, consulte la Guía del usuario de Amazon VPC.

Creación de una VPC con subredes públicas y privadas

Utilice el siguiente procedimiento para crear una VPC con subredes públicas y privadas.

Para crear una VPC y las subredes

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En la esquina superior derecha de la AWS Management Console, elija la región en la que desea crear la VPC. En este ejemplo se utiliza la región Este de EE. UU. (Ohio).
3. En la esquina superior izquierda, elija VPC Dashboard (Panel de control VPC). Para comenzar a crear una VPC, elija Create VPC (Crear una VPC).
4. En Resources to create (Recursos para crear), en VPC settings (Configuración VPC), elija VPC and more (VPC y más).
5. Para el resto de opciones de VPC settings (Configuración de la VPC), defina estos valores:
   - Name tag auto-generation (Generación automática de etiquetas de nombre): **`tutorial-dual-stack`**
   - IPv4 CIDR block (Bloque de CIDR IPv4): **`10.0.0.0/16`**
   - IPv6 CIDR block (Bloque de CIDR IPv6): bloque de CIDR IPv6 proporcionado por Amazon
   - Tenancy (Tenencia): predeterminada
   - Number of Availability Zones (AZs) (Número de zonas de disponibilidad): 2
   - Customize AZs (Personalizar AZ): conserve los valores predeterminados.
   - Number of public subnet (Número de subredes públicas): 2
   - Number of private subnets (Número de subredes privadas): 2

- Customize subnets CIDR blocks (Personalizar bloques CIDR de subredes): conserve los valores predeterminados.
- NAT gateways ($) (Puertas de enlace NAT): ninguna
- Egress only internet gateway (Puerta de enlace de internet solo de salida): no
- VPC endpoints (Puntos de conexión de VPC): ninguna
- DNS options (Opciones de DNS): conserve los valores predeterminados.

> **Note**
>
> Amazon RDS requiere al menos dos subredes en dos zonas de disponibilidad diferentes para admitir implementaciones de instancias de base de datos multi-AZ. En este tutorial se crea una implementación Single-AZ, pero el requisito facilita la conversión a una implementación de instancia de base de datos Multi-AZ en el futuro.

6. Seleccione Crear VPC.

Para crear un grupo de seguridad de la VPC para una instancia de Amazon EC2 pública

Primero debe crear un grupo de seguridad para el acceso público. Para conectarse a instancias EC2 públicas, añada reglas de entrada al grupo de seguridad de la VPC que permitan el tráfico para las conexiones desde internet.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Security group name (Nombre de grupo de seguridad: **`tutorial-dual-stack-securitygroup`**
   - Description: **`Tutorial Dual-Stack Security Group`**
   - VPC: elija la VPC que creó en el paso anterior, por ejemplo, vpc-***`identificador`***(tutorial-dual-stack-vpc)

4. Agregar reglas de entrada al grupo de seguridad

   a. Determine la dirección IP que usará para conectarse a las instancias de EC2 mediante Secure Shell (SSH).

      Un ejemplo de dirección del protocolo de internet versión 4 (IPv4) es `203.0.113.25/32`. Un ejemplo de rango de direcciones del protocolo de internet versión 6 (IPv6) es `2001:db8:1234:1a00::/64`.

      En muchos casos, puede conectarse a través de un proveedor de internet (ISP) o protegido por un firewall sin una dirección IP estática. Si es así, busque el rango de direcciones IP utilizadas por los ordenadores cliente.

      > **Warning**
      >
      > Si utiliza `0.0.0.0/0` para IPv4 o `::0` para IPv6, permitirá que todas las direcciones IP tengan acceso a las instancias públicas mediante SSH. Este método es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En los entornos de producción, debe autorizar el acceso a sus instancias únicamente a una dirección IP o a un rango de direcciones IP específicos.

   b. En la sección Inbound rules (Reglas de entrada), elija Add rule (agregar regla).

   c. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el acceso Secure Shell (SSH) a la instancia de Amazon EC2. Si lo hace, podrá conectarse a la instancia de EC2 para instalar clientes SQL y otras aplicaciones. Especifique una dirección IP para permitir poder acceder a su instancia de EC2:

      - Tipo: **`SSH`**
      - Origen: la dirección IP o el rango del paso a. Un ejemplo de dirección IP IPv4 es **`203.0.113.25/32`**. Un ejemplo de dirección IP IPv6 es **`2001:DB8::/32`**.

5. Para crear el grupo de seguridad, elija Create security group (Crear grupo de seguridad).

   Anote el ID del grupo de seguridad, ya que lo necesitará más tarde en este tutorial.

Creación de un grupo de seguridad de VPC para una instancia de base de datos privada

Para que una instancia de base de datos sea privada, debe crear un segundo grupo de seguridad para el acceso privado. Para conectarse a instancias de base de datos privadas en su VPC, añada reglas de entrada a su grupo de seguridad de VPC. Estos permiten el tráfico de su instancia de Amazon EC2 solamente.

Para crear un grupo de seguridad de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija VPC Dashboard (Panel VPC), seguido de Security Groups (Grupos de seguridad) y, por último, Create Security Group (Crear grupo de seguridad).
3. En la página Create Security Group (Crear grupo de seguridad), establezca estos valores:
   - Security group name (Nombre de grupo de seguridad: **`tutorial-dual-stack-db-securitygroup`**
   - Description: **`Tutorial Dual-Stack DB Instance Security Group`**
   - VPC: elija la VPC que creó en el paso anterior, por ejemplo, vpc-***`identificador`***(tutorial-dual-stack-vpc)
4. Agregar reglas de entrada al grupo de seguridad:
   a. En la sección Inbound rules (Reglas de entrada), elija Add rule (gregar regla).
   b. Establezca los siguientes valores para la regla de entrada nueva con objeto de permitir el tráfico de MySQL en el puerto 3306 desde la instancia de Amazon EC2. Si lo hace, podrá conectarse desde su instancia de EC2 a su instancia de base de datos. Esto significa que puede enviar datos desde la instancia de EC2 a la base de datos.
      - Type (Tipo): MySQL/Aurora
      - Source (Origen): identificador del grupo de seguridad tutorial-dual-stack-securitygroup que creó anteriormente en este tutorial, por ejemplo, sg-9edd5cfb.
5. Para crear el grupo de seguridad, elija Crear grupo de seguridad.

Creación de un grupo de subredes de base de datos

Un grupo de subredes de base de datos es una colección de subredes que se crea en una VPC y que después se asigna a las instancias de bases de datos. Un grupo de subredes de base de

datos le permite especificar una VPC específica al crear instancias de bases de datos. Para crear un grupo de subredes de base de datos que sea compatible con DUAL, todas las subredes deben ser compatibles con DUAL. Para que sea compatible con DUAL, una subred debe tener asociado un CIDR IPv6.

Para crear un grupo de subredes de base de datos

1. Identifique las subredes privadas de la base de datos en la VPC.
   a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
   b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Subnets (Subredes).
   c. Anote los ID de subred de las subredes denominadas tutorial-subred-dual-stack-private1-us-west-2a y tutorial-subred-dual-stack-private2-us-west-2b.

      Necesitará los ID de subred cuando cree el grupo de subredes de base de datos.
2. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

   Asegúrese de conectarse a la consola de Amazon RDS, no a la consola de Amazon VPC.
3. En el panel de navegación, elija Subnet groups.
4. Elija Create DB Subnet Group (Crear grupo de subredes de base de datos).
5. En la página Create DB subnet group (Crear grupo de subredes de base de datos), establezca estos valores en Subnet group details (Detalles del grupo de subredes):
   - Name: **`tutorial-dual-stack-db-subnet-group`**
   - Description: **`Tutorial Dual-Stack DB Subnet Group`**
   - VPC: tutorial-dual-stack-vpc (vpc-***`identificador`***)
6. En la sección Add subnets (Agregar subredes) elija las Availability Zones (Zonas de disponibilidad) y las Subnets (Subredes).

   Para este tutorial, elija us-east-2a y us-east-2b en Availability Zones (Zonas de disponibilidad). En Subnets (Subredes), elija las subredes privadas que identificó en el paso anterior.
7. Seleccione Create (Crear).

El nuevo grupo de subredes de base de datos aparece en la lista de grupos de subredes de base de datos de la consola de RDS. Puede elegir el grupo de subredes de base de datos para ver la

información detallada, que incluye los protocolos de direcciones compatibles y todas las subredes asociadas al grupo y al tipo de red admitidos por el grupo de subredes de base de datos.

Crear una instancia de Amazon EC2 en el modo de pila doble

Para crear una instancia de Amazon EC2, siga las instrucciones indicadas en Lanzar una instancia con el nuevo asistente de inicialización de instancias en la Guía del usuario de Amazon EC2.

En la página Configure Instance Details (Configurar detalles de instancia), defina estos valores y mantenga los demás con sus valores predeterminados:

- Red: elija una VPC existente con las subredes pública y privada, como tutorial-dual-stack-vpc (vpc-*identificador*) creada en Creación de una VPC con subredes públicas y privadas
- Subnet (Subred): elija una subred pública existente, como subnet-***identificador*** | tutorial-dual-stack-subnet-public1-us-east-2a | us-east-2a, creada en Para crear un grupo de seguridad de la VPC para una instancia de Amazon EC2 pública.
- Auto-assign Public IP (Asignar automáticamente IP pública): elija Enable (Habilitar).
- Auto-assign IPv6 IP (Asignar automáticamente IP IPv6): elija Enable (Habilitar).
- Firewall (security groups) (Firewall [grupos de seguridad]): elija Select an existing security group (Seleccionar un grupo de seguridad existente).
- Common security groups (Grupos de seguridad comunes): elija un grupo de seguridad existente, como el `tutorial-securitygroup` creado en Para crear un grupo de seguridad de la VPC para una instancia de Amazon EC2 pública. Asegúrese de que el grupo de seguridad que elija incluya reglas de entrada para acceso Secure Shell (SSH) y HTTP.

Crear una instancia de base de datos en el modo de pila doble

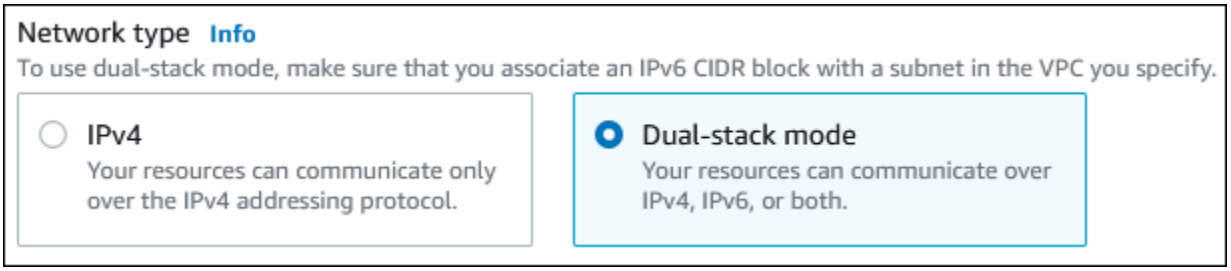
En este paso, debe crear una instancia de base de datos que se ejecute en modo de pila doble.

Para crear una instancia de base de datos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la consola, elija la Región de AWS en la que desea crear la instancia de base de datos. En este ejemplo se utiliza la región Este de EE. UU. (Ohio).
3. En el panel de navegación, seleccione Databases (Bases de datos).
4. Elija Create database (Crear base de datos).

5. En la página Create database (Crear base de datos), asegúrese de que la opción Standard Create (Creación estándar) esté seleccionada y luego, elija el tipo de motor de base de datos MySQL.
6. En la sección Conectivity (Conectividad), establezca estos valores:

   - Network type (Tipo de red): elija Dual-stack mode (Modo de pila doble)



   - Virtual private cloud (VPC) (Nube privada virtual [VPC]): elija una VPC existente con las subredes pública y privada, como tutorial-dual-stack-vpc (vpc-*identificador*) creada en Creación de una VPC con subredes públicas y privadas

     La VPC debe tener subredes en diferentes zonas de disponibilidad.
   - DB subnet group (Grupo de subredes de base de datos): grupo de subredes de base de datos para la VPC, como tutorial-dual-stack-db-subnet-group, creado en Creación de un grupo de subredes de base de datos
   - Public access (Acceso público): elija No.
   - VPC security group (firewall) (Grupo de seguridad de VPC [firewall]): seleccione Choose existing (Elegir existente).
   - Existing VPC security groups (Grupos de seguridad de la VPC existentes): elija un grupo de seguridad de la VPC existente configurado para el acceso público, como tutorial-dual-stack-db-securitygroup creado en Creación de un grupo de seguridad de VPC para una instancia de base de datos privada.

     Elimine otros grupos de seguridad, como el grupo de seguridad predeterminado, seleccionando la X asociada con cada uno de ellos.
   - Availability Zone (Zona de disponibilidad): elija us-west-2a.

     Para evitar el tráfico entre zonas de disponibilidad, asegúrese de que la instancia de base de datos y la instancia de EC2 estén en la misma zona de disponibilidad.

7. En el resto de secciones, especifique los ajustes de configuración de la instancia de base de datos. Para obtener más información acerca de cada ajuste, consulte Configuración de instancias de base de datos.

Conectarse a la instancia de Amazon EC2 y a la instancia de base de datos

Después de crear la instancia de base de datos y la instancia de Amazon EC2 en el modo de pila doble, puede conectarse a cada una mediante el protocolo IPv6. Para conectarse a una instancia de Amazon EC2 mediante el protocolo IPv6, siga las instrucciones indicadas en Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2.

Para conectarse a su instancia de base de datos de RDS para MySQL desde la instancia de Amazon EC2, siga las instrucciones de Conectarse a una instancia de base de datos de MySQL.

Eliminación de la VPC

Después de crear la VPC y otros recursos para este tutorial, puede eliminarlos si ya no son necesarios.

Si agregó recursos en la VPC que creó para este tutorial, es posible que primero tenga que eliminar estos para poder eliminar la VPC. Algunos ejemplos de recursos son las instancias de Amazon EC2 o las instancias de base de datos. Para obtener más información, consulte Eliminación de la VPC en la Guía del usuario de Amazon VPC.

Para eliminar una VPC y los recursos relacionados

1. Elimine el grupo de subredes de base de datos:
    a. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
    b. En el panel de navegación, elija Subnet groups.
    c. Seleccione el grupo de subredes de base de datos a eliminar, como tutorial-db-subnet-group.
    d. Elija Delete (Eliminar) y, a continuación, elija Delete (Eliminar) en la ventana de confirmación.
2. Anote el ID de la VPC:
    a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
    b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione VPCs.

c. En la lista, identifique la VPC que creó, como, por ejemplo, tutorial-dual-stack-vpc.

d. Anote el ID de la VPC que ha creado. Necesitará el ID de la VPC en los pasos subsiguientes.

3. Elimine los grupos de seguridad:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione Security Groups (Grupos de seguridad).

c. Seleccione el grupo de seguridad de la instancia de base de datos de Amazon RDS, como, por ejemplo, tutorial-dual-stack-db-securitygroup.

d. En Actions (Acciones), elija Delete security groups (Eliminar grupos de seguridad) y, a continuación, seleccione Delete (Eliminar) en la página de confirmación.

e. En la página Security Groups (Grupos de seguridad), seleccione el grupo de seguridad para la instancia de Amazon EC2, como, por ejemplo, tutorial-dual-stack-securitygroup.

f. En Actions (Acciones), elija Delete security groups (Eliminar grupos de seguridad) y, a continuación, seleccione Delete (Eliminar) en la página de confirmación.

4. Elimine la puerta de enlace NAT:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione NAT Gateways (Puertas de enlace NAT).

c. Seleccione la puerta de enlace NAT de la VPC que creó. Utilice el ID de VPC para identificar la puerta de enlace NAT correcta.

d. En Actions (Acciones), seleccione Delete NAT gateway (Eliminar puerta de enlace NAT).

e. En la página de confirmación, introduzca **`delete`** y elija Eliminar.

5. Elimine la VPC:

a. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

b. Seleccione VPC Dashboard (Panel de control de VPC) y, a continuación, seleccione VPCs.

c. Seleccione la VPC que desea eliminar, como, por ejemplo tutorial-dual-stack-vpc.

d. En Actions (Acciones), elija Delete VPC (Eliminar VPC).

La página de confirmación muestra otros recursos asociados a la VPC que también se eliminarán, incluidas las subredes asociadas a ella.

e. En la página de confirmación, introduzca **`delete`** y elija Eliminar.

6. Libere las direcciones IP elásticas:

   a. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

   b. Seleccione EC2 Dashboard (Panel de EC2) y, a continuación, seleccione Elastic IPs (Direcciones IP elásticas).

   c. Seleccione la dirección IP elástica que desea liberar.

   d. Desde Actions (Acciones), elija Release Elastic IP addresses (Liberar direcciones IP elásticas).

   e. En la página de confirmación, seleccione Release (Liberar).

Traslado de una instancia de base de datos que no está en una VPC a una VPC

Algunas instancias de bases de datos heredadas existentes en la plataforma EC2-Classic no están en una VPC. Si la instancia de base de datos no está en una VPC, puede utilizar la AWS Management Console para mover fácilmente la instancia de base de datos a una VPC. Para poder trasladar a una VPC una instancia de base de datos que no está en una VPC, debe crear la VPC.

EC2-Classic se retirará el 15 de agosto de 2022. Si todavía no ha migrado de EC2-Classic a una VPC, le recomendamos que migre lo antes posible. Para obtener más información, consulte el tema sobre migrar de EC2-Classic a una VPC en la guía del usuario de Amazon EC2 y la publicación del blog sobre EC2-Classic Networking se retira: cómo prepararse.

Important

Si es un cliente nuevo de Amazon RDS, si nunca ha creado una instancia de base de datos antes o si está creando una instancia de base de datos en una región de AWS que no ha utilizado antes, en la mayoría de los casos estará en la plataforma EC2-VPC y tendrá una VPC predeterminada. Para obtener información sobre cómo trabajar con instancias de base de datos en una VPC, consulte Uso de una instancia de base de datos en una VPC.

Siga estos pasos para crear una VPC para la instancia de base de datos.

- Paso 1: Crear una VPC
- Paso 2: Crear un grupo de subredes de base de datos
- Paso 3: Crear un grupo de seguridad de VPC

Después de crear la VPC, siga estos pasos para trasladar la instancia de base de datos a la VPC.

- Actualización de la VPC para una instancia de base de datos

Le recomendamos encarecidamente que cree una copia de seguridad de su instancia de base de datos inmediatamente antes de la migración. Al hacerlo, se garantiza que puede restaurar los datos

si se produce un error en la migración. Para obtener más información, consulte Copia de seguridad, restauración y exportación de datos.

A continuación se indican algunas limitaciones para trasladar una instancia de base de datos a una VPC.

- Clases de instancia de base de datos de generación anterior: las clases de instancia de base de datos de generación anterior es posible que no sean compatibles en la plataforma VPC. Al mover una instancia de base de datos a una VPC, elija una clase de instancia de base de datos db.m3 o db.r3. Después de mover la instancia de base de datos a una VPC, puede escalar la instancia de base de datos para utilizar una clase de instancia de base de datos posterior. Para obtener una lista completa de las clases de instancia compatibles con la VPC, consulte Tipos de instancias de Amazon RDS.
- Multi-AZ: actualmente no es posible trasladar a una VPC una instancia de base de datos Multi-AZ que no está en una VPC. Para mover la instancia de base de datos a una VPC, modifique primero la instancia de base de datos para que sea una implementación Single-AZ. Cambie la configuración de la implementación Multi-AZ a No. Después de mover la instancia de base de datos a una VPC, vuelva a modificarla para convertirla en una implementación Multi-AZ. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.
- Réplicas de lectura: actualmente no es posible mover a una VPC una instancia de base de datos con réplicas de lectura que no está en una VPC. Para mover la instancia de base de datos a una VPC, primero elimine todas sus réplicas de lectura. Después de mover la instancia de base de datos a una VPC, vuelva a crear las réplicas de lectura. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.
- Grupos de opciones: si mueve la instancia de base de datos a una VPC y la instancia de base de datos utiliza un grupo de opciones personalizado, cambie el grupo de opciones asociado a la instancia de base de datos. Los grupos de opciones son específicos de la plataforma, y el traslado a una VPC es un cambio de plataforma. Para utilizar un grupo de opciones personalizado en este caso, asigne el grupo de opciones predeterminado de la VPC a la instancia de base de datos, asigne un grupo de opciones utilizado por otras instancias de bases de datos de la VPC a la que está realizando el traslado, o cree un grupo de opciones nuevo y asígneselo la instancia de base de datos. Para obtener más información, consulte Trabajo con grupos de opciones.

Alternativas para mover una instancia de base de datos que no esté en una VPC a una VPC con un tiempo de inactividad mínimo

Mediante las siguientes alternativas, puede mover una instancia de base de datos que no esté en una VPC a una VPC con un tiempo de inactividad mínimo. Estas alternativas provocan una interrupción mínima en la instancia de base de datos de origen y le permiten servir tráfico de usuarios durante la migración. Sin embargo, el tiempo necesario para migrar a una VPC variará según el tamaño de la base de datos y las características de la carga de trabajo activa.

- AWS Database Migration Service (AWS DMS) – AWS DMS habilita la migración activa de datos mientras mantiene la instancia de base de datos de origen completamente operativa, pero replica solo un conjunto limitado de sentencias DDL. AWS DMS no propaga elementos como índices, usuarios, privilegios, procedimientos almacenados y otros cambios de base de datos que no estén directamente relacionados con los datos de la tabla. Además, AWS DMS no utiliza automáticamente instantáneas de RDS para la creación inicial de la instancia de base de datos, lo que puede prolongar el tiempo de migración. Para obtener más información, consulte AWS Database Migration Service.
- Restauración de instantáneas de base de datos o recuperación a un momento dado: puede mover una instancia de base de datos a una VPC restaurando una instantánea de la instancia de base de datos o restaurando una instancia de base de datos a un punto en el tiempo. Para obtener más información, consulte Restauración a una instancia de base de datos y Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Cuotas y restricciones para Amazon RDS

A continuación puede ver una descripción de las cuotas de recursos y las restricciones de nomenclatura para Amazon RDS.

Temas

- Cuotas en Amazon RDS
- Restricciones de la nomenclatura en Amazon RDS
- Número máximo de conexiones de base de datos
- Límites de tamaño de archivo en Amazon RDS

Cuotas en Amazon RDS

Cada cuenta de AWS tiene cuotas, para cada región de AWS, según la cantidad de recursos de Amazon RDS que se pueden crear. Una vez que se alcance la cuota de un recurso, las llamadas adicionales para crear ese recurso dejan de funcionar con una excepción.

En la siguiente tabla se enumeran los recursos y las cuotas por AWS región.

Nombre	Valor predeterminado	Ajusta	Descripción
Autorizaciones por grupo de seguridad de base de datos	Cada región admitida: 20	No	Número de autorizaciones de grupos de seguridad por grupo de seguridad de base de datos
Versiones del motor personalizadas	Cada región admitida: 40	Sí	Número máximo de versiones de motor personalizado permitidas en esta cuenta en la región actual

Nombre	Valor predeterminado	Ajusta	Descripción
Grupos de parámetros de clúster de bases de datos	Cada región admitida: 50	No	Número máximo de grupos de parámetros de clúster de base de datos
Clústeres de base de datos	Cada región admitida: 40	Sí	Número máximo de clústeres de Aurora permitido en esta cuenta en la región actual
Instancias de base de datos	Cada región admitida: 40	Sí	Número máximo de instancias de base de datos permitidas en esta cuenta en la región actual
Grupos de subred de base de datos	Cada región admitida: 50	Sí	Número máximo de grupos de subredes de base de datos
Tamaño del cuerpo de la solicitud HTTP de la API de datos	Cada región admitida: 4 megabytes	No	Tamaño máximo permitido para el cuerpo de la solicitud HTTP.
Pares de secreto de clúster simultáneos máximos de la API de datos	Cada región admitida: 30	No	El número máximo de pares únicos de clústeres y secretos de base de datos de Aurora sin servidor v1 en solicitudes simultáneas a la API de datos para esta cuenta y la región de AWS actual.

Nombre	Valor predeterminado	Ajusta	Descripción
Solicitudes simultáneas máximas de la API de datos	Cada región admitida: 500	No	El número máximo de solicitudes de la API de datos a un clúster de bases de datos de Aurora sin servidor v1 que utilizan el mismo secreto y se pueden procesar al mismo tiempo. Las solicitudes adicionales se ponen en cola y se procesan a medida que se completan las solicitudes en proceso.
Tamaño máximo del conjunto de resultados de la API de datos	Cada región admitida: 1 megabyte	No	Tamaño máximo del conjunto de resultados de la base de datos que puede devolver la API de datos.
Tamaño máximo de la API de datos de la cadena de respuesta JSON	Cada región admitida: 10 megabytes	No	Tamaño máximo de la cadena de respuesta JSON simplificada que devuelve la API de datos de RDS.

Nombre	Valor predeterminado	Ajusta	Descripción
Solicitudes de la API de datos por segundo	Cada región admitida: 1000 por segundo	No	El número máximo de solicitudes a la API de datos por segundo permitido en esta cuenta en la región de AWS actual. Esta cuota solo se aplica a los clústeres de Amazon Aurora sin servidor v1.
Suscripciones de eventos	Cada región admitida: 20	Sí	Número máximo de suscripciones a eventos
Roles de IAM por clúster de bases de datos	Cada región admitida: 5	Sí	Número máximo de roles de IAM asociados con un clúster de base de datos
Roles de IAM por instancia de base de datos	Cada región admitida: 5	Sí	Número máximo de roles de IAM asociados con una instancia de base de datos
Integraciones	Cada región admitida: 100	No	El número máximo de integraciones permitidas en esta cuenta para la región de AWS actual
Instantánea de clúster de bases de datos manual	Cada región admitida: 100	Sí	Número máximo de instantáneas de clúster de base de datos manuales

Nombre	Valor predeterminado	Ajusta	Descripción
Instantáneas de la instancia de base de datos manuales	Cada región admitida: 100	Sí	Número máximo de instantáneas de instancia de base de datos manuales
Grupos de opciones	Cada región admitida: 20	Sí	Número máximo de grupos de opciones
Grupos de parámetros	Cada región admitida: 50	Sí	Número máximo de grupos de parámetros
Proxies	Cada región admitida: 20	Sí	Número máximo de proxies permitidos en esta cuenta en la región AWS actual
Réplicas de lectura por principal	Cada región admitida: 15	Sí	El número máximo de réplicas de lectura por instancia principal de base de datos. Esta cuota no se puede ajustar para Amazon Aurora.
Instancias de base de datos reservadas	Cada región admitida: 40	Sí	Número máximo de instancias de base de datos reservadas permitidas en esta cuenta en la región AWS actual
Reglas por grupo de seguridad	Cada región admitida: 20	No	Número máximo de reglas por grupo de seguridad de base de datos

Nombre	Valor predeterminado	Ajusta	Descripción
Grupos de seguridad	Cada región admitida: 25	Sí	Número máximo de grupos de seguridad de base de datos
Grupos de seguridad (VPC)	Cada región admitida: 5	No	Número máximo de grupos de seguridad de base de datos por Amazon VPC
Subredes por grupo de subredes de base de datos	Cada región admitida: 20	No	Número máximo de subredes por grupo de subredes de base de datos
Etiquetas por recurso	Cada región admitida: 50	No	Número máximo de etiquetas por recurso de Amazon RDS
Almacenamiento total para todas las instancias de base de datos	Cada región admitida: 100 000 gigabytes	Sí	El almacenamiento total máximo (en GB) en volúmenes de EBS para todas las instancias de base de datos de Amazon RDS sumadas. Esta cuota no se aplica a Amazon Aurora, que tiene un volumen máximo de clúster de 128 TiB para cada clúster de base de datos.

> **Note**
>
> De forma predeterminada, puede tener un total de 40 instancias de base de datos. Dentro de esta cuota se tienen en cuenta las instancias de base de datos de RDS, las instancias de base de datos de Aurora, las instancias de Amazon Neptune y las instancias de Amazon DocumentDB.
> Se aplican las siguientes limitaciones a las instancias de base de datos de Amazon RDS:
>
> - 10 para cada edición de SQL Server (Enterprise, Standard, Web y Express) bajo el modelo «licencia incluida»
> - 10 para Oracle bajo el modelo «licencia incluida»
> - 40 para Db2 según el modelo de licencia “traiga su propia licencia” (BYOL).
> - 40 para MySQL, MariaDB o PostgreSQL
> - 40 para Oracle según el modelo de licencia “traiga su propia licencia” (BYOL).
>
> Si la aplicación requiere más instancias de base de datos, puede solicitar instancias de base de datos adicionales; solo tiene que abrir la consola de Service Quotas. En el panel de navegación, elija serviciosAWS. Elija Amazon Relational Database Service (Amazon RDS), elija una cuota y siga las instrucciones para solicitar un aumento de cuota. Para obtener más información, consulte este tema acerca de cómo solicitar un aumento de cuota en la Guía del usuario de Service Quotas.
> Para RDS para Oracle y RDS para SQL Server, el límite de réplica de lectura es de 5 por base de datos de origen para cada región.
> Las copias de seguridad administradas por AWS Backup se consideran instantáneas de manuales, pero no cuentan para la cuota de instantáneas de manuales. Para obtener más información acerca de AWS Backup, consulte la Guía para desarrolladores de AWS Backup.

Si utiliza cualquier operación de la API de RDS y supera la cuota predeterminada de la cantidad de llamadas por segundo, la API de Amazon RDS genera un error como el siguiente.

ClientError: An error occurred (ThrottlingException) when calling the API_name operation: Rate exceeded.

En este caso, reduzca la cantidad de llamadas por segundo. La cuota está destinada a cubrir la mayoría de los casos de uso. Si se necesitan cuotas superiores, puede solicitar aumentos de cuota mediante una de las siguientes opciones:

- Desde la consola, abra la consola Service Quotas.
- Desde la AWS CLI, utilice el comando request-service-quota-increase de la AWS CLI.

Para obtener más información, consulte la Guía del usuario de Service Quotas.

Restricciones de la nomenclatura en Amazon RDS

Las restricciones de la nomenclatura en Amazon RDS son las siguientes:

- Identificador de instancia de base de datos:
  - Deben contener entre 1 y 63 caracteres alfanuméricos o guiones.
  - El primer carácter debe ser una letra.
  - No se pueden incluir dos guiones consecutivos ni acabar con guion.
  - Debe ser único para todas las instancias de base de datos por AWS cuenta, por AWS región.
- Nombre inicial de la base de datos:
  - Las restricciones de los nombres de base de datos difieren para cada motor de base de datos. Para obtener más información, consulte la configuración disponible al crear cada instancia de base de datos.
  - SQL Server: cree las bases de datos después de crear la instancia de base de datos.
- Nombre de usuario maestro: las restricciones en los nombres de usuario maestros son distintas para cada motor de base de datos. Para obtener más información, consulte la configuración disponible al crear cada instancia de base de datos.
- Contraseña maestra:
  - La contraseña del usuario maestro de base de datos puede ser cualquier carácter ASCII imprimible excepto `/`, `'`, `"`, `@` o un espacio.

    Para Oracle, `&` es una limitación de caracteres adicional.
  - La contraseña puede contener el siguiente número de caracteres ASCII imprimibles, según el motor de base de datos.
    - Db2: 8–255
    - MariaDB y MySQL: 8–41
    - Oracle: 8–30
    - SQL Server y PostgreSQL: 8–128
- Grupo de parámetros de base de datos:

  - Deben incluir entre 1 y 255 caracteres alfanuméricos.
  - El primer carácter debe ser una letra.
  - Los guiones están permitidos, pero el nombre no puede terminar por un guion o contener dos guiones seguidos.
- Grupo de subred de base de datos:
  - Debe contener entre 1 y 255 caracteres.
  - Se permiten los caracteres alfanuméricos, guiones, guiones bajos y puntos.

Número máximo de conexiones de base de datos

El número máximo de conexiones de base de datos simultáneas varía según el tipo de motor de base de datos y la asignación de memoria para la clase de instancia de base de datos. El número máximo de conexiones se establece, por lo general, en el grupo de parámetros asociado a la instancia de base de datos. La excepción es Microsoft SQL Server, donde se establece en las propiedades del servidor para la instancia de base de datos en SQL Server Management Studio (SSMS).

Las conexiones de base de datos consumen memoria. Establecer uno de estos parámetros demasiado alto puede hacer que una condición de memoria baja haga que una instancia de base de datos se coloque en el estado incompatible-parameters. Para obtener más información, consulte Diagnóstico y resolución del estado de parámetros incompatibles para un límite de memoria.

Si sus aplicaciones abren y cierran conexiones con frecuencia, o mantienen abierto un gran número de conexiones de larga duración, le recomendamos que utilice Amazon RDS Proxy. El RDS Proxy es un proxy de base de datos totalmente administrado y de alta disponibilidad que utiliza agrupación de conexiones para compartir conexiones de base de datos de forma segura y eficiente. Para obtener más información acerca de RDS Proxy, consulteAmazon RDS Proxy .

> **Note**
>
> Para Oracle, establecerá el número máximo de procesos de usuario y sesiones de usuario y sistema.
> En el caso de Db2, no puede establecer el número máximo de conexiones. El límite es 64 000.

La siguiente tabla muestra información sobre el número máximo de conexiones a bases de datos para diferentes motores de base de datos.

Motor de base de datos	Parámetro	Valores permitidos	Valor predeterminado	Descripción
MariaDB y MySQL	`max_connections`	1–100000	Predeterminado para todas las versiones de MariaDB y MySQL, excepto MariaDB versión 10.5 y 10.6: {DBInstanceClassMemory/12582880} La fórmula equivale a MB/12. Predeterminado para MariaDB versión 10.5 y 10.6: LEAST({DBInstanceClassMemory/25165760},12000) La fórmula equivale a MB/25. En cualquiera de los casos, si el cálculo del valor predeterminado da como resultado un valor superior a 16 000, Amazon RDS establece el límite en 16 000 para las instancias de base	Número de conexiones cliente simultáneas permitidas

Motor de base de datos	Parámetro	Valores permitidos	Valor predeterminado	Descripción
			de datos de MariaDB y MySQL.	
Oracle	`processes`	80–20000	LEAST({DBInstanceClassMemory/9868951}, 20000)	Procesos de usuario
Oracle	`sessions`	100–65535	No aplicable	Sesiones de usuario y sistema
PostgreSQL	`max_connections`	6–8388607	LEAST({DBInstanceClassMemory/9531392}, 5000)	Número máximo de conexiones simultáneas
SQL Server	Número máximo de conexiones simultáneas	0–32767	0 (ilimitadas)	Número máximo de conexiones simultáneas

`DBInstanceClassMemory` está en bytes. Para obtener información detallada acerca de cómo se calcula este valor, consulte Especificación de parámetros de base de datos. Debido a la memoria reservada para el sistema operativo y los procesos de administración de RDS, este tamaño de memoria es menor que el valor en gibibytes (GiB) que se muestra en Especificaciones de hardware para clases de instancia de base de datos .

Por ejemplo, algunas clases de instancias de base de datos tienen 8 GiB de memoria, lo que equivale a 8 589 934 592 bytes. Para una instancia de base de datos MySQL que se ejecute en una clase de instancia de base de datos con 8 GiB de memoria, como db.m7g.large, la ecuación que utiliza la memoria total sería `8589934592/12582880=683`. Sin embargo, la variable `DBInstanceClassMemory` resta automáticamente las cantidades reservadas al sistema operativo y a los procesos RDS que administran la instancia de base de datos. El resto de la resta se divide entre 12.582.880. Este cálculo da como resultado aproximadamente 630 para el valor de `max_connections` en lugar de 683. Este valor depende de la clase de instancia de base de datos y el motor de base de datos.

Cuando una instancia de base de datos MariaDB o MySQL se ejecuta en una clase de instancia de base de datos pequeña, como db.t3.micro o db.t3.small, la memoria total disponible es baja. Para estas clases de instancias de base de datos, RDS reserva una parte importante de la memoria disponible, lo que afecta al valor `max_connections`. Por ejemplo, el número máximo predeterminado de conexiones para una instancia de base de datos de MySQL que se ejecuta en una clase de instancia de base de datos db.t3.micro es de aproximadamente 60. Para determinar el valor `max_connections` de su instancia de base de datos MariaDB o MySQL, conéctese a ella y ejecute el siguiente comando SQL:

```
SHOW GLOBAL VARIABLES LIKE 'max_connections';
```

Límites de tamaño de archivo en Amazon RDS

Los límites de tamaño de archivo se aplican a determinadas instancias de base de datos de Amazon RDS. Para obtener más información, consulte los siguientes límites específicos del motor:

- Límites de tamaño de archivo de MariaDB en Amazon RDS
- Límites de tamaño de archivo de MySQL en Amazon RDS
- Límites de tamaño de archivo Oracle en Amazon RDS

Solución de problemas de Amazon RDS

Utilice las siguientes secciones como ayuda para solucionar los problemas que puedan presentarse con instancias de base de datos en Amazon RDS y Amazon Aurora.

Temas

- No puede conectarse a la instancia de base de datos de Amazon RDS
- Problemas de seguridad de Amazon RDS
- Solución de problemas de estado de red incompatible
- Restablecimiento de la contraseña del propietario de la instancia de base de datos
- Interrupción o reinicio de una instancia de base de datos de Amazon RDS
- Los cambios de parámetros de base de datos de Amazon RDS no surten efecto
- La instancia de base de datos de Amazon RDS se está quedando sin espacio de almacenamiento
- Instancias de bases de datos de Amazon RDS disponibles insuficientes
- Problemas de memoria que se puede liberar en Amazon RDS
- Problemas de MySQL y MariaDB
- No se puede establecer el período de retención de copia de seguridad en 0

Para obtener información sobre los problemas de depuración del uso de la API de Amazon RDS, consulte Solución de problemas de aplicaciones en Amazon RDS.

No puede conectarse a la instancia de base de datos de Amazon RDS

Cuando no puede conectarse a una instancia de base de datos, estas suelen ser las causas habituales:

- Reglas de entrada: las reglas de acceso impuestas por el firewall local y las direcciones IP a las que autorizó el acceso a la instancia de base de datos podrían no coincidir. Lo más probable es que el problema se encuentre en las reglas de entrada de su grupo de seguridad.

  De forma predeterminada, las instancias de base de datos no permiten el acceso. El acceso se concede a través de un grupo de seguridad asociado a la VPC que permite el tráfico de entrada

y salida de la instancia de base de datos. Si es necesario, agregue reglas de entrada y salida al grupo de seguridad según su situación particular. Puede especificar una dirección IP, un rango de direcciones IP u otro grupo de seguridad de VPC.

> **Note**
>
> Al agregar una nueva regla de entrada, puede elegir My IP (Mi IP) en Source (Origen) para permitir el acceso a la instancia de base de datos desde la dirección IP detectada en su navegador.

Para obtener más información acerca de la configuración de grupos de seguridad, consulte Proporcionar acceso a la instancia de base de datos en la VPC mediante la creación de un grupo de seguridad.

> **Note**
>
> La conexiones de cliente desde direcciones IP en el rango 169.254.0.0/16 no están permitidas. Este es el rango de direccionamiento IP privado automático (APIPA), que se utiliza para direccionamiento de enlace local.

- Accesibilidad pública: para conectarse a la instancia de base de datos desde fuera de la VPC, por ejemplo mediante una aplicación cliente, la instancia debe tener asignada una dirección IP pública.

  Para que la instancia sea accesible públicamente, modifíquela y elija Yes (Sí) en Public accessibility (Accesibilidad pública). Para obtener más información, consulte Cómo ocultar una instancia de base de datos en una VPC desde Internet..
- Puerto: el puerto especificado al crear la instancia de base de datos no puede usarse para enviar o recibir comunicaciones debido a las restricciones del firewall local. Para determinar si su red permite el uso del puerto especificado para comunicación de entrada y salida, consulte al administrador de red.
- Disponibilidad: en el caso de una instancia de base de datos recién creada, esta tendrá el estado `creating` hasta que esté lista para el uso. Cuando el estado cambie a `available`, podrá conectarse a la instancia de base de datos. Dependiendo del tamaño de la instancia de base de datos, es posible que la instancia tarde hasta 20 minutos en estar disponible.
- Gateway de Internet: para que una instancia de base de datos sea accesible públicamente, las subredes del grupo de subredes de base de datos deben tener una gateway de Internet.

Para configurar una gateway de Internet para una subred

1. Inicie sesión en AWS Management Console y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En el panel de navegación, elija Databases (Bases de datos) y, a continuación, elija el nombre de la instancia de base de datos.
3. En la pestaña Connectivity & security (Conectividad y seguridad), anote los valores del ID de la VPC en VPC y el ID de la subred en Subnets (Subredes).
4. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
5. En el panel de navegación, elija Internet Gateways (Gateways de Internet). Verifique que hay una gateway de Internet adjunta a la VPC. Si no la hay, elija Create Internet Gateway (Crear gateway de Internet) para crear una gateway de Internet. Seleccione la gateway de Internet y, después, elija Attach to VPC (Conectar a la VPC) y siga las instrucciones para adjuntarla a la VPC.
6. En el panel de navegación, elija Subnets (Subredes) y, a continuación, seleccione la suya.
7. En la pestaña Route Table (Tabla de ruteo), verifique que haya una ruta con `0.0.0.0/0` como destino y la gateway de Internet de la VPC como destino.

   Si está conectando con la instancia utilizando la dirección IPv6, verifique que existe una ruta para todo el tráfico IPv6 (`::/0`) que apunte a la gateway de Internet. De lo contrario, realice lo siguiente:

   a. Elija el ID de la tabla de ruteo (rtb-xxxxxxxx) para navegar a la tabla de ruteo.
   b. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas). Elija Add route (Añadir ruta) y utilice `0.0.0.0/0` como destino y la gateway de Internet como objetivo.

      Para IPv6, elija Add route (Añadir ruta) y utilice `::/0` como destino y la gateway de Internet como objetivo.
   c. Elija Save routes (Guardar rutas).

   Además, si intenta conectarse al punto de conexión IPv6, asegúrese de que el rango de direcciones IPv6 del cliente esté autorizado para conectarse a la instancia de base de datos.

Para obtener más información, consulte Uso de una instancia de base de datos en una VPC.

Para obtener información sobre problemas de conexión específicos del motor, consulte los temas siguientes:

- Solución de problemas de conexión a la instancia de base de datos de SQL Server
- Solución de problemas de conexiones a la instancia de base de datos de Oracle
- Solución de problemas de conexiones a la instancia de RDS for PostgreSQL
- Máximo de conexiones de MySQL y MariaDB

Comprobar una conexión a una instancia de base de datos

Puede comprobar la conexión a una instancia de base de datos con las herramientas habituales de Microsoft Windows o Linux.

Desde un terminal de Linux o Unix, puede comprobar la conexión escribiendo lo siguiente. Sustituya *DB-instance-endpoint* por el punto de conexión y *port* por el puerto de la instancia de base de datos.

```
nc -zv DB-instance-endpoint port
```

Por ejemplo, a continuación se muestra un comando de ejemplo y el valor de retorno.

```
nc -zv postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299

  Connection to postgresql1.c6c8mn7fake0.us-west-2.rds.amazonaws.com 8299 port [tcp/
vvr-data] succeeded!
```

Los usuarios de Windows pueden usar Telnet para comprobar la conexión a una instancia de base de datos. Las acciones de Telnet solo se admiten para la comprobación de la conexión. Si la conexión es correcta, la acción no devuelve ningún mensaje. Si la conexión no es correcta, recibe un mensaje de error como el siguiente.

```
C:\>telnet sg-postgresql1.c6c8mntfake0.us-west-2.rds.amazonaws.com 819

  Connecting To sg-postgresql1.c6c8mntfake0.us-west-2.rds.amazonaws.com...Could not
 open
  connection to the host, on port 819: Connect failed
```

Si las acciones de Telnet indican que la conexión es correcta, el grupo de seguridad se ha configurado correctamente.

> **Note**
>
> Amazon RDS no acepta el tráfico del protocolo de mensaje de control de Internet (ICMP), ping incluido.

Solución de problemas de autenticación de conexión

En algunos casos, puede conectarse a su instancia de base de datos, pero recibe errores de autenticación. En estos casos, sería aconsejable restablecer la contraseña de usuario principal para la instancia de base de datos. Puede hacerlo modificando la instancia de RDS.

Para obtener más información acerca de la modificación de una instancia de base de datos de , consulte Modificación de una instancia de base de datos de Amazon RDS.

Problemas de seguridad de Amazon RDS

Para evitar problemas de seguridad, no utilice nunca la contraseña ni la dirección de correo electrónico del usuario raíz de Cuenta de AWS en una cuenta de usuario. El procedimiento recomendado consiste en utilizar el usuario raíz para crear usuarios y asignarlos a cuentas de usuario de base de datos. También puede utilizar el usuario raíz para crear, si fuera necesario, otras cuentas de usuario.

Para obtener información sobre cómo crear usuarios, consulte Creación de un usuario de IAM en la Cuenta de AWS. Para obtener información sobre cómo crear usuarios en AWS IAM Identity Center, consulte Manage identities in IAM Identity Center (Administrar identidades en el Centro de identidades de IAM).

Mensaje de error "No se pudieron recuperar los atributos de cuenta. Determinadas funciones de la consola pueden estar deterioradas".

Puede obtener este error por varias razones. Puede deberse a que la cuenta no tiene permisos o a que no se ha configurado correctamente. Si la cuenta es nueva, es posible que no haya esperado a que esté lista. Si se trata de una cuenta existente, podría carecer de permisos en sus políticas

de acceso para realizar determinadas acciones, como crear una instancia de base de datos. Para solucionar este problema, el administrador debe proporcionar los roles necesarios a su cuenta. Para obtener más información, consulte la documentación de IAM.

Solución de problemas de estado de red incompatible

El estado de red incompatible significa que es posible que se puede acceder a la base de datos a nivel de base de datos, pero no es posible modificarla ni reiniciarla.

Causas

El estado de red incompatible de la instancia de base de datos podría deberse a una de las siguientes acciones:

- Modificación de la clase de instancia de base de datos.
- Modificación de la instancia de base de datos para utilizar una implementación de un clúster de base de datos Multi-AZ.
- Sustitución de un host debido a un evento de mantenimiento.
- Lanzamiento de una instancia de base de datos de reemplazo.
- Restauración a partir de una instantánea.
- Inicio de una instancia de base de datos que se había detenido.

Resolución

Utilice el comando start-db-instance

Para reparar una base de datos que se encuentra en un estado de red incompatible, siga estas instrucciones:

1. Abra la https://console.aws.amazon.com/rds/ y elija Bases de datos en el panel de navegación.
2. Elija la instancia de base de datos que se encuentra en el estado de red incompatible y tome nota del identificador de la instancia de base de datos, el ID de la VPC y los ID de subred de la pestaña Conectividad y seguridad.
3. Utilice la AWS CLI para ejecutar el comando `start-db-instance`. Especifique el valor `--db-instance-identifier`.

> **Note**
>
> La ejecución de este comando cuando la base de datos está en modo incompatible podría provocar algo de tiempo de inactividad.
> El comando `start-db-instance` no resuelve este problema en el caso de instancias de base de datos de RDS para SQL Server.

El estado de la base de datos cambia a Disponible si el comando se ejecuta correctamente.

Si la base de datos se reinicia, la instancia de base de datos podría ejecutar la última operación ejecutada en la instancia antes de que pasara al estado de red incompatible. Esto podría hacer que la instancia volviera al estado de red incompatible.

Si el comando `start-db-instance` no funciona o la instancia vuelve al estado de red incompatible, abra la página Bases de datos en la consola de RDS y seleccione la base de datos. Vaya a la sección Registros y eventos. La sección Eventos recientes muestra pasos de resolución adicionales que puede seguir. Los mensajes se clasifican de la siguiente manera:

- COMPROBACIÓN DE RECURSOS INTERNOS: es posible que haya problemas con sus recursos internos.
- COMPROBACIÓN DE DNS: compruebe la resolución de DNS y los nombres de host de la VPC en la consola de la VPC.
- COMPROBACIÓN DE ENI: es posible que la interfaz de red elástica (ENI) de esta base de datos no exista.
- COMPROBACIÓN DE PUERTA DE ENLACE: la puerta de enlace de Internet de su base de datos disponible públicamente no está conectada a la VPC.
- COMPROBACIÓN DE IP: no hay direcciones IP libres en sus subredes.
- COMPROBACIÓN DE GRUPO DE SEGURIDAD: no hay grupos de seguridad asociados a la base de datos o los grupos de seguridad no son válidos.
- COMPROBACIÓN DE SUBRED: no hay subredes válidas en su grupo de subredes de base de datos o hay problemas con la subred.
- COMPROBACIÓN DE VPC: la VPC asociada a la base de datos no es válida.

Realizar una recuperación en un momento dado

Se recomienda tener una copia de seguridad (instantánea o lógica) en caso de que la base de datos entre en un estado de red incompatible. Consulte Introducción a las copias de seguridad. Si ha activado las copias de seguridad automáticas, detenga temporalmente cualquier escritura en la base de datos y realice una recuperación en un momento dado.

> **Note**
>
> Cuando una instancia pasa al estado de red incompatible, es posible que no se pueda acceder a la instancia de base de datos para realizar una copia de seguridad lógica.

Si no ha activado las copias de seguridad automáticas, cree una nueva instancia de base de datos. A continuación, migre los datos mediante AWS Database Migration Service (AWS DMS) o mediante una herramienta de copia de seguridad y restauración.

Si esto no resuelve el problema, contacte con Soporte para obtener ayuda adicional.

Restablecimiento de la contraseña del propietario de la instancia de base de datos

Si se bloquea la instancia de base de datos, puede iniciar sesión como usuario maestro. A continuación, puede restablecer las credenciales para otros usuarios o roles administrativos. Si no puede iniciar sesión como usuario maestro, el propietario de la AWS cuenta puede restablecer la contraseña del usuario maestro. Para obtener información detallada sobre las cuentas administrativas o roles que puede tener que restablecer, consulte Privilegios de la cuenta de usuario maestro.

La contraseña de la instancia de base de datos se puede cambiar por medio de la consola de Amazon RDS, el comando modify-db-instance de la AWS CLI o la operación de la API ModifyDBInstance. Para obtener más información acerca de la modificación de una instancia de base de datos de , consulte Modificación de una instancia de base de datos de Amazon RDS.

Interrupción o reinicio de una instancia de base de datos de Amazon RDS

Cuando se reinicia una instancia de base de datos puede producirse una interrupción de la instancia de base de datos. También puede producirse cuando dicha instancia se pone en un estado que impide el acceso a ella y cuando se reinicia la base de datos. Puede producirse un reinicio al al reiniciar de forma manual su instancia de base de datos. Un reinicio también puede ocurrir cuando se cambia una configuración de la instancia de la base de datos que requiere un reinicio antes de que pueda surtir efecto.

El reinicio de una instancia de base de datos se produce cuando cambia una configuración que exige un reinicio o cuando efectúa un reinicio manualmente. El reinicio puede producirse inmediatamente si cambia una configuración y solicita que el cambio surta efecto de inmediato. O puede ocurrir durante el período de mantenimiento de la instancia de base de datos.

El reinicio de la instancia de base de datos se produce inmediatamente en una de las siguientes situaciones:

- Cambie el periodo de retención de copia de seguridad de una instancia de base de datos de cero a un valor distinto de cero o de un valor distinto de cero a cero. A continuación, configure Apply Immediately (Aplicar inmediatamente) en `true`.
- El usuario cambia la clase de la instancia de base de datos y Apply Immediately (Aplicar inmediatamente) se establece en `true`.
- Puede cambiar el tipo de almacenamiento de Magnetic (Standard) (Magnético [estándar]) a General Purpose (SSD) (Propósito general [SSD]) o Provisioned IOPS (SSD) (IOPS aprovisionadas [SSD]), o de Provisioned IOPS (SSD) (IOPS aprovisionadas [SSD]) o General Purpose (SSD) (Propósito general [SSD]) a Magnetic (Standard) (Magnético [estándar]).

El reinicio de la instancia de base de datos se produce durante el período de mantenimiento en una de las siguientes situaciones:

- El usuario cambia el período de retención de copia de seguridad de una instancia de base de datos, de cero a un valor distinto de cero o viceversa, y Apply Immediately (Aplicar inmediatamente) se establece en `false`.
- El usuario cambia la clase de la instancia de base de datos y Apply Immediately (Aplicar inmediatamente) se establece en `false`.

Cuando se cambia un parámetro estático en un grupo de parámetros de base de datos, el cambio no surtirá efecto hasta que se reinicie la instancia de base de datos asociada al grupo. El cambio requiere un reinicio manual. La instancia de base de datos no se reinicia automáticamente durante el período de mantenimiento.

Para ver una tabla que muestra acciones de la instancia de base de datos y el efecto que tiene configurar el valor Apply Immediately, consulte Modificación de una instancia de base de datos de Amazon RDS.

Los cambios de parámetros de base de datos de Amazon RDS no surten efecto

En algunos casos, es posible que cambie un parámetro en un grupo de parámetros de base de datos, pero no vea que los cambios surtan efecto. Si es así, es probable que necesite reiniciar la instancia de base de datos asociada con el grupo de parámetros de base de datos. Cuando se cambia un parámetro dinámico, el cambio surte efecto inmediatamente. Cuando se cambia un parámetro estático, el cambio no surtirá efecto hasta que reinicie la instancia de base de datos asociada al grupo de parámetros.

Puede reiniciar una instancia de base de datos a través de la consola de RDS. O bien, puede llamar explícitamente a la operación de la API `RebootDBInstance`. Puede reiniciar sin conmutación por error si la instancia de base de datos se encuentra en una implementación Multi-AZ. El requisito de reiniciar la instancia de base de datos asociada después de cambiar un parámetro estático ayuda a mitigar el riesgo de que una configuración errónea del parámetro afecte a una llamada a la API. Un ejemplo sería llamar a `ModifyDBInstance` para cambiar la clase de instancia de base de datos. Para obtener más información, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.

La instancia de base de datos de Amazon RDS se está quedando sin espacio de almacenamiento

Si su instancia de base de datos se queda sin espacio de almacenamiento, es posible que ya no esté disponible. Recomendamos encarecidamente que monitoree de manera regular la métrica de `FreeStorageSpace` publicada en CloudWatch para asegurarse de que la instancia de base de datos tenga suficiente espacio de almacenamiento libre.

Si la instancia de base de datos se queda sin espacio de almacenamiento, su estado cambia a `storage-full`. Por ejemplo, una llamada a la operación de la API `DescribeDBInstances` para la instancia de base de datos que ha utilizado todo su espacio de almacenamiento produce lo siguiente.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance

DBINSTANCE  mydbinstance  2009-12-22T23:06:11.915Z  db.m5.large  mysql8.0  50  sa
storage-full  mydbinstance.clla4j4jgyph.us-east-1.rds.amazonaws.com  3306
us-east-1b  3
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Para recuperarse de esta situación, agregue más espacio de almacenamiento a su instancia mediante la operación de la API `ModifyDBInstance` o el siguiente comando de la AWS CLI.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --allocated-storage 60 \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --allocated-storage 60 ^
    --apply-immediately
```

```
DBINSTANCE  mydbinstance  2009-12-22T23:06:11.915Z  db.m5.large  mysql8.0  50  sa
storage-full  mydbinstance.clla4j4jgyph.us-east-1.rds.amazonaws.com  3306
us-east-1b  3  60
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Ahora, cuando describa su instancia de base de datos, verá que esta tendrá el estado `modifying`, lo que indica el escalado del almacenamiento.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

```
DBINSTANCE  mydbinstance  2009-12-22T23:06:11.915Z  db.m5.large  mysql8.0  50  sa
modifying  mydbinstance.clla4j4jgyph.us-east-1.rds.amazonaws.com
3306  us-east-1b  3  60
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Una vez que se ha completado el escalado de almacenamiento, el estado de la instancia de base de datos cambia a `available`.

```
aws rds describe-db-instances --db-instance-identifier mydbinstance
```

```
DBINSTANCE  mydbinstance  2009-12-22T23:06:11.915Z  db.m5.large  mysql8.0  60  sa
available  mydbinstance.clla4j4jgyph.us-east-1.rds.amazonaws.com  3306
us-east-1b  3
 SECGROUP  default  active
 PARAMGRP  default.mysql8.0  in-sync
```

Puede recibir notificaciones cuando se ha agotado su espacio de almacenamiento mediante la operación `DescribeEvents`. Por ejemplo, en esta situación, si realiza una llamada `DescribeEvents` después de estas operaciones, verá el siguiente resultado.

```
aws rds describe-events --source-type db-instance --source-identifier mydbinstance
```

```
2009-12-22T23:44:14.374Z  mydbinstance  Allocated storage has been exhausted db-
instance
2009-12-23T00:14:02.737Z  mydbinstance  Applying modification to allocated storage db-
instance
2009-12-23T00:31:54.764Z  mydbinstance  Finished applying modification to allocated
 storage
```

Instancias de bases de datos de Amazon RDS disponibles insuficientes

El error `InsufficientDBInstanceCapacity` se puede devolver cuando intenta crear, iniciar o modificar una instancia de base de datos. También se puede devolver cuando intenta restaurar una instancia de base de datos a partir de una instantánea de base de datos. Cuando se recibe este error, una causa común es que la clase de instancia de base de datos específica no está disponible

en la zona de disponibilidad solicitada. Puede intentar una de las siguientes propuestas para resolver el problema:

- Volver a intentar la solicitud con una clase de instancia de base de datos distinta.
- Volver a intentar la solicitud con una zona de disponibilidad distinta.
- Volver a intentar la solicitud sin especificar una zona de disponibilidad explícita.

Para obtener más información acerca de la solución de problemas relacionados con la capacidad de la instancia para Amazon EC2, consulte el tema sobre capacidad insuficiente de las instancias en la guía del usuario de Amazon EC2.

Para obtener más información acerca de la modificación de una instancia de base de datos, consulte Modificación de una instancia de base de datos de Amazon RDS.

Problemas de memoria que se puede liberar en Amazon RDS

La memoria que se puede liberar es el total de memoria de acceso aleatorio (RAM) de una instancia de base de datos que se puede poner a disposición del motor de base de datos. Es la suma de la memoria libre del sistema operativo (SO) y de la memoria intermedia y la memoria caché de página disponibles. El motor de base de datos utiliza la mayor parte de la memoria del host, pero los procesos del sistema operativo también utilizan algo de RAM. La memoria actualmente asignada al motor de base de datos o que utilizan los procesos del sistema operativo no está incluida en la memoria que se puede liberar. Cuando el motor de base de datos se queda sin memoria, la instancia de base de datos puede utilizar el espacio temporal que normalmente se usa para el almacenamiento en búfer y en caché. Como se mencionó anteriormente, este espacio temporal se incluye en la memoria que se puede liberar.

La métrica `FreeableMemory` de Amazon CloudWatch se utiliza para supervisar la memoria que se puede liberar. Para obtener más información, consulte Supervisión de herramientas de Amazon RDS.

Si su instancia de base de datos se queda constantemente sin memoria que se pueda liberar o utiliza espacio de intercambio, considere la psibilidad de escalar verticalmente a una clase de instancia de base de datos más grande. Para obtener más información, consulte Clases de instancia de base de datos de .

También puede cambiar la configuración de memoria. Por ejemplo, en RDS para MySQL, podría ajustar el tamaño del parámetro `innodb_buffer_pool_size`. Este parámetro está establecido de

forma predeterminada al 75 % de la memoria física. Para obtener más consejos sobre la solución de problemas de MySQL, consulte How can I troubleshoot low freeable memory in an Amazon RDS para MySQL database? (¿Cómo puedo solucionar un problema de poca memoria que se puede liberar en una base de datos de Amazon RDS para MySQL?).

Problemas de MySQL y MariaDB

Puede diagnosticar y corregir problemas con las instancias de base de datos MySQL y MariaDB.

Temas

- Máximo de conexiones de MySQL y MariaDB
- Diagnóstico y resolución del estado de parámetros incompatibles para un límite de memoria
- Diagnóstico y resolución de retardos entre réplicas de lectura
- Diagnóstico y solución de un error de replicación de lectura de MySQL o MariaDB
- La creación de desencadenadores con registro binario habilitado exige privilegios SUPER
- Diagnóstico y resolución de errores de restauración a un momento dado
- Error de replicación detenida
- Se produce un error en la creación de la réplica de lectura o la replicación se interrumpe con el error grave 1236
- La replicación de réplicas de lectura no puede inicializar la estructura de metadatos

Máximo de conexiones de MySQL y MariaDB

El número máximo de conexiones permitidas a una instancia de base de datos de RDS para MySQL o de RDS para MariaDB se basa en la cantidad de memoria disponible para la clase de instancia de base de datos. Una clase de instancia de base de datos con más memoria disponible da como resultado un mayor número de conexiones disponibles. Para obtener más información acerca de las clases de instancias de bases de datos, consulte Clases de instancia de base de datos de .

El límite de conexiones para una instancia de base de datos se define de forma predeterminada en el número máximo para la clase de instancia de base de datos. Puede limitar el número de conexiones simultáneas a cualquier valor hasta el número máximo de conexiones permitidas. Utilice el parámetro `max_connections` en el grupo de parámetros para la instancia de base de datos. Para obtener más información, consulte Número máximo de conexiones de base de datos y Grupos de parámetros para Amazon RDS.

Puede recuperar el número máximo de conexiones permitidas para una instancia de base de datos de MySQL o MariaDB ejecutando la siguiente consulta.

```
SELECT @@max_connections;
```

Puede recuperar el número de conexiones activas para una instancia de base datos de MySQL o MariaDB ejecutando la siguiente consulta.

```
SHOW STATUS WHERE `variable_name` = 'Threads_connected';
```

Diagnóstico y resolución del estado de parámetros incompatibles para un límite de memoria

Una instancia de base de datos de MariaDB o MySQL puede tener el estado incompatible-parameters para un límite de memoria cuando se cumplen las condiciones siguientes:

- La instancia de base de datos se reinicia al menos tres veces en una hora o al menos cinco veces en un día, cuando el estado de la instancia de base de datos es Disponible.
- Se produce un error al intentar reiniciar la instancia de base de datos porque una acción de mantenimiento o un proceso de monitorización no han podido reiniciar la instancia de base de datos.
- El uso potencial de memoria de la instancia de base de datos supera 1,2 veces la memoria asignada a su clase de instancia de base de datos.

Cuando una instancia de base de datos se reinicia por tercera vez en una hora o por quinta vez en un día, realiza una comprobación del uso de memoria. La comprobación realiza el cálculo del uso potencial de memoria de la instancia de base de datos. El valor devuelto por el cálculo es la suma de los siguientes valores:

- Valor 1: la suma de los siguientes parámetros:
  - `innodb_additional_mem_pool_size`
  - `innodb_buffer_pool_size`

    Puede cambiar el valor de `innodb_buffer_pool_size`. Sin embargo, el valor no siempre coincidirá con lo que introduzca. Esta falta de coincidencia se produce por varias razones. En primer lugar, si la instancia de base de datos es una microinstancia de base de datos,

sustituimos el valor predeterminado y lo establecemos en 256 MB. Para obtener más información, consulte Anulación de innodb_buffer_pool_size.

En segundo lugar, nos aseguramos de reservar 500 MB de memoria en la instancia de base de datos para el administrador del host, el motor, el sistema operativo y el kernel.

Por último, optimizamos `innodb_buffer_pool_size` dividiéndolo en unidades. El administrador del host redondea hacia abajo al múltiplo más cercano de esas unidades. Las unidades se calculan multiplicando `innodb_buffer_pool_chunk_size` por `innodb_buffer_pool_instances`. Para obtener más información, consulte Configuring InnoDB Buffer Pool Size en la documentación de MySQL.

El valor predeterminado para `innodb_buffer_pool_instances` es 8, a menos que `innodb_buffer_pool_size` sea inferior a 1 GB. Si `innodb_buffer_pool_size` es inferior a 1 GB, el valor predeterminado para `innodb_buffer_pool_instances` es 1. El valor predeterminado para `innodb_buffer_pool_chunk_size` es de 128 MB.

  - `innodb_log_buffer_size`
  - `key_buffer_size`
  - `query_cache_size` (versión 5.7 de MySQL únicamente)
  - `tmp_table_size`
- Valor 2_ el parámetro `max_connections` multiplicado por la suma de los siguientes parámetros:
  - `binlog_cache_size`
  - `join_buffer_size`
  - `read_buffer_size`
  - `read_rnd_buffer_size`
  - `sort_buffer_size`
  - `thread_stack`
- Valor 3 – Si el parámetro `performance_schema` está habilitado, multiplique el parámetro `max_connections` por 429498.

  Si el parámetro `performance_schema` está deshabilitado, entonces este valor es cero.

Por lo tanto, el valor devuelto por el cálculo es el siguiente:

```
Value 1 + Value 2 + Value 3
```

Cuando este valor supera 1,2 veces la memoria asignada a la clase de instancia de base de datos utilizada por la instancia de base de datos, la instancia de base de datos se coloca en el estado de parámetros incompatibles. Para obtener información acerca de la memoria asignada a las clases de instancia de base de datos, consulte Especificaciones de hardware para clases de instancia de base de datos .

El cálculo multiplica el valor del parámetro `max_connections` por la suma de varios parámetros. Si el parámetro `max_connections` se establece en un valor grande, podría hacer que la comprobación devuelva un valor extremadamente alto del uso potencial de memoria de la instancia de base de datos. En este caso, considere bajar el valor del parámetro `max_connections`.

Para resolver el problema, siga los pasos siguientes:

1. Ajuste los parámetros de memoria del grupo de parámetros de base de datos asociado a la instancia de base de datos. Hágalo de forma que el uso potencial de memoria sea inferior a 1,2 veces la memoria asignada a su clase de instancia de base de datos.

   Para obtener información acerca de cómo configurar los parámetros, consulte Modificación de los parámetros de un grupo de parámetros de base de datos en Amazon RDS.
2. Reinicie la instancia de base de datos.

   Para obtener información acerca de cómo configurar los parámetros, consulte Inicio de una instancia de base de datos de Amazon RDS parada previamente.

Diagnóstico y resolución de retardos entre réplicas de lectura

Después de crear una réplica de lectura de MySQL o MariaDB y de que dicha réplica esté disponible, Amazon RDS replica en primer lugar los cambios realizados en la instancia de base de datos de origen desde el momento en que se inició la operación de creación de réplica de lectura. Durante esta fase, el retraso de replicación para la réplica de lectura es mayor que 0. También puede monitorizar este retardo en Amazon CloudWatch viendo la métrica `ReplicaLag` de Amazon RDS.

La métrica `ReplicaLag` indica el valor del campo `Seconds_Behind_Master` del comando `SHOW REPLICA STATUS` de MariaDB o MySQL. Para obtener más información, consulte HOW REPLICA STATUS Statement (Instrucción HOW REPLICA STATUS) en la documentación de MySQL.

Cuando la métrica `ReplicaLag` llegue a 0, la réplica estará funcionando al mismo ritmo que la instancia de base de datos de origen. Si la métrica `ReplicaLag` devuelve -1, la replicación podría no estar activa. Para solucionar problemas de error de replicación, consulte Diagnóstico y solución de

un error de replicación de lectura de MySQL o MariaDB. Un valor `ReplicaLag` de -1 también puede significar que el valor `Seconds_Behind_Master` no se puede determinar o es `NULL`.

> **Note**
>
> Versiones anteriores de MariaDB utilizaban `SHOW SLAVE STATUS` en lugar de `SHOW REPLICA STATUS`. Si usa una versión de MariaDB anterior a la 10.5, utilice `SHOW SLAVE STATUS`.

La métrica `ReplicaLag` devuelve -1 durante una interrupción de la red o cuando se aplica un parche durante el período de mantenimiento. En este caso, espere a que se restaure la conectividad de la red o a que finalice el período de mantenimiento antes de volver a comprobar la métrica `ReplicaLag` .

La tecnología de replicación de lectura de MySQL y MariaDB es asíncrona. Por lo tanto, cabe esperar aumentos ocasionales para la métrica `BinLogDiskUsage` en la instancia de base de datos de origen y para la métrica `ReplicaLag` en la réplica de lectura. Por ejemplo, considere una situación en la que se pueden realizar en paralelo un gran volumen de operaciones de escritura en la instancia de base de datos de origen. Al mismo tiempo, las operaciones de escritura en la réplica de lectura se serializan utilizando un único subproceso de E/S. Tal situación puede provocar un retraso entre la instancia de origen y la réplica de lectura.

Para obtener más información acerca de las réplicas de lectura y MySQL, consulte Replication Implementation Details en la documentación de MySQL. Para obtener más información acerca de las réplicas de lectura y MariaDB, consulte Descripción de replicación en la documentación de MariaDB.

Puede hacer varias cosas para reducir el retraso entre las actualizaciones de una instancia de base de datos de origen y las actualizaciones posteriores de la réplica de lectura:

- Configure la clase de instancia de base de datos de la réplica de lectura para que tenga un tamaño de almacenamiento comparable al de la instancia de base de datos de origen.
- Asegúrese de que la configuración de parámetros de los grupos de parámetros de base de datos utilizados en la instancia de base de datos de origen y la réplica de lectura sean compatibles. Para obtener más información y un ejemplo, consulte el análisis del parámetro `max_allowed_packet` en la siguiente sección.
- Deshabilite la caché de consultas. Para tablas que se modifican a menudo, el uso de la caché de consultas puede aumentar el retardo de réplica porque la caché se bloquea y actualiza

con frecuencia. Si esto fuera así, podría ver menos retardo de réplica si deshabilita la caché de consultas. Puede deshabilitar la caché de consultas estableciendo `query_cache_type` `parameter` en 0 en el grupo de parámetros de base de datos para la instancia de base de datos. Para obtener más información sobre la caché de consultas, consulte Query Cache Configuration.

- Active el grupo de búferes en la réplica de lectura de InnoDB para MySQL o MariaDB. Por ejemplo, suponga que tiene un conjunto pequeño de tablas que se actualiza con frecuencia y está utilizando el esquema de tablas InnoDB o XtraDB. En este caso, puede volcar esas tablas en la réplica de lectura. Al hacer esto, el motor de base de datos examina las filas de esas tablas desde el disco y, a continuación, las almacena en la caché en el grupo del búfer. Este enfoque puede reducir el retraso de la réplica. A continuación se muestra un ejemplo.

  Para Linux, macOS o Unix:

```
PROMPT> mysqldump \
    -h <endpoint> \
    --port=<port> \
    -u=<username> \
    -p <password> \
    database_name table1 table2 > /dev/null
```

  Para Windows:

```
PROMPT> mysqldump ^
    -h <endpoint> ^
    --port=<port> ^
    -u=<username> ^
    -p <password> ^
    database_name table1 table2 > /dev/null
```

Diagnóstico y solución de un error de replicación de lectura de MySQL o MariaDB

Amazon RDS supervisa el estado de replicación de las réplicas de lectura. RDS actualiza el campo Replication State (Estado de replicación) de la instancia de réplica de lectura a `Error` si la replicación se detiene por cualquier motivo. Puede revisar los detalles del error asociado que muestran los motores de MySQL o MariaDB visualizando el campo Replication Error (Error de replicación). También se generan eventos que indican el estado de la réplica de lectura, entre

los que se incluyen RDS-EVENT-0045, RDS-EVENT-0046 y RDS-EVENT-0057. Para obtener más información acerca de los eventos y la suscripción a ellos, consulte Uso de notificaciones de eventos de Amazon RDS. Si aparece un mensaje de error de MySQL, compruebe el error en la documentación de mensajes de error de MySQL. Si aparece un mensaje de error de MariaDB, compruebe el error en la documentación de mensajes de error de MariaDB.

Estas son algunas de las situaciones comunes que pueden causar errores de replicación:

- El valor para el parámetro `max_allowed_packet` para una réplica de lectura es inferior al parámetro `max_allowed_packet` para la instancia de base de datos de origen.

  El parámetro `max_allowed_packet` es un parámetro personalizado que puede establecer en un grupo de parámetros de base de datos. El parámetro `max_allowed_packet` se utiliza para especificar el tamaño máximo del lenguaje de manipulación de datos (DML) que se puede ejecutar en la base de datos. En algunos casos, el valor de `max_allowed_packet` de la instancia de base de datos de origen puede ser superior al valor de `max_allowed_packet` para la réplica de lectura. Si es así, el proceso de replicación puede generar el error y detener la replicación. El error más común es `packet bigger than 'max_allowed_packet' bytes`. Puede resolver el error haciendo que el origen y la réplica de lectura usen grupos de parámetros de base de datos con los mismos valores del parámetro `max_allowed_packet`.
- Escritura en tablas en una réplica de lectura. Si desea crear índices en una réplica de lectura, debe establecer el parámetro `read_only` en 0 para crear los índices. Si se escribe en las tablas de la réplica de lectura, puede interrumpirse la replicación.
- Uso de un motor de almacenamiento no transaccional como MyISAM. Las réplicas de lectura requieren un motor de almacenamiento transaccional. La reproducción solo se admite para los siguientes motores de almacenamiento: InnoDB for MySQL o MariaDB.

  Puede convertir una tabla MyISAM a InnoDB con el siguiente comando:

  ```
  alter table <schema>.<table_name> engine=innodb;
  ```
- Uso de consultas no deterministas que no sean seguras, como `SYSDATE()`. Para obtener más información, consulte Determination of Safe and Unsafe Statements in Binary Logging en la documentación de MySQL.

Los siguientes pasos pueden ayudar a solucionar su error de replicación:

- Si se encuentra ante un error lógico y decide que es seguro hacer caso omiso, siga los pasos que se describen en Omisión del error de replicación actual de RDS para MySQL. La

instancia de base de datos MySQL o MariaDB debe estar ejecutando una versión que incluya el procedimiento `mysql_rds_skip_repl_error`. Para obtener más información, consulte mysql.rds_skip_repl_error.

- Si se encuentra ante un problema de posición de registro binario (binlog), puede cambiar la posición de reproducción de la réplica con el comando mysql.rds_next_source_log (RDS para las versiones principales de MySQL 8.4 y superiores) o mysql.rds_next_master_log (RDS para MariaDB y RDS para las versiones principales de MySQL 8.0 e inferiores).
- Es posible que encuentre un problema de rendimiento temporal debido a la alta carga de DML. Si es así, puede establecer el parámetro `innodb_flush_log_at_trx_commit` en 2 en el grupo de parámetros de base de datos de la réplica de lectura. Hacer esto puede ayudar a la réplica de lectura a ponerse al corriente, si bien reduce temporalmente las propiedades de atomicidad, coherencia, aislamiento y durabilidad (ACID).
- Puede eliminar la réplica de lectura y crear una instancia con el mismo identificador de instancias de bases de datos. De este modo, el punto de enlace seguirá siendo el mismo que en la réplica de lectura antigua.

Si se corrige un error de replicación, Replication State cambia a replicating. Para obtener más información, consulte Solución de problemas de réplicas de lectura de MySQL.

La creación de desencadenadores con registro binario habilitado exige privilegios SUPER

Al intentar crear desencadenadores en una instancia de base de datos de RDS para MySQL o RDS para MariaDB, podría recibir el siguiente error.

```
"You do not have the SUPER privilege and binary logging is enabled"
```

Para utilizar desencadenadores cuando el registro binario está habilitado, se necesitan privilegios SUPER, que están restringidos para las instancias de base de datos de RDS para MySQL y RDS para MariaDB. Puede crear disparadores cuando el registro binario está habilitado sin privilegios SUPER estableciendo el parámetro `log_bin_trust_function_creators` en true. Para establecer `log_bin_trust_function_creators` en true, cree un grupo de parámetros de base de datos nuevo o modifique un grupo existente.

Puede crear un nuevo grupo de parámetros de base de datos para poder crear desencadenadores en su instancia de base de datos de RDS para MySQL o RDS para MariaDB con el registro binario

activado. Para ello, utilice los siguientes comandos de CLI. Para modificar un grupo de parámetros existente, comience por el paso 2.

Para crear un grupo de parámetros nuevo que permita disparadores con el registro binario habilitado mediante la CLI

1. Cree un nuevo grupo de parámetros.

   Para Linux, macOS o Unix:

   ```
   aws rds create-db-parameter-group \
       --db-parameter-group-name allow-triggers \
       --db-parameter-group-family mysql8.0 \
       --description "parameter group allowing triggers"
   ```

   Para Windows:

   ```
   aws rds create-db-parameter-group ^
       --db-parameter-group-name allow-triggers ^
       --db-parameter-group-family mysql8.0 ^
       --description "parameter group allowing triggers"
   ```

2. Modifique el grupo de parámetros de base de datos para permitir disparadores.

   Para Linux, macOS o Unix:

   ```
   aws rds modify-db-parameter-group \
       --db-parameter-group-name allow-triggers \
       --parameters "ParameterName=log_bin_trust_function_creators,
    ParameterValue=true, ApplyMethod=pending-reboot"
   ```

   Para Windows:

   ```
   aws rds modify-db-parameter-group ^
       --db-parameter-group-name allow-triggers ^
       --parameters "ParameterName=log_bin_trust_function_creators,
    ParameterValue=true, ApplyMethod=pending-reboot"
   ```

3. Modifique su instancia de base de datos para usar el nuevo grupo de parámetros de base de datos.

Para Linux, macOS o Unix:

```
aws rds modify-db-instance \
    --db-instance-identifier mydbinstance \
    --db-parameter-group-name allow-triggers \
    --apply-immediately
```

Para Windows:

```
aws rds modify-db-instance ^
    --db-instance-identifier mydbinstance ^
    --db-parameter-group-name allow-triggers ^
    --apply-immediately
```

4. Para que los cambios surtan efecto, reinicie manualmente la instancia de base de datos.

```
aws rds reboot-db-instance --db-instance-identifier mydbinstance
```

Diagnóstico y resolución de errores de restauración a un momento dado

Restauración de una instancia de base de datos que incluye tablas temporales

Al intentar una restauración a un momento dado (PITR) de una instancia de base de datos MySQL o MariaDB, podría recibir el siguiente error.

```
Database instance could not be restored because there has been incompatible database
 activity for restore
functionality. Common examples of incompatible activity include using temporary tables,
 in-memory tables,
or using MyISAM tables. In this case, use of Temporary table was detected.
```

PITR usa instantáneas de copia de seguridad y registros binarios (binlogs) de MySQL o MariaDB para restaurar su instancia de base de datos a un momento específico. La información de las tablas temporales podría no ser fiable en binlogs y causar un error de PITR. Si utiliza tablas temporales en su instancia de base de datos de MySQL o MariaDB, puede reducir las posibilidades de un error de PITR realizando copias de seguridad más frecuentes. Un error de PITR es más probable en el tiempo que transcurre entre la creación de la tabla temporal y la siguiente instantánea de copia de seguridad.

Restauración de una instancia de base de datos que incluye tablas en memoria

Podría encontrarse con un problema al restaurar una base de datos que tiene tablas en memoria. Las tablas en memoria se purgan durante un reinicio. Como consecuencia, sus tablas en memoria podrían estar vacías después de un reinicio. Recomendamos que cuando utilice tablas en memoria, diseñe su solución para que controle tablas vacías en caso de producirse un reinicio. Si utiliza tablas en memoria con instancias de base de datos replicadas, tal vez deba recrear las réplicas de lectura después de un reinicio. Esto puede ser necesario si una réplica de lectura se reinicia y no puede restaurar datos de una tabla en memoria vacía.

Para obtener más información acerca de copias de seguridad y PITR, consulte Introducción a las copias de seguridad y Restauración de una instancia de base de datos a un momento especificado para Amazon RDS.

Error de replicación detenida

Cuando llame al comando `mysql.rds_skip_repl_error`, es posible que reciba un mensaje de error en el que se indique que la reproducción tiene un error o está deshabilitada.

Este mensaje de error aparece porque la replicación se ha detenido y no se puede reiniciar.

Si tiene que omitir un número de errores elevado, el retardo de réplica puede aumentar por encima del periodo de retención predeterminado para los archivos de registro binarios. En este caso, puede producirse un error irrecuperable debido a que los archivos de registro binario se están limpiando antes de reproducirse de nuevo en la réplica. Esta limpieza hace que la replicación se detenga y ya no se puede llamar al comando `mysql.rds_skip_repl_error` para omitir los errores de replicación.

Puede mitigar este problema incrementando el número de horas que los archivos de registro binarios se retienen en el origen de la replicación. Después de incrementar el tiempo de retención de los archivos binlog, puede reiniciar la replicación y llamar al comando `mysql.rds_skip_repl_error` si es necesario.

Para establecer el tiempo de retención del binlog, utilice el procedimiento mysql.rds_set_configuration. Especifique un parámetro de configuración de "horas de retención del binlog" junto con el número de horas de retención de los archivos binlog en el clúster de base de datos, hasta un máximo de 720 (30 días). El ejemplo siguiente define el periodo de retención de los archivos binlog en 48 horas.

```
CALL mysql.rds_set_configuration('binlog retention hours', 48);
```

Se produce un error en la creación de la réplica de lectura o la replicación se interrumpe con el error grave 1236

Después de cambiar los valores de los parámetros predeterminados para una instancia de base de datos MySQL o MariaDB, podría encontrarse ante uno de los siguientes problemas:

- No puede crear una réplica de lectura para la instancia de base de datos.
- Error de replicación co `fatal error 1236`.

Algunos valores de parámetros predeterminados para instancias de base de datos MySQL o MariaDB ayudan a garantizar que la base de datos cumple las propiedades ACID y que las réplicas de lectura están a prueba de bloqueo. Esto se logra asegurándose de que cada confirmación esté totalmente sincronizada mediante la escritura de la transacción en el registro binario antes de su confirmación. Cambiar los valores predeterminados de estos parámetros para mejorar el rendimiento puede provocar un error en la replicación si no se ha escrito una transacción en el registro binario.

Para resolver este problema, establezca los siguientes valores de parámetros:

- `sync_binlog = 1`
- `innodb_support_xa = 1`
- `innodb_flush_log_at_trx_commit = 1`

La replicación de réplicas de lectura no puede inicializar la estructura de metadatos

Cuando intentó iniciar la replicación, se recibió el siguiente mensaje de error:

```
Read Replica Replication Error - SQLError: 13124, reason: Replica failed to initialize
 applier metadata structure from the repository
```

Este error se produce cuando hay un problema con la estructura de metadatos de la réplica. Para corregir la estructura de los metadatos, debe crear una nueva réplica.

Para evitar que esto ocurra en el futuro, lleve a cabo alguna de las siguientes acciones:

- Si es posible, desactive los subprocesos múltiples en las réplicas. A partir de MySQL 8.0.27, los subprocesos múltiples están habilitados de forma predeterminada.

- Si necesita utilizar subprocesos múltiples en las réplicas, le recomendamos que utilice la replicación basada en GTID. Para obtener más información, consulte Uso de la replicación basada en GTID.

No se puede establecer el período de retención de copia de seguridad en 0

Existen varios motivos por los que es posible que tenga que establecer el período de retención de copia de seguridad en 0. Por ejemplo, puede deshabilitar las copias de seguridad automáticas inmediatamente estableciendo el período de retención en 0.

En algunos casos, podría establecer el valor en 0 y recibir un mensaje indicando que el período de retención debe estar entre 1 y 35. En estos casos, compruebe que no ha configurado una réplica de lectura para la instancia. Las réplicas de lectura requieren copias de seguridad para administrar los registros de réplica de lectura y, por lo tanto, no puede establecer el período de retención de 0.

Referencia de la API de Amazon RDS

Además de AWS Management Console y la AWS Command Line Interface (AWS CLI), Amazon RDS también proporciona una API. Puede utilizar la API para automatizar las tareas de administración de instancias de base de datos y otros objetos en Amazon RDS.

- Para ver una lista de acciones de la API ordenada alfabéticamente, consulte el tema relacionado con las acciones.
- Para ver una lista de tipos de datos ordenada alfabéticamente, consulte el tema relacionado con los Tipos de datos.
- Para ver una lista de parámetros de consulta comunes, consulte el tema relacionado con los Parámetros comunes.
- Para ver las descripciones de los códigos de error, consulte el tema relacionado con los Errores comunes.

Para obtener más información acerca de AWS CLI, consulte la referencia de AWS Command Line Interface para Amazon RDS.

Temas

- Uso de la API de consulta
- Solución de problemas de aplicaciones en Amazon RDS

Uso de la API de consulta

En las siguientes secciones se explican brevemente los parámetros y la autenticación de solicitudes que se utilizan con la API de consulta.

Para obtener información general acerca del funcionamiento de la API de consulta, consulte Solicitudes de consulta en la Amazon EC2 API Reference.

Parámetros de consulta

Las solicitudes basadas en consultas HTTP son solicitudes HTTP que utilizan el verbo HTTP GET o POST y un parámetro de consulta denominado `Action`.

Cada solicitud de consulta debe incluir algunos parámetros comunes para realizar la autenticación y la selección de una acción.

Algunas operaciones toman listas de parámetros. Estas listas se especifican utilizando la notación `param.`*n*. Los valores de *n* son números enteros a partir de 1.

Para obtener más información acerca de las regiones y los puntos de conexión de Amazon RDS, vaya a Amazon Relational Database Service (RDS) en la sección Regiones y puntos de conexiones de la Referencia general de Amazon Web Services.

Autenticación de solicitudes de consulta

Solo se pueden enviar solicitudes de consulta a través de HTTPS, y cada una de ellas debe incluir una firma. Debe utilizar Signature Version 4 o Signature Version 2 de AWS. Para obtener más información, consulte Proceso de firma de Signature Version 4 y Proceso de firma de Signature Version 2.

Solución de problemas de aplicaciones en Amazon RDS

Amazon RDS proporciona errores específicos y descriptivos para ayudarle a solucionar problemas durante la interacción con la API de Amazon RDS.

Temas

- Recuperación de errores
- Consejos para la solución de problemas

Para obtener más información sobre la solución de problemas para instancias de base de datos de Amazon RDS, consulte Solución de problemas de Amazon RDS.

Recuperación de errores

Normalmente, conviene que una aplicación compruebe si una solicitud generó un error antes de emplear tiempo en procesar los resultados. La forma más fácil de averiguar si se ha producido un error, consiste en buscar un nodo `Error` en la respuesta de la API de Amazon RDS.

La sintaxis XPath proprciona una forma simple de buscar la presencia de un nodo `Error`. También proporciona una forma relativamente fácil de recuperar el código y el mensaje de error. La partición de código siguiente utiliza Perl y el módulo XML::XPath para determinar si se ha producido un error

durante una solicitud. Si es así, el código imprime el primer mensaje de error y su código en la respuesta.

```
use XML::XPath;
    my $xp = XML::XPath->new(xml =>$response);
    if ( $xp->find("//Error") )
    {print "There was an error processing your request:\n", " Error code: ",
    $xp->findvalue("//Error[1]/Code"), "\n", " ",
    $xp->findvalue("//Error[1]/Message"), "\n\n"; }
```

Consejos para la solución de problemas

Recomendamos los siguientes procesos para diagnosticar y solucionar problemas con la API de Amazon RDS:

- Verifique si Amazon RDS funciona normalmente en la región de AWS de destino consultando http://status.aws.amazon.com.
- Comprobar la estructura de la solicitud.

  Cada operación de Amazon RDS tiene una página de referencia en la Referencia de la API de Amazon RDS. Compruebe que está utilizando los parámetros correctamente. Para obtener ideas sobre lo que podría estar mal, mire las solicitudes de ejemplo o los escenarios de usuario para ver si esos ejemplos hacen operaciones similares.
- Comprobar AWS re:Post

  Existe una comunidad de desarrolladores de Amazon RDS donde puede buscar soluciones a los problemas que otras personas han experimentado al utilizar este servicio. Para ver los temas, vaya a AWS re:Post.

Historial de revisión

Versión actual de la API: 31/10/2014

En la siguiente tabla se describen los cambios importantes en cada versión de la Guía del usuario de Amazon RDS posteriores a mayo de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

> **Note**
>
> Puede filtrar nuevas características de Amazon RDS en la página Novedades de Database. En el filtro Products (Productos), elija Amazon RDS. Después, busque con palabras clave como **`RDS Proxy`** o **`Oracle 2023`**.

Cambio	Descripción	Fecha
Amazon RDS es compatible con MySQL 8.0.39	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.39 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	12 de agosto de 2024
Actualización de una política existente	Amazon RDS ha eliminado el permiso `sns:Publish` de `AmazonRDSPreviewServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSPreview`. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de	7 de agosto de 2024

	las políticas administradas de AWS).	
Actualización de una política existente	Amazon RDS ha eliminado el permiso `sns:Publish` de `AmazonRDSBetaServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDSBeta` . Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	7 de agosto de 2024
Amazon RDS admite MySQL 8.4 en el entorno de vista previa de bases de datos	MySQL 8.4 ya está disponible en el entorno de vista previa de bases de datos en la Región de AWS Este de EE. UU. (Ohio). Para obtener más información, consulte MySQL version 8.4 in the Database Preview environment.	1 de agosto de 2024

Actualización de permisos de roles vinculados a servicios de IAM	Ahora, la política `AmazonRDSCustomServiceRolePolicy` otorga permisos adicionales para comunicarse con los servicios de Amazon RDS en otra Región de AWS y para copiar imágenes de EC2. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	18 de julio de 2024
Amazon RDS admite MariaDB 11.4 en el entorno de vista previa de bases de datos	MariaDB 11.4 ya está disponible en el entorno de vista previa de bases de datos en la Región de AWS Este de EE. UU. (Ohio). Para obtener más información, consulte MariaDB version 11.4 in the Database Preview environment.	18 de julio de 2024
Controlador ODBC de AWS para MySQL disponible de forma general	El controlador ODBC de Amazon Web Services (AWS) para MySQL es un controlador de cliente diseñado para la alta disponibilidad de RDS para MySQL. Para obtener más información, consulte Conexión a RDS para MySQL con el controlador ODBC de Amazon Web Services (AWS) para MySQL.	18 de julio de 2024

Actualización de una política existente	Amazon RDS ha eliminado el permiso `sns:Publish` de `AmazonRDSServiceRolePolicy` del rol vinculado a un servicio `AWSServiceRoleForRDS` . Para obtener más información, consulte Política administrada por:AWS Amazon RDSServiceRolePolicy.	2 de julio de 2024
Oferta privada de AWS Marketplace para Db2	AWS Marketplace ahora admite ofertas privadas de una licencia de Db2 a través de AWS Marketplace para Amazon RDS para Db2. Para obtener más información, consulte Obtención de una oferta privada.	1 de julio de 2024
Exportación de datos de instantáneas de clúster de base de datos multi-AZ a Amazon S3	Ahora puede exportar datos de instantáneas de clúster de base de datos multi-AZ a Amazon S3. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3.	27 de junio de 2024

Amazon RDS para Oracle admite clases de instancia optimizada para memoria r6i preconfiguradas	Las clases de instancia de base de datos de Oracle db.r6i están optimizadas para cargas de trabajo que requieren memoria, almacenamiento y E/S adicionales por vCPU. Por ejemplo, db.r6i.8xlarge.tpc2.mem4x tiene activado el multiproceso y proporciona 4 veces más memoria que db.r6i.8xlarge. Para obtener más información, consulte los datos sobre las clases de instancias de RDS para Oracle.	21 de junio de 2024
Soporte extendido de Amazon RDS versión 5.7.44-RDS.20240529 para RDS para MySQL	El soporte extendido de RDS versión 5.7.44-RDS.20240529 ahora se encuentra disponible para RDS para MySQL. Para obtener más información, consulte Amazon RDS Extended Support versions for RDS for MySQL.	20 de junio de 2024
Amazon RDS es compatible con MySQL 8.0.37	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.37 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	18 de junio de 2024

Amazon RDS es compatible con MariaDB 10.11.8, 10.6.18, 10.5.25 y 10.4.34	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.11.8, 10.6.18, 10.5.25 y 10.4.34. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	14 de junio de 2024
Amazon RDS va a finalizar el soporte de las clases de instancia de base de datos db.m4, db.r4 y db.t2	Para los motores de base de datos RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL, ya no puede crear instancias de base de datos que utilicen las clases de instancia db.m4, db.r4 y db.t2. RDS actualiza automáticamente las instancias de base de datos existentes que utilizan estas clases a una generación más reciente. Para obtener más información, consulte Tipos de clase de instancia de base de datos.	4 de junio de 2024
Clústeres de bases de datos Multi-AZ disponibles en Regiones de AWS adicionales	Puede crear clústeres de base de datos Multi-AZ en más Regiones de AWS. Para ver una tabla que muestra todas las regiones compatibles, consulte Regiones y motores de base de datos admitidos para clústeres de bases de datos Multi-AZ en Amazon RDS.	29 de mayo de 2024

El controlador de Python de AWS está disponible de forma general	El controlador de Python de Amazon Web Services (AWS) se ha diseñado como un contenedor de Python avanzado. Este contenedor complementa y amplía la funcionalidad del controlador de Psycopg de código abierto. Para obtener más información, consulte Conexión a instancias de base de datos con los controladores de AWS.	23 de mayo de 2024
RDS Proxy está disponible en más regiones	RDS Proxy ya está disponible en las regiones de Asia-Pacífico (Hyderabad), Asia Pacífico (Melbourne), Medio Oriente (EAU), Israel (Tel Aviv), Israel (Tel Aviv), Oeste de Canadá (Calgary) y Europa (Zúrich). Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	21 de mayo de 2024
Licencia de Db2 a través de AWS Marketplace	Con la licencia Db2 a través de AWS Marketplace, ahora puede pagar una tarifa por hora para suscribirse a licencias de Db2 para Amazon RDS para Db2. Para obtener más información, consulte Opciones de licencias de Amazon RDS para Db2.	21 de mayo de 2024

Amazon RDS admite un acceso detallado para Información sobre rendimiento	Ahora es posible permitir o denegar el acceso a dimensiones individuales en Información sobre rendimiento. Este acceso detallado se puede utilizar para acciones `GetResourceMetrics`, `DescribeDimensionKeys` y `GetDimensionKeyDetails`. Para obtener más información, consulte Concesión de acceso detallado para Información sobre rendimiento.	21 de mayo de 2024
Versiones de soporte extendido de Amazon RDS para RDS for MySQL	Puede ver todas las versiones del soporte extendido de RDS para las versiones de RDS para MySQL. Para obtener más información, consulte Amazon RDS Extended Support versions for RDS for MySQL.	16 de mayo de 2024
Amazon RDS admite MySQL 8.3 en el entorno de vista previa de base de datos	MySQL 8.3 ya está disponible en el entorno de vista previa de bases de datos en la Región de AWS Este de EE. UU. (Ohio). Para obtener más información, consulte MySQL version 8.3 in the Database Preview environment.	30 de abril de 2024

Amazon RDS para Db2 admite zonas horarias	RDS para Db2 ahora admite la configuración de zonas horarias locales para instancias de bases de datos Db2. Para obtener más información, consulte Local time zones for Amazon RDS for Db2 DB instances.	25 de abril de 2024
Actualización de permisos de roles vinculados a servicios de IAM	La política `AmazonRDSCustomServiceRolePolicy` ahora otorga permisos adicionales para asociar un rol de servicio como perfil de instancia a una instancia de RDS Custom. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	19 de abril de 2024
Amazon RDS para Oracle admite la transición de Oracle Data Guard en todas las Regiones de AWS	Ahora puede utilizar la transición de Oracle Data Guard en todas las regiones compatibles. Para obtener más información, consulte Información general sobre transiciones de Oracle Data Guard.	16 de abril de 2024

RDS Custom para Oracle admite Oracle Standard Edition 2	Ahora puede crear instancias de base de datos utilizando Standard Edition 2 en Oracle Database 12c versión 1 (12.1), 12c versión 2 (12.2), 18c y 19c. Puede crear tanto CDB como no CDB. Para obtener más información, consulte Compatibilidad de ediciones y licencias con RDS Custom para Oracle.	11 de abril de 2024
Amazon RDS para Oracle admite Oracle APEX versión 23.2.v1	Puede utilizar APEX 23.2.v1 con Oracle Database 19c y versiones posteriores. Para obtener más información, consulte Oracle Application Express.	11 de abril de 2024
Actualización de los permisos de roles vinculados a servicios de RDS Custom	`AmazonRDSCustomServiceRolePolicy` ahora otorga permisos adicionales para permitir que RDS Custom para SQL Server obtenga información del tipo de instancia de EC2 y modifique el tipo de instancia de host de base de datos. Para obtener más información, consulte Actualizaciones a políticas administradas por AWS.	8 de abril de 2024

Amazon RDS Custom para Oracle admite la clase de instancia de base de datos db.x2iezn	Ahora puede utilizar la clase de instancia db.x2iezn para las instancias de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.	26 de marzo de 2024
Amazon RDS admite las clases de instancia db.c6gd para clústeres de bases de datos multi-AZ	Ahora puede usar las clases de instancias db.c6gd para las implementaciones de clústeres de bases de datos multi-AZ. Para obtener más información, consulte Disponibilidad de clases de instancia para clústeres de bases de datos multi-AZ.	21 de marzo de 2024

Soporte extendido de Amazon RDS	Al crear o restaurar una base de datos de RDS para MySQL 5.7 o RDS para PostgreSQL 11, ahora esa base de datos se inscribe automáticamente en el Soporte extendido de Amazon RDS para que las aplicaciones existentes sigan funcionando como siempre. Puede cancelar el Soporte extendido de RDS para evitar que se le cobre después de la fecha del fin del soporte estándar de RDS para su motor de base de datos. Para obtener más información, consulte Uso del soporte extendido de Amazon RDS.	21 de marzo de 2024
Integración de RDS para Db2 con AWS License Manager	RDS para Db2 ahora está integrado con AWS License Manager. Si utiliza el modelo Traiga su propia licencia, la integración AWS License Manager le ayudará a monitorear el uso de licencias de Db2 dentro de su organización. Para obtener más información, consulte Integración con AWS License Manager.	20 de marzo de 2024

Rotación de certificados de CA para clústeres de bases de datos multi-AZ	Ahora puede rotar los certificados de CA de clústeres de bases de datos multi-AZ. Considere la posibilidad de utilizar uno de los nuevos certificados de CA rds-ca-rsa2048-g1, rds-ca-rsa4096-g1 o rds-ca-ecc384-g1. Para obtener más información, consulte Rotar certificados SSL/TLS.	6 de marzo de 2024
Amazon RDS admite el almacenamiento io2 Block Express	Ahora puede crear instancias de base de datos de RDS que utilicen el tipo de almacenamiento io2 Block Express. Para obtener más información, consulte io2 Block Express storage.	6 de marzo de 2024
RDS Custom para SQL Server admite las clases de instancia de base de datos db.r5b y db.x2iedn	Ahora puede utilizar las clases de instancia db.r5b y db.x2iedn para las instancias de base de datos de RDS Custom para SQL Server. Para obtener más información, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para SQL.	4 de marzo de 2024

RDS Custom para Oracle está disponible en la región de Oriente Medio (UAE)	Puede crear instancias de base de datos de RDS Custom para Oracle en la región de Oriente Medio (UAE). Para ver una tabla con todas las Regiones de AWS que se admiten, consulte Supported Regions and DB engines for RDS Custom for Oracle.	4 de marzo de 2024
Nueva política administrada de AWS	Amazon RDS agregó una nueva política administrada denominada `AmazonRDSCustomInstanceProfileRolePolicy` para permitir a RDS Custom realizar acciones de automatización y tareas de administración de bases de datos a través de un perfil de instancia de EC2. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	27 de febrero de 2024
Amazon RDS es compatible con MariaDB 10.11.7, 10.6.17, 10.5.24 y 10.4.33	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.11.7, 10.6.17, 10.5.24 y 10.4.33 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	26 de febrero de 2024

Los clústeres de base de datos de Amazon RDS Multi-AZ admiten el volumen de almacenamiento gp3 de Amazon EBS	Los clústeres de bases de datos multi-AZ admiten ahora volúmenes EBS basados en SSD (gp3). Para obtener más información, consulte Almacenamiento gp3.	26 de febrero de 2024
Compatibilidad con Amazon RDS para AWS Secrets Manager en la región Israel (Tel Aviv)	Amazon RDS es compatible con Secrets Manager en la región Israel (Tel Aviv). Para obtener más información, consulte Password management with Amazon RDS and AWS Secrets Manager (Administración de contraseñas con Amazon RDS y AWS Secrets Manager).	21 de febrero de 2024
Amazon RDS para Db2 admite el registro de auditorías	RDS para Db2 ahora admite el registro de auditorías en el nivel de base de datos. Al habilitar el registro de auditoría para una base de datos de RDS para Db2, Amazon RDS registra la actividad de la base de datos y almacena los registros de auditoría en Amazon S3. Para obtener más información, consulte Db2 audit logging.	15 de febrero de 2024

Soporte extendido de Amazon RDS	Amazon RDS ya habilita el Soporte extendido de Amazon RDS de manera automática cuando las versiones principales de los motores de RDS para MySQL y RDS para PostgreSQL en sus instancias de base de datos y clústeres de base de datos multi-AZ llegan a la fecha de finalización del soporte estándar de RDS. Para obtener más información, consulte Uso del soporte extendido de Amazon RDS.	15 de febrero de 2024
Amazon RDS es compatible con MySQL 8.0.36	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.36 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	12 de febrero de 2024
Amazon RDS admite la intercalación EBCDIC en RDS para Db2	Ahora puede crear bases de datos Db2 que utilicen secuencias de intercalación EBCDIC para ordenar el contenido en las bases de datos. Para obtener más información, consulte Intercalación EBCDIC para bases de datos Db2 en Amazon RDS.	29 de enero de 2024

Actualización al certificado de CA predeterminado	El certificado de CA predeterminado está establecido en `rds-ca-rsa2048-g1` . A fin de obtener más información, consulte Uso de SSL/TLS para cifrar una conexión a una instancia de base de datos.	26 de enero de 2024
Amazon RDS para PostgreSQL admite dos cajas nuevas para PL/Rust, croaring-rs y num-bigint	Puede utilizar dos cajas nuevas en Amazon RDS para PostgreSQL. Para obtener más información, consulte Uso de cajas con PL/Rust.	24 de enero de 2024
Amazon RDS para PostgreSQL admite la versión 1.3 de TLS	Puede utilizar la versión 1.3 de seguridad de la capa de transporte (TLS) en RDS para PostgreSQL. Para obtener más información, consulte Uso de SSL con una instancia de base de datos de PostgreSQL.	24 de enero de 2024
RDS Custom para SQL Server admite Microsoft SQL Server 2022	Ahora puede crear instancias de base de datos de RDS Custom para SQL Server que utilicen SQL Server 2022. Para obtener más información, consulte Trabajar con RDS Custom para SQL Server.	22 de enero de 2024

Actualización de los permisos de políticas administradas por AWS	La `AmazonRDSServiceRolePolicy` del rol vinculado al servicio `AWSServiceRoleForRDS` tiene nuevos identificadores de instrucciones. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	19 de enero de 2024
RDS Custom para Oracle es compatible con la región Europa (París)	Puede crear instancias de base de datos de RDS Custom para Oracle en la región Europa (París). Para obtener más información, consulte Supported Regions and DB engines for RDS Custom for Oracle.	18 de enero de 2024
Amazon RDS para MySQL admite la replicación de varios orígenes	Ahora puede utilizar la replicación de varios orígenes en instancias de base de datos de RDS para MySQL. Para obtener más información, consulte Configuración de la replicación de varios orígenes de RDS para MySQL.	16 de enero de 2024

Amazon RDS es compatible con MySQL 8.2 en el entorno de vista previa de base de datos	MySQL 8.2 ya está disponible en el entorno de vista previa de bases de datos en la Región de AWS Este de EE. UU. (Ohio). Para obtener más información, consulte MySQL version 8.2 in the Database Preview environment.	11 de enero de 2024
RDS Proxy está disponible en la región de Europa (España)	RDS Proxy ya está disponible en la región de Europa (España). Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	8 de enero de 2024
Amazon RDS está disponible en la región de Oeste de Canadá (Calgary)	Amazon RDS ya está disponible en la región de Oeste de Canadá (Calgary). Para obtener más información, consulte Regiones y zonas de disponibilidad.	20 de diciembre de 2023
Amazon RDS para Db2 admite 5000 usuarios locales	Ahora puede añadir hasta 5000 usuarios locales a una lista de autorización. Para obtener más información, consulte rdsadmin.add_user.	20 de diciembre de 2023

Amazon RDS es compatible con la visualización y respuesta a las recomendaciones	Las recomendaciones de Amazon RDS ahora incluyen recomendaciones proactivas basadas en umbrales y reactivas basadas en el machine learning para RDS para PostgreSQL. Para obtener más información, consulte Visualización y respuesta a las recomendaciones de Amazon RDS.	19 de diciembre de 2023
Amazon RDS admite las versiones 10.11.6, 10.6.16, 10.5.23 y 10.4.32 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.11.6, 10.6.16, 10.5.23 y 10.4.32 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	12 de diciembre de 2023
Amazon RDS presenta integraciones sin ETL con Amazon Redshift (vista previa)	Las integraciones sin ETL proporcionan una solución totalmente administrada que permite que los datos transaccionales estén disponibles en Amazon Redshift en cuestión de segundos después de escribirlos en una instancia de base de datos de RDS para MySQL. Para obtener más información, consulte Working with Amazon RDS zero-ETL integrations with Amazon Redshift (preview).	28 de noviembre de 2023

Amazon RDS admite motores de bases de datos IBM Db2	Ahora puede ejecutar motores de bases de datos IBM Db2 en Amazon RDS. Para obtener más información, consulte Amazon RDS para Db2.	27 de noviembre de 2023
RDS para PostgreSQL admite actualizaciones de versiones principales a PostgreSQL 16.1 y actualizaciones de versiones secundarias a 15.5, 14.10, 13.13, 12.17 y 11.22	Con RDS para PostgreSQL, ahora puede actualizar el motor de base de datos a la versión principal 16.1 y a las versiones secundarias 15.5, 14.10, 13.13, 12.17 y 11.22. Para obtener más información, consulte Actualización del motor de base de datos de PostgreSQL para Amazon RDS.	17 de noviembre de 2023
RDS Custom para Oracle admite grupos de opciones	Puede crear o modificar un grupo de opciones y asociarlo a una instancia de base de datos de RDS Custom para Oracle. Ya se admite la opción `Timezone`. Para obtener más información, consulte Working with option groups in RDS Custom for Oracle.	17 de noviembre de 2023

Amazon RDS para MySQL admite el complemento Group Replication	Ahora puede configurar un clúster activo-activo con instancias de base de datos de RDS para MySQL versión 8.0.35 o posteriores mediante el complemento Group Replication que desarrolla y mantiene la comunidad de MySQL. Para obtener más información, consulte Configuración de clústeres activo-activo para RDS para MySQL.	17 de noviembre de 2023
Amazon RDS Proxy admite RDS Proxy con RDS para PostgreSQL 16.1	Ahora puede crear proxy mediante RDS Proxy para instancias de base de datos RDS para PostgreSQL 16.1. Para obtener más información, consulte Uso de Amazon RDS Proxy.	17 de noviembre de 2023
RDS Custom para SQL Server admite Microsoft SQL Server 2019 Developer Edition	Ahora puede crear instancias de base de datos de RDS Custom para SQL Server que utilicen SQL Server 2019 Developer Edition. Para obtener más información, consulte el tema Bring Your Own Media con RDS Custom para SQL Server.	16 de noviembre de 2023

Actualizaciones de versiones secundarias de clústeres de base de datos multi-AZ con un tiempo de inactividad mínimo	Cuando realiza la actualización de una versión secundaria de un clúster de base de datos multi-AZ, Amazon RDS ahora actualiza las instancias de base de datos del lector antes que la instancia de base de datos del escritor, lo que reduce considerablemente el tiempo de inactividad. Puede reducir aún más el tiempo de inactividad a un segundo o menos mediante RDS Proxy. Para obtener más información, consulte Actualización de la versión del motor de un clúster de base de datos Multi-AZ.	16 de noviembre de 2023
RDS para SQL Server admite Microsoft SQL Server 2022	Ahora puede crear instancias de base de datos de RDS que utilicen SQL Server 2022. Para obtener más información, consulte Versiones de Microsoft SQL Server en Amazon RDS.	15 de noviembre de 2023

RDS para MySQL permite actualizar instantáneas de la versión 5.7 a la versión 8.0	Ahora puede actualizar la versión del motor de una instantánea de RDS para MySQL de la versión 5.7 a la versión 8.0. Puede hacerlo mediante la AWS Managemen t Console o la operación `ModifyDBSnapshot` de la API de RDS o AWS CLI. Para obtener más información, consulte Upgrading a MySQL DB snapshot engine version.	15 de noviembre de 2023
RDS Custom para SQL Server admite la recuperación a un momento dado de 1000 bases de datos	Ahora puede hacer que hasta 1000 bases de datos sean aptas para una copia de seguridad completa y una recuperación a un momento dado en su instancia de base de datos de RDS Custom para SQL Server. Para obtener más información, consulte Restoring an RDS Custom for SQL Server instance to a point in time.	15 de noviembre de 2023

RDS Custom para SQL Server admite el uso de una clave maestra de servicio	RDS Custom para SQL Server admite ahora el uso de una clave maestra de servicio (SMK). Una SMK permite cifrar objetos, como las credenciales, y utilizar características de SQL Server, como el TDE y el cifrado de columnas. Para obtener más información, consulte Using a Service Master Key with RDS Custom for SQL Server.	13 de noviembre de 2023
Amazon RDS es compatible con MySQL 8.1 en el entorno de vista previa de base de datos	MySQL 8.1 ya está disponibl e en el entorno de vista previa de base de datos en la Región de AWS del este de EE. UU. (Ohio). Para obtener más información, consulte MySQL version 8.1 in the Database Preview environment.	10 de noviembre de 2023
RDS es compatible con MySQL 8.0.35 y MySQL 5.7.44	Ahora puede crear instancia s de base de datos de Amazon RDS que ejecuten las versiones 8.0.35 y 5.7.44. de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	9 de noviembre de 2023
RDS Proxy es compatible con los clústeres de base de datos Multi-AZ	RDS Proxy ya es compatible con los clústeres de base de datos Multi-AZ Para obtener más información, consulte Trabajo con puntos de enlace del proxy de Amazon RDS.	9 de noviembre de 2023

RDS Custom para Oracle está disponible en las AWS GovCloud (US) Regions	Amazon RDS ya está disponible en las AWS GovCloud (US) Regions. Para obtener más información, consulte Supported Regions and DB engines for RDS Custom for Oracle.	9 de noviembre de 2023
Escrituras optimizadas para Amazon RDS es compatible con la clase de instancia de base de datos db.r5	Escrituras optimizadas para Amazon RDS ya es compatible con la clase de instancia de base de datos db.r5. Para obtener más información, consulte Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB y Mejora del rendimiento de escritura con escrituras optimizadas para Amazon RDS para MySQL.	9 de noviembre de 2023

Amazon RDS para Oracle es compatible con la configuración de varios inquilinos de la arquitectura CDB	Con la característica de varios inquilinos de RDS para Oracle, RDS ofrece una experiencia y arquitectura Oracle multitenencia y totalmente administrada para las bases de datos de Oracle. Puede utilizar las API de RDS para crear varios PDB, denominados bases de datos de inquilinos, en una CDB. RDS ofrece la configuración de varios inquilinos de la arquitectura CDB como alternativa a la configuración antigua de un solo inquilino. Para obtener más información, consulte Multi-tenant configuration of the CDB architecture.	8 de noviembre de 2023
Amazon RDS publica métricas de Performance Insights en Amazon CloudWatch	Performance Insights le permite exportar los paneles de métricas preconfiguradas o personalizadas en Amazon CloudWatch. Los paneles de métricas exportadas se pueden ver en la consola de CloudWatch. También puede exportar un widget seleccionado de métricas de Performance Insights y ver los datos de las métricas en la consola de CloudWatch. Para obtener más información, consulte Exporting Performance Insights metrics to CloudWatch.	8 de noviembre de 2023

Amazon RDS Custom para Oracle le permite actualizar el sistema operativo de una instancia de base de datos	Ahora puede actualizar la base de datos o el sistema operativo (SO) de una instancia de base de datos de RDS Custom para Oracle mediante el comando `modify-db-instance` de la CLI. Para obtener más información, consulte Actualización de una instancia de base de datos para Amazon RDS Custom for Oracle.	7 de noviembre de 2023
RDS Proxy es compatible con el protocolo extendido de RDS para PostgreSQL	Ahora puede ejecutar protocolos de consulta ampliados en una instancia de base de datos de RDS para PostgreSQL. Para obtener más información, consulte Uso de Amazon RDS Proxy.	6 de noviembre de 2023
Soporte de RDS para PostgreSQL para las implementaciones azul/verde de RDS	Ahora puede crear una implementación azul/verde a partir de una instancia de base de datos de RDS para PostgreSQL. Para obtener más información, consulte Using Amazon RDS Blue/Green Deployments for database updates (Uso de implementaciones azul/verde de Amazon RDS para las actualizaciones de bases de datos).	26 de octubre de 2023

Actualización a las políticas administradas de AWS	Las políticas administradas `AmazonRDSPerformanceInsightsReadOnly` y `AmazonRDSPerformanceInsightsFullAccess` incluyen ahora `Sid` (ID de instrucción) como identificador en las instrucciones de la política. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	23 de octubre de 2023
RDS Custom para Oracle es compatible con la región de Europa (Milán)	Para obtener más información, consulte Supported Regions and DB engines for RDS Custom for Oracle.	23 de octubre de 2023

Habilitar las escrituras optimizadas de RDS en bases de datos existentes	Ahora puede habilitar las escrituras optimizadas de RDS en una instancia de base de datos existente, aunque se haya creado con una versión de motor, una clase de instancia de base de datos o una configuración de sistema de archivos que no sea compatible con esta caracterí stica. Para obtener más información, consulte Habilitar las escrituras optimizadas para RDS en una base de datos existente para RDS para MySQL y Habilitar las escrituras optimizadas para RDS en una base de datos existente para RDS para MariaDB.	19 de octubre de 2023
Amazon RDS admite el uso de un volumen de registro dedicado (DLV).	Ahora puede usar un volumen de registro dedicado (DLV) con RDS para MariaDB, RDS para MySQL y RDS para PostgreSQL. Los DLV son ideales para bases de datos con gran capacidad de almacenamiento asignado, requisitos elevados de E/S por segundo (IOPS) o cargas de trabajo donde la latencia es muy importante. Para obtener más información, consulte Uso de un volumen de registro específico (DLV).	17 de octubre de 2023

Amazon RDS para PostgreSQL, MySQL y MariaDB admite nuevas clases de instancia de base de datos	Puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL, MySQL y MariaDB y que utilicen las clases de instancia de base de datos db.m6.in, db.m6idn, db.r6.in y db.r6.idn. Para obtener más información, consulte Motores de base de datos compatibles para todas las clases de instancia de base de datos disponibles.	12 de octubre de 2023
Amazon RDS para PostgreSQL admite pgactive	La extensión pgactive está disponible en Amazon RDS para PostgreSQL. Para obtener más información, consulte Uso de extensiones PostgreSQL con Amazon RDS para PostgreSQL.	9 de octubre de 2023
RDS Custom para Oracle está disponible en la región Asia-Pacífico (Yakarta)	Puede crear instancias de base de datos de RDS Custom para Oracle en la región Asia-Pacífico (Yakarta). Para obtener más información, consulte Supported Regions and DB engines for RDS Custom for Oracle.	5 de octubre de 2023

RDS Custom para SQL Server admite nuevas intercalaciones a nivel de servidor	RDS Custom para SQL Server ahora admite una amplia variedad de intercalaciones de servidores, tanto en codificación tradicional como en UTF-8, para las configuraciones regionales SQL_Latin, japonés, alemán y árabe. Para obtener más información, consulte Compatibilidad de intercalación y caracteres para instancias de base de datos de RDS Custom para SQL Server.	26 de septiembre de 2023
Actualización de los permisos de políticas administradas por AWS	El `AmazonRDSCustomServiceRolePolicy` del rol vinculado al servicio `AWSServiceRoleForRDSCustom` tiene nuevos permisos que permiten a RDS Custom crear, modificar y eliminar reglas administradas de EventBridge. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	20 de septiembre de 2023

Amazon RDS publica métricas de contador de Información sobre rendimiento en Amazon CloudWatch.	La función matemática de métricas DB_PERF_INSIGHTS de la consola de CloudWatch sirve para consultar Amazon RDS para conocer las métricas de los contadores de Información sobre rendimiento. Para obtener más información, consulte Creación de alarmas de CloudWatch para supervisar Amazon RDS.	20 de septiembre de 2023
Información sobre rendimiento admite estadísticas de resúmenes para SQL Server	Cuando utiliza Información sobre rendimiento, puede ver estadísticas de SQL tanto en el nivel de instrucción como en el de resumen de Amazon RDS para SQL Server. Para obtener más información, consulte Análisis de consultas en ejecución en SQL Server.	18 de septiembre de 2023

Amazon RDS para PostgreSQL, MySQL y MariaDB admiten los tipos de clase de instancia de base de datos db.m6.id y db.r6.id	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL, MySQL y MariaDB que utilicen tipos de clase de instancia de base de datos db.m6.id y db.r6.id. Estos tipos ofrecen almacenamiento SSD local basado en NVMe. Para obtener más información, consulte Motores de base de datos compatibles para todas las clases de instancia de base de datos disponibles.	11 de septiembre de 2023
Compatibilidad con actualizaciones de versiones principales para clústeres de bases de datos Multi-AZ de RDS para PostgreSQL	Ahora puede realizar actualizaciones de versiones principales de clústeres de bases de datos Multi-AZ de RDS para PostgreSQL. Para obtener más información, consulte Actualización de la versión del motor de un clúster de base de datos Multi-AZ.	7 de septiembre de 2023
Amazon RDS admite MariaDB 10.11.5, 10.6.15, 10.5.22 y 10.4.31	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.11.5, 10.6.15, 10.5.22 y 10.4.31. de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	7 de septiembre de 2023

Soporte extendido de Amazon RDS	Amazon RDS anuncia que próximamente podrá seguir ejecutando las versiones principales de los motores de RDS para MySQL y RDS para PostgreSQL en sus instancias de base de datos una vez pasada la fecha de finalización del soporte estándar de RDS. Para obtener más información, consulte Uso del soporte extendido de Amazon RDS.	1 de septiembre de 2023
RDS Custom admite el inicio y la detención de una instancia de base de datos de RDS Custom para SQL Server	RDS Custom ahora admite el inicio y la detención de una instancia de base de datos de RDS Custom para SQL Server. Para obtener más información, consulte Iniciar y detener una instancia de base de datos de RDS Custom para SQL Server.	31 de agosto de 2023
Escrituras optimizadas para Amazon RDS admite la clase de instancia de base de datos db.r5	Escrituras optimizadas para Amazon RDS ahora admite la clase de instancia de base de datos db.r5 DB. Para obtener más información, consulte Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB y Mejora del rendimiento de escritura con escrituras optimizadas para Amazon RDS para MySQL.	31 de agosto de 2023

Amazon RDS para Oracle admite la actualización automática de archivos de zona horaria para CDB	Con la opción `TIMEZONE_FILE_AUTOUPGRADE`, puede actualizar el archivo de zona horaria actual a la versión más reciente de su base de datos de contenedores (CDB) de RDS para Oracle. Para obtener más información, consulte Autoactualización automática del archivo de la zona horaria Oracle.	29 de agosto de 2023
Escrituras optimizadas para Amazon RDS admite las clases de instancia de base de datos db.m6g y db.m6i	Escrituras optimizadas para Amazon RDS ahora admite las clases de instancia de base de datos db.m6g y db.m6i. Para obtener más información, consulte Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB y Mejora del rendimiento de escritura con escrituras optimizadas para Amazon RDS para MySQL.	28 de agosto de 2023
Amazon RDS admite MariaDB 10.11	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 10.11 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	21 de agosto de 2023

Actualización de los permisos de políticas administradas por AWS	La `AmazonRDSCustomServiceRolePolicy` del rol vinculado al servicio `AWSServiceRoleForRDSCustom` tiene nuevos permisos que permiten a RDS Custom crear interfaces de red. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	18 de agosto de 2023
Actualización de los permisos de políticas administradas por AWS	La política administrada `AmazonRDSFullAccess` tiene nuevos permisos que le permiten generar, ver y eliminar el informe de análisis de rendimiento durante un período de tiempo. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	17 de agosto de 2023

Actualización de los permisos de políticas administradas por AWS	La adición de nuevos permisos a la política administrada `AmazonRDSPerformanceInsightsReadOnly` y la adición de una nueva política administrada `AmazonRDSPerformanceInsightsFullAccess` le permite generar un informe de análisis de carga de base de datos para un período de tiempo. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	16 de agosto de 2023
Amazon RDS admite el análisis del rendimiento durante un período de tiempo	La Información de rendimiento le permite crear y ver informes de análisis de rendimiento para un período de tiempo específico. El informe proporciona información identificada y las recomendaciones para resolver los problemas de rendimiento. Para obtener más información, consulte Análisis de la carga de la base de datos durante un período de tiempo.	16 de agosto de 2023

Amazon RDS Custom para Oracle admite las clases de instancia de base de datos db.r5b y db.x2iedn	Ahora puede utilizar las clases de instancia db.r5b y db.x2iedn para las instancias de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.	16 de agosto de 2023
Amazon RDS Custom para Oracle admite las clases de instancia de base de datos db.m6i, db.r6i y db.t3	Ahora puede utilizar las clases de instancia db.m6i, db.r6i y db.t3 para las instancias de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Compatibilidad de clases de instancias de base de datos con RDS Custom para Oracle.	15 de agosto de 2023
Amazon RDS para PostgreSQL ahora es compatible con la versión 16 Beta 3 de PostgreSQL en el entorno de vista previa de base de datos	La versión 16 Beta 3 de PostgreSQL ya está disponible en el entorno de vista previa de la base de datos en la Región de AWS de Este de EE. UU. (Ohio). Para obtener más información, consulte Working with the database preview environment (Uso del entorno de vista previa de base de datos).	11 de agosto de 2023

Amazon RDS admite las versiones 8.0.34 y 5.7.43 de MySQL	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 8.0.34 y 5.7.43. de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	9 de agosto de 2023
RDS para SQL Server admite la visualización de métricas del SO para la réplica en espera	Ahora puede ver las métricas del SO para la réplica en espera de RDS para SQL Server. Para obtener más información, consulte Visualización de métricas del SO en la consola de RDS.	3 de agosto de 2023
RDS para Oracle admite Oracle Data Guard para CBD	RDS para Oracle admite las réplicas de lectura de Data Guard para las bases de datos contenedores (CDB) de Oracle Database 19c y 21c. Puede crear, administrar y promover réplicas de lectura en una CDB, del mismo modo que en una que no sea CDB, mediante las API de RDS actuales. Para obtener más información acerca de las réplicas de lectura, consulte Réplicas de lectura multitenencia.	1 de agosto de 2023

Amazon RDS ya está disponible en la región de Israel (Tel Aviv)	Amazon RDS ya está disponible en la región de Israel (Tel Aviv). Para obtener más información, consulte Regiones y zonas de disponibilidad.	1 de agosto de 2023
Amazon RDS admite Oracle APEX versión 23.1.v1	Puede utilizar APEX 23.1.v1 con Oracle Database 19c y versiones posteriores. Para obtener más información, consulte Oracle Application Express.	26 de julio de 2023
Amazon RDS Custom para Oracle admite un SID de Oracle no predeterminado	Al crear una instancia de base de datos RDS Custom para Oracle mediante Oracle Database 19c, puede especificar un identificador de sistema Oracle (SID de Oracle) no predeterminado. Este valor también es el nombre del CDB. Para obtener más información, consulte Consideraciones sobre la arquitectura multiusuario.	21 de julio de 2023

RDS para SQL Server admite Active Directory autoadmin istrado	Ahora puede usar Active Directory autoadministrado para unir directamente sus instancias de base de datos de RDS para SQL Server a sus dominios de Microsoft Active Directory (AD). Los dominios de AD autoadmin istrados pueden estar en las instalaciones o en la nube. Para obtener más informaci ón, consulte Working with Self Managed Active Directory.	7 de julio de 2023
Compatibilidad de replicación lógica de PostgreSQL para clústeres de base de datos multi-AZ	Ahora puede utilizar la replicación lógica de PostgreSQL con su clúster de base de datos multi-AZ para replicar y sincronizar tablas individuales en lugar de toda la instancia de base de datos. Para obtener más información, consulte Using PostgreSQL logical replication with Multi-AZ DB clústers.	6 de julio de 2023

Amazon RDS para PostgreSQL ahora es compatible con la versión 16 Beta 2 de PostgreSQL en el entorno de vista previa de base de datos	La versión 16 Beta 2 de PostgreSQL ya está disponible en el entorno de vista previa de la base de datos en la Región de AWS de Este de EE. UU. (Ohio). Para obtener más información, consulte Working with the database preview environment (Uso del entorno de vista previa de base de datos).	6 de julio de 2023
Actualización de los permisos de políticas administradas por AWS	La `AmazonRDSCustomServiceRolePolicy` del rol vinculado al servicio `AWSServiceRoleForRDSCustom` tiene nuevos permisos que permiten a RDS Custom para Oracle utilizar instantáneas. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	23 de junio de 2023
RDS admite las versiones 10.6.14, 10.5.21 y 10.4.30 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.6.14, 10.5.21 y 10.4.30 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	22 de junio de 2023

RDS admite las versiones 8.0.33 y 5.7.42 de MySQL	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 8.0.33 y 5.7.42 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	15 de junio de 2023
RDS admite las versiones 10.6.13, 10.5.20, 10.4.29 y 10.3.39 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.6.13, 10.5.20, 10.4.29 y 10.3.39 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	15 de junio de 2023
RDS para Oracle admite espacios de tabla transportables	Puede migrar datos de una base de datos de Oracle en las instalaciones a una instancia de base de datos de RDS para Oracle mediante espacios de tabla transportables. Esta técnica no requiere licencias adicionales y es la técnica de migración con el menor tiempo de inactividad. Para obtener más información, consulte el tema sobre migración mediante espacios de tabla transportables de Oracle.	15 de junio de 2023

Amazon RDS admite RDS Proxy con RDS para MariaDB versión 10.6	Ahora ya puede crear una RDS Proxy con una base de datos de RDS para MariaDB versión 10.6. Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	15 de junio de 2023
RDS Custom para SQL Server admite Bring Your Own Media (BYOM)	Ahora puede crear una versión de motor personalizada (CEV) con sus propios medios de SQL Server. Para obtener más información, consulte el tema Bring Your Own Media con RDS Custom para SQL Server.	8 de junio de 2023
RDS para Oracle puede convertir una base de datos de Oracle 19c que no sea CDB en CDB	Si su instancia de base de datos ejecuta Oracle Database 19c con una RU de abril de 2021 o superior, puede convertir una base de datos que no sea CDB en una CDB (base de datos de contenedores). Después de convertir la arquitectura, puede actualizar su CDB de 19c a un CDB de 21c. Este paso es necesario porque no puede actualizar la base de datos ni convertir la arquitectura con un solo comando. Para obtener más información, consulte el tema sobre cómo convertir una base de datos que no es CDB de RDS para Oracle en una CDB.	31 de mayo de 2023

Los clústeres de bases de datos Multi-AZ están disponibles en las regiones de China	Los clústeres de base de datos Multi-AZ ya están disponibles en las Regiones de AWS de China (Pekín) y China (Ningxia). Para obtener más información, consulte Supported Regions and DB engines for Multi-AZ DB clústers in Amazon RDS.	30 de mayo de 2023
Las lecturas optimizadas para Amazon RDS admiten los clústeres de bases de datos Multi-AZ	Ahora, las lecturas optimizadas para Amazon RDS admiten los clústeres de bases de datos Multi-AZ. Para obtener más información, consulte Mejora del rendimiento de las consultas de RDS para MySQL con lecturas optimizadas de Amazon RDS y Mejora del rendimiento de las consultas de RDS para PostgreSQL con lecturas optimizadas para Amazon RDS.	30 de mayo de 2023
RDS Custom para Oracle admite la región Asia-Pacífico (Yakarta)	Para obtener más información, consulte Supported Regions and DB engines for RDS Custom for Oracle.	29 de mayo de 2023

Crear una réplica de lectura de instancia de base de datos con un clúster de base de datos multi-AZ de RDS para PostgreSQL de origen	Ahora puede crear una réplica de lectura de instancia de base de datos con un clúster de base de datos multi-AZ de RDS para PostgreSQL como origen. Anteriormente, solo se admitía RDS para MySQL. Para obtener más informaci ón, consulte Creating a DB instance read replica from a Multi-AZ DB clúster (Creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ).	24 de mayo de 2023
Amazon RDS ofrece una vista combinada de las métricas de Información de rendimiento y CloudWatch en el panel de Información de rendimiento	Amazon RDS ahora ofrece una vista consolidada de las métricas de Información de rendimiento y CloudWatch en el panel de Información de rendimiento. Para obtener más información, consulte Consulta de las métricas combinada s en la consola de Amazon RDS.	24 de mayo de 2023

Lecturas optimizadas para Amazon RDS disponibles en las regiones de China	Lecturas optimizadas para Amazon RDS ya está disponible en las Regiones de AWS China (Pekín) y China (Ningxia). Para obtener más información, consulte Mejora del rendimiento de las consultas de RDS para MariaDB con lecturas optimizadas para Amazon RDS y Mejora del rendimiento de las consultas de RDS para MySQL con lecturas optimizadas para Amazon RDS.	24 de abril de 2023
Soporte de Amazon RDS para AWS Secrets Manager en las regiones de China	Amazon RDS admite Secrets Manager en las regiones China (Pekín) y China (Ningxia) y China (Ningxia) y China (Ningxia). Para obtener más información, consulte Password management with Amazon RDS and AWS Secrets Manager (Administración de contraseñas con Amazon RDS y AWS Secrets Manager).	20 de abril de 2023

RDS Custom para Oracle admite la reutilización de ID de AMI para CEV nuevas	Al crear una versión de motor personalizada (CEV), RDS Custom para Oracle utiliza de forma predeterminada la Imagen de máquina de Amazon (AMI) más reciente disponible. Ahora puede especificar un ID de AMI que se usó en una CEV anterior. Para obtener más informaci ón, consulte Creación de una CEV.	19 de abril de 2023
Amazon RDS admite la publicación de eventos con etiquetas para los suscriptores de temas	Las notificaciones de eventos de Amazon RDS enviadas a Amazon Simple Notificat ion Service (Amazon SNS) o Amazon EventBridge contienen ahora etiquetas de eventos en el cuerpo del mensaje. Estas etiquetas proporcionan los datos del recurso afectado por el evento de servicio. Para obtener más información, consulte Amazon RDS event notification tags and attributes (Etiquetas y atributos de notificación de eventos de Amazon RDS).	17 de abril de 2023

Compre instancias reservadas para un clúster de base de datos multi-AZ	Ahora puede comprar instancias de base de datos reservadas para un clúster de base de datos multi-AZ. Para obtener más información, consulte Reserved DB instances for a Multi-AZ DB clúster (Instancias de base de datos reservadas para un clúster de base de datos multi-AZ).	12 de abril de 2023
Amazon RDS admite las clases de instancia db.m7g y db.r7g	Ahora puede utilizar las clases de instancia db.m7g y db.r7g para instancias de base de datos de RDS para MySQL, RDS para MariaDB y RDS para PostgreSQL. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	12 de abril de 2023
Actualización de los permisos de roles vinculados a servicios de Amazon RDS Custom	`AmazonRDSCustomServiceRolePolicy` ahora otorga permisos adicionales para permitir que RDS Custom para SQL Server utilice Amazon SQS y cree instantáneas. Para obtener más información, consulte Actualizaciones de Amazon RDS a las políticas administradas por AWS.	6 de abril de 2023

Migre a un clúster de base de datos multi-AZ de RDS para MySQL mediante una réplica de lectura	Ahora puede utilizar una réplica de lectura para migrar una implementación single-AZ o una implementación de instancia de base de datos multi-AZ de RDS para MySQL a una implementación de clúster de base de datos multi-AZ de RDS para MySQL con menos tiempo de inactividad. Para obtener más informaci ón, consulte Migrating to a Multi-AZ DB clúster using a read replica (Migración a un clúster de base de datos Multi-AZ mediante una réplica de lectura).	6 de abril de 2023
Cree una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ	Ahora puede crear una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ para escalar por encima de la capacidad de cálculo del clúster de origen. Para obtener más información, consulte Creating a DB instance read replica from a Multi-AZ DB clúster (Creación de una réplica de lectura de instancia de base de datos desde un clúster de base de datos multi-AZ).	6 de abril de 2023

Amazon RDS Custom para SQL Server admite multi-AZ	Puede crear una implement ación multi-AZ con RDS Custom para SQL Server. Para obtener más información, consulte Managing a Multi-AZ deployment for RDS Custom for SQL Server (Administ ración de una implementación multi-AZ para RDS Custom para SQL Server).	6 de abril de 2023
Actualización de los permisos de políticas administradas por AWS	Las políticas `AmazonRDS FullAccess` y `AmazonRDS ReadOnlyAccess` ahora otorgan permisos adicional es para permitir mostrar los resultados de Amazon DevOps Guru en la consola de RDS. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualiz aciones de Amazon RDS de las políticas administradas de AWS).	30 de marzo de 2023
Amazon RDS admite Oracle APEX versión 22.2.v1	Puede utilizar APEX 22.2.v1 con todas las versiones compatibles de Oracle Database. Para obtener más información, consulte Oracle Application Express.	30 de marzo de 2023

Amazon DevOps Guru está disponible para RDS para PostgreSQL	RDS para PostgreSQL le alerta sobre las anomalías recientes detectadas por Amazon DevOps Guru. La página de detalles de la base de datos de la consola le avisa sobre las anomalías actuales y las que se han producido en las últimas 24 horas. DevOps Guru publica información proactiva con recomenda ciones para ayudarlo a solucionar los problemas de sus bases de datos RDS para PostgreSQL antes de que se produzcan. Para obtener más información, consulte How DevOps Guru for RDS works (Cómo funciona DevOps Guru par RDS).	30 de marzo de 2023
RDS Custom admite el volumen de almacenamiento gp3 de Amazon EBS	RDS Custom para Oracle y RDS Custom para SQL Server admiten los volúmenes de EBS basados en SSD io1, gp2 y gp3. Para obtener más información, consulte Requisitos generales de RDS Custom para Oracle y Requisitos generales de RDS Custom para SQL Server.	29 de marzo de 2023

Actualización de los permisos de políticas administradas por AWS	Las políticas `AmazonRDSFullAccess` y `AmazonRDSReadOnlyAccess` ahora otorgan permisos adicionales a Amazon CloudWatch. Para obtener más información, consulte Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	16 de marzo de 2023
El proxy de RDS está disponible en las regiones de China	El proxy de RDS ya está disponible en las regiones China (Pekín) y China (Ningxia). Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	15 de marzo de 2023
El proxy de RDS está disponible en la región Asia-Pacífico (Yakarta)	El proxy de RDS ya está disponible en la región Asia-Pacífico (Yakarta). Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	8 de marzo de 2023

Escrituras optimizadas para Amazon RDS mejora el rendimiento de las transacciones de escritura de RDS para MariaDB	Puede mejorar el rendimiento de las transacciones de escritura para instancias de base de datos de RDS para MariaDB con Escrituras optimizadas para Amazon RDS. Para obtener más información, consulte Improving write performance with Amazon RDS Optimized Writes for MariaDB (Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MariaDB).	7 de marzo de 2023
Versiones 15.2 de Amazon RDS para PostgreSQL	Las nuevas características de Amazon RDS para PostgreSQL 15.2 incluyen el comando MERGE estándar de SQL para las consultas SQL condicionales, las mejoras de rendimiento en la ordenación en memoria y en disco y la compatibilidad con la confirmación en dos fases y el filtrado de filas/columnas para la replicación lógica.	27 de febrero de 2023
RDS Custom para Oracle está disponible en las regiones de Canadá (centro) y América del Sur (São Paulo)	Para ver una tabla con todas las Regiones de AWS que se admiten, consulte Supported Regions and DB engines for RDS Custom for Oracle.	22 de febrero de 2023

Amazon RDS admite copias de seguridad automáticas entre regiones para RDS para MariaDB y RDS para MySQL	Ahora puede replicar instantán eas de base de datos y registros de transacciones entre Regiones de AWS para instancias de base de datos de RDS para MariaDB y RDS para MySQL. Para obtener más información, consulte Replicación de copias de seguridad automáticas en otra .	22 de febrero de 2023
Amazon RDS para Oracle admite la notificación anticipad a de actualizaciones de versiones secundarias automáticas	RDS le notifica con antelació n la fecha en que estará disponible una nueva versión secundaria del motor de RDS para Oracle. RDS comienza a programar actualizaciones automáticas de versiones secundarias de sus instancia s de base de datos de RDS para Oracle en la fecha en que están disponibles. Para obtener más información, consulte Before an automatic minor version upgrade is scheduled (Antes de programar una actualización automática de una versión secundaria).	21 de febrero de 2023

Amazon RDS para SQL Server admite flujos de actividad de base de datos	Ahora puede supervisar una instancia de base de datos de SQL Server mediante flujos de actividad de base de datos. Una instancia de base de datos de SQL Server tiene la auditoría del servidor que administra Amazon RDS. Puede definir políticas para registrar los eventos del servidor en la especificación de auditoría del servidor. Puede crear una especific ación de auditoría de base de datos y definir políticas para registrar eventos de la base de datos. La secuencia de actividades se recopila y se transmite a Amazon Kinesis. Desde Kinesis, puede supervisar el flujo de actividad para un análisis posterior. Para obtener más información, consulte la sección Supervisi ón de Amazon RDS para Oracle mediante los flujos de actividad de la base de datos.	15 de febrero de 2023
RDS admite MySQL 8.0.32 y 5.7.41	Ahora puede crear instancia s de base de datos de Amazon RDS que ejecuten las versiones 8.0.32 y 5.7.41 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	7 de febrero de 2023

Amazon RDS para Oracle es compatible con nuevos conjuntos de cifrado para SSL	Si ejecuta Oracle Database 19c o 21c, puede especificar seis conjuntos de cifrado nuevos en la opción SSL de RDS para Oracle. Estos conjuntos son compatibles con FIPS y cumplen la norma FedRAMP. Para obtener más información, consulte Capa de conexión segura de Oracle.	3 de febrero de 2023
Amazon RDS para Oracle es compatible con nuevos conjuntos de cifrado para Oracle Enterprise Manager	Puede utilizar cuatro nuevos conjuntos de cifrado que cumplan la norma FedRAMP para la opción OEM. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.	3 de febrero de 2023
RDS para Oracle es compatible con flujos de actividad de base de datos en las regiones de Asia Pacífico (Hyderabad), Europa (España) y Oriente Medio (UAE).	Para obtener más información, consulte Supported Regions and DB engines for database activity streams in Amazon RDS.	27 de enero de 2023

Migrar a un clúster de base de datos Multi-AZ de RDS para PostgreSQL mediante una réplica de lectura	Mediante una réplica de lectura, puede migrar una implementación Single-AZ o una implementación de instancia de base de datos Multi-AZ de RDS para PostgreSQL a una implement ación de clúster de base de datos Multi-AZ de RDS para PostgreSQL con menos tiempo de inactividad. Para obtener más información, consulte Migrating to a Multi-AZ DB clúster using a read replica (Migración a un clúster de base de datos Multi-AZ mediante una réplica de lectura).	23 de enero de 2023
Amazon RDS está disponible en la región de Asia-Pacífico (Melbourne)	Amazon RDS está disponibl e ahora en la región de Asia-Pacífico (Melbourne). Para obtener más información, consulte Regiones y zonas de disponibilidad.	23 de enero de 2023

RDS para MariaDB admite la aplicación de conexiones SSL/TLS	RDS para MariaDB ahora admite la aplicación de conexiones SSL/TLS mediante la configuración del parámetro `require_secure_transport` en `ON`. Para obtener más información, consulte Requiring SSL/TLS for all connections to a MariaDB DB instance (Requerir SSL/TLS para todas las conexiones a una instancia de base de datos de MariaDB).	19 de enero de 2023
Las lecturas optimizadas de Amazon RDS mejoran el rendimiento de las consultas de RDS para MariaDB	Puede lograr un procesamiento de consultas más rápido para las instancias de base de datos de RDS para MariaDB con las lecturas optimizadas de Amazon RDS. Para obtener más información, consulte Improving query performance for RDS para MariaDB with Amazon RDS Optimized Reads (Mejorar el rendimiento de consulta para RDS para MariaDB con las lecturas optimizadas de Amazon RDS).	11 de enero de 2023

Restaurar una instantánea de clúster de base de datos Multi-AZ en una instancia de base de datos	Ahora puede restaurar una instantánea de clúster de base de datos Multi-AZ a una implementación Single-AZ o a una implementación de instancia de base de datos Multi-AZ. Para obtener más información, consulte Restoring from a Multi-AZ DB clúster snapshot to a DB instance (Restauración desde una instantánea de clúster de base de datos Multi-AZ a una instancia de base de datos).	10 de enero de 2023
Especificar la entidad de certificación (CA) durante la creación de la instancia de base de datos	Ahora puede especificar qué CA usar para el certificado de servidor de una instancia de base de datos al crear la instancia de base de datos. Para obtener más información, consulte Certificate authorities (Entidades de certificación).	5 de enero de 2023

RDS Custom para SQL Server admite versiones de motor personalizadas	Una versión de motor personalizada (CEV) de RDS Custom para SQL Server es una Imagen de máquina de Amazon (AMI) con Microsoft SQL Server preinstalado. Elija una AMI de Amazon EC2 para Windows para usarla como imagen base. Además, puede instalar otro software en el sistema operativo (SO). Puede personalizar la configuración del sistema operativo y de SQL Server para satisfacer las necesidades de su empresa. Para obtener más informaci ón, consulte Working with custom engine versions for RDS Custom for SQL Server (Trabajar con versiones de motor personalizadas para RDS Custom para SQL Server).	28 de diciembre de 2022
Uso de las implementaciones azul/verde de Amazon RDS, disponibles en Regiones de AWS adicionales	La función de implement aciones azul/verde ya está disponible en las regiones de China (Pekín) y China (Ningxia). Para obtener más información, consulte Using Amazon RDS Blue/Green Deployments for database updates (Uso de implement aciones azul/verde de Amazon RDS para las actualizaciones de bases de datos).	22 de diciembre de 2022

Actualización de permisos de roles vinculados a servicios de IAM	La política AmazonRDS ServiceRolePolicy ahora otorga permisos adicional es a AWS Secrets Manager. Para obtener más informaci ón, consulta Amazon RDS updates to AWS managed policies (Actualizaciones de Amazon RDS de las políticas administradas de AWS).	22 de diciembre de 2022
Amazon RDS admite el cambio de nombre de un clúster de base de datos Multi-AZ	Ahora puede cambiar el nombre de un clúster de base de datos Multi-AZ. Para obtener más información, consulte Renaming a Multi-AZ DB clúster (Cambiar el nombre de un clúster de base de datos Multi-AZ).	22 de diciembre de 2022
Amazon RDS se integra con AWS Secrets Manager para la administración de contraseñas	Amazon RDS puede administr ar la contraseña de usuario maestro de una instancia de base de datos o de un clúster de base de datos Multi-AZ en Secrets Manager. Para obtener más informaci ón, consulte Password management with Amazon RDS and AWS Secrets Manager (Administración de contraseñas con Amazon RDS y AWS Secrets Manager).	22 de diciembre de 2022

Amazon RDS Optimized Writes admite las clases de instancia de base de datos db.r6g y db.r6gd	Amazon RDS Optimized Writes ya admite las clases de instancia de base de datos db.r6g y db.r6gd. Para obtener más información, consulte Improving write performance with Amazon RDS Optimized Writes (Mejorar el rendimiento de escritura con Amazon RDS Optimized Writes).	22 de diciembre de 2022
Amazon RDS Custom para Oracle admite la nueva Regiones de AWS	Puede crear instancias de base de datos de RDS Custom para Oracle en las regiones Asia Pacífico (Seúl) y Asia Pacífico (Osaka). Para obtener más información, consulte Supported Regions and DB engines for RDS Custom for Oracle.	21 de diciembre de 2022
Amazon RDS en AWS Outposts compatible con réplicas de lectura	Ahora puede crear una réplica de lectura a partir de un RDS en una instancia de base de datos MySQL o PostgreSQL de Outposts. Para obtener más informaci ón, consulte Creating read replicas for Amazon RDS on AWS Outposts (Crear réplicas de lectura para Amazon RDS en AWS Outposts).	19 de diciembre de 2022

RDS Custom para Oracle admite la modificación de clases de instancias de base de datos	Ahora puede modificar la clase de instancia de su instancia de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Modifying your RDS Custom for Oracle DB instance (Modificar la instancia de base de datos de RDS Custom para Oracle).	16 de diciembre de 2022
RDS para MySQL y RDS para PostgreSQL admiten las clases de instancia de base de datos db.x2iedn	Ahora puede utilizar las clases de instancia de base de datos db.x2iedn para RDS para MySQL y RDS para PostgreSQL. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	14 de diciembre de 2022
Amazon RDS Optimized Writes admite las clases de instancia de base de datos db.x2iedn	Amazon RDS Optimized Writes ya admite las clases de instancia de base de datos db.x2iedn. Para obtener más información, consulte Improving write performance with Amazon RDS Optimized Writes (Mejorar el rendimiento de escritura con Amazon RDS Optimized Writes).	14 de diciembre de 2022

Amazon RDS permite copiar grupos de opciones de base de datos al copiar instantáneas de base de datos	Ahora puede copiar un grupo de opciones en Cuentas de AWS como parte de una solicitud de copia instantánea para bases de datos RDS para Oracle. Para obtener información, consulte Option group considerations (Consideraciones de grupo de opciones).	13 de diciembre de 2022
Amazon RDS admite RDS Proxy con RDS para PostgreSQL versión 14	Ahora ya puede crear una RDS Proxy con una base de datos de RDS para PostgreSQL versión 14. Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	13 de diciembre de 2022
Amazon RDS para Oracle admite las clases de instancias db.x2idn, db.x2iedn y db.x2iezn	Ahora puede utilizar las clases de instancia db.x2idn, db.x2iedn y db.x2iezn para las instancias de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Supported DB engines for DB instance classes (Motores de base de datos compatibles para clases de instancia de base de datos) y Supported RDS para Oracle instance classes (Clases de instancia de RDS para Oracle admitidas).	12 de diciembre de 2022

Las instancias de base de datos de RDS para PostgreSQL admiten extensiones de lenguaje de confianza para PostgreSQL	Las extensiones de lenguaje de confianza para PostgreSQL son un kit de desarrollo de código abierto que le permite crear extensiones de PostgreSQL de alto rendimiento y ejecutarlas de forma segura en su instancia de base de datos de RDS para PostgreSQL. Para obtener más información, consulte Working with Trusted Language Extensions for PostgreSQL (Trabajar con extensiones de lenguaje de confianza para PostgreSQL).	30 de noviembre de 2022
Uso de las implementaciones azul/verde de Amazon RDS para actualizar las bases de datos	Puede realizar cambios en una instancia de base de datos en un entorno transitorio y probar los cambios sin que ello afecte a la instancia de base de datos de producción. Cuando esté listo, puede promover el entorno transitorio para que sea el nuevo entorno de producción, con un tiempo de inactividad mínimo. Para obtener más información, consulte Using Amazon RDS Blue/Green Deployments for database updates (Uso de implementaciones azul/verde de Amazon RDS para las actualizaciones de bases de datos).	27 de noviembre de 2022

Amazon RDS Optimized Writes mejora el rendimiento de las transacciones de escritura de RDS para MySQL	Puede mejorar el rendimiento de las transacciones de escritura para instancias de base de datos de RDS para MySQL con Amazon RDS Optimized Writes. Para obtener más información, consulte Improving write performance with Amazon RDS Optimized Writes (Mejora del rendimiento de escritura con Escrituras optimizadas para Amazon RDS para MySQL).	27 de noviembre de 2022
Amazon RDS Optimized Reads mejora el rendimiento de las consultas de RDS para MySQL	Puede lograr un procesamiento de consultas más rápido para las instancias de base de datos de RDS para MySQL con Amazon RDS Optimized Reads. Para obtener más información, consulte Improving query performance with Amazon RDS Optimized Reads (Mejorar el rendimiento de consulta con Amazon RDS Optimized Reads).	27 de noviembre de 2022
Amazon RDS está disponible en la región de Asia-Pacífico (Hyderabad)	Amazon RDS ya está disponible en la región de Asia-Pacífico (Hyderabad). Para obtener más información, consulte Regiones y zonas de disponibilidad.	22 de noviembre de 2022

RDS admite las versiones 10.6.11, 10.5.18, 10.4.27 y 10.3.37 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.6.11, 10.5.18, 10.4.27 y 10.3.37 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	18 de noviembre de 2022
RDS Custom para Oracle admite la configuración de parámetros de instalación no predeterminados en una versión de motor personalizada (CEV)	Al crear una CEV, puede establecer valores no predeterminados para la base de Oracle, el inicio de Oracle, el nombre de usuario y el ID de UNIX, y el nombre e ID del grupo de UNIX. De este modo, tendrá más control sobre la instalación de base de datos en su instancia de base de datos de RDS Custom para Oracle. Para obtener más información, consulte Preparing the CEV manifest (Preparación del manifiesto CEV).	18 de noviembre de 2022
Amazon RDS admite Oracle APEX versión 22.1.v1	Puede utilizar APEX 22.1.v1 con todas las versiones compatibles de Oracle Database. Para obtener más información, consulte Oracle Application Express.	18 de noviembre de 2022

RDS para Oracle es compatible con réplicas de lectura entre regiones	Ahora puede crear una réplica de lectura entre regiones para mejorar la capacidad de recuperación de desastres, reducir la latencia de lectura de las aplicaciones y descargar las cargas de trabajo de lectura de la instancia de base de datos principal. Para obtener más información, consulte Creating a read replica in a different Región de AWS (Crear una réplica de lectura en una Región de AWS distinta).	16 de noviembre de 2022
Amazon RDS está disponible en la región de Europa (España)	Amazon RDS ya está disponible en la región de Europa (España). Para obtener más información, consulte Regiones y zonas de disponibilidad.	16 de noviembre de 2022
RDS para SQL Server admite servidores enlazados para la base de datos de Oracle	Ahora puede crear un servidor vinculado para acceder a bases de datos de Oracle externas para leer datos y ejecutar comandos SQL. Para obtener más información, consulte Linked Servers with Oracle OLEDB with RDS for SQL Server (Servidores vinculados con Oracle OLEDB con RDS para SQL Server).	15 de noviembre de 2022

RDS Custom para Oracle admite Oracle Multitenant	Puede crear una instancia de base de datos de RDS Custom para Oracle como base de datos de contenedores (CDB). Tras la creación, la CDB contiene la raíz de la CDB, la semilla de la PDB y una PDB. Puede añadir más PDB manualmente mediante Oracle SQL. Para obtener más información, consulte Overview of Amazon RDS Custom for Oracle architecture (Información general de la arquitectura de Amazon RDS Custom para Oracle).	15 de noviembre de 2022
Amazon RDS para Oracle admite la integración de Amazon EFS	Si agrega la opción `EFS_INTEGRATION` a su grupo de opciones, puede transferir archivos entre su instancia de base de datos de RDS para Oracle y un sistema de archivos Amazon EFS. Para obtener más información, consulte Amazon EFS.	15 de noviembre de 2022
RDS admite MySQL 8.0.31 y 5.7.40	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 8.0.31 y 5.7.40 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	10 de noviembre de 2022

Amazon RDS está disponible en la región de Europa (Zúrich)	Amazon RDS ya está disponible en la región de Europa (Zúrich). Para obtener más información, consulte Regiones y zonas de disponibilidad.	9 de noviembre de 2022
Acceso a las copias de seguridad del registro de transacciones ya disponible para RDS para SQL Server	Ahora puede ver y copiar las copias de seguridad del registro de transacciones de base de datos en un bucket de Amazon S3. Para obtener más información, consulte Access to transaction log backups (Acceso a las copias de seguridad del registro de transacciones).	7 de noviembre de 2022
Clústeres de bases de datos Multi-AZ compatibles con Regiones de AWS adicionales	Los clústeres de bases de datos Multi-AZ ya son compatibles con Regiones de AWS adicionales. Para obtener más información, consulte Supported Regions and DB engines for Multi-AZ DB clústers in Amazon RDS.	4 de noviembre de 2022

Amazon RDS admite el almacenamiento gp3	Ahora puede crear instancias de base de datos de Amazon RDS que utilicen volúmenes de almacenamiento SSD de uso general (gp3) de Amazon EBS, lo que le permite personalizar el rendimiento del almacenamiento independientemente de la capacidad de almacenamiento. Para obtener más información, consulte General Purpose SSD storage (Almacenamiento SSD de uso general).	4 de noviembre de 2022
Amazon RDS admite un nuevo evento de actualizaciones del sistema operativo	Amazon RDS ahora admite un nuevo evento de instancia de base de datos, RDS-EVENT-0230, en la categoría de eventos de parches de seguridad. Este nuevo evento le avisa cuando una actualización del sistema operativo está disponible para su instancia de base de datos. Para obtener más información, consulte Monitoring Amazon RDS events (Supervisión de eventos de Amazon RDS) y Working with operating system updates (Uso de actualizaciones del sistema operativo).	28 de octubre de 2022

Amazon RDS para Oracle admite clases de instancia optimizada para memoria r5b preconfiguradas	Las clases de instancia de base de datos de Oracle db.r5b están optimizadas para cargas de trabajo que requieren memoria, almacenamiento y E/S adicionales por vCPU. Por ejemplo, db.r5b.4xlarge.tpc2.mem2x tiene activado el subproceso múltiple y proporciona el doble de memoria que db.r5b.4xlarge. Para obtener más información, consulte los datos sobre las clases de instancias de RDS para Oracle.	27 de octubre de 2022
Amazon RDS admite 15 réplicas de lectura de RDS para instancias de base de datos de MariaDB, MySQL y PostgreSQL	Ahora puede crear hasta 15 réplicas de lectura de RDS para instancias de base de datos de MariaDB, MySQL y PostgreSQL. Para obtener más información, consulte Working with read replicas (Uso de réplicas de lectura).	20 de octubre de 2022

Amazon RDS para PostgreSQL ahora admite la versión 15 RC 3 de PostgreSQL en el entorno de vista previa de base de datos	La versión 15 Beta 3 de PostgreSQL ya está disponible en el entorno de vista previa de la base de datos en la Región de AWS de Este de EE. UU. (Ohio). Para obtener más información, consulte Working with the database preview environment (Uso del entorno de vista previa de base de datos).	18 de octubre de 2022
Amazon RDS admite la configuración automática de la conectividad entre una base de datos de RDS y una instancia EC2	Puede utilizar la AWS Management Console para configurar la conectividad entre una instancia de base de datos de RDS o un clúster de base de datos Multi-AZ existente y una instancia de EC2. Para obtener más información, consulte Connecting an EC2 instance and an RDS database automatically (Conectar una instancia EC2 y una base de datos RDS automáticamente).	14 de octubre de 2022

Controlador JDBC de AWS para PostgreSQL disponible de forma general	Controlador JDBC de AWS para MySQL es un controlador de cliente diseñado para RDS para PostgreSQL. El controlador JDBC de AWS para MySQL está ahora disponible de forma general. Para obtener más información, consulte Conexión con el controlador JDBC de AWS para PostgreSQL.	6 de octubre de 2022
Amazon RDS para Oracle da soporte Oracle APEX versión 21.2.v1	APEX 21.2 incluye el parche 33420059. Para obtener información, consulte Requisitos de la versión de APEX.	3 de octubre de 2022
RDS admite MySQL 5.7.39	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.39. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	29 de septiembre de 2022
RDS admite la versión 10.6.10 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 10.6.10 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	29 de septiembre de 2022

El proxy RDS es compatible con RDS para SQL Server	Ahora puede crear un RDS Proxy para una instancia de base de datos de RDS Server que ejecute la versión 2014 o superior de Microsoft Server. Para obtener más informaci ón sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	19 de septiembre de 2022
RDS admite las versiones 10.5.17, 10.4.26 y 10.3.36 de MariaDB	Ahora puede crear instancia s de base de datos de Amazon RDS que ejecuten las versiones 10.5.17, 10.4.26 y 10.3.36. de MariaDB. Para obtener más informaci ón, consulte MariaDB en versiones de Amazon RDS.	15 de septiembre de 2022

Amazon RDS para Oracle admite el almacenamiento de la instancia local para datos temporales	Ahora puede lanzar Amazon RDS para Oracle en los tipos de instancia db.r5d y db.m5d de Amazon EC2 con el espacio de tablas temporal y Database Smart Flash Cache (la caché flash) configurados para utilizar un almacén de instancias. Al almacenar los datos temporales de forma local, se pueden conseguir menores latencias de lectura y escritura en comparación con el almacenamiento estándar basado en Amazon EBS. Para obtener más información, consulte Almacenamiento de datos temporales de Oracle en el almacén de instancias.	14 de septiembre de 2022
Performance Insights muestra las 25 principales consultas SQL	En el panel de Performance Insights, la pestaña Top SQL (SQL principales) muestra las consultas SQL que más contribuyen a la carga de base de datos. Para obtener más información, consulte Información general sobre la pestaña Top SQL (SQL principales).	13 de septiembre de 2022

RDS es compatible con MySQL 8.0.30	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.30 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	9 de septiembre de 2022
Amazon RDS está disponible en la región de Oriente Medio (UAE)	Amazon RDS está disponible ahora en la región de Oriente Medio (UAE). Para obtener más información, consulte Regiones y zonas de disponibilidad.	30 de agosto de 2022
Amazon RDS para SQL Server admite suscripciones de correo electrónico de SSRS	Ahora puede usar la extensión de correo electrónico de SQL Server Reporting Services (SSRS) para enviar informes a los usuarios y suscribirse a los informes en el servidor de informes. Para obtener más información, consulte Compatibilidad con SQL Server Reporting Services en Amazon RDS para SQL Server.	26 de agosto de 2022

RDS para Oracle es compatible con copias de seguridad de réplicas de lectura	Puede activar las copias de seguridad automáticas y crear instantáneas manuales de réplicas de RDS para Oracle. Para obtener más información, consulte Working with RDS para Oracle replica backups (Trabajar con copias de seguridad de réplicas de RDS para Oracle).	23 de agosto de 2022
RDS para Oracle admite la conmutación de Oracle Data Guard	Una conmutación es una inversión de roles entre una base de datos principal y una réplica de Oracle montada o abierta. Durante una conmutación, la base de datos principal original pasa a un rol en espera, mientras que la base de datos en espera original pasa al rol principal. Para obtener más información, consulte Realización de una conmutación de Oracle Data Guard.	23 de agosto de 2022

Amazon RDS admite la configuración automática de la conectividad con una instancia EC2	Cuando cree una instancia de base de datos o un clúster de base de datos Multi-AZ, puede utilizar la AWS Management Console para configurar la conectividad entre una instancia de Amazon Elastic Compute Cloud y la nueva instancia de base de datos o clúster de base de datos. Para obtener más información, consulte Configurar la conectividad de red automática con una instancia de EC2 para una nueva instancia de base de datos y Configurar la conectividad de red automática con una instancia de EC2 para un clúster de base de datos nuevo.	22 de agosto de 2022

RDS Custom para Oracle admite la promoción de réplicas de Oracle	Si utiliza RDS Custom para Oracle, puede promocionar sus réplicas de Oracle administradas mediante el comando de CLI `promote-read-replica`. Además, puede eliminar la instancia de base de datos principal, lo que hace que RDS Custom para Oracle promueva sus réplicas de Oracle administradas a instancias independientes. Para obtener más información, consulte Trabajar con réplicas de Oracle para RDS Custom para Oracle.	5 de agosto de 2022
RDS para MySQL admite la aplicación de conexiones SSL/TLS	RDS para MySQL ahora admite la aplicación de conexiones SSL/TLS mediante la configuración del parámetro `require_secure_transport` para `ON`. Para obtener más información, consulte Requerir una conexión SSL/TLS a una instancia de base de datos MySQL.	1 de agosto de 2022

Amazon RDS dejará de ser compatible con Oracle Database 12c versión 1 (12.1.0.2)	La versión 12.1.0.2 ha dejado de ser compatible tanto para los modelos de licencia BYOL como para los modelos de licencia LI. El 1 de agosto de 2022, RDS para Oracle comenzó a realizar actualizaciones automáticas de las instancias de base de datos 12c versión 1 (12.1.0.2) y restauró las instantáneas 12.1.0.2 a Oracle Database 19c. Para obtener más información, consulte la cronología de fin del soporte en AWS re:Post.	1 de agosto de 2022
RDS Proxy admite RDS para MariaDB	Ahora puede crear un RDS Proxy para una instancia de base de datos de RDS que ejecute las versiones 10.2, 10.3, 10.4 o 10.5 de MariaDB. La compatibilidad con MariaDB se incluye en la familia de motores MySQL. Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	26 de julio de 2022

RDS para MariaDB admite las clases de instancia de base de datos db.r5b	Ahora puede crear instancias de base de datos de RDS para MariaDB que utilicen las clases de instancia de base de datos db.r5b. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	25 de julio de 2022
RDS para Oracle admite la modificación de secuencias de actividades de la base de datos	Si usa RDS para Oracle, puede cambiar el estado de la política de auditoría de una secuencia de actividades de base de datos a bloqueado (predeterminado) o desbloqueado. En lugar de detener una secuencia de actividades, puede desbloquear su estado de política, personalizar la política de auditoría y, a continuación, volver a bloquear el estado de la política. Para obtener más información, consulte Modificación de una secuencia de actividades de la base de datos.	22 de julio de 2022

Performance Insights admite la región Asia-Pacífico (Yakarta)	Anteriormente, no se podía usar Performance Insights en la región Asia-Pacífico (Yakarta). Esta restricción se ha eliminado. Para obtener más información, consulte Supported Regions and DB engines for Performance Insights in Amazon RDS.	21 de julio de 2022
Microsoft SQL Server 2012 ha llegado al final del soporte en Amazon RDS	Microsoft SQL Server 2012 ha llegado a su fin de soporte, que coincide con el plan de Microsoft para finalizar el soporte extendido para esta versión el 12 de julio de 2022. Todas las instancias existentes de Microsoft SQL Server 2012 se actualizarán automáticamente a la última versión secundaria de Microsoft SQL Server 2014 a partir del 1 de junio de 2022. Para obtener más información, consulte Compatibilidad de Microsoft SQL Server 2012 en Amazon RDS.	12 de julio de 2022

RDS admite MariaDB 10.6.8, 10.5.16, 10.4.25, 10.3.35 y 10.2.44	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.6.8, 10.5.16, 10.4.25, 10.3.35 y 10.2.44 de MariaDB. Para obtener más información, consulte Versiones de MariaDB compatibles en Amazon RDS.	8 de julio de 2022
RDS Performance Insights admite períodos de retención adicionales	Anteriormente, Performance Insights ofrecía solo dos períodos de retención: 7 días (predeterminado) o 2 años (731 días). Ahora, si necesita retener los datos de rendimiento durante más de 7 días, puede especificar entre 1 y 24 meses. Para obtener más información, consulte Precios y retención de datos para Performance Insights.	1 de julio de 2022
RDS Custom admite las regiones de Asia-Pacífico (Bombay) y Europa (Londres)	Puede crear instancias de base de datos de RDS Custom para Oracle y RDS Custom para SQL Server en dos nuevas:Regiones de AWS Asia-Pacífico (Bombay) y Europa (Londres). Para obtener más información, consulte Región de AWS compatibles con RDS Custom para Oracle y Región de AWS compatibles con RDS Custom para SQL Server.	21 de junio de 2022

RDS Custom para Oracle admite Oracle Database 18c y 12c versión 2 (12.2)	Ahora puede crear un CEV para RDS Custom para Oracle con archivos de instalación de Oracle Database 18c y 12c versión 2 (12.2). Puede utilizar estos CEV para crear una instancia de base de datos de RDS Custom para Oracle. Para obtener más informaci ón, consulte Trabajo con versiones de motor personali zadas para Amazon RDS Custom for Oracle.	21 de junio de 2022
Los clústeres de base de datos Multi-AZ admiten las clases de instancia de base de datos db.m5d y db.r5d	Ahora puede crear clústeres de base de datos Multi-AZ que utilicen las clases de instancia de base de datos db.m5d y db.r5d. Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ y Tipos de clase de instancia de base de datos.	21 de junio de 2022
Clústeres de bases de datos Multi-AZ disponibles en Regiones de AWS adicionales	Ahora puede crear clústeres de base de datos Multi-AZ en las siguientes regiones: Europa (Fráncfort) y Europa (Estocolmo). Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ.	21 de junio de 2022

RDS para Microsoft SQL Server admite la migración de bases de datos que utilizan el cifrado de datos transparente (TDE)	RDS para SQL Server ahora es compatible con la migración de bases de datos de Microsoft SQL Server con TDE activado, mediante la copia de seguridad y restauración nativas. Para obtener más información, consulte Compatibilidad con el cifrado de datos transparente en SQL Server.	14 de junio de 2022
Amazon RDS admite la publicación de eventos en temas cifrados de Amazon SNS	Amazon RDS ahora puede publicar eventos en los temas de Amazon Simple Notification Service (Amazon SNS) que tengan habilitado el cifrado del servidor (SSE), para ofrecer una protección adicional de los eventos que incluyen datos confidenciales. Para obtener más información, consulte Suscripción a notificaciones de eventos de Amazon RDS.	1 de junio de 2022
RDS admite MySQL 5.7.38	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.38. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	31 de mayo de 2022

RDS para PostgreSQL admite réplicas de lectura en cascada	Ahora puede utilizar réplicas de lectura en cascada con RDS para PostgreSQL versión 14.1 y versiones posteriores. Para obtener más informaci ón, consulte Uso de réplicas de lectura de PostgreSQL en Amazon RDS.	4 de mayo de 2022
Amazon RDS en AWS Outposts admite operaciones de almacenamiento a escala y escalado automático	Ahora puede cambiar los tamaños de almacenamiento de las instancias de base de datos en su Outpost y utilizar el escalado automático de almacenamiento. Para obtener más información, consulte Compatibilidad de Amazon RDS on AWS Outposts con las características de Amazon RDS.	2 de mayo de 2022
Clústeres de bases de datos Multi-AZ disponibles en Regiones de AWS adicionales	Ahora puede crear clústeres de bases de datos Multi-AZ en las siguientes regiones: Asia-Pacífico (Singapur) y Asia-Pacífico (Sídney)). Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ.	29 de abril de 2022

Amazon RDS admite el modo de pila doble	Las instancias de base de datos ahora se pueden ejecutar en modo de pila doble. En modo de pila doble, los recursos se pueden comunicar con la instancia de base de datos mediante IPv4, IPv6 o ambos. Para obtener más información, consulte Direccionamiento IP de instancias Amazon EC2.	29 de abril de 2022
Amazon RDS publica métricas de uso en Amazon CloudWatch	El espacio de nombres `AWS/Usage` en Amazon CloudWatch incluye métricas de uso de nivel de cuenta para sus cuotas de servicio de Amazon RDS. Para obtener más información, consulte Métricas de uso de Amazon CloudWatch para Amazon RDS.	28 de abril de 2022
Amazon RDS for MySQL admite las clases de instancia de base de datos db.m6i y db.r6i	Ahora puede usar las clases de instancia de base de datos db.m6i y db.r6i para las instancias de base de datos de Amazon RDS que ejecuten MySQL. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	28 de abril de 2022

Amazon RDS for PostgreSQL admite las clases de instancia de base de datos db.m6i y db.r6i	Ahora puede usar las clases de instancia de base de datos db.m6i y db.r6i para las instancias de base de datos de Amazon RDS que ejecuten PostgreSQL. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	27 de abril de 2022
Amazon RDS para MariaDB admite las clases de instancia de base de datos db.m6i y db.r6i	Ahora puede usar las clases de instancia de base de datos db.m6i y db.r6i para las instancias de base de datos de Amazon RDS que ejecuten MariaDB. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	26 de abril de 2022
Amazon RDS en AWS Outposts admite implementaciones Multi-AZ	Ahora puede crear una instancia de base de datos en espera en otro Outpost. Para obtener más información, consulte Compatibilidad de Amazon RDS on AWS Outposts con las características de Amazon RDS.	19 de abril de 2022

Amazon RDS para Oracle admite las clases de instancia de base de datos db.m6i y db.r6i	Si ejecuta Oracle Database 19c, puede utilizar las clases de instancia db.m6i y db.r6i. Las clases db.m6i son instancias de uso general adecuadas para un amplio rango de cargas de trabajo. Para obtener más información, consulte los datos sobre las clases de instancias de RDS para Oracle.	8 de abril de 2022
Amazon RDS for SQL Server admite la replicación de trabajos del Agente SQL Server	Al activar esta característica, los trabajos del Agente SQL Server creados, modificados o eliminados en el host principal se sincronizan automátic amente con el host secundario en una configuración Multi-AZ. Para obtener más información, consulte Uso del Agente SQL Server.	7 de abril de 2022
Amazon RDS admite RDS Proxy con RDS for PostgreSQ L versión 13	Ahora puede crear una RDS Proxy con una base de datos de RDS for PostgreSQL versión 13. Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	4 de abril de 2022

Amazon RDS tiene pensado dar de baja Oracle Database 12c	Oracle Database 12c va a dejar de usarse. Oracle Corporation ya no proporcionará parches para Oracle Database 12c después de las fechas de finalización del soporte. Amazon RDS planea comenzar a actualizar automáticamente las instancias de Oracle Database 12c a Oracle Database 19c.	22 de marzo de 2022
Notas de la versión de Amazon RDS para PostgreSQL	Ahora hay una guía aparte para las notas de la versión de Amazon RDS para PostgreSQL. Para obtener más información, consulte las notas de la versión de Amazon RDS para PostgreSQL.	22 de marzo de 2022
Notas de la versión de Amazon RDS para Oracle	Ahora hay una guía aparte para las notas de la versión de Amazon RDS para Oracle. Para obtener más información, consulte las notas de la versión de Amazon RDS para Oracle.	22 de marzo de 2022
Clústeres de bases de datos Multi-AZ disponibles en Regiones de AWS adicionales	Ahora puede crear clústeres de bases de datos Multi-AZ en las siguientes regiones: Este de EE. UU. (Ohio) y Asia-Pacífico (Tokio). Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ.	15 de marzo de 2022

Amazon RDS para PostgreSQL versiones 14.2, 13.6, 12.10, 11.15 y 10.20	RDS for PostgreSQL ahora es compatible con las versiones 14.2, 13.6, 12.10, 11.15 y 10.20. Las versiones 14.2 y 13.6 añaden compatibilidad con dos nuevos contenedores de datos externos. La extensión `mysql_fdw` permite a PostgreSQL trabajar con datos almacenados en bases de datos MySQL, MariaDB y Aurora MySQL. La extensión `tds_fdw` permite a PostgreSQL trabajar con los datos almacenados en las bases de datos de SQL Server. Para obtener más información, consulte Versiones de base de datos de PostgreSQL compatibles.	12 de marzo de 2022
RDS admite MySQL 5.7.37	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.37. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	11 de marzo de 2022

Amazon RDS for SQL Server admite nuevas clases de instancia de base de datos	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten Microsoft SQL Server y utilicen las clases de instancia de base de datos db.m6i y db.r6i. Para obtener más información, consulte Compatibilidad con las clases de instancias de bases de datos de Microsoft SQL Server.	9 de marzo de 2022
Amazon RDS para Oracle es compatible con Oracle Database 21c	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle Database 21c (21.0.0.0). Esta es la primera versión de Oracle Database que solo admite la arquitectura multitenant (CDB). Para más información, consulte Oracle Database 21c con Amazon RDS.	7 de marzo de 2022
RDS admite las versiones 10.6.7, 10.5.15, 10.4.24, 10.3.34 y 10.2.43 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.6.7, 10.5.15, 10.4.24, 10.3.34 y 10.2.43 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	3 de marzo de 2022

AWS JDBC Driver for MySQL disponible de forma general	AWS JDBC Driver for MySQL es un controlador de cliente diseñado para RDS for MySQL. AWS JDBC Driver for MySQL está ahora disponibl e de forma general. Para obtener más información, consulte Conexión con Amazon Web Services JDBC Driver for MySQL.	2 de marzo de 2022
Clústeres de base de datos Multi-AZ disponibles de forma general	La implementación de un clúster de bases de datos Multi-AZ es un modo de implementación de alta disponibilidad de Amazon RDS con dos instancias de base de datos en espera legibles. Los clústeres de base de datos Multi-AZ ahora están disponibles de forma general. Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ.	1 de marzo de 2022
RDS es compatible con MySQL 8.0.28	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.28 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	28 de febrero de 2022

Amazon RDS para Oracle es compatible con la nueva configuración de cifrado de red nativo (NNE)	Para controlar si los clientes pueden conectarse con métodos de cifrado y suma de comprobación no seguros, configure `SQLNET.ALLOW_WEAK_CRYPTO_CLIENTS` y `SQLNET.ALLOW_WEAK_CRYPTO` en la opción NNE. Algunos ejemplos de métodos inseguros incluyen DES, 3DES, RC4 y MD5. Para obtener más información, consulte Configuración de opciones NNE.	25 de febrero de 2022
Amazon RDS for SQL Server admite grupos de disponibilidad Always On para Microsoft SQL Server 2017 Standard Edition	Cuando se crea una instancia de base de datos mediante la configuración Multi-AZ en SQL Server 2017 Standard Edition 14.00.3401.7 y versiones superiores, RDS utiliza automáticamente grupos de disponibilidad. Para obtener más información, consulte Implementaciones Multi-AZ para Microsoft SQL Server.	18 de febrero de 2022
RDS para Oracle admite flujos de actividad de base de datos en la región Asia-Pacífico (Yakarta)	Para obtener más información, consulte Compatibilidad de los flujos de actividad de bases de datos con las Regiones de AWS.	16 de febrero de 2022

Amazon RDS Custom for Oracle compatible con Oracle Database 12.1	Ahora puede crear versiones de motor personalizadas para RDS Custom for Oracle que utilizan Oracle Database 12.1 Enterprise Edition. Para obtener más informaci ón, consulte Trabajo con versiones de motor personali zadas para Amazon RDS Custom for Oracle.	4 de febrero de 2022
Amazon RDS para MariaDB admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 10.6 de MariaDB. Para obtener más información, consulte Compatibilidad con MariaDB 10.6 en Amazon RDS.	3 de febrero de 2022

Información sobre rendimiento admite la captura de planes para las consultas de Oracle	La consola de Información sobre rendimiento admite una nueva dimensión de plan para SQL principal. Cuando se divide por planes, se puede ver qué planes se utilizan en las principales consultas de Oracle. Si una consulta utiliza varios planes, puede comparar los planes en la consola y determinar cuál es el más eficiente. También puede desglosar para ver qué pasos de un plan tienen el mayor costo. Para obtener más información, consulte Analyzing Oracle execution plans using the Performance Insights dashboard (Análisis de los planes de ejecución de Oracle mediante el panel de Información sobre rendimiento).	27 de enero de 2022

Información sobre rendimiento admite nuevas API	Información sobre rendimiento admite las siguientes API: `GetResourceMetadata`, `ListAvailableResourceDimensions` y `ListAvailableResourceMetrics`. Para obtener información, consulte Recuperación de métricas con la API de Información sobre rendimiento en este manual y la Referencia de la API de Información sobre rendimiento de Amazon RDS.	12 de enero de 2022
RDS Proxy admite eventos	RDS Proxy ahora genera eventos a los que puede suscribirse y ver en CloudWatch Events o configurar para enviarlos a Amazon EventBridge. Para obtener más información, consulte Trabajo con eventos de RDS Proxy.	11 de enero de 2022
Amazon RDS for SQL Server admite el modo multidimensional de SSAS	RDS for SQL Server admite la ejecución de SQL Server Analysis Services (SSAS) en modo tabular. Para obtener más información, consulte Compatibilidad con SQL Server Analysis Services en Amazon RDS for SQL Server.	7 de enero de 2022

RDS Proxy está disponible en más Regiones de AWS	RDS Proxy ya está disponible en las siguientes regiones: África (Ciudad del Cabo), Asia-Pacífico (Hong Kong), Asia-Pacífico (Osaka), Europa (Milán), Europa (París), Europa (Estocolmo), Medio Oriente (Baréin) y América del Sur (São Paulo). Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	5 de enero de 2022
RDS es compatible con MySQL 8.0.27	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.27 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	21 de diciembre de 2021
Amazon RDS está disponible en la región de Asia-Pacífico (Yakarta)	Amazon RDS ahora está disponible en la región Asia-Pacífico (Yakarta). Para obtener más información, consulte Regiones y zonas de disponibilidad.	13 de diciembre de 2021
Amazon RDS es compatible con MariaDB 10.5.13, 10.4.22, 10.3.32 y 10.2.41	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.5.13, 10.4.22, 10.3.32 y 10.2.41 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	8 de diciembre de 2021

Amazon RDS Custom for SQL Server	Amazon RDS Custom es un servicio de base de datos administrado para aplicaciones heredadas, personalizadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Con Amazon RDS Custom, obtiene la automatización de Amazon RDS y la flexibilidad de Amazon EC2. Para obtener más información, consulte Working with Amazon RDS Custom (Uso de Amazon RDS Custom).	1 de diciembre de 2021
Clústeres de base de datos Multi-AZ (versión preliminar)	Ahora puede crear clústeres de base de datos Multi-AZ para RDS for MySQL y RDS for PostgreSQL. La implementación de un clúster de bases de datos Multi-AZ es un modo de implementación de alta disponibilidad de Amazon RDS con dos instancias de base de datos en espera legibles. Los clústeres de base de datos Multi-AZ están en versión preliminar. Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ (versión preliminar).	23 de noviembre de 2021

Amazon RDS admite RDS Proxy con RDS for PostgreSQL versión 12	Ahora puede crear una RDS Proxy con una base de datos de RDS for PostgreSQL versión 12. Para obtener más información sobre RDS Proxy, consulte Uso de Amazon RDS Proxy.	22 de noviembre de 2021
Amazon RDS on AWS Outposts admite copias de seguridad locales	Puede almacenar copias de seguridad automatizadas e instantáneas manuales en su Región de AWS o de manera local en su Outpost. Para obtener más información, consulte Compatibilidad de Amazon RDS on AWS Outposts con las características de Amazon RDS.	22 de noviembre de 2021
Amazon RDS es compatible con el acceso entre cuentas AWS KMS keys	Para el cifrado, puede usar una clave KMS desde otra cuenta de AWS cuando exporte instantáneas de base de datos a Amazon S3. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3.	3 de noviembre de 2021

Amazon RDS on AWS Outposts admite la publicación de registros del motor de base de datos en CloudWatch Logs	RDS on Outposts ahora admite la publicación de registros del motor de base de datos en CloudWatch Logs. Para obtener más informaci ón, consulte Compatibilidad de Amazon RDS en AWS Outposts con las caracterí sticas de Amazon RDS.	2 de noviembre de 2021
Amazon RDS Custom for Oracle	Amazon RDS Custom es un servicio de base de datos administrado para aplicacio nes heredadas, personali zadas y empaquetadas que requieren acceso al sistema operativo y al entorno de base de datos subyacentes. Con Amazon RDS Custom, obtiene la automatización de Amazon RDS y la flexibilidad de Amazon EC2. Para obtener más información, consulte Working with Amazon RDS Custom (Uso de Amazon RDS Custom).	26 de octubre de 2021

Compatibilidad con la replicación retardada de la versión 8.0 de RDS for MySQL	A partir de la versión 8.0.26 de RDS for MySQL, se puede configurar la replicación retardada para instancias de base de datos de la versión 8.0 de RDS for MySQL. Para obtener más información, consulte Configuración de la replicación retrasada con MySQL.	25 de octubre de 2021
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 8.0.26 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	25 de octubre de 2021
Compatibilidad con la replicación basada en GTID de la versión 8.0 de RDS for MySQL	A partir de la versión 8.0.26 de RDS for MySQL, puede configurar la replicación basada en GTID para instancias de base de datos de la versión 8.0 de RDS for MySQL. Para obtener más información, consulte Uso de la replicación basada en GTID de RDS for MySQL.	25 de octubre de 2021
Amazon RDS admite RDS Proxy con RDS for MySQL 8.0	Ahora puede crear una RDS Proxy para una instancia de base de datos de RDS for MySQL 8.0. Para obtener más información, consulte Uso de Amazon RDS Proxy.	21 de octubre de 2021

Amazon RDS on AWS Outposts admite versiones adicionales de RDS for PostgreSQL	RDS on Outposts ahora admite las versiones 8.0.23 y 8.0.25 de RDS for PostgreSQL. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	20 de octubre de 2021
Amazon RDS para PostgreSQL ahora admite la versión 14 RC 1 de PostgreSQL en el entorno de vista previa de base de datos	La versión 14 RC 1 de PostgreSQL ya está disponible en el entorno de vista previa de la base de datos en la Región de AWS de Este de EE. UU. (Ohio). Para obtener más información, consulte Working with the database preview environment (Uso del entorno de vista previa de base de datos).	19 de octubre de 2021
Amazon RDS admite Información sobre rendimiento en Regiones de AWS adicionales	Información sobre rendimiento está disponible en las regiones de Medio Oriente (Baréin), África (Ciudad del Cabo), Europa (Milán) y Asia-Pacífico (Osaka). Para obtener más información, consulte Supported Regions and DB engines for Performance Insights in Amazon RDS.	5 de octubre de 2021

Información sobre rendimiento admite estadísticas de resúmenes para Oracle	Cuando utiliza Información sobre rendimiento, puede ver estadísticas de SQL tanto en el nivel de instrucción como en el de resumen de Amazon RDS para Oracle. Para obtener más información, consulte Análisis de consultas en ejecución en Oracle.	4 de octubre de 2021
Amazon RDS en AWS Outposts admite versiones adicionales de RDS for PostgreSQL	RDS en Outposts ahora admite las versiones 12.8 y 13.4 de RDS for PostgreSQL. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	1 de octubre de 2021
Amazon RDS admite Oracle APEX versión 21.1.v1	Puede utilizar APEX 21.1.v1 con todas las versiones compatibles de Oracle Database. Para obtener más información, consulte Oracle Application Express.	24 de septiembre de 2021

Amazon RDS para Oracle admite el cifrado del lado del cliente para NNE	Cuando configure NNE, es posible que desee evitar forzar el cifrado en el lado del servidor. Por ejemplo, es posible que no desee forzar todas las comunicaciones del cliente para que utilicen el cifrado porque el servidor lo requiere. En este caso, puede forzar el cifrado en el lado del cliente mediante las opciones de `SQLNET.*CLIENT`. Para obtener más informaci ón, consulte Oracle Native Network Encryption.	24 de septiembre de 2021
Amazon RDS for MySQL y RDS for PostgreSQL admiten las nuevas clases de instancia de base de datos	Ahora puede utilizar las clases de instancia db.r5b, db.t4g y db.x2g para crear instancias de base de datos de Amazon RDS que ejecuten MySQL o PostgreSQL. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	15 de septiembre de 2021

Amazon RDS for Microsoft SQL Server es compatible con Java Database Connectivity (JDBC) con el Coordinador de transacciones distribuidas de Microsoft (MSDTC)	Las transacciones XA de JDBC son compatibles con MSDTC para SQL Server 2017 versión 14.00.3223.3 y posteriores, así como con SQL Server 2019. Para obtener más información, consulte Compatibilidad con el Coordinador de transacciones distribuidas de Microsoft en RDS for SQL Server.	7 de septiembre de 2021
Amazon RDS admite las versiones 10.5.12, 10.4.21, 10.3.31 y 10.2.40 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.5.12, 10.4.21, 10.3.31 y 10.2.40 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	2 de septiembre de 2021
Amazon RDS ha finalizado el soporte para Oracle Database 18c	Solo se pueden crear instancias de base de datos para Oracle Database 12c y Oracle Database 19c. Si tiene instantáneas de Oracle Database 18c, actualícelas a una versión posterior. Para obtener más información, consulte Actualización de una instantánea de base de datos de Oracle.	17 de agosto de 2021

Amazon RDS for SQL Server admite las actualizaciones de versiones secundarias	Ahora puede hacer que sus instancias de base de datos de RDS para SQL Server se actualicen automáticamente a la versión secundaria más reciente. Para obtener más información, consulte Actualización del motor de base de datos Microsoft SQL Server.	13 de agosto de 2021
Amazon RDS for PostgreSQL ahora es compatible con PostgreSQL versión 14 Beta 2 en el entorno de vista previa de base de datos	Para obtener más información sobre PostgreSQL versión 14 Beta 1, consulte las notas de la versión de PostgreSQL 14 Beta 1. Para obtener más información sobre PostgreSQL versión 14 Beta 2, consulte las notas de la versión de PostgreSQL 14 Beta 2. Para obtener más información acerca del entorno de vista previa de base de datos, consulte Trabajo con el entorno de vista previa de base de datos.	9 de agosto de 2021

Amazon RDS admite RDS Proxy en una VPC compartida	A partir de ahora puede crear un proxy RDS en una VPC compartida. Para obtener más información acerca del proxy de RDS, consulte “Administración de conexiones con el proxy de Amazon RDS” en la Guía del usuario de Amazon RDS o en la Guía del usuario de Aurora.	6 de agosto de 2021
Amazon RDS admite la versión 10.2.39 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten la versión 10.2.39 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	4 de agosto de 2021
Amazon RDS para Oracle agrega la opción `TIMEZONE_FILE_AUTOUPGRADE`	Con esta opción, puede actualizar el archivo de zona horaria actual a la versión más reciente de su instancia de base de datos de Oracle. Para obtener más información, consulte Autoactualización automática del archivo de la zona horaria Oracle.	30 de julio de 2021
Amazon RDS extiende los soportes para copias de seguridad automatizados entre regiones	Ahora puede replicar instantáneas de base de datos y registros de transacciones entre más Regiones de AWS. Para obtener más información, consulte Replicación de copias de seguridad automatizadas en otra región de AWS.	19 de julio de 2021

Compatibilidad con MySQL 5.7.34	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.34. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	8 de julio de 2021
Amazon RDS en AWS Outposts admite versiones adicionales de RDS for PostgreSQL	RDS en Outposts ahora admite las versiones 12.7 y 13.3 de RDS for PostgreSQL. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	8 de julio de 2021
Amazon RDS for PostgreSQL admite oracle_fdw	Ahora puede utilizar la extensión oracle_fdw para proporcionar un contenedor de datos externo para acceder a las bases de datos de Oracle. Para obtener más información, consulte el acceso a datos externos con la extensión oracle_fdw.	8 de julio de 2021

Amazon RDS admite Oracle Management Agent (OMA) versión 13.5	Puede utilizar Oracle Management Agent (OMA) versión 13.5 con Oracle Enterprise Manager (OEM) Cloud Control 13c versión 5 y superior. Amazon RDS para Oracle instala OMA, que se comunica con Oracle Management Service (OMS) para proporcionar información de monitoreo. Si ejecuta OMS 13.5, puede administrar bases de datos con la instalación de OMA 13.5. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.	7 de julio de 2021

Amazon RDS para Oracle admite la descarga de registros de Amazon S3	Si los registros de rehacer archivados no se encuentran en su instancia, pero están protegidos por el periodo de retención de copia de seguridad, puede usar `rdsadmin.rdsadmin_archive_log_download` para descargarlos de Amazon S3. RDS para Oracle guarda los registros en el directorio de `/rdsdbdata/log/arch` en la instancia de base de datos. Para obtener más información, consulte los datos para descargar los registros de rehacer archivados de Amazon S3.	2 de julio de 2021
Amazon RDS admite las versiones 10.4.18 y 10.5.9 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.4.18 y 10.5.9 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	30 de junio de 2021

Amazon RDS para Oracle admite transmisiones de actividad de la base de datos	Ahora puede monitorear una instancia de base de datos de Oracle mediante transmisiones de actividad de la base de datos. Una base de datos de Oracle escribe registros de auditoría en los registros de seguimien to de auditoría unificada. Al iniciar una transmisión de actividad de la base de datos en una instancia de base de datos de Oracle, Amazon Kinesis transmite todas las actividades que coinciden con las políticas de auditoría de Oracle Database. Para obtener más información, consulte la sección Supervisi ón de Amazon RDS para Oracle mediante los flujos de actividad de la base de datos.	23 de junio de 2021
Amazon RDS para Oracle introduce clases de instancia de memoria optimizada	Las nuevas clases de instancia de base de datos de Oracle están optimizad as para cargas de trabajo que requieren memoria, almacenamiento y E/S adicionales por vCPU. Para obtener más información, consulte los datos sobre las clases de instancias de RDS para Oracle.	23 de junio de 2021

Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.25. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	18 de junio de 2021
Amazon RDS en AWS Outposts admite versiones adicionales de RDS for PostgreSQL	RDS en Outposts ahora admite las versiones 12.5, 12.6, 13.1 y 13.2 de RDS for PostgreSQL. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	28 de mayo de 2021
Amazon RDS admite las versiones 10.2.37 y 10.3.28 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.2.37 y 10.3.28 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	27 de mayo de 2021

Amazon RDS para Oracle admite base de datos de contenedores de varios inquilinos (CDB)	Una arquitectura de varios inquilinos permite que una base de datos Oracle sea una CDB. En Oracle Database 19c, la CDB puede incluir una única PDB. La experienc ia del usuario con una PDB es en su mayoría idéntica a la experiencia del usuario sin una CDB. Para obtener más información, consulte la arquitectura de RDS para Oracle.	25 de mayo de 2021
Amazon RDS en AWS Outposts admite Amazon RDS for SQL Server	RDS en Outposts ahora soporta Amazon RDS for SQL Server. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	11 de mayo de 2021
Amazon RDS extiende los soportes para copias de seguridad automatizados entre regiones	Ahora puede configurar instancias de base de datos de Amazon RDS que ejecutan Microsoft SQL Server para replicar instantáneas de base de datos y registros de transacciones en una región de AWS diferente. Para obtener más información, consulte Replicación de copias de seguridad automatizadas en otra región de AWS.	7 de mayo de 2021

Amazon RDS admite copias de seguridad automatizadas entre regiones para instancias de base de datos cifradas	Ahora puede replicar instantáneas de base de datos y registros de transacciones en una región de AWS diferente para bases de datos de Amazon RDS cifradas que ejecutan Oracle o PostgreSQL. Para obtener más información, consulte Replicación de copias de seguridad automatizadas en otra región de AWS.	3 de mayo de 2021
Amazon RDS en AWS Outposts admite supervisión de Amazon CloudWatch	RDS en Outposts ahora admite Amazon CloudWatch el monitoreo. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	21 de abril de 2021
RDS for PostgreSQL admite funciones de AWS Lambda	Ahora puede invocar funciones de AWS Lambda para las instancias de base de datos de RDS for PostgreSQL. A fin de obtener más información, consulte Invocación de una función de AWS Lambda desde una instancia de base de datos de RDS for PostgreSQL.	13 de abril de 2021

RDS for SQL Server admite eventos extendidos	Puede utilizar eventos extendidos de SQL Server para capturar información de depuración y solución de problemas. Para obtener más información, consulte Uso de eventos extendidos con Amazon RDS para Microsoft SQL Server.	8 de abril de 2021
Compatibilidad con MySQL 8.0.23, 5.7.33 y 5.6.51	Ahora puede crear instancia s de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.23, 5.7.33 y 5.6.51. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	31 de marzo de 2021
Fallo en la reversión automátic a de la actualización de Amazon RDS for MySQL	Si falla una actualización de instancia de base de datos de MySQL versión 5.7 a MySQL versión 8.0, Amazon RDS revierte automáticamente los cambios realizados para la actualización. Luego de la reversión, la instancia de base de datos de MySQL ejecuta MySQL versión 5.7. Para obtener más información, consulte Reversión después de no actualizar de MySQL 5.7 a 8.0 .	18 de marzo de 2021

Amazon RDS admite réplicas de lectura entre regiones en regiones registradas	Ahora puede replicar instancias de base de datos en regiones registradas. Para obtener más información, consulte Creación de una réplica de lectura en una región de AWS diferente.	18 de marzo de 2021
Amazon RDS tiene pensado dar de baja Oracle Database 18c	Oracle Database 18c (18.0.0.0) está en una ruta de desuso. Oracle Corporation ya no proporcionará parches para Oracle Database 18c después de la fecha de finalización del soporte. El 1 de julio de 2021, Amazon RDS planea comenzar a actualizar automáticamente las instancias de Oracle Database 18c a Oracle Database 19c. Antes de que comiencen las actualizaciones automáticas, recomendamos encarecidamente que actualice manualmente las instancias existentes de Oracle Database 18c a Oracle Database 19c. Para obtener más información, consulte Preparación para la actualización automática de Oracle Database 18c.	11 de marzo de 2021

Amazon RDS ha finalizado el soporte para Oracle Database 11g	Solo puede crear instancias de base de datos para Oracle Database 12c versión 1 (12.1.0.2) y versiones posteriores. Si tiene instantáneas de Oracle Database 11g, actualícelas a una versión posterior. Para obtener más información, consulte Actualización de una instantánea de base de datos de Oracle.	11 de marzo de 2021
Amazon RDS admite copias de seguridad continuas de instancias de base de datos en AWS Backup	Ahora puede crear copias de seguridad automatizadas en AWS Backup y restaurar instancias de base de datos desde estas copias de seguridad a un tiempo especificado. Para obtener más información, consulte UtilizarAWS Backup para administrar copias de seguridad automatizadas.	10 de marzo de 2021

Amazon RDS admite Oracle Management Agent (OMA) versión 13.4	Puede utilizar Oracle Management Agent (OMA) versión 13.4 con Oracle Enterprise Manager (OEM) Cloud Control 13c Release 4 Update 9. Amazon RDS para Oracle instala OMA, que se comunica con Oracle Management Service (OMS) para proporcionar información de monitoreo. Si ejecuta OMS 13.4, puede administrar bases de datos con la instalación de OMA 13.4. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.	10 de marzo de 2021

Mejoras de puntos de enlace de proxy de RDS	Puede crear puntos de enlace adicionales asociados con cada proxy de RDS. La creación de un punto de enlace en una VPC diferente permite el acceso entre VPC para el proxy. Los proxies para los clústeres de Aurora MySQL también pueden tener puntos de enlace de solo lectura. Estos puntos de enlace del lector se conectan a las instancias de base de datos del lector en los clústeres y pueden mejorar la escalabilidad de lectura y la disponibilidad para aplicaciones que requieren un uso intensivo de consultas. Para obtener más información acerca del proxy de RDS, consulte “Administración de conexiones con el proxy de Amazon RDS” en la Guía del usuario de Amazon RDS o en la Guía del usuario de Aurora.	8 de marzo de 2021

Amazon RDS amplía los soportes para copias de seguridad automatizados entre regiones	Ahora puede configurar instancias de base de datos de Amazon RDS que ejecutan PostgreSQL para replicar instantáneas de base de datos y registros de transacciones en una región de AWS diferente. Para obtener más información, consulte Replicación de copias de seguridad automatizadas en otra región de AWS.	8 de marzo de 2021
Compatibles con filtros de reproducción para Amazon RDS para MariaDB y MySQL en las regiones de China (Pekín) y China (Ningxia)	Ahora es compatible con el filtrado de reproducción en las regiones de China (Pekín) y China (Ningxia). Para obtener más información, consulte Configuración de filtros de reproducción con MariaDB y Configuración de filtros de reproducción con MySQL.	5 de marzo de 2021
Amazon RDS admite copia instantánea de base de datos entre regiones en regiones registradas	Ahora puede copiar instantáneas de base de datos desde y hacia regiones de AWS registradas. Para obtener más información, consulte Copiar instantáneas en las regiones de AWS.	4 de marzo de 2021

Amazon RDS for SQL Server admite grupos de disponibilidad de funcionamiento continuo para Standard Edition	Cuando se crea una instancia de base de datos mediante la configuración Multi-AZ en SQL Server 2019 para el motor de base de datos Standard Edition, RDS utiliza automáticamente grupos de disponibilidad. Para obtener más información, consulte Implementaciones Multi-AZ para Microsoft SQL Server.	23 de febrero de 2021
Amazon RDS para Oracle introduce procedimientos relacionados con asesores	El paquete de `rdsadmin_util` incluye los procedimientos `advisor_task_set_parameter`, `advisor_task_drop` y `dbms_stats_init`. Puede utilizar estos procedimientos para modificar, detener y volver a habilitar tareas del asesor como `AUTO_STATS_ADVISOR_TASK`. A fin de obtener más información, consulte Configuración de parámetros para tareas de asesor.	23 de febrero de 2021

Amazon RDS proporciona razones de conmutación por error para instancias de base de datos Multi-AZ	Ahora puede ver explicaciones más detalladas cuando una instancia de base de datos Multi-AZ conmuta por error a una réplica en espera. Para obtener más información, consulte Proceso de conmutación por error de Amazon RDS.	18 de febrero de 2021
Amazon RDS amplía el soporte para exportar instantáneas a Amazon S3	Ahora puede exportar datos de instantáneas de base de datos a Amazon S3 en China. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3.	17 de febrero de 2021
Filtros de reproducción Amazon RDS para MariaDB y MySQL	Puede configurar filtros de reproducción para instancias de MySQL y MariaDB. Los filtros de reproducción especifican qué bases de datos y tablas se replican en una réplica de lectura. Puede crear listas de bases de datos y tablas para incluir o excluir en cada réplica de lectura. Para obtener más información, consulte Configuración de filtros de reproducción con MariaDB y Configuración de filtros de reproducción con MySQL.	12 de febrero de 2021

RDS para Oracle admite APEX 20.2v1	Puede utilizar APEX 20.2.v1 con todas las versiones compatibles de Oracle Database. Para obtener más información, consulte Oracle Application Express.	2 de febrero de 2021
Amazon RDS for SQL Server admite el almacenamiento de la instancia local en la base de datos tempdb	Ahora puede iniciar Amazon RDS for SQL Server en tipos de instancia Amazon EC2 db.r5d y db.m5d con la base de datos tempdb configurada para utilizar un almacén de instancias. Al ubicar archivos de datos tempdb y archivos de registro localmente, puede lograr latencias de lectura y escritura menores en comparación con el almacenamiento estándar basado en Amazon EBS. A fin de obtener más informaci ón, vea Soporte del almacén de instancias para la base de datos tempdb en Amazon RDS para SQL Server.	27 de enero de 2021

Amazon RDS for PostgreSQL admite pg_partman y pg_cron	Amazon RDS para PostgreSQL ahora admite las extensiones pg_partman y pg_cron. Para obtener más información acerca de la extensión pg_partman, consulte Administración de particiones de PostgreSQL con la extensión pg_partman. Para obtener más información acerca de la extensión pg_cron, consulte Programación de mantenimiento con la extensión pg_cron de PostgreSQL.	12 de enero de 2021
Amazon RDS admite la publicación del registro de Oracle Management Agent en registros de Amazon Cloudwatch	El registro de Oracle Management Agent consta de emctl.log, emdctlj.log, gcagent.log, gcagent_errors.log, emagent.nohup y secure.log. Amazon RDS publica cada uno de estos registros como una secuencia de registro independiente de CloudWatch. Para obtener más información, consulte Publicación de registros de Oracle en registros de Amazon Cloudwatch.	28 de diciembre de 2020

Amazon RDS en AWS Outposts admite versiones adicionales de bases de datos	RDS on Outposts ahora admite versiones adicionales de MySQL y PostgreSQL. Para obtener más información, consulte Compatibilidad de Amazon RDS en AWS Outposts con las características de Amazon RDS.	23 de diciembre de 2020
Amazon RDS en AWS Outposts admite CoIP	RDS on Outposts ahora admite direcciones IP propiedad del cliente (CoIP). Las CoIP proporcionan conectividad local o externa a los recursos de sus subredes Outpost a través de su red local. Para obtener más información, consulte Direcciones IP propiedad del cliente para RDS on Outposts.	22 de diciembre de 2020

Amazon RDS para Oracle planea actualizar instancias BYOL 11g a 19c	El 4 de enero de 2021, planeamos comenzar a actualizar automáticamente todas las ediciones de instancias de Oracle Database 11g del modelo Bring Your Own License (BYOL) a Oracle Database 19c. Todas las instancias de Oracle 11g, incluidas las instancia s reservadas, pasarán a la última actualización de versiones (RU) disponible. Para obtener más información, consulte Preparación para la actualización automática de Oracle Database 11g BYOL.	11 de diciembre de 2020
Amazon RDS admite la reproducción de copias de seguridad automatizadas en otra región de AWS	Ahora puede configurar sus instancias de base de datos de Amazon RDS para replicar los registros de transacci ones e instantáneas en una región de AWS de destino de su elección. Para obtener más información, consulte Replicación de copias de seguridad automatizadas en otra región de AWS.	4 de diciembre de 2020

Amazon RDS para Oracle y Microsoft SQL Server admiten una nueva clase de instancia de base de datos	Ahora puede utilizar la clase de instancia db.r5b para crear instancias de base de datos de Amazon RDS que ejecuten Oracle o SQL Server. Para obtener más información, consulte Motores de base de datos compatibles para clases de instancia de base de datos.	4 de diciembre de 2020
Compatibilidad con MariaDB 10.2.32	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.2.32. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	25 de noviembre de 2020
Amazon RDS for SQL Server admite el conjunto de inteligencia empresarial de Microsoft en SQL Server 2019	Ahora puede ejecutar los servicios de análisis, integración e informes de SQL Server en instancias de base de datos utilizando la versión principal más reciente. Para obtener más información, consulte Opciones para el motor de base de datos de Microsoft SQL Server.	24 de noviembre de 2020
Amazon RDS for PostgreSQL, versión 13 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL ahora admite PostgreSQL versión 13 en el entorno de vista previa de base de datos. Para obtener más información, consulte Versiones 13 de PostgreSQL.	24 de noviembre de 2020

La información sobre rendimiento de Amazon RDS introduce nuevas dimensiones	Puede agrupar la carga de la base de datos según los grupos de dimensiones para la base de datos (PostgreSQL, MySQL y MariaDB), la aplicación (PostgreSQL) y el tipo de sesión (PostgreSQL). Amazon RDS también admite las dimensiones db.name (PostgreSQL, MySQL y MariaDB), db.application.name (PostgreSQL) y db.session_type.name (PostgreSQL). Para obtener más información, consulte Tabla de carga superior.	24 de noviembre de 2020
Amazon RDS para MariaDB admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB, versión 10.5. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	23 de noviembre de 2020
Compatibilidad con MySQL 5.6.49	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL, versión 5.6.49. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	20 de noviembre de 2020

Compatibilidad con MySQL 5.5.62	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL, versión 5.5.62. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	20 de noviembre de 2020
La información sobre rendimiento admite el análisis de las estadísticas de ejecución de consultas de PostgreSQL	Puede analizar las estadísticas de ejecución de consultas con la información sobre rendimiento para las instancias de base de datos de PostgreSQL. Para obtener más información, consulte Estadísticas de PostgreSQL.	18 de noviembre de 2020
Amazon RDS amplía el soporte para el escalado automático de almacenamiento	Ahora puede habilitar el escalado automático de almacenamiento al crear una réplica de lectura, restaurar una instancia de base de datos a un momento especificado o restaurar una instancia de base de datos de MySQL desde una copia de seguridad de Amazon S3. Para obtener más información, consulte Administrar la capacidad automáticamente con el escalado automático de almacenamiento de Amazon RDS.	18 de noviembre de 2020

Amazon RDS for SQL Server admite Database Mail	Con Database Mail puede enviar mensajes de correo electrónico desde su instancia de base de datos de Amazon RDS for SQL Server. Después de especificar los destinatarios del correo electrónico, puede agregar archivos o resultados de consulta al mensaje que va a enviar. Para obtener más información, consulte Uso de Database Mail en Amazon RDS for SQL Server.	4 de noviembre de 2020
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.21. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	22 de octubre de 2020
Amazon RDS amplía el soporte para exportar instantáneas a Amazon S3	Ahora puede exportar datos de instantáneas de base de datos a Amazon S3 en todas las regiones comerciales de AWS. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3.	22 de octubre de 2020

Amazon RDS for PostgreSQL admite actualizaciones de réplica de lectura	Con Amazon RDS para PostgreSQL, cuando realiza una actualización de la versión principal de la instancia de base de datos principal, las réplicas de lectura también se actualizan automáticamente. Para obtener más información, consulte Actualización del motor de base de datos de PostgreSQL.	15 de octubre de 2020
Amazon RDS para MariaDB, MySQL y PostgreSQL admiten las clases de instancia de base de datos Graviton2	Ahora puede utilizar las clases de instancia de base de datos Graviton2 db.m6g.x y db.r6g.x para crear instancias de base de datos de Amazon RDS que ejecuten MariaDB, MySQL o PostgreSQL. Para obtener más información, consulte Motores de base de datos compatibles para todas las clases de instancia de base de datos disponibles.	15 de octubre de 2020
Amazon RDS for SQL Server admite actualizaciones a SQL Server 2019	Puede actualizar las instancias de base de datos de SQL Server a SQL Server 2019. Para obtener más información, consulte Actualización del motor de base de datos Microsoft SQL Server.	6 de octubre de 2020

Amazon RDS para Oracle admite la especificación del juego de caracteres nacional	El conjunto de caracteres nacionales, también denominado conjunto de caracteres NCHAR, se utiliza en los tipos de datos `NCHAR`, `NVARCHAR2` y `NCL0B`. Al crear una base de datos, puede especificar AL16UTF16 (predeterminado) o UTF8 como juego de caracteres NCHAR. Para obtener más información, consulte Juegos de caracteres de Oracle admitidos en Amazon RDS.	2 de octubre de 2020
Compatibilidad con MySQL 5.7.31	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.31. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	1 de octubre de 2020
Amazon RDS for PostgreSQL permite exportar datos a Amazon S3	Puede consultar los datos de una instancia de base de datos de PostgreSQL y exportarlos directamente a archivos almacenados en un bucket de Amazon S3. Para obtener más información, consulte Exporting Data from an RDS for PostgreSQL DB Instance to Amazon S3.	24 de septiembre de 2020

Amazon RDS for MySQL 8.0 admite Percona XtraBackup	Ahora puede usar Percona XtraBackup para restaurar una copia de seguridad en una instancia de base de datos de Amazon RDS for MySQL 8.0. Para obtener más informaci ón, consulte Restauración de una copia de seguridad en una instancia de base de datos de MySQL.	17 de septiembre de 2020
Amazon RDS for SQL Server admite copias de seguridad y restauración nativas en instancias de base de datos con réplicas de lectura	Puede restaurar una copia de seguridad nativa de SQL Server en una instancia de base de datos que tenga réplicas de lectura configuradas. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server.	16 de septiembre de 2020
Amazon RDS for SQL Server admite más zonas horarias	Puede hacer coincidir la zona horaria de la instancia de base de datos con la zona horaria elegida. Para obtener más información, consulte Zona horaria local para las instancias de base de datos de Microsoft SQL Server.	11 de septiembre de 2020

Amazon RDS for PostgreSQL versión 13 Beta 3 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL ahora es compatible con PostgreSQL versión 13 Beta 3 en el entorno de vista previa de base de datos. Para obtener más información, consulte Versiones 13 de PostgreSQL.	9 de septiembre de 2020
Amazon RDS for SQL Server admite el indicador de rastreo 692	Ahora puede utilizar el indicador de rastreo 692 como parámetro de inicio utilizando grupos de parámetros de base de datos. Al habilitar este indicador de rastreo, se desactivan las inserciones rápidas mientras se cargan datos de forma masiva en el montón o en los índices agrupados en clústeres. Para obtener más información, consulte Desactivación de inserciones rápidas durante la carga masiva.	27 de agosto de 2020
Amazon RDS for SQL Server admite Microsoft SQL Server 2019	Ahora puede crear instancias de base de datos de RDS que utilicen SQL Server 2019. Para obtener más información, consulte Versiones de Microsoft SQL Server en Amazon RDS.	26 de agosto de 2020

RDS para Oracle admite bases de datos de réplica montadas	Al crear o modificar una réplica de Oracle, puede colocarla en modo montado. Debido a que la base de datos de réplica no acepta conexiones de usuario, no puede servir una carga de trabajo de solo lectura. La réplica montada elimina los archivos de registro REDO archivados después de aplicarlos. El uso principal de las réplicas montadas es la recuperación de desastres entre regiones. Para obtener más información, consulte Información general sobre las réplicas de Oracle.	13 de agosto de 2020
RDS para Oracle planea la actualización de instancias 11g SE1 LI	El 1 de noviembre de 2020, tenemos previsto comenzar a actualizar automáticamente instancias de Database Oracle 11g SE1 License Included (LI) a Oracle Database 19c para Amazon RDS para Oracle. Todas las instancia s 11g, incluidas las instancia s reservadas, se moverán a la última actualización de versiones de Oracle (RU) disponible. A fin de obtener más información, consulte Preparación para la actualiza ción automática de Oracle Database 11g SE1.	31 de julio de 2020

Amazon RDS admite nuevas clases de instancia de base de datos de Graviton2 en la versión de vista previa para PostgreSQL y MySQL	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL o MySQL que utilicen las clases de instancia de base de datos db.m6g.x y db.r6g.x. Para obtener más información, consulte Motores de base de datos compatibles para todas las clases de instancia de base de datos disponibles.	30 de julio de 2020
RDS para Oracle admite APEX 20.1v1	Puede utilizar APEX 20.1v1 con todas las versiones compatibles de Oracle Database. Para obtener más información, consulte Oracle Application Express.	28 de julio de 2020
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.20. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	23 de julio de 2020

Amazon RDS para MariaDB y MySQL admite nuevas clases de instancia de base de datos	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB y MySQL que utilicen las clases de instancia de base de datos db.m5.16xlarge, db.m5.8xlarge, db.r5.16xlarge y db.r5.8xlarge. Para obtener más información, consulte Motores de base de datos compatibles para todas las clases de instancia de base de datos disponibles.	23 de julio de 2020
RDS para SQL Server admite la desactivación de versiones antiguas de TLS y cifrados	Puede activar y desactivar determinados protocolos de seguridad y cifrados. Para obtener más información, consulte Configuración de protocolos de seguridad y cifrados.	21 de julio de 2020
RDS admite Oracle Spatial en SE2	Puede utilizar Oracle Spatial en Standard Edition 2 (SE2) para todas las versiones de 12.2, 18c y 19c. Para obtener más información, consulte Oracle Spatial.	9 de julio de 2020

Amazon RDS admite AWS PrivateLink	Amazon RDS ahora admite la creación de puntos de enlace de Amazon VPC para llamadas a la API de Amazon RDS a fin de mantener el tráfico entre aplicaciones y Amazon RDS en la red de AWS. Para obtener más información, consulte los datos sobre los puntos de enlace de la VPC de tipo interfaz y Amazon RDS (AWS PrivateLink).	9 de julio de 2020
Las versiones 9.4.x de Amazon RDS para PostgreSQL han llegado a su fin de soporte.	Amazon RDS para PostgreSQL ya no admite las versiones 9.4.x. Para obtener información sobre las versiones compatibles, consulte Versiones de bases de datos de PostgreSQL compatibles.	8 de julio de 2020
Compatibilidad para MariaDB 10.3.23 y 10.4.13	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.3.23. y 10.4.13 Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	6 de julio de 2020
Amazon RDS en AWS Outposts	Puede crear instancias de base de datos de Amazon RDS en AWS Outposts. Para obtener más información, consulte Trabajo con Amazon RDS en AWS Outposts.	6 de julio de 2020

Amazon RDS para Oracle crea archivos de inventario automáticamente	Para abrir solicitudes de servicio para clientes BYOL, Oracle Support solicita archivos de inventario generados por Opatch. Amazon RDS para Oracle crea archivos de inventario automáticamente cada hora en el directorio de BDUMP. Para obtener más información, consulte Acceso a los archivos de Opatch.	6 de julio de 2020
Compatibilidad con MySQL 5.7.30 y 5.6.48	Ahora puede crear instancia s de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.30 y 5.6.48. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	25 de junio de 2020

Amazon RDS para Oracle admite ADRCI	La utilidad Automatic Diagnostic Repository Command Interpreter (ADRCI) es una herramienta de línea de comandos de Oracle que se utiliza para administrar datos de diagnóstico. Al utilizar las funciones del paquete de Amazon RDS `rdsadmin_adrci_util` , puede obtener un listado de problemas e incidentes y empaquetarlos, así como mostrar archivos de seguimiento. Para obtener más información, consulte Tareas comunes de diagnóstico de administración de bases de datos para instancias de bases de datos Oracle.	17 de junio de 2020
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.19. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	2 de junio de 2020

MySQL 8.0 admite nombres de tablas en minúsculas	Ahora puede establecer el parámetro `lower_case_table_names` en 1 para instancias de base de datos de Amazon RDS que ejecutan MySQL versión 8.0.19 y versiones posteriores a la 8.0. Para obtener más información, consulte Excepciones de parámetros de MySQL para instancias de base de datos de Amazon RDS.	2 de junio de 2020
Amazon RDS for Microsoft SQL Server admite SQL Server Integration Services (SSIS)	SSIS es una plataforma para aplicaciones de integración de datos y flujo de trabajo. Puede habilitar SSIS en instancias de base de datos ya existentes o nuevas. Está instalado en la misma instancia de base de datos que su motor de base de datos. Para obtener más información, consulte Compatibilidad de SQL Server Integration Services en SQL Server.	19 de mayo de 2020

Amazon RDS for Microsoft SQL Server es compatible con SQL Server Reporting Services (SSRS)	SSRS es una aplicación basada en servidor utilizada para la generación y distribución de informes. Puede habilitar SSRS en instancias de base de datos ya existentes o nuevas. Está instalado en la misma instancia de base de datos que su motor de base de datos. Para obtener más información, consulte la sección sobre soporte para SQL Server Reporting Services en SQL Server.	15 de mayo de 2020
Amazon RDS for Microsoft SQL Server admite la integración de S3 en instancias Multi-AZ	Ahora puede utilizar Amazon S3 con características de SQL Server como la inserción masiva en instancias de base de datos Multi-AZ. Para obtener más información, consulte Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3.	15 de mayo de 2020
Amazon RDS para Oracle admite la depuración de la papelera de reciclaje	El procedimiento `rdsadmin.rdsadmin_util.purge_dba_recyclebin` depura la papelera de reciclaje. Para obtener más información, consulte Depuración de la Papelera de reciclaje.	13 de mayo de 2020

Amazon RDS para Oracle mejora la capacidad de administración de Automatic Workload Repository (AWR)	Los procedimientos `rdsadmin.rdsadmin_diagnostic_util` generan informes AWR y extraen datos AWR en archivos de volcado. Para obtener más información, consulte Generación de informes de rendimiento con Automatic Workload Repository (AWR).	13 de mayo de 2020
Amazon RDS for Microsoft SQL Server es compatible con el Coordinador de transacciones distribuidas de Microsoft (MSDTC)	Amazon RDS for SQL Server admite transacciones distribuidas entre alojamientos. Para obtener más información, consulte Compatibilidad con el Coordinador de transacciones distribuidas de Microsoft en SQL Server.	4 de mayo de 2020
Amazon RDS for Microsoft SQL Server admite nuevas versiones	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten SQL Server versiones 2017 CU19 14.00.3281.6, 2016 SP2 CU11 13.00.5598.27, 2014 SP3 CU4 12.00.6329.1 y 2012 SP4 GDR 11.0.7493.4 para todas las ediciones. Para obtener más información, consulte Versiones de Microsoft SQL Server en Amazon RDS.	28 de abril de 2020

Amazon RDS está disponible en Región Europa (Milán)	Amazon RDS ahora está disponible en Región Europa (Milán). Para obtener más información, consulte Regiones y zonas de disponibilidad.	28 de abril de 2020
Compatibilidad de Amazon RDS con Local Zones	Ahora puede lanzar instancias de base de datos en una subred de zona local. Para obtener más información, consulte Regiones, zonas de disponibilidad y zonas locales.	23 de abril de 2020
Amazon RDS está disponible en Región de África (Ciudad del Cabo)	Amazon RDS ahora está disponible en Región de África (Ciudad del Cabo). Para obtener más información, consulte Regiones y zonas de disponibilidad.	22 de abril de 2020
Amazon RDS for Microsoft SQL Server da soporte a SQL Server Analysis Services (SSAS)	SSAS es una herramienta de procesamiento analítico en línea (OLAP) y minería de datos instalada en SQL Server. Puede habilitar SSAS en instancias de base de datos ya existentes o nuevas. Está instalado en la misma instancia de base de datos que su motor de base de datos. Para obtener más información, consulte la sección sobre soporte para SQL Server Analysis Services en SQL Server.	17 de abril de 2020

Proxy de Amazon RDS for PostgreSQL	Ahora, el proxy de Amazon RDS está disponible para PostgreSQL. Puede utilizar el proxy de RDS para reducir la sobrecarga de la administración de conexiones en la instancia de base de datos y también la posibilidad de que se produzcan errores de “demasiadas conexiones”. El proxy de RDS se encuentra actualmente en vista previa pública para PostgreSQL. Para obtener más información, consulte Administración de conexiones con el proxy de Amazon RDS (vista previa).	8 de abril de 2020
Amazon RDS para Oracle da soporte Oracle APEX versión 19.2.v1	Amazon RDS para Oracle ahora da soporte a Oracle Application Express (APEX) versión 19.2.v1. Para obtener más información, consulte Oracle Application Express.	8 de abril de 2020
Amazon RDS para MariaDB admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.4. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	6 de abril de 2020

Información sobre rendimiento de Amazon RDS está disponible para Amazon RDS para MariaDB 10.4	Amazon RDS La información sobre rendimiento está ahora disponible para Amazon RDS para MariaDB versión 10.4. Para obtener más información, consulte Uso de Información sobre rendimiento de Amazon RDS.	6 de abril de 2020
Las versiones 9.3.x de Amazon RDS para PostgreSQL han llegado a su fin de soporte	Amazon RDS para PostgreSQL ya no admite las versiones 9.3.x. Para obtener información sobre las versiones compatibles, consulte Versiones de bases de datos de PostgreSQL compatibles.	3 de abril de 2020
Amazon RDS for Microsoft SQL Server es compatible réplicas de lectura	Ahora puede crear réplicas de lectura para instancias de base de datos de SQL Server. Para obtener más información, consulte Trabajo con réplicas de lectura.	3 de abril de 2020
Amazon RDS for Microsoft SQL Server es compatible copias de seguridad de varios archivos	Ahora puede realizar una copia de seguridad de bases de datos para varios archivos mediante la copia de seguridad y restauración nativa de SQL Server. Para obtener más información, consulte Copia de seguridad de una base de datos.	2 de abril de 2020

Integración de Amazon RDS para Oracle conAWS License Manager	Amazon RDS para Oracle ahora está integrado con AWS License Manager. Si utiliza el modelo Bring Your Own License, la integración de AWS License Manager facilita el control del uso de la licencia de Oracle dentro de su organización. Para obtener más información, consulte Integración con AWS License Manager.	23 de marzo de 2020
Compatibilidad con 64 TiB en instancias db.r5 en Amazon RDS para MariaDB y MySQL	Ahora puede crear instancias de base de datos para Amazon RDS para MariaDB y MySQL que utilicen la clase de instancia de base de datos db.r5 con hasta 64 TiB de almacenamiento. Para obtener más información, consulte Factores que afectan al rendimiento del almacenamiento.	18 de marzo de 2020
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.17. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	10 de marzo de 2020

Información sobre rendimiento de Amazon RDS está disponible para Amazon RDS for MySQL	Información sobre rendimiento de Amazon RDS ahora está disponible para Amazon RDS for MySQL versión 8.0.17 y versiones posteriores a 8.0. Para obtener más información, consulte Uso de Información sobre rendimiento de Amazon RDS.	10 de marzo de 2020
Compatibilidad con MySQL 5.6.46	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.6.46. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	28 de febrero de 2020
Información sobre rendimiento de Amazon RDS está disponible para Amazon RDS para MariaDB 10.3	Información sobre rendimiento de Amazon RDS ahora está disponible para Amazon RDS para MariaDB versión 10.3.13 y versiones posteriores a 10.3. Para obtener más información, consulte Uso de Información sobre rendimiento de Amazon RDS.	26 de febrero de 2020
Compatibilidad con MySQL 5.7.28	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.28. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	20 de febrero de 2020

Compatibilidad con MariaDB 10.3.20	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.3.20. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	20 de febrero de 2020
Amazon RDS for Microsoft SQL Server es compatible con una nueva clase de instancia de base de datos	Puede crear instancias de base de datos de Amazon RDS que ejecuten SQL Server y utilicen las clases de instancia de base de datos db.z1d. Para obtener más información, consulte Compatibilidad con las clases de instancias de bases de datos de Microsoft SQL Server.	19 de febrero de 2020
Compatibilidad con dominios de Active Directory entre cuentas y VPC en Amazon RDS for SQL Server	Amazon RDS for Microsoft SQL Server ahora es compatible con la asociación de instancias de base de datos con dominios de Active Directory propiedad de diferentes cuentas y VPC. Para obtener más información, consulte Uso de la autenticación de Windows con una instancia de base de datos de Microsoft SQL Server.	13 de febrero de 2020

Opción de Oracle OLAP	Amazon RDS para Oracle ahora es compatible con la opción de procesamiento analítico en línea (OLAP) para las instancias de base de datos de Oracle. Puede utilizar Oracle OLAP para analizar grandes cantidades de datos mediante la creación de cubos y objetos dimensionales de acuerdo con el estándar OLAP. Para obtener más información, consulte Oracle OLAP.	13 de febrero de 2020
Compatibilidad de FIPS 140-2 para Oracle	Amazon RDS para Oracle es compatible con el estándar federal de procesamiento de información 140-2 (FIPS 140-2) para conexiones SSL/TLS. Para obtener más información, consulte Compatibilidad de FIPS.	11 de febrero de 2020

Amazon RDS for PostgreSQL es compatible con las nuevas clases de instancia de base de datos	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL y utilicen las clases de instancia de base de datos db.m5.16xlarge, db.m5.8xlarge, db.r5.16xlarge y db.r5.8xlarge. Para obtener más información, consulte Motores de base de datos compatibles para todas las clases de instancia de base de datos disponibles.	11 de febrero de 2020
Información sobre rendimiento es compatible con el análisis de las estadísticas de la ejecución de consultas de MariaDB y MySQL.	Puede analizar las estadísticas de ejecución de consultas con Información sobre rendimiento para las instancias de base de datos de MariaDB y MySQL. Para obtener más información, consulte Análisis de estadísticas de la ejecución de consultas.	4 de febrero de 2020
Soporte para exportar datos de instantáneas de base de datos a Amazon S3 para MariaDB, MySQL y PostgreSQL	Amazon RDS admite la exportación de datos de instantáneas de base de datos a Amazon S3 para MariaDB, MySQL y PostgreSQL. Para obtener más información, consulte Exportación de datos de instantáneas de bases de datos a Amazon S3.	23 de enero de 2020

Amazon RDS for MySQL admite la autenticación Kerberos	Ahora puede usar la autenticación Kerberos para autenticar a los usuarios cuando estos se conecten a sus instancias de base de datos de Amazon RDS for MySQL. Para obtener más información, consulte Uso de la autenticación Kerberos para MySQL.	21 de enero de 2020
Información sobre rendimiento de Amazon RDS permite ver más texto SQL para Amazon RDS for Microsoft SQL Server	Información sobre rendimiento de Amazon RDS permite ahora ver más texto SQL en el panel de Información sobre rendimiento para Amazon RDS for Microsoft SQL Server para instancias de base de datos. Para obtener más información, consulte Visualización de más texto SQL en el panel de Información sobre rendimiento.	17 de diciembre de 2019

Proxy de Amazon RDS	Puede reducir la sobrecarga de la administración de conexiones en el clúster y reducir la posibilidad de que se produzcan errores de «demasiadas conexiones» mediante el Proxy de Amazon RDS. Asocie cada proxy a una instancia de base de datos de RDS o clúster de bases de datos de Aurora. A continuación, utiliza el punto de enlace de proxy en la cadena de conexión para su aplicación. El proxy de Amazon RDS se encuentra actualmente en estado de vista previa pública. Es compatible con el motor de base de datos de RDS para MySQL. Para obtener más información, consulte Administración de conexiones con el proxy de Amazon RDS (vista previa).	3 de diciembre de 2019

Amazon RDS en AWS Outposts (previsualización)	Con Amazon RDS en AWS Outposts, puede crear bases de datos relacionales administradas por AWS en sus centros de datos en las instalaciones. RDS en Outposts le permite ejecutar bases de datos de RDS en AWS Outposts. Para obtener más información, consulte Amazon RDS en AWS Outposts (previsualización).	3 de diciembre de 2019
Amazon RDS para Oracle es compatible con réplicas de lectura entre regiones	Amazon RDS para Oracle ahora es compatible con réplicas de lectura entre regiones con Active Data Guard. Para obtener más información, consulte Trabajo con réplicas de lectura y Trabajo con réplicas de lectura de Oracle.	26 de noviembre de 2019
La información sobre rendimiento es compatible con el análisis de las estadísticas de la ejecución de consultas de Oracle.	Puede analizar las estadísticas de ejecución de consultas con la información sobre el rendimiento para las instancias de base de datos de Oracle. Para obtener más información, consulte Análisis de estadísticas de la ejecución de consultas.	25 de noviembre de 2019

Amazon RDS for Microsoft SQL Server es compatible con la publicación de registros en CloudWatch Logs	Puede configurar su instancia de base de datos de Amazon RDS for SQL Server a fin de publicar eventos de registro directamente en registros de Amazon Cloudwatch. Para obtener más informaci ón, consulte Publicación de registros de SQL Server en registros de Amazon Cloudwatch.	25 de noviembre de 2019
Amazon RDS for Microsoft SQL Server admite nuevas clases de instancia de base de datos	Puede crear instancias de base de datos de Amazon RDS que ejecuten SQL Server y utilicen las clases de instancia de base de datos db.x1e y db.x1 DB. Para obtener más información, consulte Compatibilidad con las clases de instancias de bases de datos de Microsoft SQL Server.	25 de noviembre de 2019
Amazon RDS for Microsoft SQL Server es compatible con restablecimientos de registros y diferenciales.	Puede restaurar los registros y las copias de seguridad diferenciales utilizando una restauración y copia de seguridad nativa de SQL Server. Para obtener más información, consulte Uso de restauración y copia de seguridad nativas.	25 de noviembre de 2019

Multi-AZ compatible con Amazon RDS for Microsoft SQL Server en nuevas regiones	Multi-AZ en SQL Server ahora está disponible en China, Medio Oriente (Baréin) y Europa (Estocolmo). Para obtener más información, consulte Implementaciones Multi-AZ para Microsoft SQL Server.	22 de noviembre de 2019
Amazon RDS for Microsoft SQL Server ahora es compatible con la inserción masiva y la integración con S3	Puede transferir archivos entre una instancia de base de datos de SQL Server y un bucket de Amazon S3. Después puede utilizar Amazon S3 con caracterí sticas de SQL Server como la inserción masiva. Para obtener más información, consulte Integración de una instancia de base de datos de Amazon RDS for SQL Server con Amazon S3.	21 de noviembre de 2019
Contadores de informaci ón sobre rendimiento para Amazon RDS for Microsoft SQL Server	Ahora puede añadir contadore s de rendimiento a sus gráficos de información sobre rendimiento para las instancias de base de datos de Microsoft SQL Server. Para obtener más informaci ón, consulte Contadores de información sobre rendimien to para Amazon RDS for Microsoft SQL Server.	12 de noviembre de 2019

Amazon RDS for Microsoft SQL Server ahora es compatible con nuevos tamaños de instancia de base de datos.	Puede crear instancias de base de datos de Amazon RDS que ejecuten SQL Server y utilicen los tamaños de instancias 8xlarge y 16xlargelas para las clases de instancia de base de datos db.m5 y db.r5. Los tamaños de instancias desde pequeño a 2xlarge ahora están disponibles para la clase de instancia db.t3. Para obtener más información, consulte Compatibilidad con las clases de instancias de bases de datos de Microsoft SQL Server.	11 de noviembre de 2019
Soporte para las actualizaciones de instantáneas de PostgreSQL	Si dispone de instantáneas de base de datos manuales existentes de sus instancias de base de datos de PostgreSQL en Amazon RDS, ahora puede actualizarlas a una versión posterior del motor de base de datos de PostgreSQL. Para obtener más información, consulte Actualización de una instantánea de base de datos de PostgreSQL.	7 de noviembre de 2019

Amazon RDS para Oracle admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle Database 19c (19.0). Para más información, consulte Oracle Database 19c con Amazon RDS.	7 de noviembre de 2019
Amazon RDS for PostgreSQL versión 12.0 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL ahora es compatible con PostgreSQL versión 12.0 en el entorno de vista previa de base de datos. Para obtener más información, consulte PostgreSQL versión 12.0 en el entorno de vista previa de base de datos.	1 de noviembre de 2019
Amazon RDS for PostgreSQL admite autenticación Kerberos	Ahora puede usar la autenticación Kerberos para autenticar los usuarios cuando se conecten a su instancia de base de datos de Amazon RDS en la que se ejecuta PostgreSQL. Para obtener más información, consulte Uso de la autenticación Kerberos con Amazon RDS para PostgreSQL.	28 de octubre de 2019

Tareas de bases de datos de OEM Management Agent para las instancias de bases de datos Oracle	Instancias de bases de datos de Amazon RDS para Oracle ahora admite procedimientos para invocar a determina dos comandos de EMCTL en Management Agent. Para obtener más información, consulte Tareas de base de datos de OEM Agent.	24 de octubre de 2019
Amazon RDS for PostgreSQ L admite bases de datos transportables de PostgreSQL	Las bases de datos transport ables de PostgreSQL proporcionan un método extremadamente rápido de transportar una base de datos de PostgreSQL de RDS entre dos instancias de base de datos. Para obtener más información, consulte Transporte de bases de datos PostgreSQL entre instancias de base de datos.	8 de octubre de 2019
Amazon RDS para Oracle admite autenticación Kerberos	Ahora puede usar la autentica ción Kerberos para autentica r los usuarios cuando se conecten a su instancia de base de datos de Amazon RDS en la que se ejecuta Oracle. Para obtener más información, consulte Uso de la autenticación Kerberos con Amazon RDS para Oracle.	30 de septiembre de 2019

Amazon RDS for PostgreSQL versión 12 Beta 3 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL admite ahora PostgreSQL, versión 12 Beta 3 en el entorno de vista previa de base de datos Para más información, consulte PostgreSQL Versión 12 Beta 3 en Amazon RDS en el entorno de vista previa de base de datos.	28 de agosto de 2019
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.16. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	19 de agosto de 2019
Amazon RDS para Oracle admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle Database 18c (18.0). Para más información, consulte Oracle Database 18c con Amazon RDS.	15 de agosto de 2019

Management Agent para OEM 13c Versión 3	Las instancias de base de datos de Amazon RDS para Oracle son ahora compatibles con Management Agent para Oracle Enterprise Manager (OEM) Cloud Control 13c Versión 3. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.	7 de agosto de 2019
Amazon RDS for PostgreSQL versión 12 Beta 2 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL admite ahora PostgreSQL Versión 12 Beta 2 en el entorno de vista previa de base de datos Para más información, consulte PostgreSQL Versión 12 Beta 2 en Amazon RDS en el entorno de vista previa de base de datos.	6 de agosto de 2019
Amazon RDS admite intercalaciones del servidor para SQL Server	Amazon RDS for SQL Server admite un selección de intercalaciones para las nuevas instancias de base de datos. Para obtener más información, consulte Intercalaciones y conjuntos de caracteres para Microsoft SQL Server.	29 de julio de 2019

Amazon RDS para Oracle admite Oracle APEX versión 19.1.v1	Amazon RDS para Oracle ya admite Oracle Application Express (APEX) versión 19.1.v1. Para obtener más información, consulte Oracle Application Express.	28 de junio de 2019
Amazon RDS for PostgreSQL versión 13 Beta 1 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL ahora admite PostgreSQL Versión 13 Beta 1 en el entorno de vista previa de base de datos. Para obtener más información, consulte Versiones 13 de PostgreSQL.	22 de junio de 2019
Escalado automático de almacenamiento de Amazon RDS	El escalado automático de almacenamiento para instancias de base de datos de Amazon RDS permite a Amazon RDS ampliar automáticamente el almacenamiento asociado a una instancia de base de datos para reducir las probabilidades de situaciones de falta de espacio. Para obtener información sobre el escalado automático de almacenamiento, consulte Trabajar con el almacenamiento para instancias de base de datos de Amazon RDS.	20 de junio de 2019

Amazon RDS para Oracle admite las clases de instancia de base de datos db.z1d	Puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle y utilicen las clases de instancia de base de datos db.z1d. Para obtener más información, consulte Clase de instancia de base de datos.	13 de junio de 2019
Amazon RDS Performance Insights admite la visualización de más texto SQL para Amazon RDS para Oracle	Amazon RDS Performance Insights es ahora compatible con la visualización de más texto SQL en el panel de Performance Insights para instancias de base de datos de Amazon RDS para Oracle. Para obtener más información, consulte Visualización de más texto SQL en el panel de Información sobre rendimiento.	10 de junio de 2019
Amazon RDS admite restauraciones nativas de bases de datos de SQL Server hasta 16 TB.	Ahora puede ejecutar restauraciones nativas de hasta 16 TB desde SQL Server hasta Amazon RDS. Para obtener más información, consulte Amazon RDS para SQL Server: limitaciones y recomendaciones.	4 de junio de 2019

Amazon RDS proporciona soporte para Microsoft SQL Server Audit	Mediante Amazon RDS for Microsoft SQL Server, podrá auditar eventos de nivel de base de datos y servidor mediante SQL Server Audit, y ver los resultados en su instancia de base de datos o enviar los archivos de registro de auditoría directamente a Amazon S3. Para obtener más información, consulte SQL Server Audit.	23 de mayo de 2019
Mejoras en las recomendaciones de Amazon RDS	Amazon RDS ha mejorado las recomendaciones automatizadas de recursos de la base de datos. Por ejemplo, Amazon RDS proporciona ahora recomendaciones para parámetros de base de datos. Para obtener más información, consulte Usar recomendaciones de Amazon RDS.	22 de mayo de 2019
Compatibilidad con más bases de datos por instancia de base de datos para Amazon RDS for SQL Server	Puede crear un máximo de 30 bases de datos en cada una de las instancias de base de datos en las que se ejecuta Microsoft SQL Server. Para obtener más información, consulte Límites para las instancias de base de datos de Microsoft SQL Server.	21 de mayo de 2019

Compatibilidad de 64 TiB y 80 000 IOPS de almacenamiento para Amazon RDS para MariaDB, MySQL y PostgreSQL	Ahora puede crear instancias de base de datos de Amazon RDS para MariaDB, MySQL y PostgreSQL con hasta 64 TiB de almacenamiento y hasta 80 000 IOPS provisionadas. Para obtener más información, consulte Almacenamiento de instancias de base de datos.	20 de mayo de 2019
Amazon RDS for MySQL admite comprobaciones previas de actualización	Cuando actualice una instancia de base de datos de MySQL 5.7 a MySQL 8.0, Amazon RDS realiza comprobaciones previas en busca de incompatibilidades. Para obtener más información, consulte Comprobaciones previas de actualizaciones de la versión 5.7 a la 8.0 de MySQL.	17 de mayo de 2019
Compatibilidad del complemento de validación de contraseñas de MySQL	Ahora puede utilizar el complemento `validate_password` de MySQL para obtener una seguridad mejorada de instancias de base de datos de Amazon RDS for MySQL. Para obtener más información, consulte Uso del complemento de validación de contraseñas.	16 de mayo de 2019

Contadores de Performance Insights para Amazon RDS para Oracle	Ahora puede añadir contadores de rendimiento a sus gráficos de Performance Insights para las instancias de base de datos de Oracle. Para obtener más información, consulte Contadores de Información sobre rendimiento para Amazon RDS para Oracle.	8 de mayo de 2019
Compatibilidad con facturación por segundo	Amazon RDS se factura ahora en incrementos de 1 segundo en todas las regiones de AWS, excepto GovCloud (EE. UU.) de AWS para las instancias en diferido. Para obtener más información, consulte Facturación de instancias de base de datos para Amazon RDS.	25 de abril de 2019
Compatibilidad para la importación de datos desde Amazon S3 para Amazon RDS for PostgreSQL	Ahora puede importar datos de un archivo Amazon S3 en una tabla en una instancia de base de datos de RDS PostgreSQL. Para obtener más información, consulte Importación de datos de Amazon S3 en una instancia de base de datos de RDS PostgreSQL.	24 de abril de 2019

Compatibilidad de restauración de copias de seguridad de 5.7 desde Amazon S3	Ahora puede crear una copia de seguridad de una base de datos de la versión 5.7 de MySQL, almacenarla en Amazon S3 y luego restaurar el archivo de copia de seguridad en una nueva instancia de base de datos de Amazon RDS que ejecute MySQL. Para obtener más información, consulte Restauración de una copia de seguridad en una instancia de base de datos de MySQL.	17 de abril de 2019
Compatibilidad de varias actualizaciones de versiones principales para Amazon RDS for PostgreSQL	Con Amazon RDS para PostgreSQL, puede ahora elegir entre varias versiones principales cuando actualiza el motor de base de datos. Esta característica le permite dirigirse a una versión principal más reciente cuando actualiza versiones de motor de PostgreSQL seleccionadas. Para obtener más información, consulte Actualización del motor de base de datos de PostgreSQL.	16 de abril de 2019

Compatibilidad de 64 TiB de almacenamiento para Amazon RDS para Oracle	Ahora puede crear instancias de base de datos de Amazon RDS para Oracle con hasta 64 TiB de almacenamiento y hasta 80 000 IOPS provisionadas. Para obtener más información, consulte Almacenamiento de instancias de base de datos.	4 de abril de 2019
Compatibilidad con MySQL 8.0.26	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0.15. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	3 de abril de 2019
Compatibilidad con MariaDB 10.3.13	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.3.13. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	3 de abril de 2019

Microsoft SQL Server 2008 R2 ha llegado a su fin de soporte en Amazon RDS	Microsoft SQL Server 2008 R2 ha llegado a su fin de soporte, que coincide con el plan de Microsoft para finalizar el soporte extendido para esta versión el 9 de julio de 2019. Las instantáneas de Microsoft SQL Server 2008 R2 existentes se actualizarán automáticamente a la versión secundaria más reciente de Microsoft SQL Server 2012 a partir del 1 de junio de 2019. Para obtener más informaci ón, consulte Compatibilidad de Microsoft SQL Server 2008 R2 en Amazon RDS.	2 de abril de 2019
Grupos de disponibilidad Always On compatibles en Microsoft SQL Server 2017	Ahora puede utilizar grupos de disponibilidad Always On en SQL Server 2017 Enterpris e Edition 14.00.3049.1 o versiones posteriores. Para obtener más información, consulte Implementaciones Multi-AZ para Microsoft SQL Server.	29 de marzo de 2019

Visualización de métricas de volumen	Ahora puede visualizar las métricas para los volúmenes de Amazon Elastic Block Store (Amazon EBS), que son los dispositivos físicos utilizados para el almacenamiento de registros y base de datos. Para obtener más información, consulte Visualización de la monitorización mejorada.	20 de marzo de 2019
Compatibilidad con MySQL 5.7.25	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 5.7.25. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	19 de marzo de 2019
Amazon RDS para Oracle admite tareas DBA de RMAN	Amazon RDS para Oracle admite ahora tareas DBA de Oracle Recovery Manager (RMAN), incluidas copias de seguridad de RMAN. Para obtener más información, consulte Tareas de Recovery Manager (RMAN) DBA frecuentes para instancias de base de datos de Oracle.	14 de marzo de 2019
Amazon RDS for PostgreSQL admite la versión 11.1	Ahora puede crear instancias de base de datos de Amazon RDS que ejecutan la versión 11.1 de PostgreSQL. Para obtener información, consulte Versión 11.1 de PostgreSQL en Amazon RDS.	12 de marzo de 2019

La restauración de varios archivos está disponible en Amazon RDS for SQL Server	Ahora puede restaurar desde varios archivos con Amazon RDS for SQL Server. Para obtener más información, consulte Restauración de una base de datos.	11 de marzo de 2019
MariaDB 10.2.21	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.2.21. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	11 de marzo de 2019
Amazon RDS para Oracle es compatible con réplicas de lectura	Amazon RDS para Oracle ahora es compatible con réplicas de lectura con Active Data Guard. Para obtener más información, consulte Trabajo con réplicas de lectura y Trabajo con réplicas de lectura de Oracle.	11 de marzo de 2019
Amazon RDS Performance Insights está disponible para Amazon RDS para MariaDB	Amazon RDS Performance Insights está ahora disponibl e para Amazon RDS para MariaDB. Para obtener más información, consulte Uso de Performance Insights de Amazon RDS.	11 de marzo de 2019

MySQL 8.0.13 y 5.7.24	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 8.0.13 y 5.7.24 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	8 de marzo de 2019
Amazon RDS Performance Insights está disponible para Amazon RDS for SQL Server	Amazon RDS Performance Insights está ahora disponible para Amazon RDS for SQL Server. Para obtener más información, consulte Uso de Performance Insights de Amazon RDS.	4 de marzo de 2019
Amazon RDS para Oracle admite la integración de Amazon S3	Puede transferir los archivos entre una instancia de base de datos de Amazon RDS para Oracle y un bucket de Amazon S3. Para obtener más información, consulte Integración de Amazon RDS para Oracle y Amazon S3.	26 de febrero de 2019
Amazon RDS for MySQL y Amazon RDS para MariaDB admiten clases de instancias de base de datos db.t3	Puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL o MariaDB y utilicen las clases de instancia de base de datos db.t3 Para obtener más información, consulte Clase de instancia de base de datos.	20 de febrero de 2019

Amazon RDS for MySQL y Amazon RDS para MariaDB admiten clases de instancias de base de datos db.r5	Puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL o MariaDB y utilicen las clases de instancia de base de datos db.r5. Para obtener más información, consulte Clase de instancia de base de datos.	20 de febrero de 2019
Contadores de información sobre rendimiento para RDS para MySQL y PostgreSQL	Ahora puede agregar contadores de rendimiento a sus gráficos de información sobre rendimiento para instancias de base de datos de MySQL y PostgreSQL. Para obtener más información, consulte Componentes del panel de Información sobre rendimiento.	19 de febrero de 2019
Amazon RDS for PostgreSQL admite ahora el ajuste de parámetros autovacuum adaptativos	El ajuste de parámetros autovacuum adaptativos con Amazon RDS para PostgreSQL ayuda a evitar el reinicio del identificador de transacción mediante el ajuste automático de los valores de los parámetros autovacuum. Para obtener más información, consulte Reducción de la probabilidad de reinicio del identificador de transacción.	12 de febrero de 2019

Amazon RDS para Oracle admite Oracle APEX, versiones 18.1.v1 y 18.2.v1	Amazon RDS para Oracle admite ahora Oracle Application Express (APEX), versiones 18.1.v1 y 18.2.v1. Para obtener más información, consulte Oracle Application Express.	11 de febrero de 2019
La información sobre rendimiento de Amazon RDS admite la visualización de más texto SQL para RDS para MySQL	La información sobre rendimiento de Amazon RDS ahora admite la visualización de más texto SQL en el panel de información sobre rendimiento para instancias de base de datos de MySQL. Para obtener más información, consulte Visualización de más texto SQL en el panel de Información sobre rendimiento.	6 de febrero de 2019
Amazon RDS for PostgreSQL admite las clases de instancia de base de datos db.t3	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL y utilicen las clases de instancia de base de datos db.t3. Para obtener más información, consulte Clase de instancia de base de datos.	25 de enero de 2019

Amazon RDS para Oracle admite las clases de instancia de base de datos db.t3	Puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle y utilicen las clases de instancia de base de datos db.t3. Para obtener más información, consulte Clase de instancia de base de datos.	25 de enero de 2019
Amazon RDS Performance Insights admite la visualización de más texto SQL para Amazon RDS PostgreSQL	Amazon RDS Performance Insights es ahora compatible con la visualización de más texto SQL en el panel de Performance Insights para instancias de base de datos de Amazon RDS PostgreSQL. Para obtener más información, consulte Visualización de más texto SQL en el panel de Información sobre rendimiento.	24 de enero de 2019
Amazon RDS para Oracle admite una versión nueva de SQLT	Amazon RDS para Oracle ahora admite la versión de SQLT 12.2.180725. Para obtener más información, consulte Oracle SQLT.	22 de enero de 2019
Amazon RDS for PostgreSQL admite las clases de instancia de base de datos db.r5	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL y utilicen las clases de instancia de base de datos db.r5. Para obtener más información, consulte Clase de instancia de base de datos.	19 de diciembre de 2018

Amazon RDS for PostgreSQL ahora la administración de contraseñas restringida	Amazon RDS para PostgreSQL le permite restringir quién puede administrar contraseñas de usuarios y cambios en el vencimiento de las contraseñas mediante el parámetro `rds.restrict_password_commands` y el rol `rds_password` . Para obtener más información, consulte Administración de contraseñas.	19 de diciembre de 2018
Amazon RDS for PostgreSQL es compatible con la carga de registros de bases de datos en registros de Amazon Cloudwatch	Amazon RDS para PostgreSQL es compatible con la carga de registros de bases de datos en CloudWatch Logs. Para obtener más información, consulte Publicación de registros de PostgreSQL en CloudWatch Logs.	10 de diciembre de 2018
Amazon RDS para Oracle admite las clases de instancia de base de datos db.r5	Puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle y utilicen las clases de instancia de base de datos db.r5. Para obtener más información, consulte Clase de instancia de base de datos.	20 de noviembre de 2018

Conservar copias de seguridad al eliminar una instancia de base de datos	Amazon RDS permite conservar las copias de seguridad automatizadas al eliminar una instancia de base de datos. Para obtener más información, consulte Trabajar con copias de seguridad.	15 de noviembre de 2018
Amazon RDS for PostgreSQL admite las clases de instancia de base de datos db.m5	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten PostgreSQL y utilicen las clases de instancia de base de datos db.m5. Para obtener más información, consulte Clase de instancia de base de datos.	15 de noviembre de 2018
Amazon RDS para Oracle admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle versión 12.2.	13 de noviembre de 2018
Amazon RDS for SQL Server es compatible con Always On	Amazon RDS for SQL Server admite grupos de disponibilidad Always On. Para obtener más información, consulte Implementaciones Multi-AZ para Microsoft SQL Server.	8 de noviembre de 2018
Amazon RDS for PostgreSQL admite el acceso de red de salida con servidores DNS personalizados	Amazon RDS para PostgreSQL admite el acceso de red de salida con servidores DNS personalizados. Para obtener más información, consulte Uso de un servidor DNS personalizado para el acceso a red de salida.	8 de noviembre de 2018

Amazon RDS para MariaDB, MySQL y PostgreSQL admite 32 TiB de almacenamiento	Ahora puede crear instancias de base de datos de Amazon RDS con hasta 32 TiB de almacenamiento para MySQL, MariaDB, y PostgreSQL. Para obtener más información, consulte Almacenamiento de instancias de base de datos.	7 de noviembre de 2018
Amazon RDS para Oracle es compatible con tipos de datos extendidos	Ahora puede habilitar tipos de datos extendidos en instancias de base de datos de Amazon RDS que ejecutan Oracle. Con tipos de datos extendidos, el tamaño máximo es 32 767 bytes para los tipos de datos VARCHAR2, NVARCHAR2 y RAW. Para obtener más información, consulte Uso de tipos de datos ampliados.	6 de noviembre de 2018
Amazon RDS para Oracle admite las clases de instancia de base de datos db.m5	Puede crear instancias de base de datos de Amazon RDS que ejecuten Oracle y utilicen las clases de instancia de base de datos db.m5. Para obtener más información, consulte Clase de instancia de base de datos.	2 de noviembre de 2018

Migración de Amazon RDS para Oracle de SE, SE1 o SE2 a EE	Ahora es posible migrar desde cualquier Oracle Database Standard Edition (SE, SE1 o SE2) a Oracle Database Enterprise Edition (EE). Para obtener más información, consulte Migración entre ediciones de Oracle.	31 de octubre de 2018
Amazon RDS puede detener ahora instancias Multi-AZ	Amazon RDS puede detener ahora una instancia de base de datos que forme parte de una implementación Multi-AZ. En el pasado, la caracterí stica stop instance tenía una limitación para instancias Multi-AZ. Para obtener más información, consulte Parada de una instancia de base de datos de Amazon RDS temporalmente.	29 de octubre de 2018
La información sobre rendimiento de Amazon RDS está disponible para Amazon RDS para Oracle	La información sobre rendimiento de Amazon RDS está ahora disponible para Amazon RDS para Oracle. Para obtener más información, consulte Uso de Performance Insights de Amazon RDS.	29 de octubre de 2018

Amazon RDS for PostgreSQL admite PostgreSQL versión 11 en el entorno de vista previa de base de datos	Amazon RDS para PostgreSQL admite ahora PostgreSQL versión 11 en el entorno de vista previa de base de datos. Para más información, consulte PostgreSQL versión 11 en Amazon RDS en el entorno de vista previa de base de datos.	25 de octubre de 2018
MySQL; admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL versión 8.0. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	23 de octubre de 2018
MariaDB admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.3. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	23 de octubre de 2018
Amazon RDS para Oracle admite Oracle JVM	Amazon RDS para Oracle admite ahora la opción Oracle Java Virtual Machine (JVM). Para obtener más información, consulte Máquina virtual Oracle Java.	16 de octubre de 2018

Grupo de parámetros personalizado para restaurar y recuperación a un momento dado	Ahora puede especificar un grupo de parámetros personalizados cuando restaure una instantánea o realice una operación de recuperación a un momento dado. Para obtener más información, consulte Restauración desde una instantánea de base de datos y Restauración de una instancia de base de datos a un momento especificado.	15 de octubre de 2018
Amazon RDS para Oracle admite almacenamiento de 32 TiB	Ahora puede crear instancias de base de datos Oracle RDS con hasta 32 TiB de almacenamiento. Para obtener más información, consulte Almacenamiento de instancias de base de datos.	15 de octubre de 2018
Amazon RDS for MySQL admite GTID	Amazon RDS for MySQL admite ahora identificadores de transacciones globales (GTID) que sean únicos en todas las instancias de base de datos y en una configuración de replicación. Para obtener más información, consulte Uso de reproducción basada en GTID para RDS para MySQL.	10 de octubre de 2018

MySQL 5.7.23, 5.6.41 y 5.5.61	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 5.7.23, 5.6.41 y 5.5.61 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	8 de octubre de 2018
Amazon RDS para Oracle admite una versión nueva de SQLT	Amazon RDS para Oracle ahora admite la versión de SQLT 12.2.180331. Para obtener más información, consulte Oracle SQLT.	4 de octubre de 2018
Amazon RDS for PostgreSQL admite ahora la autenticación de IAM	Amazon RDS para PostgreSQL admite ahora la autenticación de IAM. Para obtener más información, consulte Autenticación de bases de datos de IAM para MySQL y PostgreSQL.	27 de septiembre de 2018
Puede habilitar la protección contra eliminación para sus instancias de base de datos de Amazon RDS	Al habilitar la protección contra eliminación para una instancia de base de datos, ningún usuario podrá eliminar dicha base de datos. Para obtener más información, consulte Eliminación de una instancia de base de datos.	26 de septiembre de 2018

Amazon RDS for MySQL y Amazon RDS para MariaDB admiten clases de instancias de base de datos db.m5	Puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL o MariaDB y utilicen las clases de instancia de base de datos db.r5. Para obtener más información, consulte Clase de instancia de base de datos.	18 de septiembre de 2018
Amazon RDS ahora admite actualizaciones a SQL Server 2017	Puede actualizar sus instancias de base de datos existentes a SQL Server 2017 desde cualquier versión salvo SQL Server 2008. Para actualizar desde SQL Server 2008, primero actualice a una de las otras versiones. Para obtener más información, consulte Actualización del motor de base de datos Microsoft SQL Server.	11 de septiembre de 2018

Amazon RDS for PostgreSQL ahora es compatible con PostgreSQL versión 11 Beta 3 en el entorno de vista previa de base de datos.	En esta versión, el segmento de registro de escritura previa (WAL) (wal_segment_size) ahora se establece en 64 MB. Para obtener más información sobre PostgreSQL versión 11 Beta 3, consulte PostgreSQL 11 Beta 3 Released. Para obtener más información acerca del entorno de vista previa de base de datos, consulte Trabajo con el entorno de vista previa de base de datos.	7 de septiembre de 2018
Guía del usuario de Amazon Aurora	La Guía del usuario de Amazon Aurora describe todos los conceptos de Amazon Aurora y contiene instrucciones acerca de cómo utilizar las diferentes características con la consola y la interfaz de línea de comandos. Esta Guía del usuario de Amazon RDS cubre motores de base de datos que no sean de Aurora.	31 de agosto de 2018
La información sobre rendimiento de Amazon RDS está disponible para RDS para MySQL	La información sobre rendimiento de Amazon RDS ahora está disponible para RDS para MySQL. Para obtener más información, consulte Uso de Performance Insights de Amazon RDS.	28 de agosto de 2018

Ahora Edición compatible con Aurora PostgreSQL admite Aurora Auto Scaling	Las réplicas de Auto Scaling de Aurora ahora está disponible para Edición compatible con Aurora PostgreSQL. Para obtener más información, consulte Uso de Amazon Aurora Auto Scaling con réplicas de Aurora.	16 de agosto de 2018
Aurora Serverless para Aurora MySQL	Aurora Serverless es una configuración de escalado automático bajo demanda para Amazon Aurora. Para obtener más información, consulte Uso de Amazon Aurora Serverless.	9 de agosto de 2018
MySQL 5.7.22 y 5.6.40	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 5.7.22 y 5.6.40 de MySQL. Para obtener más información, consulte MySQL en versiones de Amazon RDS.	6 de agosto de 2018
Aurora está ahora disponible en la región China (Ningxia)	Aurora MySQL y Aurora PostgreSQL están ahora disponibles en la región China (Ningxia). Para obtener más información, consulte Disponibilidad de Amazon Aurora MySQL y Disponibilidad de Amazon Aurora PostgreSQL.	6 de agosto de 2018

Amazon RDS for MySQL admite la replicación retrasada	Ahora, Amazon RDS for MySQL admite la replicación retrasada como estrategia de recuperación de desastres. Para obtener más información, consulte Configuración de la replicación retrasada con MySQL.	6 de agosto de 2018
Performance Insights de Amazon RDS está disponible para Aurora MySQL	Performance Insights de Amazon RDS está disponible ahora para Aurora MySQL. Para obtener más información, consulte Uso de Performance Insights de Amazon RDS.	6 de agosto de 2018
Integración de Performance Insights de Amazon RDS con Amazon CloudWatch	Amazon RDS Performance Insights publica automáticamente las métricas en Amazon CloudWatch. Para obtener más información, consulte Métricas de Información sobre rendimiento publicadas en CloudWatch.	6 de agosto de 2018
Recomendaciones de Amazon RDS	Amazon RDS proporciona ahora recomendaciones automatizadas de recursos de la base de datos. Para obtener más información, consulte Usar recomendaciones de Amazon RDS.	25 de julio de 2018

Copias de instantáneas incrementales en las regiones de AWS	Amazon RDS admite copias de instantáneas progresivas en las regiones de AWS tanto para las instancias sin cifrar como para las cifradas. Para obtener más información, consulte Copia de instantáneas en distintas regiones de AWS.	24 de julio de 2018
Performance Insights de Amazon RDS está disponible para Amazon RDS for PostgreSQL	Performance Insights de Amazon RDS ya está disponible para Amazon RDS para PostgreSQL. Para obtener más información, consulte Uso de Performance Insights de Amazon RDS.	18 de julio de 2018
Amazon RDS para Oracle admite Oracle APEX versión 5.1.4.v1	Amazon RDS para Oracle ya admite Oracle Application Express (APEX) versión 5.1.4.v1. Para obtener más información, consulte Oracle Application Express.	10 de julio de 2018
Amazon RDS para Oracle admite la publicación de registros en registros de Amazon Cloudwatch	Amazon RDS para Oracle ya admite la publicación de datos de registro de alertas, auditoría, seguimiento y escuchas en un grupo de registros en CloudWatch Logs. Para obtener más información, consulte Publicación de registros de Oracle en registros de Amazon Cloudwatch.	9 de julio de 2018

MariaDB 10.2.15, 10.1.34 y 10.0.35	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.2.15, 10.1.34 y 10.0.35 de MariaDB. Para obtener más información, consulte MariaDB en versiones de Amazon RDS.	5 de julio de 2018
Aurora PostgreSQL 1.2 está disponible y es compatible con PostgreSQL 9.6.8	Aurora PostgreSQL 1.2 ahora está disponible y es compatible con PostgreSQL 9.6.8. Para obtener más información, consulte Versión 1.2.	27 de junio de 2018
Las réplicas de lectura de Amazon RDS PostgreSQL son compatibles con implementaciones Multi-AZ	Las réplicas de lectura de RDS en Amazon RDS PostgreSQL ahora son compatibles con varias zonas de disponibilidad. Para obtener más información, consulte Uso de réplicas de lectura de PostgreSQL.	25 de junio de 2018
Performance Insights está disponible para Aurora PostgreSQL	Performance Insights está disponible con carácter general para Aurora PostgreSQL y ahora es compatible con la retención ampliada de datos de desempeño. Para obtener más información, consulte Uso de Información sobre rendimiento de Amazon RDS.	21 de junio de 2018

Aurora PostgreSQL está disponible en la región EE. UU. Oeste (Norte de California)	Aurora PostgreSQL está disponible ahora en la región EE.UU. Oeste (Norte de California). Para obtener más información, consulte Disponibilidad de Amazon Aurora PostgreSQL.	11 de junio de 2018
Amazon RDS para Oracle ahora admite la configuración de CPU	Amazon RDS para Oracle permite configurar el número de núcleos de CPU y el número de subprocesos de cada núcleo del procesador como una clase de instancia s de base de datos. Para obtener más información, consulte Configuración del procesador de la clase de instancias de base de datos.	5 de junio de 2018

Actualizaciones anteriores

En la siguiente tabla se describen los cambios importantes de cada versión de la Guía del usuario de Amazon RDS anteriores a junio de 2018.

Cambio	Descripción	Fecha de modificación
Amazon RDS para PostgreSQ L admite ahora PostgreSQL Versión 11 Beta 1 en el entorno de vista previa de base de datos	PostgreSQL versión 11 Beta 1 contiene varias mejoras que se describen en PostgreSQL 11 Beta 1 Released. Para obtener información acerca del entorno de vista previa de base de datos, consulte Trabajo con el entorno de vista previa de bases de datos.	31 de mayo de 2018

Cambio	Descripción	Fecha de modificación
Amazon RDS para Oracle ahora admite TLS versiones 1.0 y 1.2	Amazon RDS para Oracle supports Transport Layer Security (TLS) versiones 1.0 y 1.2. Para obtener más información, consulte Versiones de TLS para la opción Oracle SSL.	30 de mayo de 2018
Aurora MySQL admite la publicación de registros en registros de Amazon Cloudwatch	Aurora MySQL ahora admite la publicación de datos de registro general, lento, de auditoría y error en un grupo de registro en CloudWatch Logs. Para obtener más información, consulte Publicar Aurora MySQL en CloudWatch Logs.	23 de mayo de 2018
Entorno de vista previa de base de datos para Amazon RDS PostgreSQL	Ahora puede lanzar una nueva instancia de Amazon RDS PostgreSQL en un modo de vista previa. Para obtener más información acerca del entorno de vista previa de base de datos, consult, Trabajo con el entorno de vista previa de bases de datos.	22 de mayo de 2018
Las instancias de base de datos de Amazon RDS para Oracle admite clases de instancia de base de datos nuevas.	Las instancias de base de datos de Oracle ahora admiten las clases de instancia de base de datos db.x1e y db.x1. Para obtener más información, consulte Clases de instancia de base de datos de y Clases de instancias de base de datos de RDS para Oracle.	22 de mayo de 2018
Amazon RDS PostgreSQL ahora es compatible con postgres_fdw en una réplica de lectura.	Ahora puede utilizar postgres_fdw para conectarse a un servidor remoto desde una réplica de lectura. Para obtener más información, consulte, Uso de la extensión postgres_fdw para acceder a datos externos.	17 de mayo de 2018

Cambio	Descripción	Fecha de modificación
Amazon RDS para Oracle ahora admite la configuración de parámetros de sqlnet.ora	Ahora puede establecer parámetros de sqlnet.ora con Amazon RDS para Oracle. Para obtener más información, consulte Modificación de propiedades de conexión utilizando parámetros sqlnet.ora.	10 de mayo de 2018
Aurora PostgreSQL disponible en la región de Asia Pacífico (Seúl).	Aurora PostgreSQL ya está disponible en la región Asia Pacífico (Seúl). Para obtener más información, consulte Disponibilidad de Amazon Aurora PostgreSQL.	9 de mayo de 2018
Aurora MySQL admite búsqueda de datos anteriores	Aurora MySQL ahora admite "rebobinar" un clúster de bases de datos a un momento específico, sin restaurar datos desde una copia de seguridad. Para obtener más información, consulte Búsqueda de datos anteriores de un clúster de bases de datos de Aurora.	9 de mayo de 2018
Aurora MySQL admite la migración y replicación cifradas desde una base de datos MySQL externa	Aurora MySQL admite ahora la migración y replicación cifradas desde una base de datos MySQL externa. Para obtener más información, consulte Migración de datos desde una base de datos MySQL externa a un clúster de bases de datos de Amazon Aurora MySQL y Replicación entre Aurora y MySQL o entre Aurora y otro clúster de bases de datos de Aurora.	25 de abril de 2018
Edición compatible con Aurora PostgreSQL admite el protocolo Copy-on-Write.	Ahora puede clonar bases de datos en un clúster de bases de datos Aurora PostgreSQL. Para obtener más información, consulte Clonación de bases de datos en un clúster de bases de datos de Aurora.	10 de abril de 2018

Cambio	Descripción	Fecha de modificación
MariaDB 10.2.12, 10.1.31 y 10.0.34	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.2.12, 10.1.31 y 10.0.34 de MariaDB. Para obtener más información, consulte Versiones de MariaDB en Amazon RDS.	21 de marzo de 2018
Compatibilidad de Aurora PostgreSQL con regiones nuevas	Aurora PostgreSQL ya está disponible en las regiones UE (Londres) y Asia Pacífico (Singapur). Para obtener más información, consulte Disponibilidad de Amazon Aurora PostgreSQL.	13 de marzo de 2018
MySQL 5.7.21, 5.6.39 y 5.5.59	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 5.7.21, 5.6.39 y 5.5.59 de MySQL. Para obtener más información, consulte Versiones de MySQL en Amazon RDS.	9 de marzo de 2018
Amazon RDS para Oracle ahora admite Oracle REST Data Services	Amazon RDS para Oracle admite Oracle REST Data Services como parte de la opción de APEX. Para obtener más información, consulte Oracle Application Express.	9 de marzo de 2018
Amazon Aurora MyS Compatible Edition disponible en la nueva región de AWS	Aurora MySQL ahora está disponible en la región Asia Pacífico (Singapur). Para obtener una lista completa de las regiones de AWS para Aurora MySQL, consulte la disponibilidad para Amazon Aurora MySQL.	6 de marzo de 2018

Cambio	Descripción	Fecha de modificación
Las instancias de base de datos de Amazon RDS que ejecutan Microsoft SQL Server admiten la captura de datos de cambio (CDC)	Las instancias de base de datos que ejecutan Amazon RDS for Microsoft SQL Server ahora admiten la captura de datos de cambio (CDC). Para obtener más información, consulte Compatibilidad de captura de datos de cambio para instancias de base de datos de Microsoft SQL Server.	6 de febrero de 2018
Aurora MySQL admite una nueva versión principal	Ahora puede crear clústeres de base de datos de Aurora MySQL que ejecuten MySQL versión 5.7. Para obtener más información, consulte Actualizaciones del motor de base de datos de Amazon Aurora MySQL (06/02/2018).	6 de febrero de 2018
Publicación de logs de MySQL y MariaDB en registros de Amazon Cloudwatch	Ahora puede publicar datos de log de MySQL y MariaDB en CloudWatch Logs. Para obtener más información, consulte Publicación de registros de MySQL en Amazon CloudWatch Logs y Publicación de registros de MariaDB en Amazon CloudWatch Logs.	17 de enero de 2018
Compatibilidad con Multi-AZ para réplicas de lectura.	Ahora puede crear una réplica de lectura como instancia de base de datos Multi-AZ. Amazon RDS crea una réplica en espera en otra zona de disponibilidad para permitir la conmutación por error de la réplica. La creación de su réplica de lectura como instancia de base de datos Multi-AZ es independiente de si la base de datos de origen es una instancia de base de datos Multi-AZ. Para obtener más información, consulte Trabajo con réplicas de lectura de instancias de base de datos.	11 de enero de 2018

Cambio	Descripción	Fecha de modificación
Amazon RDS para MariaDB admite una nueva versión principal	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten MariaDB versión 10.2. Para obtener más información, consulte Compatibilidad con MariaDB 10.2 en Amazon RDS.	3 de enero de 2018
Amazon Aurora PostgreSQL-Compatible Edition disponible en la nueva región de AWS	Aurora PostgreSQL ya está disponible en la región UE (París). Para obtener una lista completa de las regiones de AWS para Aurora PostgreSQL, consulte la disponibilidad para Amazon Aurora PostgreSQL.	22 de diciembre de 2017
Aurora PostgreSQL admite tipos de instancia nuevos.	Aurora PostgreSQL ahora admite tipos de instancia nuevos. Para ver una lista completa de los tipos de instancias, consulte Selección de la clase de instancia de base de datos.	20 de diciembre de 2017
Amazon Aurora MySQL-Compatible Edition disponible en la nueva región de AWS	Aurora MySQL ya está disponible en la región UE (París). Para obtener una lista completa de las regiones de AWS para Aurora MySQL, consulte la disponibilidad para Amazon Aurora MySQL.	18 de diciembre de 2017
Aurora MySQL solo admite combinaciones hash	Esta característica puede mejorar el desempeño de las consultas si necesita unir una gran cantidad de datos mediante equijoin. Para obtener más información, consulte Trabajo con combinaciones hash en Aurora MySQL.	11 de diciembre de 2017
Aurora MySQL admite funciones nativas para invocar funciones de AWS Lambda	Puede llamar a las funciones nativas `lambda_sync` y `lambda_async` cuanto utilice Aurora MySQL. Para obtener más información, consulte Invocación de una función de Lambda desde un clúster de bases de datos de Amazon Aurora MySQL.	11 de diciembre de 2017

Cambio	Descripción	Fecha de modificación
Agregada la elegibilidad de Aurora PostgreSQL HIPAA	Ahora Aurora PostgreSQL admite la creación de aplicaciones conformes con HIPAA. Para obtener más información, consulte Trabajar con Amazon Aurora PostgreSQL.	6 de diciembre de 2017
Regiones de AWS adicionales disponibles para Amazon Aurora compatibles con PostgreSQL	La compatibilidad de Amazon Aurora con PostgreSQL ahora está disponible en cuatro nuevas regiones de AWS. Para obtener más información, consulte Disponibilidad de Amazon Aurora PostgreSQL.	22 de noviembre de 2017
Modificación del almacenamiento para instancias de base de datos de Amazon RDS que ejecuten Microsoft SQL Server	Ahora puede modificar el almacenamiento de las instancias de base de datos de Amazon RDS que ejecuten SQL Server. Para obtener más información, consulte Modificación de una instancia de base de datos de Amazon RDS.	21 de noviembre de 2017
Amazon RDS admite almacenamiento de 16 TiB para motores basados en Linux-based	Ahora puede crear instancias de base de datos de MySQL, MariaDB, PostgreSQL y Oracle RDS con hasta 16 TiB de almacenamiento. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.	21 de noviembre de 2017
Amazon RDS admite el escalado rápido del almacenamiento	Ahora puede añadir almacenamiento a instancias de base de datos de MySQL, MariaDB, PostgreSQL y Oracle RDS en pocos minutos. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.	21 de noviembre de 2017

Cambio	Descripción	Fecha de modificación
Amazon RDS admite las versiones 10.1.26 y 10.0.32 de MariaDB	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.1.26 y 10.0.32 de MariaDB. Para obtener más información, consulte Versiones de MariaDB en Amazon RDS.	20 de noviembre de 2017
Amazon RDS for Microsoft SQL Server ahora admite nuevas clases de instancia de base de datos	Puede crear instancias de base de datos de Amazon RDS que ejecuten SQL Server y utilicen las clases de instancia de base de datos db.r4 y db.m4.16xlarge. Para obtener más información, consulte Compatibilidad con clases de instancia de base de datos para Microsoft SQL Server.	20 de noviembre de 2017
Amazon RDS for MySQL y MariaDB ahora admite nuevas clases de instancia de base de datos	Puede crear instancias de base de datos de Amazon RDS que ejecuten MySQL y MariaDB y utilicen las clases de instancia de base de datos db.r4, db.m4.16xlarge db.t2.xlarge y db.t2.2xlarge. Para obtener más información, consulte Clases de instancia de base de datos de .	20 de noviembre de 2017
SQL Server 2017	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten Microsoft SQL Server 2017. También puede crear instancias de base de datos que ejecuten SQL Server 2016 SP1 CU5. Para obtener más información, consulte Amazon RDS for Microsoft SQL Server.	17 de noviembre de 2017

Cambio	Descripción	Fecha de modificación
Restaurar copias de seguridad de MySQL desde Amazon S3	Ahora puede crear una copia de seguridad de una base de datos local, almacenarlo en Amazon S3 y luego restaurar el archivo de copia de seguridad en una nueva instancia de base de datos de Amazon RDS que ejecute MySQL. Para obtener más informaci ón, consulte Restauración de una copia de seguridad en una instancia de base de datos MySQL..	17 de noviembre de 2017
Auto Scaling con réplicas de Aurora	Ahora Amazon Aurora MySQL admite Auto Scaling de Aurora. Auto Scaling de Aurora ajusta de forma dinámica el número de réplicas de Aurora en función del aumento o la disminución en la conectividad o la carga de trabajo. Para obtener más información, consulte Uso de Amazon Aurora Auto Scaling con réplicas de Aurora.	17 de noviembre de 2017
Soporte de la edición predeterm inada de Oracle	Las instancias de base de datos de Amazon RDS para Oracle ahora admiten la configuración de la edición predeterminada para la instancia de base de datos. Para obtener más información, consulte Configuración de la edición predeterminada para una instancia de base de datos.	3 de noviembre de 2017
Validación de archivos de instancias de base de datos de Oracle	Las instancias de base de datos de Amazon RDS para Oracle ahora admiten la validación de archivos de instancias de base de datos con la utilidad de validación lógica Oracle Recovery Manager (RMAN). Para obtener más información, consulte Validación de archivos de base de datos en RDS para Oracle .	3 de noviembre de 2017

Cambio	Descripción	Fecha de modificación
Management Agent para OEM 13c	Las instancias de base de datos de Amazon RDS para Oracle ahora admite Management Agent for Oracle Enterprise Manager (OEM) Cloud Control 13c. Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.	1 de noviembre de 2017
Reconfiguración del almacenamiento para las instantáneas de Microsoft SQL Server	Ahora puede reconfigurar el almacenamiento cuando restaura una instantánea a una instancia de base de datos de Amazon RDS en la que se ejecuta Microsoft SQL Server. Para obtener más información, consulte Restauración a una instancia de base de datos.	26 de octubre de 2017
Captura previa de clave asíncrona para Edición compatible con Aurora MySQL	La captura previa de clave asíncrona (AKP) mejora el desempeño de las combinaciones de índices sin almacenar en caché; para ello, efectúa una captura previa de las claves en la memoria antes de que sean necesarias. Para obtener más información, consulte Uso de la captura previa de clave asíncrona en Amazon Aurora.	26 de octubre de 2017
MySQL 5.7.19, 5.6.37 y 5.5.57	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 5.7.19, 5.6.37 y 5.5.57 de MySQL. Para obtener más información, consulte Versiones de MySQL en Amazon RDS.	25 de octubre de 2017
Disponibilidad general de Amazon Aurora compatible con PostgreSQL	Amazon Aurora compatible con PostgreSQL simplifica y hace más rentable configurar, usar y escalar las implementaciones de PostgreSQL nuevas y existentes, lo que le permitirá centrarse en su negocio y sus aplicaciones. Para obtener más información, consulte Trabajar con Amazon Aurora PostgreSQL.	24 de octubre de 2017

Cambio	Descripción	Fecha de modificación
Las instancias de base de datos de Amazon RDS para Oracle admite clases de instancia de base de datos nuevas.	Las instancias de base de datos de Amazon RDS para Oracle ahora admiten la nueva generación de clases de instancias de nueva generación (db.r4) optimizadas para memoria. Las instancias de base de datos de Amazon RDS para Oracle ahora también admiten las siguientes clases de instancia nuevas de la generación actual: db.m4.16xlarge, db.t2.xlarge y db.t2.2xlarge. Para obtener más información, consulte Clases de instancia de base de datos de y Clases de instancias de base de datos de RDS para Oracle.	23 de octubre de 2017
Nueva característica	Las instancias reservadas nuevas y existentes pueden ahora cubrir múltiples tamaños en la misma clase de instancia de base de datos. Las instancias reservadas con flexibilidad de tamaño están disponibles para las instancias de base de datos con la misma región de AWS, motor de base de datos y familia de instancias, así como en toda la configuración AZ. Las instancias reservadas con flexibilidad de tamaño están disponibles para los siguientes motores de base de datos: Amazon Aurora, MariaDB, MySQL, Oracle (Bring Your Own License) y PostgreSQL. Para obtener más información, consulte Flexibilidad del tamaño de las instancias de base de datos reservadas.	11 de octubre de 2017
Nueva característica	Ahora puede usar la opción Oracle SQLT para ajustar una instrucción SQL y obtener un desempeño óptimo. Para obtener más información, consulte Oracle SQLT.	22 de septiembre de 2017

Cambio	Descripción	Fecha de modificación
Nueva caracterí stica	Si tiene instantáneas de base de datos manuales existentes de sus instancias de base de datos de Amazon RDS para Oracle, ahora puede actualiza rlas a una versión posterior del motor de base de datos Oracle. Para obtener más información, consulte Actualización de una instantánea de base de datos de Oracle.	20 de septiembre de 2017
Nueva caracterí stica	Ahora puede utilizar la opción Oracle Spatial para almacenar, recuperar, actualizar y consultar datos espaciales en las instancias de base de datos de Amazon RDS en las que se ejecuta Oracle. Para obtener más información, consulte Oracle Spatial.	15 de septiembre de 2017
Nueva caracterí stica	Ahora puede utilizar Oracle Locator para admitir aplicaciones basadas en servicio de Internet e inalámbricas y soluciones de Sistemas de informaci ón geográfica (SIG) basadas en el partner con las instancias de base de datos de Amazon RDS en las que se ejecuta Oracle. Para obtener más información, consulte Oracle Locator.	15 de septiembre de 2017
Nueva caracterí stica	Ahora puede utilizar la opción Oracle Multimedia para almacenar, administrar y recuperar imágenes, audios y vídeos, y otros datos de medios heterogéneos en las instancias de base de datos de Amazon RDS en las que se ejecuta Oracle.	15 de septiembre de 2017
Nueva caracterí stica	Ahora puede exportar registros de auditoría desde los clústeres de base de datos Amazon Aurora MySQL a registros de Amazon Cloudwatch. Para más informaci ón, consulte Publicación de registros de Aurora MySQL en registros de Amazon Cloudwatch.	14 de septiembre de 2017

Cambio	Descripción	Fecha de modificación
Nueva característica	Amazon RDS admite ahora múltiples versiones de Oracle Application Express (APEX) para las instancias de base de datos en las que se ejecuta Oracle. Para obtener más información, consulte Oracle Application Express.	13 de septiembre de 2017
Nueva característica	Ahora puede utilizar Amazon Aurora para migrar una instantánea de base de datos no cifrada o cifrada, o una instancia de base de datos de MySQL a un clúster de bases de datos de MySQL de Aurora cifrado. Para obtener más información, consulte Migración de una instantánea de RDS para MySQL a Aurora y Migración de datos desde una instancia de base de datos de MySQL a un clúster de bases de datos de Amazon Aurora MySQL mediante una réplica de lectura de Aurora.	5 de septiembre de 2017
Nueva característica	Puede utilizar bases de datos de Amazon RDS for Microsoft SQL Server para crear aplicaciones compatibles con HIPAA. Para obtener más información, consulte Compatibilidad con el programa de conformidad de las instancias de base de datos de Microsoft SQL Server.	31 de agosto de 2017
Nueva característica	Ahora puede utilizar bases de datos de Amazon RDS para MariaDB para crear aplicaciones compatibles con HIPAA. Para obtener más información, consulte Amazon RDS para MariaDB.	31 de agosto de 2017

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede crear instancias de base de datos de Amazon RDS en las que se ejecuta Microsoft SQL Server con un almacenamiento asignado de hasta 16 TiB e IOPS provisionadas para intervalos de almacenamiento de 1:1-50:1. Para obtener más información, consulte Almacenamiento de instancias de base de datos de Amazon RDS.	22 de agosto de 2017
Nueva característica	Ahora puede usar los despliegues Multi-AZ para instancias de base de datos en las que se ejecuta Microsoft SQL Server en la región de la UE (Fráncfort). Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.	3 de agosto de 2017
Nueva característica	Ahora puede crear instancias de base de datos de Amazon RDS que ejecuten las versiones 10.1.23 y 10.0.31 de MariaDB. Para obtener más información, consulte Versiones de MariaDB en Amazon RDS.	17 de julio de 2017
Nueva característica	Amazon RDS admite ahora Microsoft SQL Server Enterprise Edition con el modelo de licencia incluida en todas las regiones de AWS. Para obtener más información, consulte Licencias de Microsoft SQL Server en Amazon RDS.	13 de julio de 2017

Cambio	Descripción	Fecha de modificación
Nueva característica	Amazon RDS para Oracle admite ahora páginas de gran tamaño del kernel de Linux para aumentar la escalabilidad de la base de datos. El uso de páginas de gran tamaño deriva en tablas de páginas más pequeñas y menos tiempo dedicado por la CPU a la administración de memoria, lo que aumenta el desempeño de instancias de base de datos grandes. Puede utilizar páginas enormes con sus instancias de base de datos de Amazon RDS en las que se ejecutan todas las ediciones de Oracle, versiones 12.1.0.2 y 11.2.0.4. Para obtener más información, consulte Activación de páginas de gran tamaño para una instancia de RDS para Oracle.	7 de julio de 2017
Nueva característica	Se ha actualizado para admitir el cifrado en reposo (EAR) para clases de instancia de base de datos db.t2.small y db.t2.medium para todos los motores de base de datos que no sean de Aurora. Para obtener más información, consulte Disponibilidad del cifrado de Amazon RDS.	27 de junio de 2017
Nueva característica	Se ha actualizado para admitir Amazon Aurora en la región Europa (Fráncfort). Para obtener más información, consulte Disponibilidad de Amazon Aurora MySQL.	16 de junio de 2017
Nueva característica	Ahora puede especificar un grupo de opciones al copiar una instantánea de base de datos entre regiones de AWS. Para obtener más información, consulte Aspectos a tener en cuenta sobre los grupos de opciones.	12 de junio de 2017

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede copiar instantáneas de base de datos creadas a partir de instancias de base de datos especializadas entre regiones de AWS. Puede copiar instantáneas de instancias de base de datos que utilizan TDE de Oracle, TDE de Microsoft SQL Server y Multi-AZ de Microsoft SQL Server con creación de reflejo. Para obtener más información, consulte Copia de una instantánea de base de datos.	12 de junio de 2017
Nueva característica	Amazon Aurora permite ahora copiar de una forma rápida y rentable todas sus bases de datos en clúster de bases de datos Amazon Aurora. Para obtener más información, consulte Clonación de bases de datos en un clúster de bases de datos de Aurora.	12 de junio de 2017
Nueva característica	Amazon RDS admite ahora Microsoft SQL Server 2016 SP1 CU2. Para obtener más información, consulte Amazon RDS for Microsoft SQL Server.	7 de junio de 2017
Vista previa	Versión preliminar pública de Amazon Aurora compatible con PostgreSQL. Para obtener más información, consulte Trabajar con Amazon Aurora PostgreSQL.	19 de abril de 2017
Nueva característica	Amazon Aurora permite ahora ejecutar una operación ALTER TABLE tbl_name ADD COLUMN col_name column_definition de manera casi instantánea. La operación se completa sin que sea necesario copiar la tabla y sin que haya un impacto material en otras instrucciones DML. Para obtener más información, consulte Modificación de las tablas de Amazon Aurora con operaciones DDL rápidas.	5 de abril de 2017

Cambio	Descripción	Fecha de modificación
Nueva caracterí stica	Hemos agregado un nuevo comando de monitoriz ación, SHOW VOLUME STATUS, para mostrar el número de nodos y discos en un volumen. Para obtener más información, consulte Visualización del estado del volumen para un clúster de bases de datos de Aurora.	5 de abril de 2017
Nueva caracterí stica	Ahora puede utilizar su propia lógica predeterm inada en las funciones de verificación de contraseñ a predeterminada para Oracle en Amazon RDS. Para obtener más información, consulte Creación de funciones personalizadas para comprobar contraseñ as.	21 de marzo de 2017
Nueva caracterí stica	Ahora puede obtener acceso a los archivos de registro REDO archivados y online en las instancias de base de datos de Oracle en Amazon RDS. Para obtener más información, consulte Acceso a los registros de rehacer en línea y archivados.	21 de marzo de 2017
Nueva caracterí stica	Ahora puede copiar instantáneas de clúster de bases de datos cifradas y sin cifrar entre cuentas en la misma región. Para obtener más información, consulte Copia de una instantánea de clúster de bases de datos entre cuentas.	7 de marzo de 2017
Nueva caracterí stica	Ahora puede compartir instantáneas de clúster de bases de datos cifradas entre cuentas en la misma región. Para obtener más información, consulte Compartir una instantánea de clúster de bases de datos.	7 de marzo de 2017

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede replicar clústeres de base de datos de Amazon Aurora MySQL cifrados para crear réplicas de Aurora entre regiones. Para obtener más información, consulte la reproducción de clústeres de base de datos de Aurora MySQL entre distintas regiones de AWS.	7 de marzo de 2017
Nueva característica	Ahora puede exigir que todas las conexiones a su instancia de base de datos que ejecute Microsoft SQL Server utilicen Capa de conexión segura (SSL). Para obtener más información, consulte ???.	27 de febrero de 2017
Nueva característica	Ahora hay 15 zonas horarias adicionales para establecer su zona horaria local. Para obtener más información, consulte Zonas horarias admitidas.	27 de febrero de 2017
Nueva característica	Ahora es posible utilizar el procedimiento Amazon RDS de `msdb.dbo.rds_shrink_tempdbfile` para reducir la base de datos tempdb en las instancias de base de datos en las que se ejecuta Microsoft SQL Server. Para obtener más información, consulte Reducción del tamaño de la base de datos tempdb.	17 de febrero de 2017
Nueva característica	Ahora puede comprimir el archivo de copia de seguridad cuando exporta la base de datos Microsoft SQL Server Enterprise and Standard Edition, desde una instancia de base de datos de Amazon RDS a Amazon S3. Para obtener más información, consulte Compresión de archivos de copia de seguridad.	17 de febrero de 2017

Cambio	Descripción	Fecha de modificación
Nueva característica	Amazon RDS admite ahora servidores DNS personalizados para resolver nombres DNS utilizados en el acceso de red de salida en las instancias de base de datos en las que se ejecuta Oracle. Para obtener más información, consulte Configuración de un servidor DNS personalizado.	26 de enero de 2017
Nueva característica	Amazon RDS ahora es compatible con la creación de una réplica de lectura cifrada en otra región. Para obtener más información, consulte Creación de una réplica de lectura en una Región de AWS distinta y CreateDBInstanceReadReplica.	23 de enero de 2017
Nueva característica	Amazon RDS ahora permite actualizar una instantánea de base de datos de MySQL desde MySQL 5.1 a MySQL 5.5.	20 de enero de 2017
Nueva característica	Amazon RDS admite ahora copiar una instantánea de base de datos cifrada en otra región para los motores de base de datos MariaDB, MySQL, Oracle, PostgreSQL y Microsoft SQL Server. Para obtener más información, consulte Copia de una instantánea de base de datos y CopyDBSnapshot.	20 de diciembre de 2016
Nueva característica	Amazon Aurora MySQL admite ahora indexación espacial. La indexación espacial mejora el desempeño de las consultas en conjuntos de datos grandes, para consultas que usan datos espaciales. Para obtener más información, consulte Amazon Aurora MySQL y datos espaciales.	14 de diciembre de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Amazon RDS admite ahora el acceso de red de salida en las instancias de base de datos en las que se ejecuta Oracle. Puede utilizar utl_http, utl_tcp y utl_smtp para conectarse a la red desde la instancia de base de datos. Para obtener más información, consulte Configuración del acceso UTL_HTTP mediante certificados y un wallet de Oracle..	5 de diciembre de 2016
Nueva característica	Amazon RDS ha retirado la compatibilidad con la versión 5.1 de MySQL. Sin embargo, puede restaurar instantáneas de MySQL 5.1 existentes a una instancia de MySQL 5.5. Para obtener más información, consulte Motores de almacenamiento admitidos por RDS for MySQL.	15 de noviembre de 2016
Nueva característica	Amazon RDS admite ahora Microsoft SQL Server 2016 RTM CU2. Para obtener más información, consulte Amazon RDS for Microsoft SQL Server.	4 de noviembre de 2016
Nueva característica	Amazon RDS admite ahora actualizaciones de versiones principales para las instancias de base de datos en las que se ejecuta Oracle. Ahora puede actualizar sus instancias de base de datos Oracle 11g a 12c. Para obtener más información, consulte Actualización del motor de base de datos de RDS para Oracle.	2 de noviembre de 2016
Nueva característica	Ahora puede crear instancias de base de datos que ejecuten Microsoft SQL Server 2014 Enterprise Edition. Amazon RDS admite ahora SQL Server 2014 SP2 para todas las ediciones y todas las regiones. Para obtener más información, consulte Amazon RDS for Microsoft SQL Server.	25 de octubre de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Amazon Aurora MySQL se integra ahora con otros servicios de AWS. Puede cargar datos de texto o XML en una tabla desde un bucket de Amazon S3 o invocar una función de AWS Lambda desde el código de la base de datos. Para obtener más información, consulte la integración de Aurora MySQL con otros servicios de AWS.	18 de octubre de 2016
Nueva característica	Ahora es posible obtener acceso a la base de datos tempdb de las instancias de base de datos de Amazon RDS en las que se ejecuta Microsoft SQL Server. Puede obtener acceso a la base de datos tempdb mediante Transact-SQL a través de Microsoft SQL Server Management Studio (SSMS) o cualquier otra aplicación cliente estándar de SQL. Para obtener más información, consulte Acceso a la base de datos tempdb de las instancias de bases de datos de Microsoft SQL Server en Amazon RDS.	29 de septiembre de 2016
Nueva característica	Ahora puede utilizar el paquete UTL_MAIL con sus instancias de base de datos de Amazon RDS en las que se ejecuta Oracle. Para obtener más información, consulte Oracle UTL_MAIL.	20 de septiembre de 2016
Nuevas características	Ahora puede establecer la zona horaria de sus nuevas instancias de base de datos de Microsoft SQL Server en una hora local para que coincida con la zona horaria de sus aplicaciones. Para obtener más información, consulte Zona horaria local para las instancias de base de datos de Microsoft SQL Server.	19 de septiembre de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede utilizar la opción Oracle Label Security para controlar el acceso a filas de tablas individuales en las instancias de base de datos de Amazon RDS en las que se ejecuta Oracle Database 12c. Con Oracle Label Security, puede aplicar la conformidad normativa con un modelo de administración basado en políticas y garantizar que el acceso a la información confidencial se restrinja únicamente a los usuarios con el nivel adecuado. Para obtener más información, consulte Oracle Label Security.	8 de septiembre de 2016
Nueva característica	Ahora es posible conectarse a un clúster de bases de datos Amazon Aurora mediante el punto de enlace del lector, el cual equilibra la carga de las conexiones entre las réplicas de Aurora que están disponibles en un clúster de bases de datos. A medida que los clientes solicitan nuevas conexiones al punto de enlace del lector, Aurora distribuye las solicitudes de conexión entre las réplicas de Aurora del clúster de bases de datos. Esta funcionalidad puede ayudar a equilibrar la carga de trabajo de lectura entre las distintas réplicas de Aurora del clúster de bases de datos. Para obtener más información, consulte Puntos de enlace de Amazon Aurora.	8 de septiembre de 2016
Nueva característica	Sus instancias de base de datos de Amazon RDS en las que se ejecuta Oracle son ahora compatibles con Oracle Enterprise Manager Cloud Control. Puede habilitar Management Agent en sus instancias de base de datos y compartir datos con Oracle Management Service (OMS). Para obtener más información, consulte Oracle Management Agent para Enterprise Manager Cloud Control.	1 de septiembre de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Esta versión incorpora compatibilidad para obtener un ARN para un recurso. Para obtener más información, consulte Obtención de un ARN existente para Amazon RDS.	23 de agosto de 2016
Nueva característica	Ahora puede asignar hasta 50 etiquetas para cada recurso de Amazon RDS para administrar recursos y hacer un seguimiento de los costos. Para obtener más información, consulte Etiquetado de los recursos de y Amazon RDS.	19 de agosto de 2016
Nueva característica	Amazon RDS admite ahora el modelo con licencia incluida para Oracle Standard Edition Two. Para obtener más información, consulte Creación de una instancia de base de datos de Amazon RDS. Ahora es posible cambiar el modelo de licencia de las instancias de base de datos de Amazon RDS en las que se ejecutan Microsoft SQL Server y Oracle. Para obtener más información, consulte Licencias de Microsoft SQL Server en Amazon RDS y Opciones de licencias de RDS para Oracle.	5 de agosto de 2016
Nueva característica	Amazon RDS admite ahora la copia de seguridad y la restauración nativos de bases de datos Microsoft SQL Server mediante los archivos de copia de seguridad completos (archivos .bak). Ahora puede migrar fácilmente bases de datos de SQL Server a Amazon RDS, así como importar y exportar bases de datos a un único archivo fácil de transportar mediante Amazon S3 para el almacenamiento y AWS KMS para el cifrado. Para obtener más información, consulte Importación y exportación de bases de datos de SQL Server por copias de seguridad y restauración nativas.	27 de julio de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede copiar los archivos de origen de una base de datos MySQL en un bucket de Amazon Simple Storage Service (Amazon S3) y, a continuación, restablecer un clúster de bases de datos Amazon Aurora a partir de dichos archivos. Esta opción puede ser bastante más rápida que migrar los datos con `mysqldump` . Para obtener más información, consulte Migración de datos desde una base de datos MySQL externa a un clúster de bases de datos de Aurora MySQL.	20 de julio de 2016
Nueva característica	Ahora puede restaurar una instantánea de clúster de bases de datos Amazon Aurora sin cifrar para crear un clúster de Amazon Aurora cifrado incluyendo una clave de cifrado de AWS Key Management Service (AWS KMS) durante la operación de restauración. Para obtener más información, consulte Cifrado de recursos de Amazon RDS.	30 de junio de 2016
Nueva característica	Puede utilizar la Repository Creation Utility (RCU) de Oracle para crear un repositorio en Amazon RDS para Oracle. Para obtener más información, consulte Uso de Oracle Repository Creation Utility en RDS para Oracle .	17 de junio de 2016
Nueva característica	Agrega compatibilidad con las réplicas de lectura entre regiones de PostgreSQL. Para obtener más información, consulte Creación de una réplica de lectura en una Región de AWS distinta.	16 de junio de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede usar la AWS Management Console para agregar fácilmente Multi-AZ con creación de reflejo a una instancia de base de datos de Microsoft SQL Server. Para obtener más información, consulte Adición de implementaciones Multi-AZ a una instancia de base de datos de Microsoft SQL Server.	9 de junio de 2016
Nueva característica	Ahora puede usar implementaciones Multi-AZ mediante la creación de reflejo de SQL Server en las siguientes regiones adicionales: Asia Pacífico (Sídney), Asia Pacífico (Tokio) y América del Sur (São Paulo). Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.	9 de junio de 2016
Nueva característica	Se ha actualizado para admitir la versión 10.1 de MariaDB. Para obtener más información, consulte Amazon RDS para MariaDB.	1 de junio de 2016
Nueva característica	Se ha actualizado para admitir clústeres de base de datos entre regiones de Amazon Aurora que sean réplicas de lectura. Para obtener más información, consulte la reproducción de clústeres de base de datos de Aurora MySQL entre distintas regiones de AWS.	1 de junio de 2016
Nueva característica	La monitorización mejorada ya está disponible para instancias de base de datos de Oracle. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada y Modificación de una instancia de base de datos de Amazon RDS.	27 de mayo de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir el uso compartido de instantáneas manuales para instantáneas de clúster de bases de datos Amazon Aurora. Para obtener más información, consulte Compartir una instantánea de clúster de bases de datos.	18 de mayo de 2016
Nueva característica	Ahora puede utilizar MariaDB Audit Plugin para registrar actividad de base de datos en instancias de base de datos MariaDB y MySQL. Para obtener más información, consulte Opciones para el motor de base de datos de MariaDB y Opciones para las instancias de bases de datos MySQL.	27 de abril de 2016
Nueva característica	Hay actualizaciones in situ de versiones principales disponibles para la actualización de la versión 5.6 a la versión 5.7 de MySQL. Para obtener más información, consulte Actualizaciones del motor de base de datos de RDS para MySQL.	26 de abril de 2016
Nueva característica	La monitorización mejorada ya está disponible para instancias de base de datos de Microsoft SQL Server. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.	22 de abril de 2016
Nueva característica	Se ha actualizado para proporcionar una vista clústers (Clústeres) de Amazon Aurora en la consola de Amazon RDS. Para obtener más información, consulte Visualización de un clúster de bases de datos de Aurora.	1 de abril de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir Multi-AZ de SQL Server con creación de reflejo en la región Asia Pacífico (Seúl). Para obtener más información, consulte Implementaciones Multi-AZ para Amazon RDS for Microsoft SQL Server.	31 de marzo de 2016
Nueva característica	Se ha actualizado para admitir Multi-AZ de Amazon Aurora con creación de reflejo en la región Asia Pacífico (Seúl). Para obtener más información, consulte Disponibilidad de Amazon Aurora MySQL.	31 de marzo de 2016
Nueva característica	Las instancias de base de datos PostgreSQL pueden exigir que las conexiones usen SSL. Para obtener más información, consulte Uso de SSL con una instancia de base de datos PostgreSQL.	25 de marzo de 2016
Nueva característica	La monitorización mejorada ya está disponible para instancias de base de datos PostgreSQL. Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.	25 de marzo de 2016
Nueva característica	Las instancias de base de datos de Microsoft SQL Server pueden usar ahora autenticación de Windows para autenticar usuarios. Para obtener más información, consulte Uso de AWS Managed Active Directory con RDS para SQL Server.	23 de marzo de 2016
Nueva característica	La monitorización mejorada está disponible en la región Asia Pacífico (Seúl). Para obtener más información, consulte Supervisión de las métricas del sistema operativo con Supervisión mejorada.	16 de marzo de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Ahora puede personalizar el orden en que se promueven las réplicas de Aurora a instancia primaria durante una conmutación por error. Para obtener más información, consulte Tolerancia a errores para un clúster de bases de datos de Aurora.	14 de marzo de 2016
Nueva característica	Se ha actualizado para admitir el cifrado al migrar a un clúster de bases de datos Aurora. Para obtener más información, consulte Migración de datos a un clúster de bases de datos de Aurora.	2 de marzo de 2016
Nueva característica	Se ha actualizado para admitir la zona horaria local para los clústeres de base de datos Aurora. Para obtener más información, consulte Zona horaria local para los clústeres de base de datos de Aurora.	1 de marzo de 2016
Nueva característica	Se ha actualizado para agregar compatibilidad con la versión 5.7 de MySQL para clases de instancia de base de datos de Amazon RDS de la generación actual.	22 de febrero de 2016
Nueva característica	Se ha actualizado para admitir clases de instancia de base de datos db.r3 y db.t2 en la región de AWS GovCloud (EE. UU. Oeste).	11 de febrero de 2016
Nueva característica	Se ha actualizado para admitir el cifrado de copias de instancia de base de datos y el uso compartido de instantáneas de base de datos cifradas. Para obtener más información, consulte Copia de una instantánea de base de datos para Amazon RDS y Uso compartido de una instantánea manual de base de datos de Amazon RDS.	11 de febrero de 2016

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir Amazon Aurora en la región Asia Pacífico (Sídney). Para obtener más información, consulte Disponibilidad de Amazon Aurora MySQL.	11 de febrero de 2016
Nueva característica	Se ha actualizado para admitir SSL para instancias de base de datos de Oracle. Para obtener más información, consulte Uso de SSL con una instancia de base de datos de RDS para Oracle.	9 de febrero de 2016
Nueva característica	Se ha actualizado para admitir la zona horaria local para instancias de base de datos MySQL y MariaDB. Para obtener más información, consulte Zona horaria local para las instancias de bases de datos MySQL y Zona horaria local para instancias de base de datos de MariaDB.	21 de diciembre de 2015
Nueva característica	Se ha actualizado para admitir la monitorización mejorada de métricas de SO para instancias de base de datos MySQL y MariaDB y clústeres de base de datos Aurora. Para obtener más información, consulte Consulta de métricas en la consola de Amazon RDS.	18 de diciembre de 2015
Nueva característica	Se ha actualizado para admitir clases de instancia de base de datos b.t2, db.r3 y db.m4 para la versión 5.5 de MySQL. Para obtener más información, consulte Clases de instancia de base de datos de .	4 de diciembre de 2015
Nueva característica	Se ha actualizado para admitir la modificación del puerto de base de datos para una instancia de base de datos existente.	3 de diciembre de 2015

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir actualizaciones de versiones principales del motor de base de datos para instancias de PostgreSQL. Para obtener más información, consulte Actualizaciones del motor de base de datos de RDS para PostgreSQL.	19 de noviembre de 2015
Nueva característica	Se ha actualizado para admitir la modificación de la accesibilidad pública de una instancia de base de datos existente. Se ha actualizado para admitir clases de instancia de base de datos estándar db.m4.	11 de noviembre de 2015
Nueva característica	Se ha actualizado para admitir el uso compartido de instantáneas de base de datos manuales. Para obtener más información, consulte Uso compartido de una instantánea manual de base de datos de Amazon RDS.	28 de octubre de 2015
Nueva característica	Se ha actualizado para admitir Microsoft SQL Server 2014 Web, Express y Standard.	26 de octubre de 2015
Nueva característica	Se ha actualizado para admitir el motor de base de datos MariaDB basado en MySQL. Para obtener más información, consulte Amazon RDS para MariaDB.	7 de octubre de 2015
Nueva característica	Se ha actualizado para admitir Amazon Aurora en la región Asia Pacífico (Tokio). Para obtener más información, consulte Disponibilidad de Amazon Aurora MySQL.	7 de octubre de 2015
Nueva característica	Se ha actualizado para admitir clases de instancia de base de datos con capacidad para ráfagas db.t2 para todos los motores de base de datos y la adición de la clase de instancia de base de datos db.t2.large. Para obtener más información, consulte Clases de instancia de base de datos de .	25 de septiembre de 2015

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir instancias de base de datos de Oracle en clases de instancia de base de datos estándar R3 and T2. Para obtener más información, consulte Clases de instancia de base de datos de .	5 de agosto de 2015
Nueva característica	Microsoft SQL Server Enterprise Edition está disponible ahora con el modelo de servicio de licencia incluida. Para obtener más información, consulte Licencias de Microsoft SQL Server en Amazon RDS.	29 de julio de 2015
Nueva característica	Se ha lanzado oficialmente Amazon Aurora. El motor de base de datos Amazon Aurora admite varias instancias de base de datos en un clúster de bases de datos. Para obtener información detallada, consulte ¿Qué es Amazon Aurora?.	27 de julio de 2015
Nueva característica	Se ha actualizado para admitir la copia de etiquetas en instantáneas de base de datos.	20 de julio de 2015
Nueva característica	Se ha actualizado para admitir aumentos en el tamaño de almacenamiento para todos los motores de base de datos y un aumento de IOPS provisionadas para SQL Server.	18 de junio de 2015
Nueva característica	Opciones actualizadas para instancias de base de datos reservadas.	15 de junio de 2015
Nueva característica	Se ha actualizado para admitir el uso de Amazon CloudHSM con instancias de base de datos de Oracle que utilizan TDE.	8 de enero de 2015
Nueva característica	Se ha actualizado para admitir el cifrado de datos en reposo y la versión de API nueva (31/10/2014).	6 de enero de 2015

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para incluir el nuevo motor de base de datos Amazon Aurora. El motor de base de datos Amazon Aurora admite varias instancias de base de datos en un clúster de bases de datos. Amazon Aurora se encuentra en versión de previsualización y está sujeto a cambios. Para obtener información detallada, consulte ¿Qué es Amazon Aurora?.	12 de noviembre de 2014
Nueva característica	Se ha actualizado para admitir réplicas de lectura de PostgreSQL.	10 de noviembre de 2014
Nueva API y nuevas características	Se ha actualizado para admitir el tipo de almacenamiento GP2 y la versión de API (01/09/2014). Se ha actualizado para admitir la capacidad de copiar una opción existente o un grupo de parámetros para crear una opción nueva o un grupo de parámetros.	7 de octubre de 2014
Nueva característica	Se actualizado para admitir el calentamiento de caché de InnoDB para instancias de base de datos en las que se ejecuta MySQL 5.6.19 y versiones posteriores.	3 de septiembre de 2014
Nueva característica	Se ha actualizado para admitir la verificación del certificado SSL al conectar con motores de base de datos MySQL (versión 5.6), SQL Server y PostgreSQL.	5 de agosto de 2014
Nueva característica	Se ha actualizado para admitir clases de instancia de base de datos con capacidad para ráfagas db.t2.	4 de agosto de 2014
Nueva característica	Se ha actualizado para admitir clases de instancia de base de datos con optimización de memoria db.r3 y usarlas con los motores de base de datos MySQL (versión 5.6), SQL Server y PostgreSQL.	28 de mayo de 2014

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir despliegues Multi-AZ para SQL Server con creación de reflejo de SQL Server.	19 de mayo de 2014
Nueva característica	Se ha actualizado para admitir actualizaciones de la versión 5.5 a la versión 5.6 de MySQL.	23 de abril de 2014
Nueva característica	Se ha actualizado para admitir Oracle GoldenGate.	3 de abril de 2014
Nueva característica	Se ha actualizado para admitir las clases de instancia de base de datos M3.	20 de febrero de 2014
Nueva característica	Se ha actualizado para admitir la opción Timezone de Oracle.	13 de enero de 2014
Nueva característica	Se ha actualizado para admitir la reproducción entre instancias de base de datos de MySQL en diferentes regiones.	26 de noviembre de 2013
Nueva característica	Se ha actualizado para el motor de base de datos PostgreSQL.	14 de noviembre de 2013
Nueva característica	Se ha actualizado para admitir el cifrado de datos transparente (TDE) de SQL Server.	7 de noviembre de 2013
Nueva API y nueva característica	Se ha actualizado para admitir las copias de instantáneas de base de datos entre regiones. Nueva versión de la API (09/09/2013).	31 de octubre de 2013
Nuevas características	Se ha actualizado para admitir Oracle Statspack.	26 de septiembre de 2013

Cambio	Descripción	Fecha de modificación
Nuevas características	Se ha actualizado para admitir el uso de la replicación para importar o exportar datos entre instancias de MySQL que se ejecutan en Amazon RDS e instancias de MySQL que se ejecutan en las instlaciones o en Amazon EC2.	5 de septiembre de 2013
Nuevas características	Se ha actualizado para admitir la clase de instancia de base de datos db.cr1.8xlarge para MySQL 5.6.	4 de septiembre de 2013
Nueva característica	Se ha actualizado para admitir la replicación de réplicas de lectura.	28 de agosto de 2013
Nueva característica	Se ha actualizado para admitir la creación de réplicas de lectura en paralelo.	22 de julio de 2013
Nueva característica	Se ha actualizado para admitir etiquetado y permisos precisos para todos los recursos de Amazon RDS.	8 de julio de 2013
Nueva característica	Se ha actualizado para admitir MySQL 5.6 para instancias nuevas, incluida la compatibilidad con la interfaz memcached de MySQL 5.6 y el acceso de registro binario.	1 de julio de 2013
Nueva característica	Se ha actualizado para admitir actualizaciones de versiones principales: de MySQL 5.1 a MySQL 5.5.	20 de junio de 2013
Nueva característica	Se han actualizado los grupos de parámetros de base de datos a fin de permitir expresiones para valores de parámetros.	20 de junio de 2013
Nueva API y nueva característica	Se ha actualizado para admitir el estado de la réplica de lectura. Nueva versión de la API (15/05/2013).	23 de mayo de 2013

Cambio	Descripción	Fecha de modificación
Nuevas caracterí sticas	Se ha actualizado para admitir características de Oracle Advanced Security para cifrado de red nativo y cifrado de datos transparente de Oracle.	18 de abril de 2013
Nuevas caracterí sticas	Se ha actualizado para admitir actualizaciones de versiones principales para SQL Server y funcionalidad adicional para IOPS provisionadas.	13 de marzo de 2013
Nueva caracterí stica	Se ha actualizado para admitir VPC de manera predeterminada para RDS.	11 de marzo de 2013
Nueva API y nueva caracterí stica	Se ha actualizado para admitir el acceso del registro. Nueva versión de la API (12/02/2013).	4 de marzo de 2013
Nueva caracterí stica	Se ha actualizado para admitir suscripciones a notificaciones de eventos de RDS.	4 de febrero de 2013
Nueva API y nueva caracterí stica	Se ha actualizado para admitir el cambio de nombre de la instancia de base de datos y la migración de miembros del grupo de seguridad de base de datos en una VPC a un grupo de seguridad de VPC.	14 de enero de 2013
Nueva caracterí stica	Se ha actualizado para admitir AWS GovCloud (EE. UU. Oeste).	17 de diciembre de 2012
Nueva caracterí stica	Se ha actualizado para admitir clases de instancia de base de datos m1.medium y m1.xlarge.	6 de noviembre de 2012
Nueva caracterí stica	Se ha actualizado para admitir la promoción de réplicas de lectura.	11 de octubre de 2012
Nueva caracterí stica	Se ha actualizado para admitir SSL en instancias de base de datos de Microsoft SQL Server.	10 de octubre de 2012

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir microinstancias de base de datos de Oracle.	27 de septiembre de 2012
Nueva característica	Se ha actualizado para admitir SQL Server 2012.	26 de septiembre de 2012
Nueva API y nueva característica	Se ha actualizado para admitir IOPS provisionadas. Versión de la API (17/09/2012).	25 de septiembre de 2012
Nuevas características	Se ha actualizado para admitir SQL Server en instancias de base de datos de la VPC y Oracle para Data Pump.	13 de septiembre de 2012
Nueva característica	Se ha actualizado para admitir el Agente SQL Server.	22 de agosto de 2012
Nueva característica	Se ha actualizado para admitir el etiquetado de instancias de base de datos.	21 de agosto de 2012
Nuevas características	Se ha actualizado para admitir Oracle APEX y XML DB, las zonas horarias de Oracle y las instancias de base de datos de Oracle en una VPC.	16 de agosto de 2012
Nuevas características	Se ha actualizado para admitir el Asistente para la optimización de motor de base de datos de SQL Server e instancias de base de datos de Oracle en la VPC.	18 de julio de 2012
Nueva característica	Se ha actualizado para admitir grupos de opciones y la primera opción, Oracle Enterprise Manager Database Control.	29 de mayo de 2012
Nueva característica	Se ha actualizado para admitir las réplicas de lectura en Amazon Virtual Private Cloud.	17 de mayo de 2012

Cambio	Descripción	Fecha de modificación
Nueva característica	Se ha actualizado para admitir Microsoft SQL Server.	8 de mayo de 2012
Nuevas características	Se ha actualizado para admitir la conmutación por error forzada, la Implementación multi-AZ de instancias de base de datos de Oracle y conjuntos de caracteres no predeterminados para instancias de base de datos de Oracle.	2 de mayo de 2012
Nueva característica	Se ha actualizado para admitir Amazon Virtual Private Cloud (VPC).	13 de febrero de 2012
Contenido actualizado	Se ha actualizado para nuevos tipos de instancias reservadas.	19 de diciembre de 2011
Nueva característica	Se ha actualizado para admitir el motor de Oracle.	23 de mayo de 2011
Contenido actualizado	Actualizaciones de consola.	13 de mayo de 2011
Contenido actualizado	Contenido editado para períodos reducidos de mantenimiento y copia de seguridad.	28 de febrero de 2011
Nueva característica	Se ha agregado compatibilidad con MySQL 5.5.	31 de enero de 2011
Nueva característica	Se ha agregado compatibilidad con réplicas de lectura.	4 de octubre de 2010
Nueva característica	Se ha agregado compatibilidad con AWS Identity and Access Management (IAM).	2 de septiembre de 2010
Nueva característica	Se ha agregado la administración de versiones del motor de base de datos.	16 de agosto de 2010

Cambio	Descripción	Fecha de modificación
Nueva caracterí stica	Se han agregado instancias de base de datos reservadas.	16 de agosto de 2010
Nueva caracterí stica	Amazon RDS ahora admite conexiones SSL a sus instancias de base de datos.	28 de junio de 2010
Nueva guía	Esta es la primera versión de la Guía del usuario de Amazon RDS.	7 de junio de 2010

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.